JAPAN SMARTPHONE SECURITY ASSOCIATION

Android Application Secure Design/Secure Coding Guidebook

February 1, 2018 Edition

Japan Smartphone Security Association (JSSEC)

Secure Coding Working Group

Document control number: JSSEC-TECA-SC-GD20180201BE

- The content of this guide is up to date as of the time of publication, but standards and environments are constantly evolving. When using sample code, make sure you are adhering to the latest coding standards and best practices.
- JSSEC and the writers of this guide are not responsible for how you use this document. Full responsibility lies with you, the user of the information provided.
- Android™ is a trademark or a registered trademark of Google Inc.

  The company names, product names and service names appearing in this document are generally the registered trademarks or trademarks of their respective companies.

  Further, the registered trademark ®, trademark (TM) and copyright © symbols are not used throughout this document.
- Parts of this document are copied from or based on content created and provided by Google, Inc. They are used here in accordance with the provisions of the Creative Commons Attribution 3.0 License

Android Application Secure Design/Secure Coding Guidebook

- Beta version -

February 1, 2018

Japan Smartphone Security Association

Secure Coding Working Group

Index

Revision history

Date	Revised contents
2014-04-01	• Initial English Edition
2014-07-01	• Added new articles below • 5.5 Handling privacy data • 5.6 Using Cryptography
2015-06-01	• We have reviewed the entire document in accordance with the following policy • Change of development environment (Eclipse -> Android Studio) • Responding to Android latest version Lollipop • Change of API Level (8 or later -> 15 or later)
2016-02-01	• Added new articles below • 4.10 Using Notifications • 5.7 Using fingerprint authentication features • Revised article below • 5.2 Permission and Protection Level
2016-09-01	• Revised articles below • 2.5 Steps to Install Sample Codes into Android Studio • 5.4 Communicating via HTTPS • 5.6 Using Cryptography
2017-02-01	• Added new articles below • 4.6.3.5 Revised specifications in Android 7.0 (API Level 24) for accessing specific directories on external storage media • 5.4.3.7 Network Security Configuration • Revised articles below • 4.1 Creating/Using Activities • 4.2 Receiving/Sending Broadcasts • 4.4 Creating/Using Services • 4.5 Using SQLite • 4.6 Handling Files • Deleted the section below • 4.8.3.4 BuildConfig.DEBUG Should Be Used in ADT 21 or Later • We have reviewed the entire document in accordance with the following policy • All discussions in the main text concerning Android 4.0.3 (API Level 15) and earlier versions have been deleted or moved to footnotes.
2018-2-01	• Added new articles below • 4.1.3.7 The Autofill framework • 5.3.3.3 Cases in which Authenticator accounts with non-matching

	signatures may be read in Android 8.0 (API Level 26) or later5.5.3.3 Version-dependent differences in handling of Android IDs
	• Revised articles below
	  • 4.2 Receiving/Sending Broadcast
	  • 5.2 Permission and Protection Level
	  • 5.3 Add In-house Accounts to Account Manager
	  • 5.4 Communicating via HTTPS
	  • 5.5 Handling privacy data
	• **Note:** For a detailed description of these revisions, see Section "1.4 Correction articles of February 1, 2018 edition"

In preparing a new version for public release, we have revised the content of this guidebook based on opinions, comments and suggestions received from readers.	

– Published by –
Japan Smartphone Security Association
Secure Coding Working Group, Smartphone Technology Committee

Leader	Akira Ando	Sony Digital Network Applications, Inc.
Member	Ken Okuyma	Android Security Japan
	Eiji Hoshimoto	Software Research Associates, Inc.
	Akihiro Shiota	NTT DATA Corporation
	Shigenori Takei	NTT Software Corporation
	Ikuya Fukumoto	Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
	Mariko Yoshida	Sony Digital Network Applications, Inc.
	Nobuaki Yamaguchi	Sony Digital Network Applications, Inc.
	Jun Ogiso	Sony Digital Network Applications, Inc.
	Junki Hisamoto	Sony Digital Network Applications, Inc.
	Masahiro Kasahara	SoftBank Corp.
	Daisuke Mitsuzono	Nihon System Kaihatsu Co., Ltd.
	Shigeru Yatabe	Fomalhaut Techno Solutions

(In no particular order)

– Authors of February 1, 2017 Edition –

Leader

Ken Okuyama	Sony Digital Network Applications, Inc.

Member

Shigeharu Araki	Android Security Japan
Eiji Shimano	Android Security Japan
Akihiro Shiota	NTT DATA Corporation
Shigenori Takei	NTT Software Corporation
Ikuya Fukumoto	Software Research Associates, Inc.
Tomomi Ohuchi	Software Research Associates, Inc.
Yoichi Yamanoi	Software Research Associates, Inc.
Hidenori Yamaji	Sony Corporation
Akira Ando	Sony Digital Network Applications, Inc.
Jun Ogiso	Sony Digital Network Applications, Inc.
Masaru Matsunami	Sony Digital Network Applications, Inc.
Tetsuya Takahashi	SQUARE ENIX CO., LTD.
Gaku Taniguchi	Tao Software, Inc.

(In no particular order)

- Authors of September 1, 2016 Edition -

Leader

Masaru Matsunami	Sony Digital Network Applications, Inc.

Member

Shigeharu Araki	Android Security Japan
Shigenori Takei	NTT Software Corporation
Ikuya Fukumoto	Software Research Associates, Inc.
Tomomi Ohuchi	Software Research Associates, Inc.
Hidenori Yamaji	Sony Corporation
Akira Ando	Sony Digital Network Applications, Inc.
Jun Ogiso	Sony Digital Network Applications, Inc.
Ken Okuyama	Sony Digital Network Applications, Inc.
Mitake Ohtani	Sony Digital Network Applications, Inc.
Daisuke Mitsuzono	Nihon System Kaihatsu Co., Ltd.
Eiji Shimano	Tao Software, Inc.
Gaku Taniguchi	Tao Software, Inc.

(In no particular order)

- Authors of February 1, 2016 Edition -

Leader

Masaru Matsunami	Sony Digital Network Applications, Inc.

Member

Masaomi Adachi	Android Security Japan
Tohru Ohzono	Cisco Systems, Inc.
Shigenori Takei	NTT Software Corporation
Masahiro Kasahara	SoftBank Mobile Corp.
Eiji Hoshimoto, Ikuya Fukumono	Software Research Associates, Inc.
Akira Ando, Ken Okuyama, Mitake Ohtani, Muneaki Nishimura, Setsuko Kaji, Taeko Ito	Sony Digital Network Applications, Inc.
Hidenori Yamaji	Sony Mobile Communications Inc.
Eiji Shimano , Gaku Taniguchi	Tao Software, Inc.

(In no particular order)

– Authors of June 1, 2015 Edition –

Leader

Masaru Matsunami	Sony Digital Network Applications, Inc.

Member

Tohru Ohzono	Cisco Systems, Inc.
Akio Kondo, Kazuma Mitake, Kyosuke Imanishi, Masato Shintani, Naohiko Shimura, Ryuji Fujita, Shohei Hara, Tomoyuki Fujisawa, Yutaka Kawahara	BRILLIANTSERVICE co., Ltd.
Shigeru Yatabe	Fomalhaut Techno Solutions
Naonobu Yatsukawa	Nihon Unisys, Ltd.
Shigenori Takei	NTT Software Corporation
Masahiro Kasahara	SoftBank Mobile Corp.
Eiji Hoshimoto	Software Research Associates, Inc.
Akira Ando, Ken Okuyama, Muneaki Nishimura	Sony Digital Network Applications, Inc.
Eiji Shimano , Gaku Taniguchi	Tao Software, Inc.

(In no particular order)

- Authors of July 1, 2014 English Edition -

Leader

Masaru Matsunami	Sony Digital Network Applications, Inc.

Member

Tohru Ohzono	Cisco Systems, Inc.
Shigeru Yatabe	Fomalhaut Techno Solutions
Keisuke Takemori, Takamasa Isohara	KDDI CORPORATION
Naonobu Yatsukawa	Nihon Unisys, Ltd.
Shigenori Takei	NTT Software Corporation
Masahiro Kasahara	SoftBank Mobile Corp.
Eiji Hoshimoto, Tsutomu Kumazawa	Software Research Associates, Inc.
Akira Ando, Ken Okuyama, Setsuko Kaji, Taeko Ito, Yoshinori Kataoka	Sony Digital Network Applications, Inc.
Eiji Shimano , Gaku Taniguchi	Tao Software, Inc.
Michiyoshi Sato	Tokyo System House Co., Ltd.

(In no particular order)

– Authors of April 1, 2014 English Edition –

Leader

Masaru Matsunami	Sony Digital Network Applications, Inc.

Member

Tomoyuki Hasegawa	Android Security Japan
Mayumi Nishiyama	BJIT Inc.
Tohru Ohzono	Cisco Systems, Inc.
Masaki Kubo	Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Daniel Burrowes, Zachary Mathis	Kobe Digital Labo Inc.
Renta Futamura	NextGen, Inc.
Naonobu Yatsukawa	Nihon Unisys, Ltd.
Shigenori Takei	NTT Software Corporation
Ikuya Fukumono, Tsutomu Kumazawa	Software Research Associates, Inc.
Akira Ando, Hiroko Nakajima, Ken Okuyama, Satoshi Fujimura, Setsuko Kaji, Taeko Ito, Yoshinori Kataoka	Sony Digital Network Applications, Inc.
Hidenori Yamaji, Takuya Nishibayashi	Sony Mobile Communications Inc.
Koji Isoda	Symantec Japan, Inc.
Gaku Taniguchi	Tao Software, Inc.
Michiyoshi Sato	Tokyo System House Co., Ltd.

(In no particular order)

– Authors of April 1, 2013 Japanese Edition –

Leader

Masaru Matsunami	Sony Digital Network Applications, Inc.

Member

Masaomi Adachi, Tomoyuki Hasegawa	Android Security Japan
Yuki Abe, Tomomi Oouchi, Tsutomu Kumazawa, Toshimi Sawada, Kiyoshi Hata, Youichi Higa, Yuu Fukui, Ikuya Fukumoto, Eiji Hoshimoto, Shun Yokoi, Takakazu Yoshizawa	Software Research Associates, Inc.
Takeshi Fujiwara	NRI SecureTechnologies, Ltd.
Shigenori Takei	NTT Software Corporation
Masaki Kubo, Hiroshi Kumagai, Yozo Toda	Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Tohru Ohzono	Cisco Systems, Inc.
Toru Asano, Akira Ando, Ryohji Ikebe, Jun Ogiso, Ken Okuyama, Yoshinori Kataoka, Muneaki Nishimura, Koji Furusawa, Kenji Yamaoka	Sony Digital Network Applications, Inc.
Gaku Taniguchi	Tao Software, Inc.
Naonobu Yatsukawa	Nihon Unisys, Ltd.
Shigeru Yatabe	Fomalhaut Techno Solutions

(In no particular order)

- Authors of November 1, 2012 Japanese Edition -

Leader

Masaru Matsunami	Sony Digital Network Applications, Inc.

Member

Katsuhiko Sato, Nakaguchi Akihiko	Android Security Japan
Tomomi Oouchi, Naoyuki Ohira, Tsutomu Kumazawa, Miki Sekikawa, Seigo Nakano, Youichi Higa, Ikuya Fukumoto, Eiji Hoshimoto, Shoichi Yasuda, Tadayuki Yahiro, Takakazu Yoshizawa	Software Research Associates, Inc.
Shigenori Takei	NTT Software Corporation
Keisuke Takemori	KDDI CORPORATION
Masaki Kubo, Hiroshi Kumagai, Yozo Toda	Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Tohru Ohzono	Cisco Systems, Inc.
Toru Asano, Akira Ando, Ryohji Ikebe, Shigeru Ichikawa, Mitake Ohtani, Jun Ogiso, Ken Okuyama, Yoshinori Kataoka, Ikue Sato, Muneaki Nishimura, Kazuo Yamaoka, Takeru Kikkawa	Sony Digital Network Applications, Inc.
Gaku Taniguchi, Eiji Shimano, Hisao Kitamura	Tao Software, Inc.
Takao Yamakawa	Japan Online Game Association
Masaki Ishihara, Yasuaki Mori	Nihon System Kaihatsu Co., Ltd.
Naonobu Yatsukawa	Nihon Unisys, Ltd.
Shigeru Yatabe	Fomalhaut Techno Solutions
Shigeki Fujii	UNIADEX, Ltd.

(In no particular order)

- Authors of June 1, 2012 Japanese Edition-

Leader

Masaru Matsunami	Sony Digital Network Applications, Inc.

Member

Katsuhiko Sato	Android Security Japan
Tomomi Oouchi, Youichi Higa, Eiji Hoshimoto	Software Research Associates, Inc.
Shigenori Takei	NTT Software Corporation
Masaki Kubo, Hiroshi Kumagai, Yozo Toda	Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Masaaki Chida	GREE, Inc.
Tohru Ohzono	Cisco Systems, Inc.
Yoichi Taguchi	System House. ING Co., Ltd.
Masahiko Sakamoto	Secure Sky Technology, Inc.
Akira Ando, Shigeru Ichikawa, Ken Okuyama, Ikue Sato, Muneaki Nishimura, Kazuo Yamaoka	Sony Digital Network Applications, Inc.
Gaku Taniguchi, Eiji Shimano, Hisao Kitamura	Tao Software, Inc.
Michiyoshi Sato	Tokyo System House Co., Ltd.
Masakazu Hattori	Trend Micro Incorporated.
Naonobu Yatsukawa	Nihon Unisys, Ltd.
Shigeru Yatabe	Fomalhaut Techno Solutions
Shigeki Fujii	UNIADEX, Ltd.

(In no particular order)

1. Introduction

1.1. Building a Secure Smartphone Society

This guidebook is a collection of tips concerning the know-how of secure designs and secure coding for Android application developers. Our intent is to have as many Android application developers as possible take advantage of this, and for that reason we are making it public.

In recent years, the smartphone market has witnessed a rapid expansion, and its momentum seems unstoppable. Its accelerated growth is brought on due to the diverse range of applications. An unspecified large number of key functions of mobile phones that were once not accessible due to security restrictions on conventional mobile phones have been made open to smartphone applications. Subsequently, the availability of varied applications that were once closed to conventional mobile phones is what makes smartphones more attractive.

With great power that comes from smartphone applications comes great responsibility from their developers. The default security restrictions on conventional mobile phones had made it possible to maintain a relative level of security even for applications that were developed without security awareness. As it has been aforementioned with regard to smartphones, since the key advantage of a smartphone is that they are open to application developers, if the developers design or code their applications without the knowledge of security issues then this could lead to risks of users' personal information leakage or exploitation by malware causing financial damage such as from illicit calls to premium-rate numbers.

Due to Android being a very open model allowing access to many functions on the smartphone, it is believed that Android application developers need to take more care about security issues than iOS application developers. In addition, responsibility for application security is almost solely left to the application developers. For example, applications can be released to the public without any screening from a marketplace such as Google Play (former Android Market), though this is not possible for iOS applications.

In conjunction with the rapid growth of the smartphone market, there has been a sudden influx of software engineers from different areas in the smartphone application development market. As a result, there is an urgent call for the sharing knowledge of secure design and consolidation of secure coding know-how for specific security issues related to mobile applications.

Due to these circumstances, Japan's Smartphone Security Association (JSSEC) has launched the Secure Coding Group, and by collecting the know-how of secure design as well as secure coding of Android applications, it has decided to make all of the information public with this guidebook. It is our intention to raise the security level of many of the Android applications that are released in the market by having many Android application developers become acquainted with the know-how of secure design and coding. As a result, we believe we will be contributing to the creation of a more reliable and safe smartphone society.

1.2. Timely Feedback on a Regular Basis Through the Beta Version

We, the JSSEC Secure Coding Group, will do our best to keep the content contained in the Guidebook as accurate as possible, but we cannot make any guarantees. We believe it is our priority to publicize and share the know-how in a timely fashion. Equally, we will upload and publicize what we consider to be the latest and most accurate correct information at that particular juncture, and will update it with more accurate information once we receive any feedback or corrections. In other words, we are taking the beta version approach on a regular basis. We think this approach would be meaningful for many of the Android application developers who are planning on using the Guidebook.

The latest version of the Guidebook and sample codes can be obtained from the URL below.

- http://www.jssec.org/dl/android_securecoding_en.pdf Guidebook (English)
- http://www.jssec.org/dl/android_securecoding_en.zip Sample Codes (English)

The latest Japanese version can be obtained from the URL below.

- http://www.jssec.org/dl/android_securecoding.pdf Guidebook (Japanese)
- http://www.jssec.org/dl/android_securecoding.zip Sample Codes (Japanese)

1.3. Usage Agreement of the Guidebook

We need your consent for the following two precautionary statements when using the Guidebook.

1. The information contained in the Guidebook may be inaccurate. Please use the information written here by your own discretion.
2. In case of finding any mistakes contained in the Guidebook, please send us an e-mail to the address listed below. However, we cannot guarantee a reply or any revisions thereof.

Japan Smartphone Security Association
Secure Coding Group Inquiry
E-mail: jssec-securecoding-qa@googlegroups.com
Subject: [Comment] Android Secure Coding Guidebook 20180201EN
Content: Name (optional), Affiliation (optional), E-mail (optional), Comment (required) and Other matters (optional)

1.4. Correction articles of February 1, 2018 edition

This section provides a list of corrections and modifications for the previous edition from the viewpoint of security, as a result of further studies.

In correcting articles, we adopted the outcomes of our studies and the valuable opinions of those who read the former editions of this guidebook.
Especially, taking in readers' opinions is considered as a key factor in making the document highly practical.

We recommend, for those who use a previous edition of the document as a reference, taking a look at the list below. Note that the list does not include the following kinds of changes and error corrections: fixes of typos, new articles added in this edition, organizational changes, and improvements in expression.

Any comments, opinions or suggestions on this guidebook are greatly appreciated.

List of revisions

Section revised in 2/1/2017 version	Section revised in this version	Revision
(not applicable)	4.1.3.7 The Autofill framework	Added a description of the Autofill framework.
4.2 Receiving/Sending Broadcasts	4.2 Receiving/Sending Broadcasts	Added a discussion of restrictions on the receipt of implicit Broadcast Intents in Android 8.0(API Level 26) and later.
5.2.3.6 Modifications to the Permission model specifications in Android versions 6.0 and later	5.2.3.6 Modifications to the Permission model specifications in Android versions 6.0 and later	Added a discussion of modifications to behavior regarding the granting of Permissions in Android 8.0 (API Level 26) and later.
5.3.2.4 Provide KEY_INTENT with Explicit Intent with the Specified Class Name of Login Screen Activity (Required	5.3.2.4 Provide KEY_INTENT with Explicit Intent with the Specified Class Name of Login Screen Activity (Required	Added a discussion of changes in the behavior of Key Intents before and after Android 4.4 (API Level 19).
5.3.2.6 Password Should Not Be Saved in Account Manager (Recommended	5.3.2.6 Password Should Not Be Saved in Account Manager (Recommended	Added a description of password storage locations for Android 7.0 (API Level 24) and later.
5.3.3.1 Usage of Account Manager and Permission	5.3.3.1 Usage of Account Manager and Permission	Added a discussion of support for Permissions and methods related to AccountManager in Android 6.0 (API

		Level 23) and later and Android 8.0 (API Level 26) and later.
(not applicable)	5.3.3.3 Cases in which Authenticator accounts with non-matching signatures may be read in Android 8.0 (API Level 26) or later	For Android 8.0 (API Level 26) and later, added a discussion of cases in which it is possible to obtain account information for Authenticators with non-matching signatures, and how to handle such cases.
5.4 Communicating via HTTPS	5.4 Communicating via HTTPS	Added a discussion of the removal of support for SSLv3 in Android 8.0 and later.
5.4.3.1 How to Create Private Certificate and Configure Server Settings	5.4.3.1 How to Create Private Certificate and Configure Server Settings	Revised the creation script to include the SubjectAltName in the private certificate.
(not applicable)	5.5.3.3 Version-dependent differences in handling of Android IDs	Added a discussion of version-dependent differences in values and generation rules for Android IDs.

2. Composition of the Guidebook

2.1. Developer's Context

Many guidebooks that have been written on secure coding include warnings about harmful coding practices and their suggested revisions. Although this approach can be useful at the time of reviewing the source code that has already been coded, it can be confusing for developers that are about to start coding, as they do not know which article to refer to.

The Guidebook has focused on the developer's context of "What is a developer trying to do at this moment?" Equally, we have taken steps to prepare articles that are aligned with the developer's context. For example, we have divided articles into project units by presuming that a developer will be involved in operations such as [Creating/Using Activities], [Using SQLite], etc.

We believe that by publishing articles that support the developer's context, developers will be able to easily locate necessary articles that will be instantly useful in their projects.

2.2. Sample Code, Rule Book, Advanced Topics

Each article is comprised of three sections: Sample Code, Rule Book, and Advanced Topics. If you are in a hurry, please look up the Sample Code and Rule Book sections. The content is provided in a way where it can be reused to a certain degree. For those who have issues that go beyond these, please refer the Advanced Topics section. We have given descriptions that will be helpful in finding solutions for individual cases.

Unless it is specifically noted, our focus of development will be targeted to platforms concerning Android 4.0.3 (API Level 15) and later. Since we have not verified the operational capability of any versions pertaining to Android versions under 4.0.3 (API Level 15), the measures described may prove ineffective on these older systems. In addition, even for versions that are covered under the scope of focus, it is important to verify their operational capability by testing them on your own environment before releasing them publically.

2.2.1. Sample Code

Sample code that serves as the basic model within the developer's context and functions as the theme of an article is published in the Sample Code section. If there are multiple patterns, we have provided source code for the different patterns and classified them accordingly. We have strived to make our commentaries as simple as possible. For example, when we want to direct the reader's attention to a security issue that requires attention, a bullet-point number will appear next to "**Point**" in the article. We will also comment on the sample code that corresponds to the bullet-point number by writing "**`*** Point (Number) ***`**." Please note that a single point may correspond to multiple pieces of sample code. There are sections throughout the entire source code, albeit very little compared to the entire code, which requires our attention for security. In order to be able to survey the sections that call for scrutiny, we try to post the entire class unit of sample code.

Please note that only a portion of sample code is posted in the Guidebook. A compressed file, which contains the entire sample code, is made public in the URL listed below. It is made public by the Apache License, Version 2.0; therefore, please feel free to copy and paste it. Please note that we have minimized the code for error processing in the sample code to prevent it from becoming too long.

- http://www.jssec.org/dl/android_securecoding_en.zip Sample Codes Archive

The projects/keystore file that is attached in the sample code is the keystore file that contains the developer key for the signature of the APK. The password is "android." Please use it when singing the APK in the In-house sample code.

We have provided the keystore file, debug.keystore, for debugging purposes. When using Android Studio for development, it is convenient for verifying the operational capability of the In-house sample code if the keystore is set for each project. In addition, for sample code that is comprised of multiple APKs, it is necessary to match the android:debuggable setting contained inside each AndroidManifest.xml in order to verify the cooperation between each APK. If the android:debuggable

setting is not explicit set when installing the APK from Android Studio, it will automatically become android:debuggable= "true."

For embedding the sample code as well as keystore file into Android Studio, please refer to "2.5 Steps to Install Sample Codes into Android Studio"

2.2.2. Rule Book

Rules and matters that need to be considered regarding security within the developer's context will be published in the Rule Book section. Rules to be handled in that section will be listed in a table format at the beginning and will be divided into two levels: "Required" and "Recommended." The rules will consist of two types of affirmative and negative statements. For example, an affirmative statement that expresses that a rule is required will say "Required." An affirmative statement that expresses a recommendation will say "Recommended." For a negative statement that expresses the requisite nature of the rule would say, "Definitely not do." For a negative sentence that expresses a recommendation would say, "Not recommended." Since these differentiations of levels are based on the subjective viewpoint of the author, it should only be used as a point of reference.

Sample code that is posted in the Sample Code section reflect these rules and matters that need to be considered, and a detailed explanation on them is available in the Rule Book section. Furthermore, rules and matters that need to be considered that are not dealt with in the Sample Code section are handled in the Rule Book section.

2.2.3. Advanced Topics

Items that require our attention, but that could not be covered in the Sample Code and Rule Book sections within the developer's context will be published in the Advanced Topics section. The Advanced Topics section can be utilized to explore ways to solve separate issues that could not be solved in the Sample Code or Rule Book sections. For example, subject matters that contain personal opinions as well as topics on the limitations of Android OS in relation the developer's context will be covered in the Advanced Topics section.

Developers are always busy. Many developers are expected to have basic knowledge of security and produce many Android applications as quickly as possible in a somewhat safe manner rather than to really understand the deep security matters. However, there are certain applications out there that require a high level of security design and implementation from the beginning. For developers of such applications, it is necessary for them to have a deep understanding concerning the security of Android OS.

In order to benefit both developers who emphasize development speed and also those who emphasize security, all articles of the Guidebook are divided into the three sections of Sample Code, Rule Book, and Advanced Topics. The aim of the Sample Code and Rule Book sections is to provide generalizations about security that anyone can benefit from and source code that will work with a minimal amount of customization and hopefully by just copying and pasting. In the Advanced Topics section, we offer materials that will help developers think in a certain way when they are facing

specific problems. It is the aim of the Advanced Topics section to help developers examine optimal secure design and coding when they are involved in building individual applications.

2.3. The Scope of the Guidebook

The purpose of the Guidebook is to collect security best practices that are necessary for general Android application developers. Consequently, our scope is focused mainly on security tips (The "Application Security" section in figure below) for the development of Android applications that are distributed primarily in a public market.

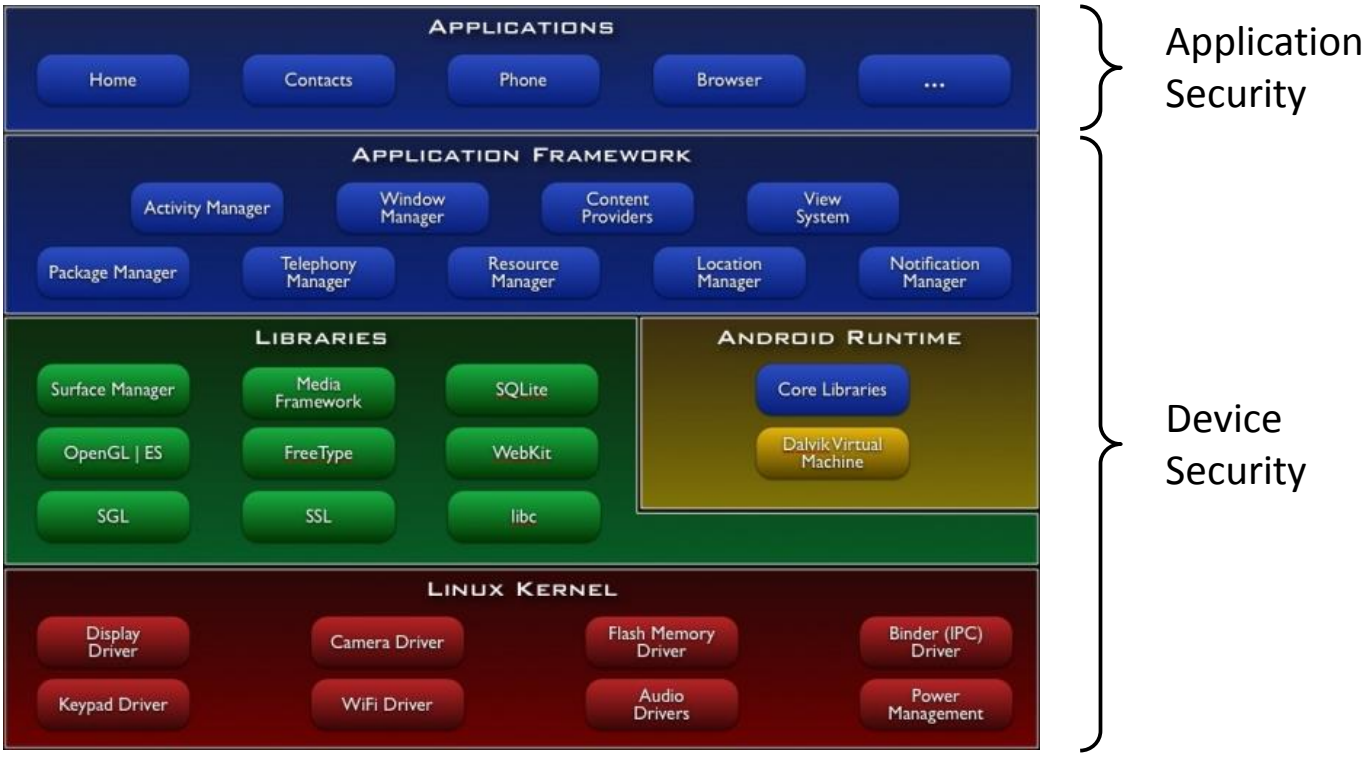


Figure 2.3-1

Security regarding the implementation of components in the Device Security of the above figure is outside the scope of this guidebook. There are differences in the viewpoint of security between general applications that are installed by users and pre-installed applications by device manufacturers. The Guidebook only handles the former and does not deal with the latter. In the current version, tips only on the implementation by Java are posted, but in future versions, we plan on posting tips on JNI implementations as well.

Also as of now we do not handle threats that results from an attacker obtaining root privileges. We will assume the premise of a secure Android device in which it is not possible to obtain root privileges and base our security advice on utilizing the Android OS security model. For handling of assets and threats, we have provided a detailed description on "3.1.3 Asset Classification and Protective Countermeasures."

2.4. Literature on Android Secure Coding

Since we are not able to discuss all of Android's secure coding in the Guidebook, we recommend that you read the literature mentioned below in conjunction with the Guidebook.

- *Android Security: Anzenna Application Wo Sakusei Surutameni (Secured Programming in Android)*
  Author: Tao Software Co., Ltd. ISBN: 978-4-8443-3134-6
  http://www.amazon.co.jp/dp/4844331345/
- *The CERT Oracle Secure Coding Standard for Java*
  Authors: Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, David Svoboda
  http://www.amazon.com/dp/0321803957

2.5. Steps to Install Sample Codes into Android Studio

This section explains how to install sample code into Android Studio. Sample code is divided into multiple projects depending on the purpose. Installing the sample code is described in, "2.5.1 Installing the Sample Project." After the installation is completed, please refer to "2.5.2 Setup the debug.keystore" and install the debug.keystore file into Android Studio. We have verified the following steps in the following environment:

- OS
  - Windows 7 Ultimate SP1
- Android Studio
  - 2.1.2
- Android SDK
  - Android 6.0(API 23)
    - Sample projects can be built through Android 6.0 (API 23) unless otherwise stated.

2.5.1. Installing the Sample Project

1. Download the sample code.
   Acquire the sample code from the URL shown in "2.2.1 Sample Code"

2. Extract the sample code.
   Right click on the sample code that has been compressed into zip file, and click on "Extract All" as shown below.

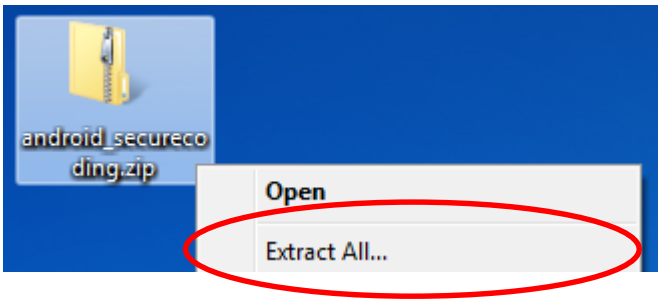


Figure 2.5-1

3. Designate where to deploy.

   Create a workspace under the name "C:¥android_securecoding" by designating "C:¥" and clicking on the "Extract" button.

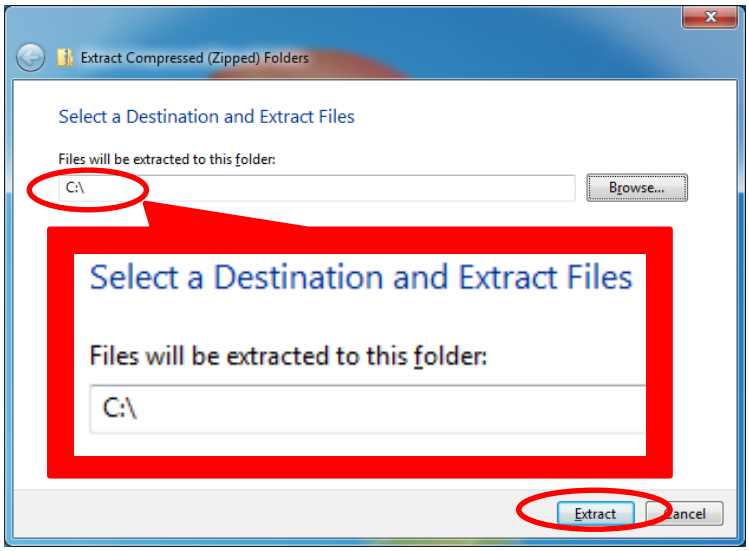


Figure 2.5-2

After clicking on the "Extract" button, right underneath "C:¥" a folder called "android_securecoding" will be created.

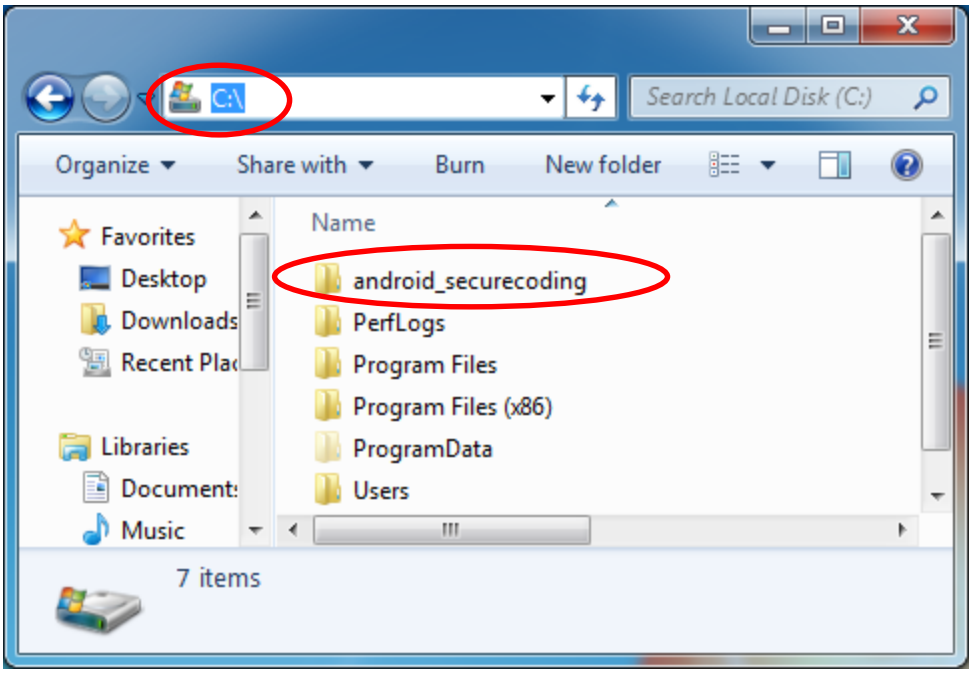


Figure 2.5-3

The sample code is contained in the “android_securecoding" folder. For example, when you want to refer to the sample code within "4.1.1.3 Creating/Using Partner Activities" of "4.1 Creating/Using Activities" please look below.

android_securecoding
└Create Use Activity
└Activity PartnerActivity

In this way, the sample code project will be located under the chapter title in the "android_securecoding" folder.

4. Designate workspace by starting up Android Studio
Launch Android Studio from the start menu or from a desktop icon.

Figure 2.5-4

After launching, import project from the dialog that appears.

Figure 2.5-5

If you have already opened a project, close the project window.

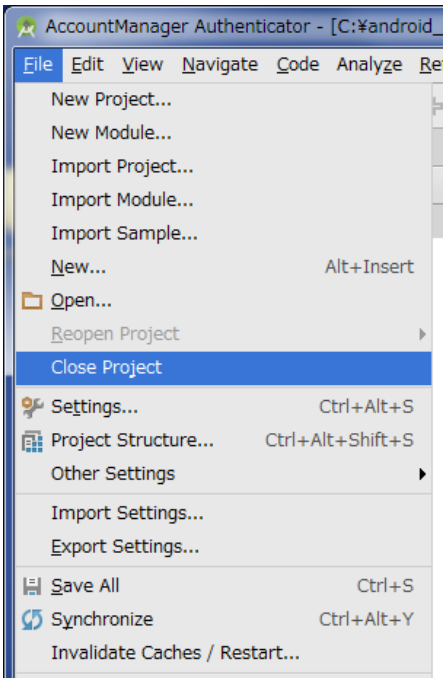


Figure 2.5-6

5. Start importing

Click "Import project (Eclipse ADT, Gradle, etc.)" from the dialog that is displayed.

Figure 2.5-7

6. Select the project

Expand the project folder you wish to import and select "gradle¥build.gradle" within that folder.

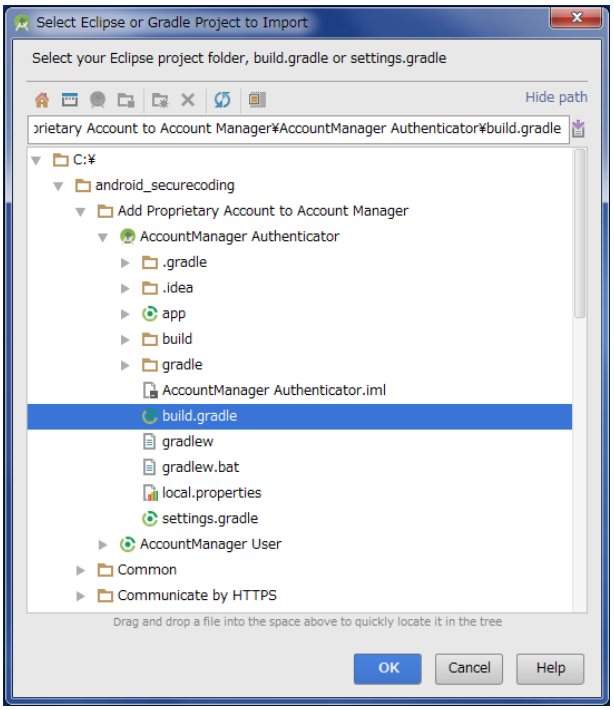


Figure 2.5-8

If the version of Gradle in the Android Studio you are using differs from the version assu med by the sample code projects in this guidebook, Gradle will be optimized.

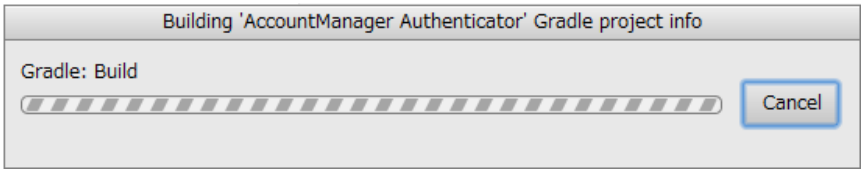


Figure 2.5-9

Following the on-screen instructions, click "Update" to initiate the update of the Android Gradle Plugin.

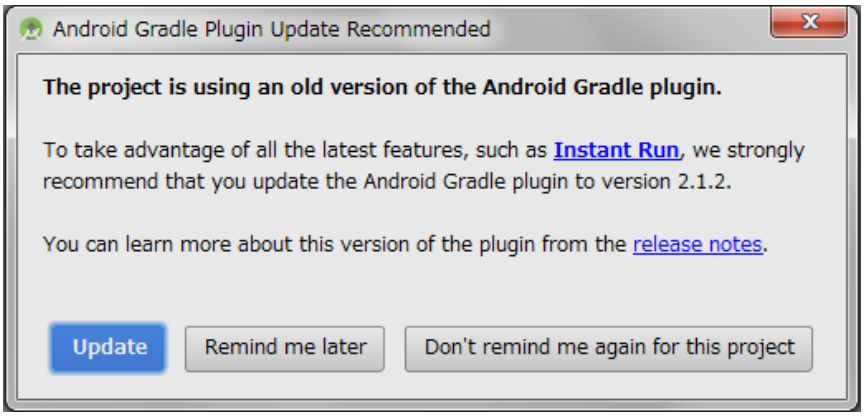


Figure 2.5-10

The message shown below is displayed. Click "Fix Gradle wrapper and re-import project Gradle setting" to update the Gradle wrapper.

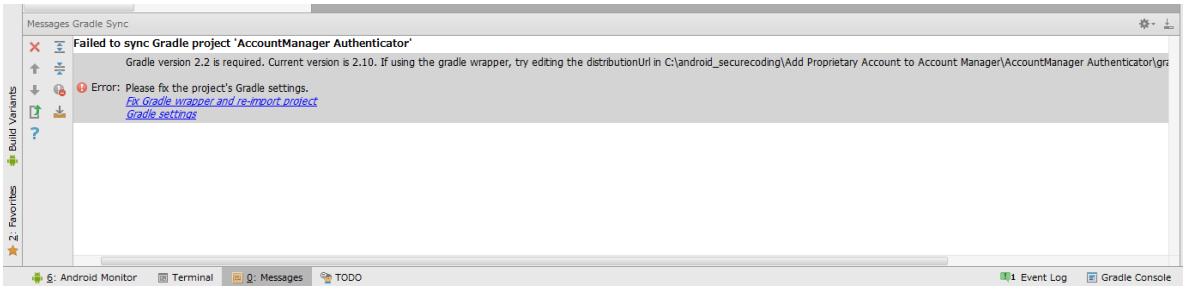


Figure 2.5-11

7. Finish importing

Automatically the project is imported.

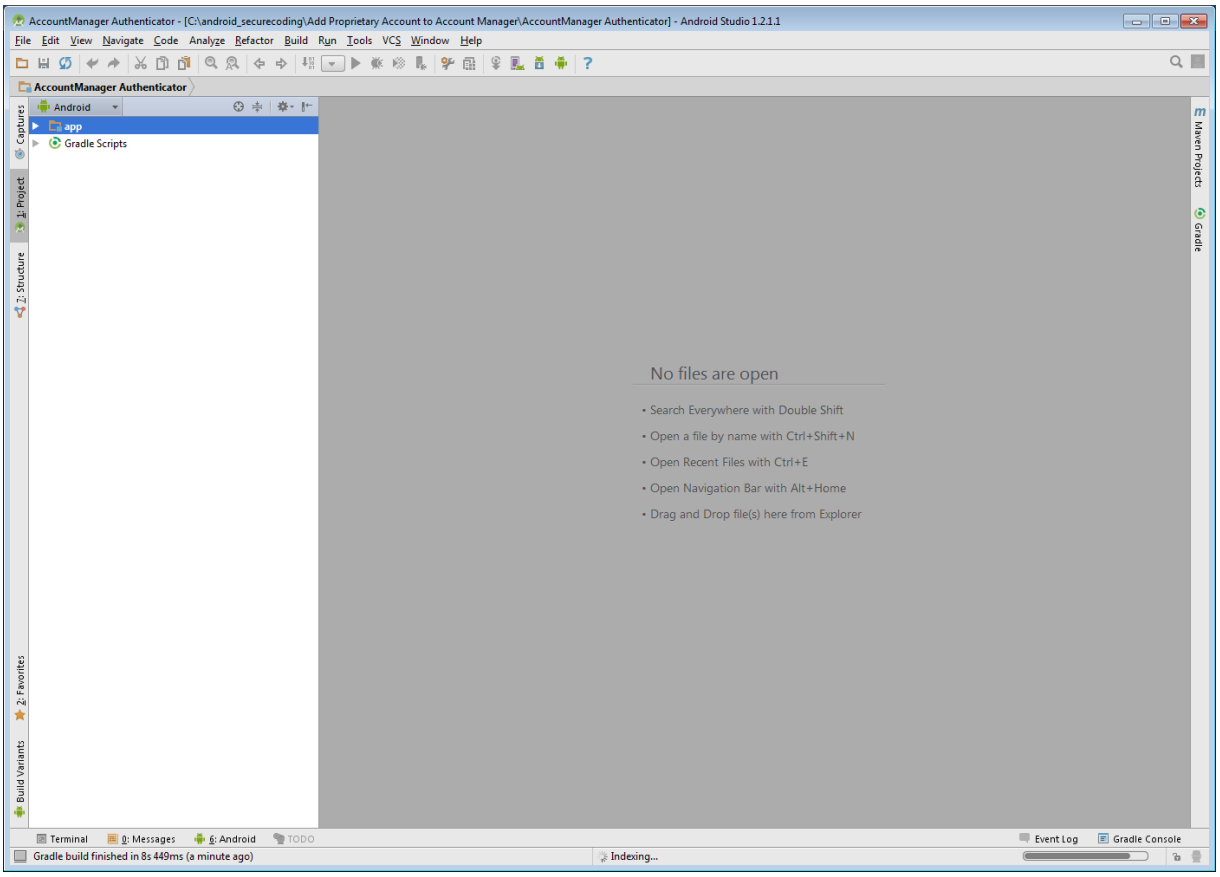


Figure 2.5-12

Android Studio, unlike Eclipse, will display a single project in a window. If you want to open and import a different project, click "File -> Import Project ...".

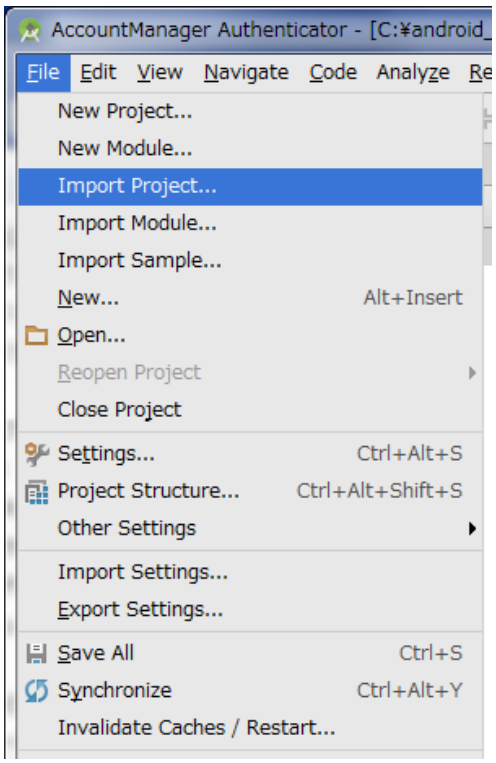


Figure 2.5-13

2.5.2. Setup the debug.keystore to run and test the Sample Code

A signature is needed in order to activate a sample-code-generated application onto an Android device or emulator. Install the debugging key file "debug.keystore" that will be used for the signature into Android Studio.

1. Click on File ->Project Structure...

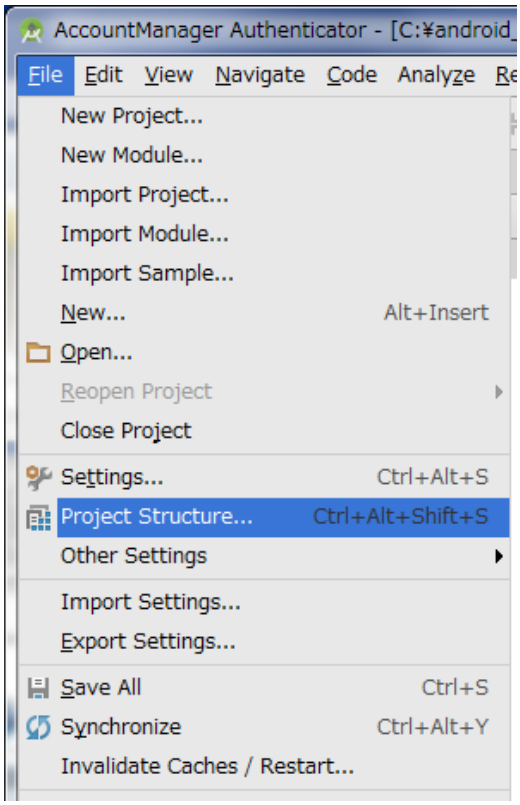


Figure 2.5-14

2. Add Signing

Select a project from Module list in left pane, selecting “Signing” tab, and then click “+” button.

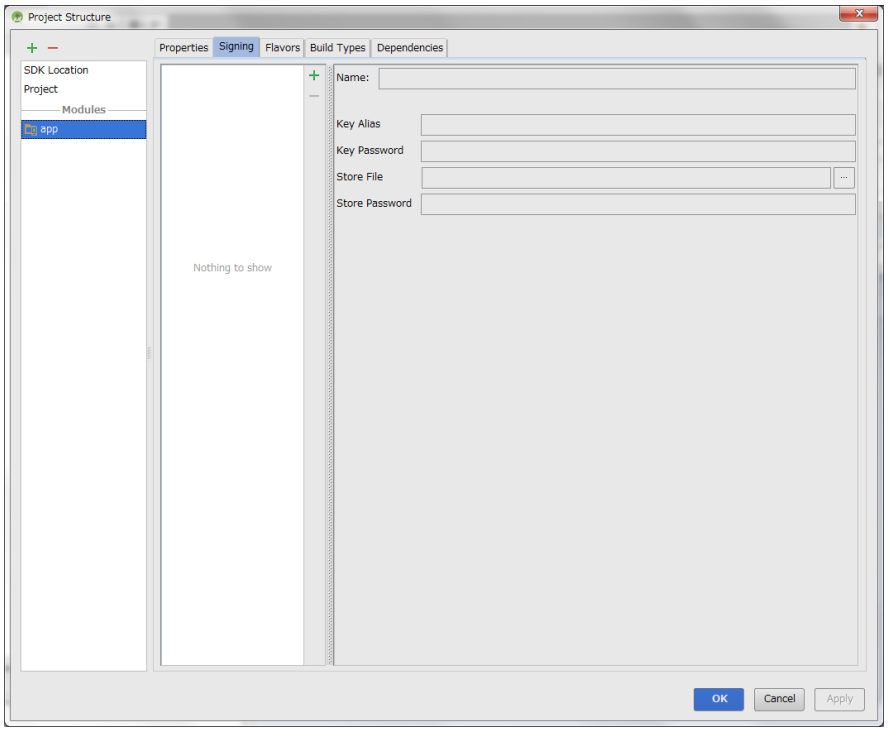


Figure 2.5-15

3. Select "debug.keystore"

Debug.keystore is contained in the sample code (underneath the android_securecoding folder)

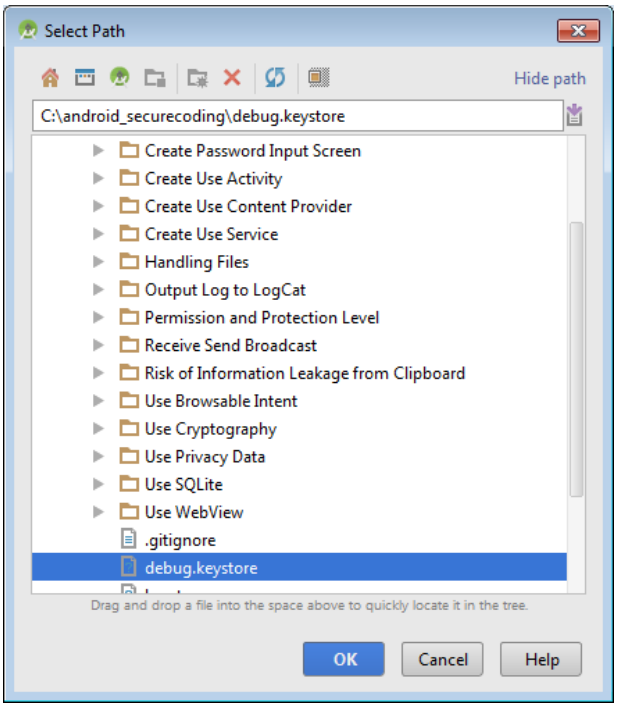


Figure 2.5-16

4. Type Signing name

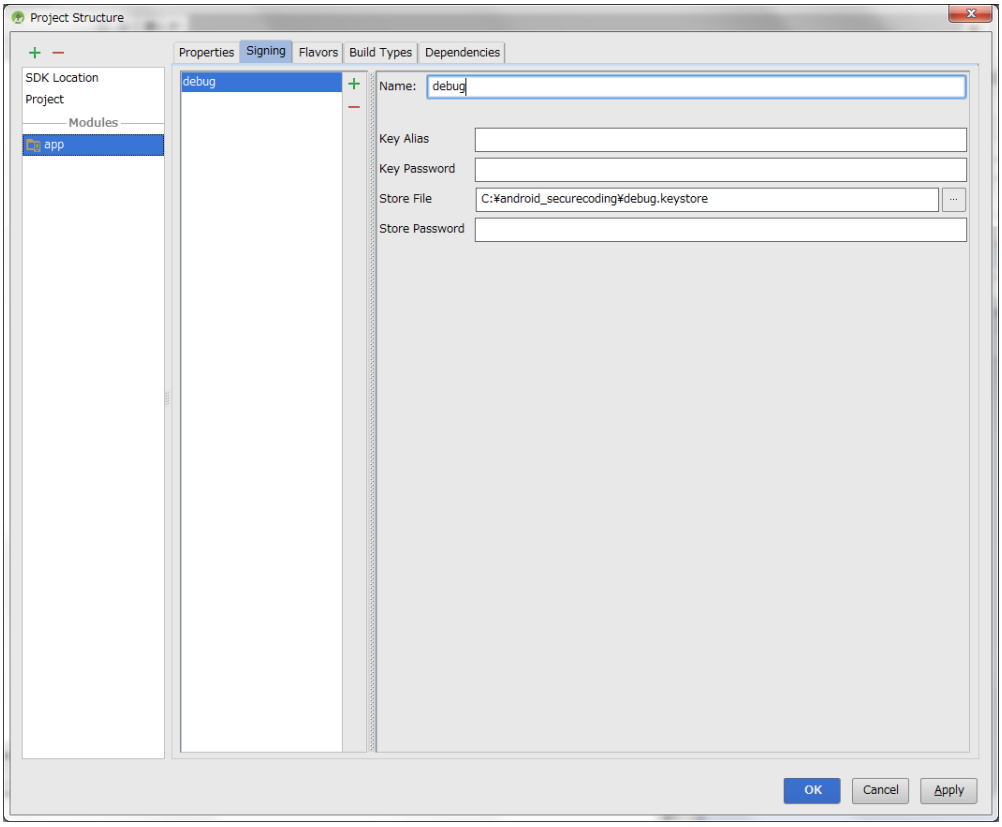


Figure 2.5-17

5. Set Signing Config

Select the Build Types tab, select signing name typed in the previous step, and then click “OK”.

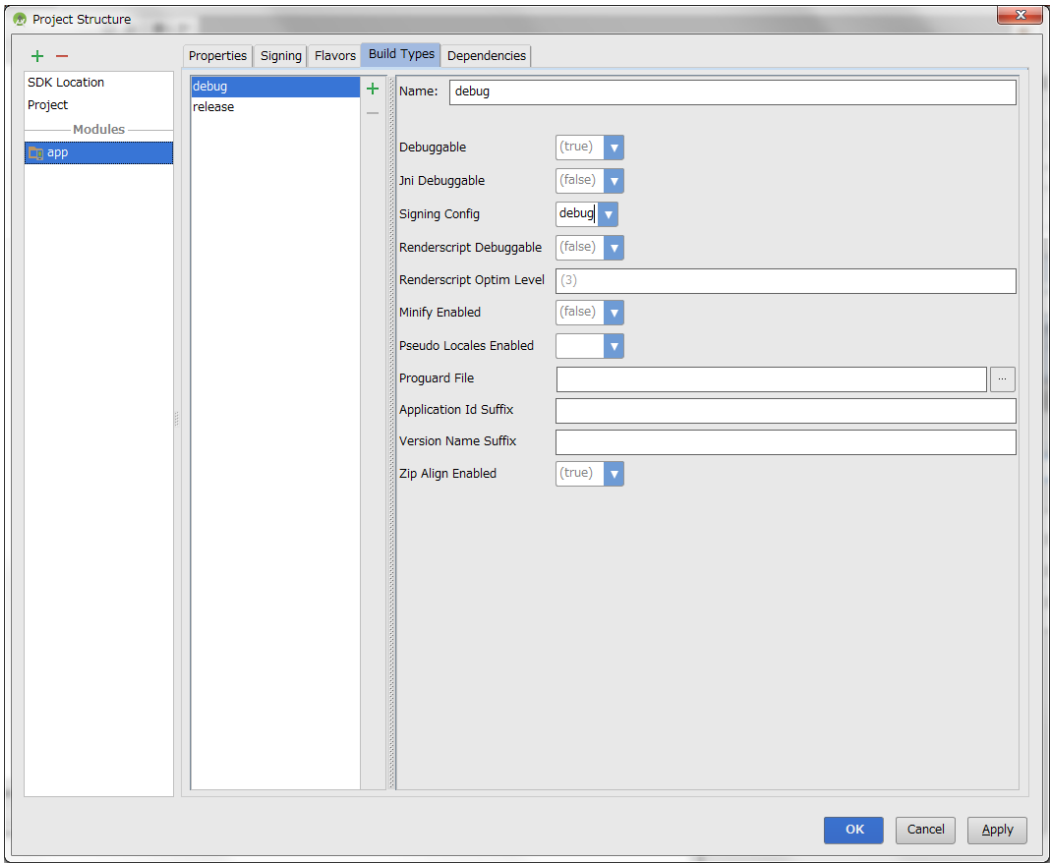


Figure 2.5-18

6. Confirm build.gradle file

The path of debug.keystore file you selected is displayed in signingConfigs, signingConfig appears in debug section of buildTypes.

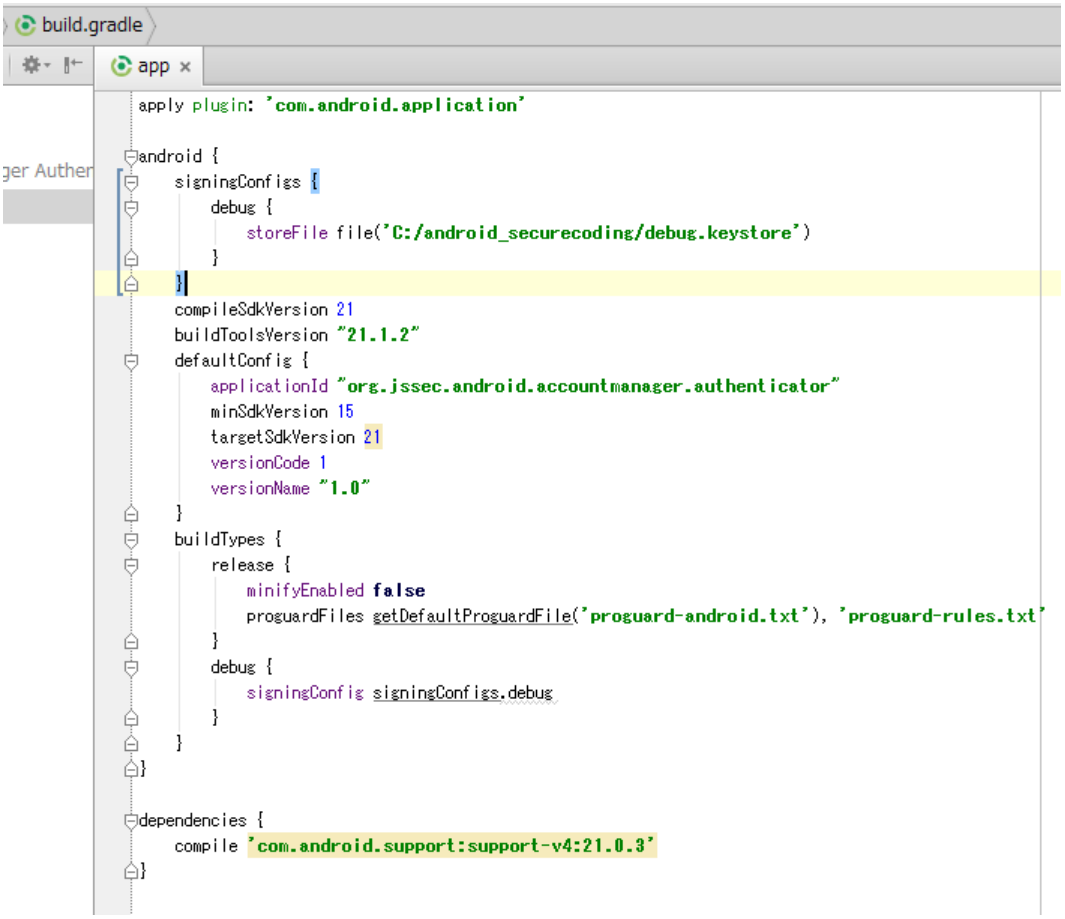


Figure 2.5-19

3. Basic Knowledge of Secure Design and Secure Coding

Although the Guidebook is a collection of security advice concerning Android application development, this chapter will deal with the basic knowledge on general secure design and secure coding of Android smartphones and tablets. Since we will be referring to secure design and coding concepts in the later chapters we recommend that you familiarize yourself with the content contained in this chapter first.

3.1. Android Application Security

There is a commonly accepted way of thinking when examining security issues concerning systems or applications. First, we need to have a grasp over the objects we want to protect. We will call these assets. Next, we want to gain an understanding over the possible attacks that can take place on an asset. We will call these threats. Finally, we will examine and implement measures to protect assets from the various threats. We will call these countermeasures.

What we mean by countermeasures here is secure design and secure coding, and will deal with these subjects after Chapter 4. In this section, we will focus on explaining assets and threats.

3.1.1. Asset: Object of Protection

There are two types of objects of protection within a system or an application: information and functions. We will call these information assets and function assets. An information asset refers to the type of information that can be referred to or changed only by people who have permission. It is a type of information that cannot be referred to or changed by anyone who does not have the permission. A function asset refers to a function that can be used only by people who have permission and no one else.

Below, we will introduce types of information assets and functional assets that exist in Android smartphones and tablets. We would like you to use the following as a point of reference to deliberate on matters with regard to assets when developing a system that utilizes Android applications or Android smartphones/tablets. For the sake of simplicity, we will collectively call Android smartphones/tablets as Android smartphones.

3.1.1.1. Information Asset of an Android Smartphone

Table 3.1-1 and Table 3.1-2 represent examples of information contained on an Android smartphone. Appropriate protection is necessary since this information is equivalent to personal information, confidential information or information that belongs to both.

Table 3.1-1 Examples of Information Managed by an Android Smartphone

Information	Remarks
Phone number	Telephone number of the smartphone itself
Call history	Time and date of incoming and outgoing calls as well as phone numbers
IMEI	Device ID of the smartphone
IMSI	Subscriber ID
Sensor information	GPS, geomagnetic, rate of acceleration, etc.
Various setup information	Wi-Fi setting value, etc...
Account information	Various account information, authentication information, etc.
Media data	Pictures, videos, music, recording, etc...
...	

Table 3.1-2 Examples of Information Managed by an Application

Information	Remarks
Contacts	Contacts of acquaintances
E-mail address	User's e-mail address
E-mail mail box	Content of incoming and outgoing e-mail, attachments, etc.
Web bookmarks	Bookmarks
Web browsing history	Browsing history
Calendar	Plans, to-do list, events, etc.
Facebook	SNS content, etc.
Twitter	SNS content, etc.
...	

The type of information seen in Table 3.1-1 is mainly the type of information that is stored on the Android smartphone itself or on an SD card. Similarly, the type of information seen in Table 3.1-2 is primarily managed by an application. In particular, the type of information seen in Table 3.1-2 grows in proportion to the number of applications installed on the device.

Table 3.1-3 is the amount of information contained in one entry case of contacts. The information here is not of the smartphone user's, but of the smartphone user's friends. In other words, we must be aware that a smartphone not only contains information on the user, but of other people too.

Table 3.1-3 Examples of Information Contained in One Contact Entry

Information	Content
Phone number	Home phone number, mobile phone number, FAX, MMS, etc.
E-mail address	Home e-mail, work e-mail, mobile phone e-mail, etc.
Photo	Thumbnail image, large image, etc.
IM address	AIM, MSN, Yahoo, Skype, QQ, Google Talk, ICQ, Jabber, Net meeting, etc.
Nicknames	Acronyms, initials, maiden names, nicknames, etc.
Address	Country, postal code, region, area, town, street name, etc.
Group membership	Favorites, family, friends, coworkers, etc.
Website	Blogs, profile site, homepage, FTP server, home, office, etc.
Events	Birthdays, anniversaries, others, etc.

Relation	Spouse, children, father, mother, manager, assistants, domestic partner, partners, etc.
SIP address	Home, work, other, etc.
…	…

Until now, we have primarily focused on information about smartphone users, however, application possesses other important information as well. Figure 3.1-1 displays a typical view of the information inside an application divided into the program portion and data portion. The program portion mainly consists of information about the application developer, and the data portion mostly pertains to user information. Since there could be information that an application developer may not want a user to have access to, it is important to provide protective countermeasures to prohibit a user from referring to or making changes to such information.

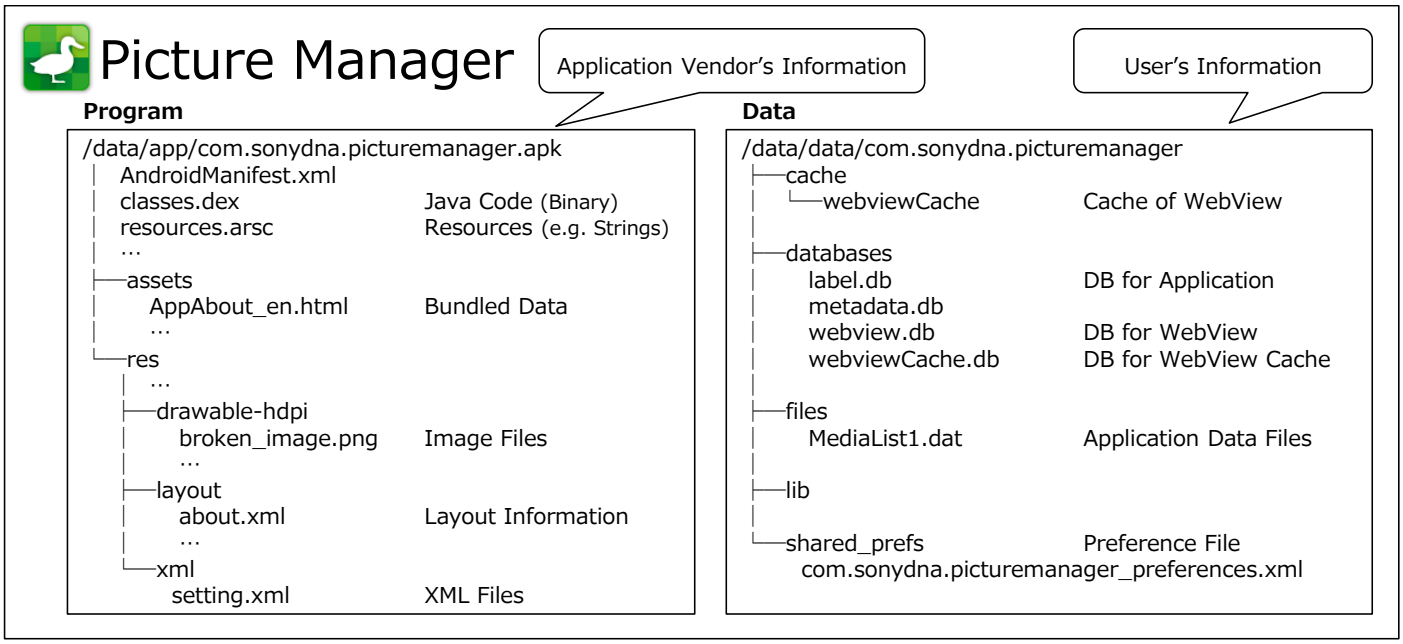


Figure 3.1-1 Information Contained in an Application

When creating an Android application, it is important to employ appropriate protective countermeasures for information that an application manages itself, such as shown in Figure 3.1-1. However, it is equally important to have robust security measure in place for information contained in the Android smartphone itself as well as for information that has been gained from other applications such as shown in Table 3.1-1, Table 3.1-2, and Table 3.1-3.

3.1.1.2. Function Assets of an Android Smartphone

Table 3.1-4 shows examples of features that an Android OS provides to an application. When these features are exploited by a malware, etc., damages in the form of unexpected charges or loss of privacy may be incurred by a user. Therefore, appropriate protective counter-measures that are equal the one extended to information asset should be set in place.

Table 3.1-4 Examples of Features an Android OS Provides to an Application

Function	Function
Sending and receiving SMS messages	Camera
Calling	Volume
Network communication	Reading the Contract List and Status of the Mobile Phone
GPS	SD card
Bluetooth communication	Change system setup
NFC communication	Reading Log Data
Internet communication (SIP)	Obtaining Information of a Running Application
...	...

In addition to the functions that the Android OS provides to an application, the inter-application communication components of Android applications are included as part of the function assets as well. Android applications can allow other applications to utilize features by accessing their internal components. We call this inter-application communication. This is a convenient feature, however, there have been instances where access to functions that should only be used inside a particular application are mistakenly given to other applications due the lack of knowledge regarding secure coding on the part of the developer. There are functions provided by the application that could be exploited by malware that resides locally on the device. Therefore, it is necessary to have appropriate protective countermeasures to only allow legitimate applications to access these functions.

3.1.2. Threats: Attacks that Threaten Assets

In the previous section, we talked about the assets of an Android smartphone. In this section, we will explain about attacks that can threaten an asset. Put simply, a threat to an asset is when a third party who should not have permission, accesses, changes, deletes or creates an information asset or illicitly uses a function asset. The act of directly or indirectly attacking such assets is called a "threat." Furthermore, the malicious person or applications that commit these acts are referred to as the source of the threats. Malicious attackers and malware are the sources of threats but are not the threats themselves. The relationship between our definitions of assets, threats, threat sources, vulnerabilities, and damage are shown below in Figure 3.1-2.

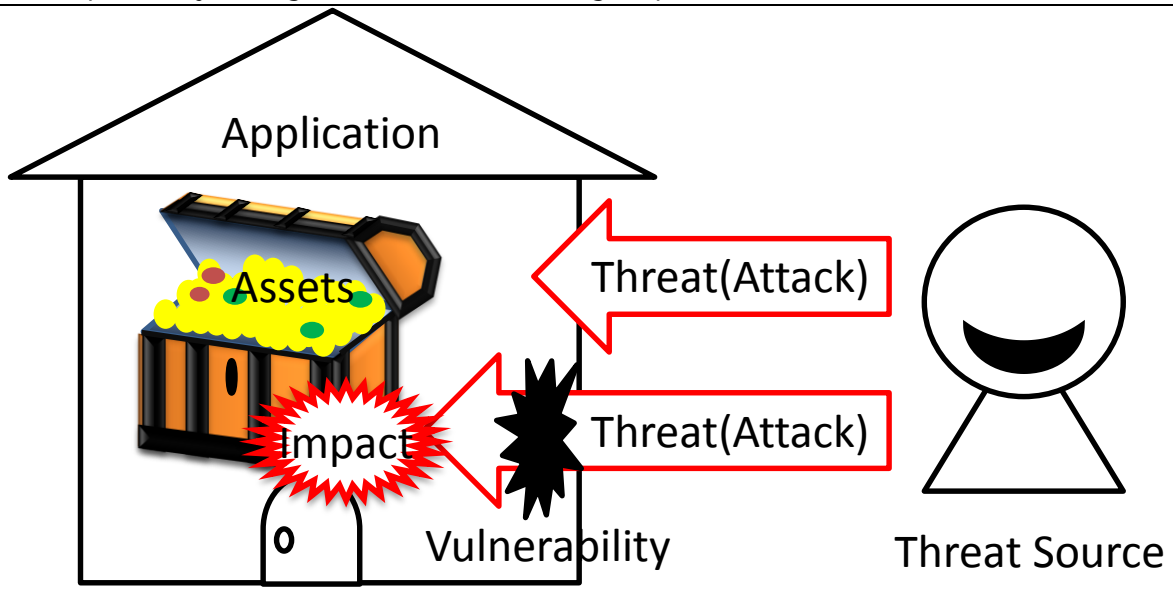


Figure 3.1-2 Relation between Asset, Threat, Threat Source, Vulnerability, and Damage

Figure 3.1-3 shows a typical environment that an Android application behaves in. From now on, in order to expand on the explanation concerning the type of threats an Android application faces by using this figure as a base, we will first learn how to view this figure.

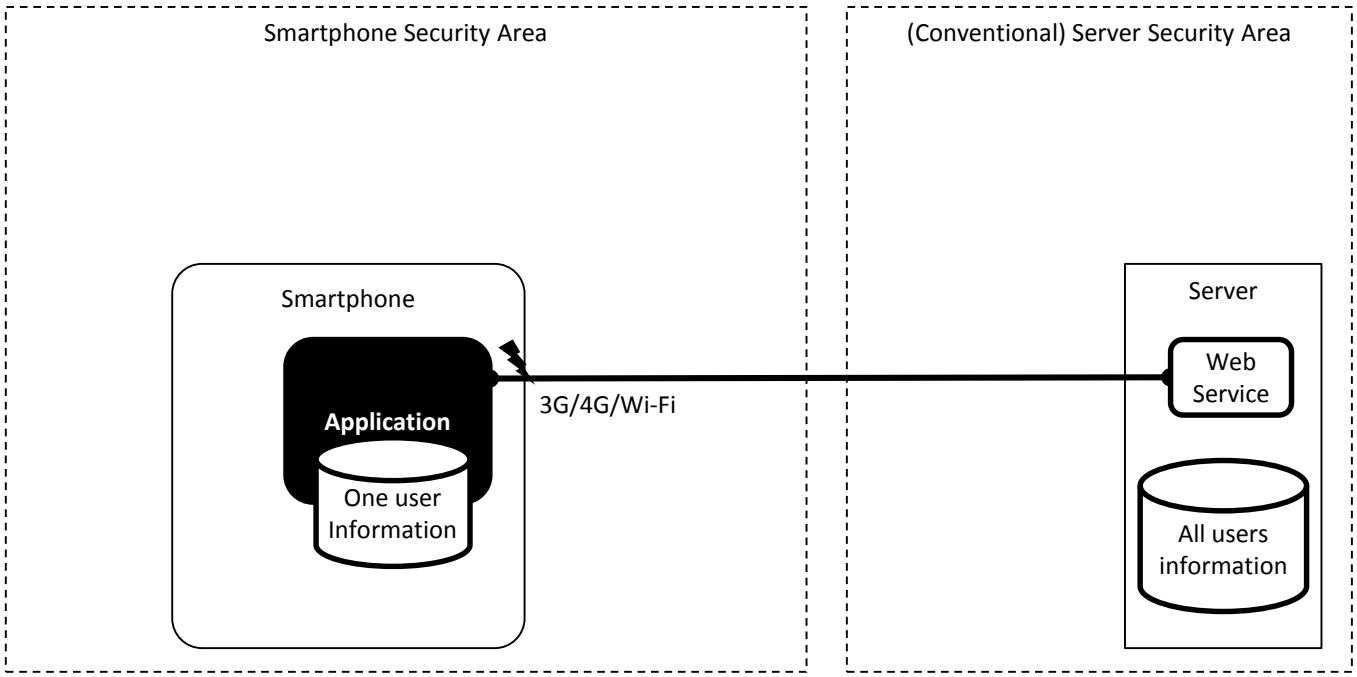


Figure 3.1-3 Typical Environment an Android Application Behaves in

The figure above depicts the smartphone on the left and server on the right. The smartphone and server communicate through the Internet over 3G/4G/Wi-Fi. Although multiple applications exist within a smartphone, we are only showing a single application in the figure in order to explain the threats clearly. Smartphone-based applications mainly handle user information, but the server-based web services collectively manage information of all of its users. Consequently, there is

no change the importance of server security as usual. We will not touch upon issues relating to server security as it falls outside of the scope of the Guidebook.

We will use the following figure to describe the type of threats that exist towards Android applications.

3.1.2.1. Network-based Third-Party

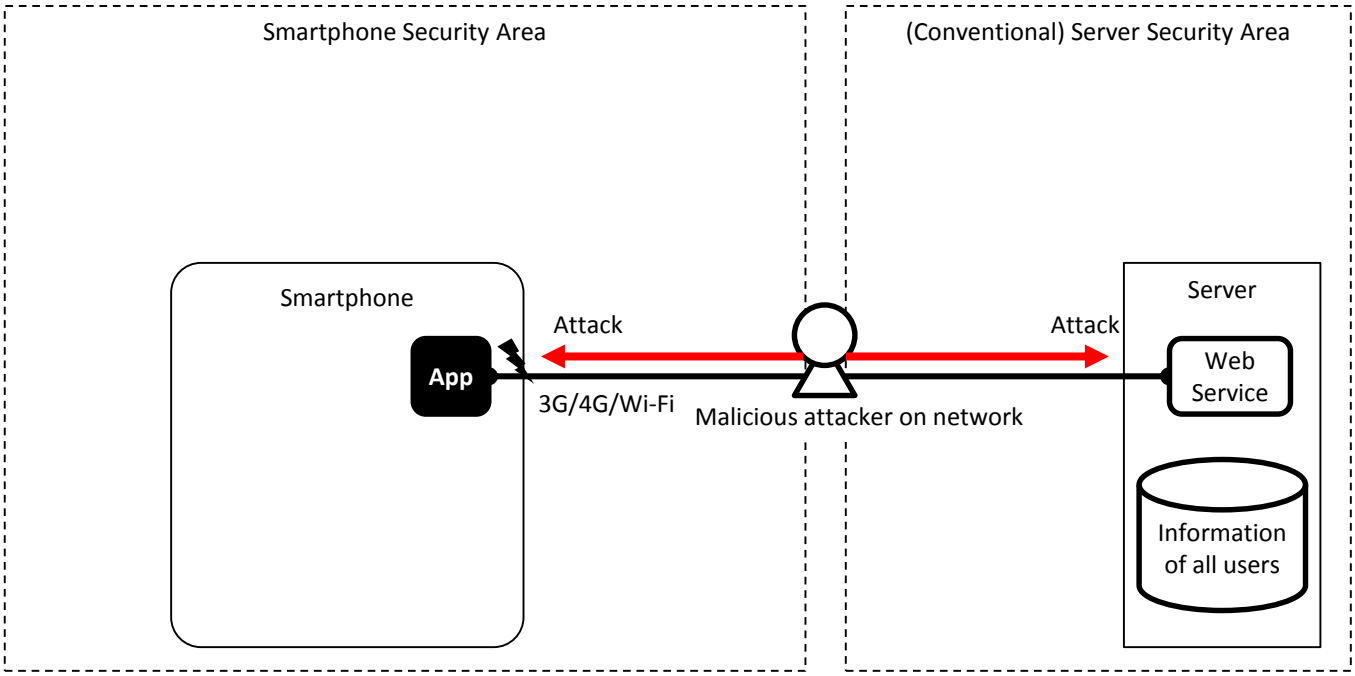


Figure 3.1-4 Network-Based Malicious Third Party Attacking an Application

Generally, a smartphone application manages user information on a server so the information assets will move between the networks connecting them. As indicated in Figure 3.1-4, a network-based malicious third party may access (sniff) any information during this communication or try to change information (data manipulation). The malicious attacker in the middle (also referred to as "Man in The Middle") can also pretend to be the real server tricking the application. Without saying, network-based malicious third parties will usually try to attack the server as well.

3.1.2.2. Threat Due to User-Installed Malware

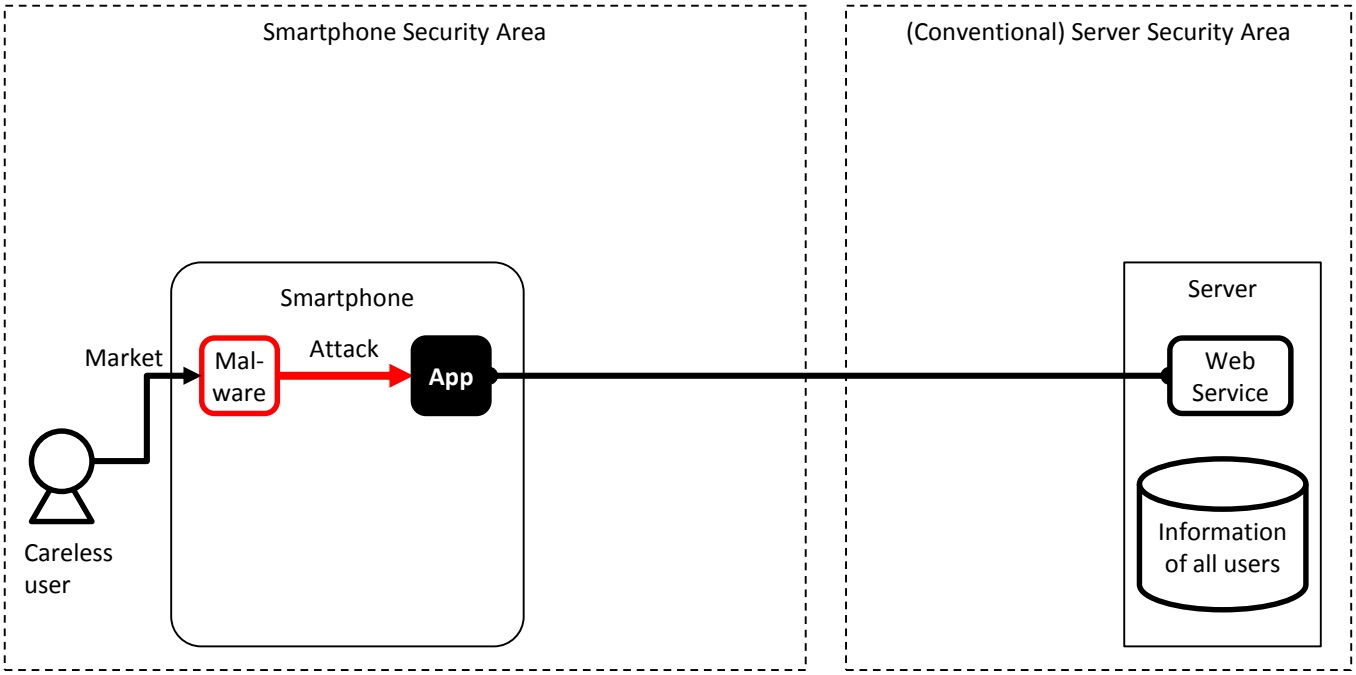


Figure 3.1-5 Malware Installed by a User Attacks an Application

The biggest selling point of a smartphone is in its ability to acquire numerous applications from the market in order to expand on its features. The downside to users being able to freely install many applications is that they will sometimes mistakenly install malware. As shown in Figure 3.1-5, malware may exploit the inter-application communication functions or a vulnerability in the application in order to gain access to information or function assets.

3.1.2.3. Threat of an Malicious File that Exploits a Vulnerability in an Application

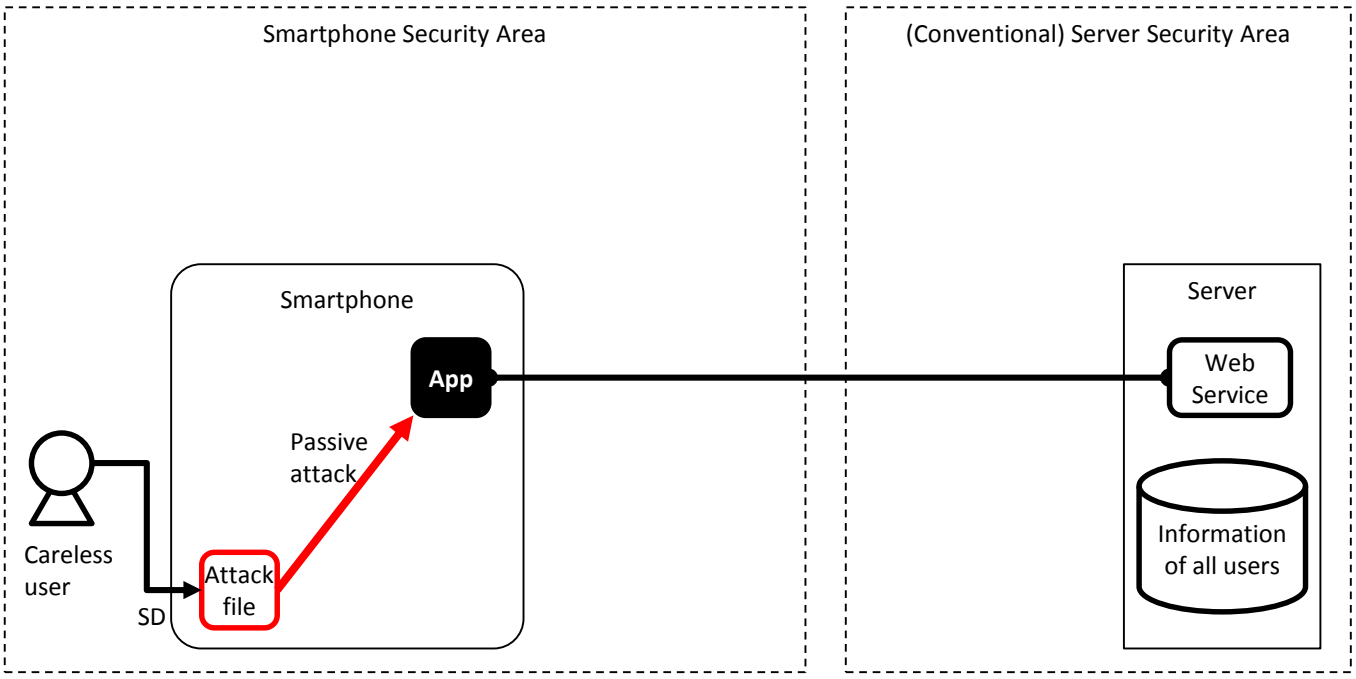


Figure 3.1-6 Attack from Malicious Files that Exploit a Vulnerability in an Application

Various types of files such as music, images, videos and documents are widely available on the

Internet and typically users will download many files to their SD card in order to use them on their smartphone. Furthermore, it is also common to download attached files sent in an e-mail. These files are later opened by a viewing or editing application.

If there is any vulnerability in the function of an application that processes these files, an attacker can use a malicious file to exploit it and gain access to information or function assets of the application. In particular, vulnerabilities are often present in processing a file format with a complex data structure. The attacker can fulfill many different goals when exploiting an application in this way.

As shown in Figure 3.1-6, an attack file stays dormant until it is opened by a vulnerable application. Once it is opened, it will start causing havoc by taking advantage of an application's vulnerability. In comparison to an active attack, we call this attack method a "Passive Attack."

3.1.2.4. Threats from a Malicious Smartphone User

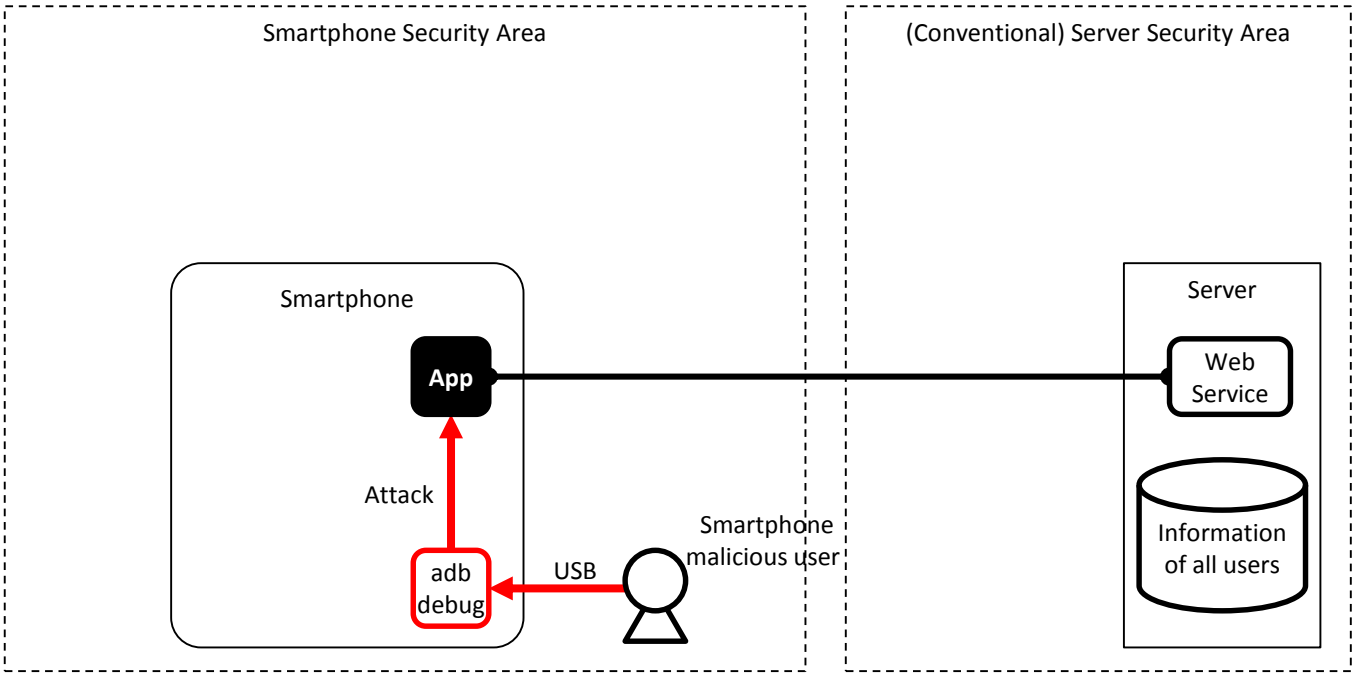


Figure 3.1-7 Attacks from a Malicious Smartphone User

With regard to application development for an Android smartphone, the environment as well as features that help to develop and analyze an application are openly provided to the general user. Among the features that are provided, the useful ADB debugging feature can be accessed by anyone without registration or screening. This feature allows an Android smartphone user to easily perform OS or application analysis.

As it is shown in Figure 3.1-7, a smartphone user with malicious intent can analyze an application by taking advantage of the debugging feature of ADB and try to gain access to information or function assets of an application. If the actual asset contained in the application belongs to the user, it poses no problem, but if the asset belongs to someone other than the user, such as the application developer, then it will become a concern. Accordingly, we need to be aware that the legitimate smartphone user can maliciously target the assets within an application.

3.1.2.5. Threats from Third Party in the Proximity of a Smartphone

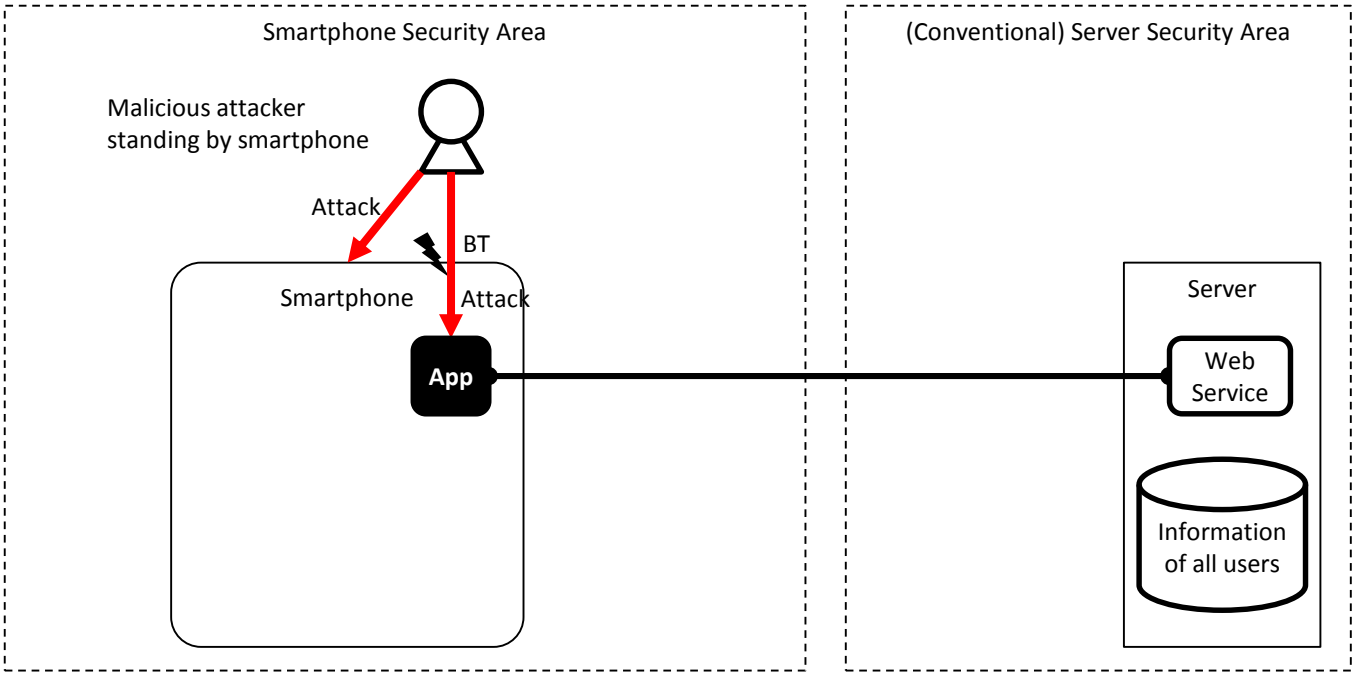


Figure 3.1-8 Attacks from a Malicious Third Party in the Proximity of a Smartphone

Due to face that most smartphones possess a variety of near-field communication mechanisms, such as NFC, Bluetooth and Wi-Fi, we must not forget that attacks can occur from a malicious attacker who is in physical proximity of a smartphone. An attacker can shoulder surf a password while peeping over a user who is inputting it in. Or, as indicated in Figure 3.1-8, an attacker can be more sophisticated and attack the Bluetooth functionality of an application from a remote distance. There is also the threat that a malicious person could steal the smartphone creating a risk of data leakage or even destroy the smartphone causing a loss of critical information. Developers need to take these risks into consideration as well as early as the design stage.

3.1.2.6. Summary of Threats

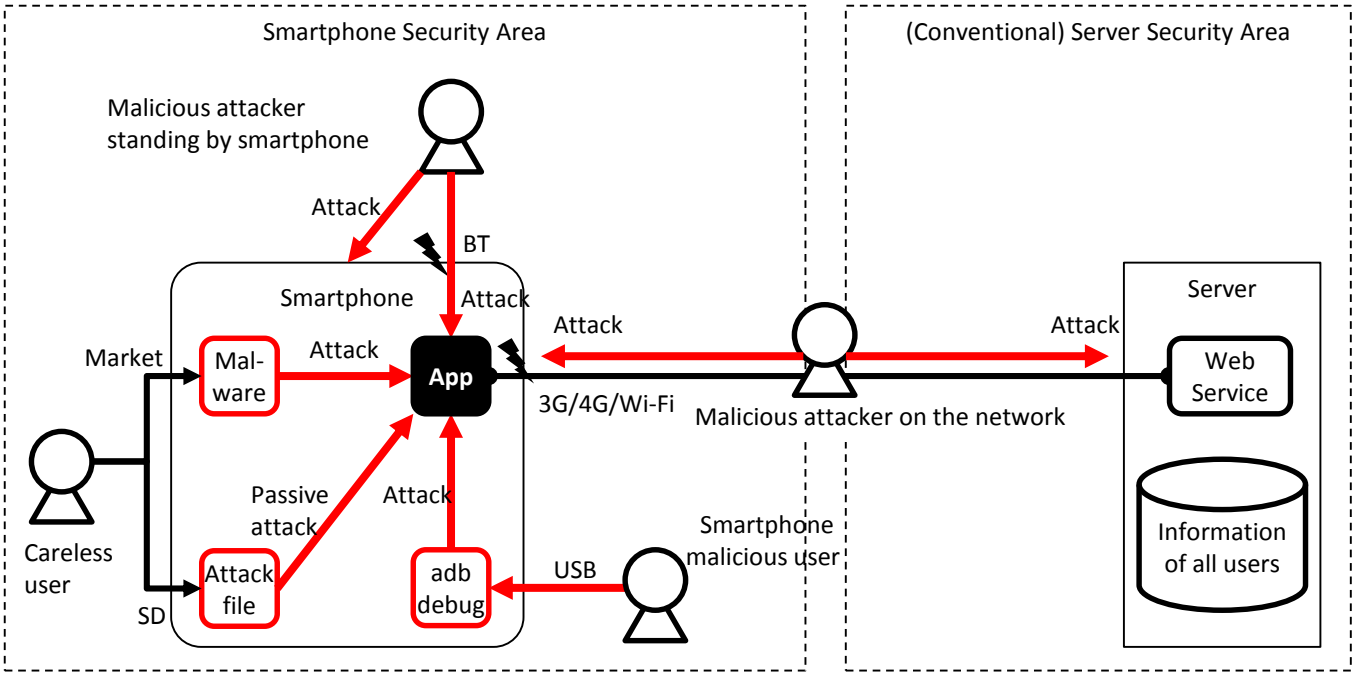


Figure 3.1-9 Summary of the Various Attacks on Smartphone Applications

Figure 3.1-9 summarizes the main types of threats explained in the previous sections. Smartphones are surrounded by a wide variety of threats and the figure above does not include all of them. Through our daily information gathering, we need to spread the awareness concerning the various threats that surround an Android application and be aware of them during the application's secure design and coding. The following literature that was created by Japan's Smartphone Security Association (JSSEC) contains other valuable information on the threats to smartphone security.

- Security Guidebook for Using Smartphones and Tablets
  http://www.jssec.org/dl/guidelines_v2.pdf [Version 2](Japanese)
  http://www.jssec.org/dl/Guidebook2012Enew_v1.0.pdf [Version 1] (English)

- Implementation Guidebook for Smartphone Network Security[Version 1]
  http://www.jssec.org/dl/NetworkSecurityGuide1.pdf (Japanese)

- Cloud Usage Guidebook for Business Purposes of Smartphones [Beta Version]
  http://www.jssec.org/dl/cloudguide2012_beta.pdf (Japanese)

- Guidebook for Reviewing the Implementation/Operation of MDM [Version1]
  http://www.jssec.org/dl/MDMGuideV1.pdf (Japanese)

3.1.3. Asset Classification and Protective Countermeasures

As was discussed in the previous sections, Android smartphones are surrounded by a variety of threats. Protecting every asset in an application from such threats could prove to be very difficult given the time it takes for development and due to technical limitations. Consequently, Android application developers should examine feasible countermeasures for their assets. This should be done according to priority level based on the developer's judgement criteria. This is a subjective matter that is based on how the importance of an asset is viewed and what the accepted level of damage is.

In order to help decide on the protective countermeasures for each asset, we will classify them and stipulate the level of protective countermeasures for each group. This will be achieved by examining the legal basis, pertaining to the level of importance regarding the impact of any damages that can occur and the social responsibility of the developer (or organization). These will prove to be the judgement criteria when deciding on how to handle each asset and the implementation of the type of countermeasures. Since this will become a standard for application developers and organizations on determining how to handle an asset and provide protective countermeasures, it is necessary to specify the classification methods and pertaining countermeasures in accordance the application developer's (or organization's) circumstances.

Asset classification and protective countermeasure levels that are adopted in the Guidebook are shown below for reference:

Table 3.1-5 Asset Classification and Protective Countermeasure Levels

Asset Classification	Asset Level	Level of Protective Counter-Measures
High	The amount of damage the asset causes is fatal and catastrophic to the organization or an individual's activity. i.e.) When an asset at this level is damaged, the organization will not be able to continue its business.	• Provide protection against sophisticated attacks that break through the Android OS security model and prevent root privilege compromises and attacks that alter the dex portion of an APK. • Ensure security takes priority over other elements such as user experience, etc.
Medium	The amount of damage the asset causes has a substantial impact the organization or an individual's activity. i.e.) When an asset at this level is damaged, the organization's profit level deteriorates, adversely affecting its business.	• Utilize the Android OS security model. It will provide protection covered under its scope. • Ensure security takes priority over other elements such as user experience, etc.
Low	The amount of damage the asset causes has a limited impact on the organization or an individual's activity. I.e.) When an asset at this level is damaged, the organization's profit level will be affected but is able to compensate its losses from other resources.	• Utilize the Android OS security model. It will provide protection covered under its scope. • Compare security countermeasures with other elements such as user experience, etc. At this level, it is possible for non-security issues to take precedence over security issues.

This Guidebook's Scope of Focus

Asset classification and protective countermeasures described in the Guidebook are proposed under the premise of a secure Android device where root privilege has not been compromised. Furthermore, it is based on the security measures that utilize the security model of Android OS. Specifically, we are hypothetically devising protective countermeasures by utilizing the Android OS security model on the premise of a functioning Android OS security model against assets that are classified lower than or equal to the medium level asset. On the other hand, we also believe in the necessity of protecting high level assets from attacks that are caused due the breaching of the Android OS security model. Such attacks include the compromise of root privileges and attacks that analyze or alter the APK binary. To protect these types of assets, we need to design sophisticated defensive countermeasures against such threats through the combination of multiple methods such as encryption, obfuscation, hardware support and server support. As the collection of know-how regarding these defenses cannot be easily written in this guidebook, and since appropriate defensive design differ in accordance to individual circumstances, we have deemed them to be outside of the Guidebook's scope. We recommend that you consult with a security specialist who is well versed in tamper resistant designs of Android if your device requires protection from sophisticated attacks that include attacks resulting from the compromise of root privileges or attacks caused by the analysis or alteration of an APK file.

3.1.4. Sensitive Information

The term "sensitive information", instead of information asset, will be used from now on in the Guidebook. As it has been aforementioned in the previous section, we have to determine the asset level and the level of protective countermeasures for each information asset that an application handles.

3.2. Handling Input Data Carefully and Securely

Validating input data is the easiest and yet most effective secure coding method. All data that is inputted into the application either directly or indirectly by an outside source needs to be properly validated. To illustrate best practices of input data validation, the following is an example of an Activity as used in a program that receives data from Intent.

It is possible that an Activity can receive data from an Intent that was tampered by an attacker. By sending data with a format or a value that a programmer is not expecting, the attacker can induce a malfunction in the application that leads to some sort of security incident. We must not forget that a user can become an attacker as well.

Intents are configured by action, data and extras, and we must be careful when accepting all forms of data that can be controlled by an attacker. We always need to validate the following items in any code that handles data from an untrusted source.

(a) Does the received data match the format that was expected by the programmer and does the value fall in the expected scope?
(b) Even if you have received the expected format and value, can you guarantee that the code which handles that data will not behave unexpectedly?

The next example is a simple sample where HTML is acquired from a remote web page in a designated URL and the code is displayed in TextView. However, there is a bug.

Sample Code that Displays HTML of a Remote Web page in TextView

```
TextView tv = (TextView) findViewById(R.id.textview);
InputStreamReader isr = null;
char[] text = new char[1024];
int read;
try {
    String urlstr = getIntent().getStringExtra("WEBPAGE_URL");
    URL url = new URL(urlstr);
    isr = new InputStreamReader(url.openConnection().getInputStream());
    while ((read=isr.read(text)) != -1) {
        tv.append(new String(text, 0, read));
    }
} catch (MalformedURLException e) { ...
```

From the viewpoint of (a), "urlstr is the correct URL", verified through the non-occurrence of a MalformedURLException by a new URL(). However, this is not sufficient. Furthermore, when a "file://..." formatted URL is designated by urlstr, the file of the internal file system is opened and is displayed in TextView rather than the remote web page. This does not fulfill the viewpoint of (b), since it does not guarantee the behavior which was expected by the programmer.

The next example shows a revision to fix the security bugs. Through the viewpoint of (a), the input data is validated by checking that "urlstr is a legitimate URL and the protocol is limited to http or https." As a result, even by the viewpoint of (b), the acquisition of an Internet-routed InputStream is guaranteed through url.openConnection().getInputStream().

Revised sample code that displays HTML of Internet-based Web page in TextView

```
TextView tv = (TextView) findViewById(R.id.textview);
InputStreamReader isr = null;
char[] text = new char[1024];
int read;
try {
    String urlstr = getIntent().getStringExtra("WEBPAGE_URL");
    URL url = new URL(urlstr);
    String prot = url.getProtocol();
    if (!"http".equals(prot) && !"https".equals(prot)) {
        throw new MalformedURLException("invalid protocol");
    }
    isr = new InputStreamReader(url.openConnection().getInputStream());
    while ((read=isr.read(text)) != -1) {
        tv.append(new String(text, 0, read));
    }
} catch (MalformedURLException e) { ...
```

Validating the safety of input data is called "Input Validation" and it is a fundamental secure coding method. Surmising from the sense of the word of Input Validation, it is quite often the case where the viewpoint of (a) is heeded but the viewpoint of (b) is forgotten. It is important to remember that damage does not take place when data enters the program but when the program uses that data in an incorrect way. We hope that you will refer the URLs listed below.

- The CERT Oracle Secure Coding Standard for Java
  https://www.securecoding.cert.org/confluence/x/Ux (English)

- Application of CERT Oracle Secure Coding Standard for Android Application Development
  https://www.securecoding.cert.org/confluence/x/C4AiBw (English)

- Rules Applicable Only to the Android Platform (DRD)
  https://www.securecoding.cert.org/confluence/x/H4ClBg (English)

- IPA "Secure Programming Course"
  http://www.ipa.go.jp/security/awareness/vendor/programmingv2/clanguage.html (Japanese)

4. Using Technology in a Safe Way

In Android, there are many specific security related issues that pertain only to certain technologies such as Activities or SQLite. If a developer does not have enough knowledge about each of the different security issues regarding each technology when designing and coding, then unexpected vulnerabilities may arise. This chapter will explain about the different scenarios that developers will need to know when using their application components.

4.1. Creating/Using Activities

4.1.1. Sample Code

The risks and countermeasures of using Activities differ depending on how that Activity is being used. In this section, we have classified 4 types of Activities based on how the Activity is being used. You can find out which type of activity you are supposed to create through the following chart shown below. Since the secure coding best practice varies according to how the activity is used, we will also explain about the implementation of the Activity as well.

Table 4.1-1 Definition of Activity Types

Type	Definition
Private Activity	An activity that cannot be launched by another application, and therefore is the safest activity
Public Activity	An activity that is supposed to be used by an unspecified large number of applications.
Partner Activity	An activity that can only be used by specific applications made by a trusted partner company.
In-house Activity	An activity that can only be used by other in-house applications.

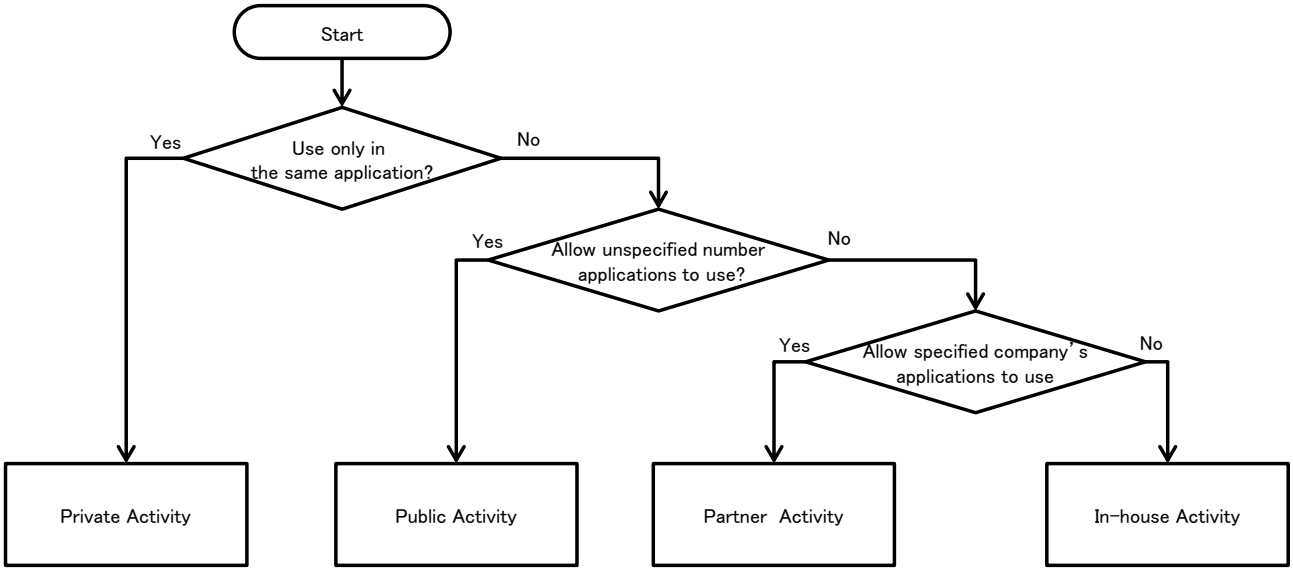


Figure 4.1-1

4.1.1.1. Creating/Using Private Activities

Private Activities are Activities which cannot be launched by the other applications and therefore it is the safest Activity.

When using Activities that are only used within the application (Private Activity), as long as you use explicit Intents to the class then you do not have to worry about accidently sending it to any other application. However, there is a risk that a third party application can read an Intent that is used to start the Activity. Therefore it is necessary to make sure that if you are putting sensitive information inside an Intent used to start an Activity that you take countermeasures to make sure that it cannot be read by a malicious third party.

Sample code of how to create a Private Activity is shown below.

Points (Creating an Activity):

1. Do not specify taskAffinity.
2. Do not specify launchMode.
3. Explicitly set the exported attribute to false.
4. Handle the received intent carefully and securely, even though the intent was sent from the same application.
5. Sensitive information can be sent since it is sending and receiving all within the same application.

To make the Activity private, set the "exported" attribute of the Activity element in the AndroidManifest.xml to false.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.activity.privateactivity" >

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- Private activity -->
        <!-- *** POINT 1 *** Do not specify taskAffinity -->
        <!-- *** POINT 2 *** Do not specify launchMode -->
        <!-- *** POINT 3 *** Explicitly set the exported attribute to false. -->
        <activity
            android:name=".PrivateActivity"
            android:label="@string/app_name"
            android:exported="false" />

        <!-- Public activity launched by launcher -->
        <activity
            android:name=".PrivateUserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
```



```
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
</application>
</manifest>
```

PrivateActivity.java

```
package org.jssec.android.activity.privateactivity;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PrivateActivity extends Activity {

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.private_activity);

        // *** POINT 4 *** Handle the received Intent carefully and securely, even though the Intent was
sent from the same application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String param = getIntent().getStringExtra("PARAM");
        Toast.makeText(this, String.format("Received param: ¥"%s¥"", param), Toast.LENGTH_LONG).show();
    }

    public void onReturnResultClick(View view) {

        // *** POINT 5 *** Sensitive information can be sent since it is sending and receiving all within
 the same application.
        Intent intent = new Intent();
        intent.putExtra("RESULT", "Sensitive Info");
        setResult(RESULT_OK, intent);
        finish();
    }
}
```

Next, we show the sample code for how to use the Private Activity.

Point (Using an Activity):

6. Do not set the FLAG_ACTIVITY_NEW_TASK flag for intents to start an activity.
7. Use the explicit Intents with the class specified to call an activity in the same application.
8. Sensitive information can be sent only by putExtra() since the destination activity is in the same application.[1]
9. Handle the received result data carefully and securely, even though the data comes from an activity within the same application.

PrivateUserActivity.java

```
package org.jssec.android.activity.privateactivity;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PrivateUserActivity extends Activity {

    private static final int REQUEST_CODE = 1;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.user_activity);
    }

    public void onUseActivityClick(View view) {

        // *** POINT 6 *** Do not set the FLAG_ACTIVITY_NEW_TASK flag for intents to start an activity.
        // *** POINT 7 *** Use the explicit Intents with the class specified to call an activity in the s
ame application.
        Intent intent = new Intent(this, PrivateActivity.class);

        // *** POINT 8 *** Sensitive information can be sent only by putExtra() since the destination act
ivity is in the same application.
        intent.putExtra("PARAM", "Sensitive Info");

        startActivityForResult(intent, REQUEST_CODE);
    }

    @Override
    public void onActivityResult(int requestCode, int resultCode, Intent data) {
        super.onActivityResult(requestCode, resultCode, data);

        if (resultCode != RESULT_OK) return;

        switch (requestCode) {
        case REQUEST_CODE:
```

[1] Caution: Unless points 1, 2 and 6 are abided by, there is a risk that Intents may be read by a third party. Please refer to sections 4.1.2.2 and 4.1.2.3 for more details.


```
            String result = data.getStringExtra("RESULT");

            // *** POINT 9 *** Handle the received data carefully and securely,
            // even though the data comes from an activity within the same application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            Toast.makeText(this, String.format("Received result: ¥"%s¥"", result), Toast.LENGTH_LONG).sh
ow();
            break;
        }
    }
}
```

4.1.1.2. Creating/Using Public Activities

Public Activities are Activities which are supposed to be used by an unspecified large number of applications. It is necessary to be aware that Public Activities may receive Intents sent from malware. In addition, when using Public Activities, it is necessary to be aware of the fact that malware can also receive or read the Intents sent to them.

The sample code to create a Public Activity is shown below.

Points (Creating an Activity):

1. Explicitly set the exported attribute to true.
2. Handle the received intent carefully and securely.
3. When returning a result, do not include sensitive information.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.activity.publicactivity" >

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- Public Activity -->
        <!-- *** POINT 1 *** Explicitly set the exported attribute to true. -->
        <activity
            android:name=".PublicActivity"
            android:label="@string/app_name"
            android:exported="true">

            <!-- Define intent filter to receive an implicit intent for a specified action -->
            <intent-filter>
                <action android:name="org.jssec.android.activity.MY_ACTION" />
                <category android:name="android.intent.category.DEFAULT" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

PublicActivity.java

```
package org.jssec.android.activity.publicactivity;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PublicActivity extends Activity {

    @Override
    public void onCreate(Bundle savedInstanceState) {
```



```
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);

        // *** POINT 2 *** Handle the received intent carefully and securely.
        // Since this is a public activity, it is possible that the sending application may be malware.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String param = getIntent().getStringExtra("PARAM");
        Toast.makeText(this, String.format("Received param: ¥"%s¥"", param), Toast.LENGTH_LONG).show();
    }

    public void onReturnResultClick(View view) {

        // *** POINT 3 *** When returning a result, do not include sensitive information.
        // Since this is a public activity, it is possible that the receiving application may be malware.
        // If there is no problem if the data gets received by malware, then it can be returned as a resu
lt.
        Intent intent = new Intent();
        intent.putExtra("RESULT", "Not Sensitive Info");
        setResult(RESULT_OK, intent);
        finish();
    }
}
```

Next, Herein after sample code of Public Activity user side.

Points (Using an Activity):

4. Do not send sensitive information.
5. When receiving a result, handle the data carefully and securely.

PublicUserActivity.java

```
package org.jssec.android.activity.publicuser;

import android.app.Activity;
import android.content.ActivityNotFoundException;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PublicUserActivity extends Activity {

    private static final int REQUEST_CODE = 1;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }

    public void onUseActivityClick(View view) {

        try {
            // *** POINT 4 *** Do not send sensitive information.
            Intent intent = new Intent("org.jssec.android.activity.MY_ACTION");
            intent.putExtra("PARAM", "Not Sensitive Info");
            startActivityForResult(intent, REQUEST_CODE);
        } catch (ActivityNotFoundException e) {
            Toast.makeText(this, "Target activity not found.", Toast.LENGTH_LONG).show();
        }
    }

    @Override
    public void onActivityResult(int requestCode, int resultCode, Intent data) {
        super.onActivityResult(requestCode, resultCode, data);

        // *** POINT 5 *** When receiving a result, handle the data carefully and securely.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        if (resultCode != RESULT_OK) return;
        switch (requestCode) {
        case REQUEST_CODE:
            String result = data.getStringExtra("RESULT");
            Toast.makeText(this, String.format("Received result: ¥"%s¥"", result), Toast.LENGTH_LONG).sh
ow();
            break;
        }
    }
}
```


4.1.1.3. Creating/Using Partner Activities

Partner activities are Activities that can only be used by specific applications. They are used between cooperating partner companies that want to securely share information and functionality.

There is a risk that a third party application can read an Intent that is used to start the Activity. Therefore it is necessary to make sure that if you are putting sensitive information inside an Intent used to start an Activity that you take countermeasures to make sure that it cannot be read by a malicious third party

Sample code for creating a Partner Activity is shown below.

Points (Creating an Activity):

1. Do not specify taskAffinity.
2. Do not specify launchMode.
3. Do not define the intent filter and explicitly set the exported attribute to true.
4. Verify the requesting application's certificate through a predefined whitelist.
5. Handle the received intent carefully and securely, even though the intent was sent from a partner application.
6. Only return Information that is granted to be disclosed to a partner application.

Please refer to "4.1.3.2 Validating the Requesting Application" for how to validate an application by a white list. Also, please refer to "5.2.1.3 How to Verify the Hash Value of an Application's Certificate" for how to verify the certificate hash value of a destination application which is specified in the whitelist.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
    android:layout_width="fill_parent"
    android:layout_height="fill_parent"
    android:orientation="vertical"
    android:padding="5dp" >
    <TextView
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_marginTop="20dp"
        android:text="@string/description" />
    <Button
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_marginTop="20dp"
        android:onClick="onReturnResultClick"
        android:text="@string/return_result" />
</LinearLayout>
```

PartnerActivity.java

```
package org.jssec.android.activity.partneractivity;

import org.jssec.android.shared.PkgCertWhitelists;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PartnerActivity extends Activity {

    // *** POINT 4 *** Verify the requesting application's certificate through a predefined whitelist.
    private static PkgCertWhitelists sWhitelists = null;
    private static void buildWhitelists(Context context) {
        boolean isdebug = Utils.isDebuggable(context);
        sWhitelists = new PkgCertWhitelists();

        // Register certificate hash value of partner application org.jssec.android.activity.partneruser
.
        sWhitelists.add("org.jssec.android.activity.partneruser", isdebug ?
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255" :
                // Certificate hash value of "partner key" in the keystore.
                "1F039BB5 7861C27A 3916C778 8E78CE00 690B3974 3EB8259F E2627B8D 4C0EC35A");

        // Register the other partner applications in the same way.
    }
    private static boolean checkPartner(Context context, String pkgname) {
        if (sWhitelists == null) buildWhitelists(context);
        return sWhitelists.test(context, pkgname);
    }

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);

        // *** POINT 4 *** Verify the requesting application's certificate through a predefined whitelis
t.
        if (!checkPartner(this, getCallingActivity().getPackageName())) {
            Toast.makeText(this,
                    "Requesting application is not a partner application.",
                    Toast.LENGTH_LONG).show();
            finish();
            return;
        }

        // *** POINT 5 *** Handle the received intent carefully and securely, even though the intent was
sent from a partner application.
        // Omitted, since this is a sample. Refer to "3.2 Handling Input Data Carefully and Securely."
        Toast.makeText(this, "Accessed by Partner App", Toast.LENGTH_LONG).show();
    }

    public void onReturnResultClick(View view) {

        // *** POINT 6 *** Only return Information that is granted to be disclosed to a partner applicati
```



```
on.
        Intent intent = new Intent();
        intent.putExtra("RESULT", "Information for partner applications");
        setResult(RESULT_OK, intent);
        finish();
    }
}
```

PkgCertWhitelists.java

```
package org.jssec.android.shared;

import java.util.HashMap;
import java.util.Map;

import android.content.Context;

public class PkgCertWhitelists {
    private Map<String, String> mWhitelists = new HashMap<String, String>();

    public boolean add(String pkgname, String sha256) {
        if (pkgname == null) return false;
        if (sha256 == null) return false;

        sha256 = sha256.replaceAll(" ", "");
        if (sha256.length() != 64) return false;    // SHA-256 -> 32 bytes -> 64 chars
        sha256 = sha256.toUpperCase();
        if (sha256.replaceAll("[0-9A-F]+", "").length() != 0) return false; // found non hex char

        mWhitelists.put(pkgname, sha256);
        return true;
    }

    public boolean test(Context ctx, String pkgname) {
        // Get the correct hash value which corresponds to pkgname.
        String correctHash = mWhitelists.get(pkgname);

        // Compare the actual hash value of pkgname with the correct hash value.
        return PkgCert.test(ctx, pkgname, correctHash);
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
```

```
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


Sample code for using a Partner Activity is described below.

Points (Using an Activity):

7. Verify if the certificate of the target application has been registered in a whitelist.
8. Do not set the FLAG_ACTIVITY_NEW_TASK flag for the intent that start an activity.
9. Only send information that is granted to be disclosed to a Partner Activity only by putExtra().
10. Use explicit intent to call a Partner Activity.
11. Use startActivityForResult() to call a Partner Activity.
12. Handle the received result data carefully and securely, even though the data comes from a partner application.

Refer to "4.1.3.2 Validating the Requesting Application" for how to validate applications by white list. Also please refer to "5.2.1.3 How to Verify the Hash Value of an Application's Certificate" for how to verify the certificate hash value of a destination application which is to be specified in a white list.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.activity.partneruser" >

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <activity
            android:name="org.jssec.android.activity.partneruser.PartnerUserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

PartnerUserActivity.java

```
package org.jssec.android.activity.partneruser;

import org.jssec.android.shared.PkgCertWhitelists;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.ActivityNotFoundException;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PartnerUserActivity extends Activity {
```

```
    // *** POINT 7 *** Verify if the certificate of a target application has been registered in a white
list.
    private static PkgCertWhitelists sWhitelists = null;
    private static void buildWhitelists(Context context) {
        boolean isdebug = Utils.isDebuggable(context);
        sWhitelists = new PkgCertWhitelists();

        // Register the certificate hash value of partner application org.jssec.android.activity.partner
activity.
        sWhitelists.add("org.jssec.android.activity.partneractivity", isdebug ?
                // The certificate hash value of "androiddebugkey" is in debug.keystore.
                "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255" :
                // The certificate hash value of "my company key" is in the keystore.
                "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA");

        // Register the other partner applications in the same way.
    }
    private static boolean checkPartner(Context context, String pkgname) {
        if (sWhitelists == null) buildWhitelists(context);
        return sWhitelists.test(context, pkgname);
    }

    private static final int REQUEST_CODE = 1;

    // Information related the target partner activity
    private static final String TARGET_PACKAGE =  "org.jssec.android.activity.partneractivity";
    private static final String TARGET_ACTIVITY = "org.jssec.android.activity.partneractivity.PartnerAc
tivity";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }

    public void onUseActivityClick(View view) {

        // *** POINT 7 *** Verify if the certificate of the target application has been registered in the
 own white list.
        if (!checkPartner(this, TARGET_PACKAGE)) {
            Toast.makeText(this, "Target application is not a partner application.", Toast.LENGTH_LONG).
show();
            return;
        }

        try {
            // *** POINT 8 *** Do not set the FLAG_ACTIVITY_NEW_TASK flag for the intent that start an ac
tivity.
            Intent intent = new Intent();

            // *** POINT 9 *** Only send information that is granted to be disclosed to a Partner Activit
y only by putExtra().
            intent.putExtra("PARAM", "Info for Partner Apps");

            // *** POINT 10 *** Use explicit intent to call a Partner Activity.
            intent.setClassName(TARGET_PACKAGE, TARGET_ACTIVITY);

            // *** POINT 11 *** Use startActivityForResult() to call a Partner Activity.
            startActivityForResult(intent, REQUEST_CODE);
        }
```



```
        catch (ActivityNotFoundException e) {
            Toast.makeText(this, "Target activity not found.", Toast.LENGTH_LONG).show();
        }
    }

    @Override
    public void onActivityResult(int requestCode, int resultCode, Intent data) {
        super.onActivityResult(requestCode, resultCode, data);

        if (resultCode != RESULT_OK) return;

        switch (requestCode) {
        case REQUEST_CODE:
            String result = data.getStringExtra("RESULT");

            // *** POINT 12 *** Handle the received data carefully and securely,
            // even though the data comes from a partner application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            Toast.makeText(this,
                   String.format("Received result: ¥"%s¥"", result), Toast.LENGTH_LONG).show();
            break;
        }
    }
}
```

PkgCertWhitelists.java

```
package org.jssec.android.shared;

import java.util.HashMap;
import java.util.Map;

import android.content.Context;

public class PkgCertWhitelists {
    private Map<String, String> mWhitelists = new HashMap<String, String>();

    public boolean add(String pkgname, String sha256) {
        if (pkgname == null) return false;
        if (sha256 == null) return false;

        sha256 = sha256.replaceAll(" ", "");
        if (sha256.length() != 64) return false;    // SHA-256 -> 32 bytes -> 64 chars
        sha256 = sha256.toUpperCase();
        if (sha256.replaceAll("[0-9A-F]+", "").length() != 0) return false; // found non hex char

        mWhitelists.put(pkgname, sha256);
        return true;
    }

    public boolean test(Context ctx, String pkgname) {
        // Get the correct hash value which corresponds to pkgname.
        String correctHash = mWhitelists.get(pkgname);

        // Compare the actual hash value of pkgname with the correct hash value.
        return PkgCert.test(ctx, pkgname, correctHash);
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


4.1.1.4. Creating/Using In-house Activities

In-house activities are the Activities which are prohibited to be used by applications other than other in-house applications. They are used in applications developed internally that want to securely share information and functionality.

There is a risk that a third party application can read an Intent that is used to start the Activity. Therefore it is necessary to make sure that if you are putting sensitive information inside an Intent used to start an Activity that you take countermeasures to make sure that it cannot be read by a malicious third party.

Sample code for creating an In-house Activity is shown below.

Points (Creating an Activity):

1. Define an in-house signature permission.
2. Do not specify taskAffinity.
3. Do not specify launchMode.
4. Require the in-house signature permission.
5. Do not define an intent filter and explicitly set the exported attribute to true.
6. Verify that the in-house signature permission is defined by an in-house application.
7. Handle the received intent carefully and securely, even though the intent was sent from an in-house application.
8. Sensitive information can be returned since the requesting application is in-house.
9. When exporting an APK, sign the APK with the same developer key as the destination application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.activity.inhouseactivity" >

    <!-- *** POINT 1 *** Define an in-house signature permission -->
    <permission
        android:name="org.jssec.android.activity.inhouseactivity.MY_PERMISSION"
        android:protectionLevel="signature" />

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- In-house Activity -->
        <!-- *** POINT 2 *** Do not specify taskAffinity -->
        <!-- *** POINT 3 *** Do not specify launchMode -->
        <!-- *** POINT 4 *** Require the in-house signature permission  -->
        <!-- *** POINT 5 *** Do not define the intent filter and explicitly set the exported attribute to
 true -->
        <activity
            android:name="org.jssec.android.activity.inhouseactivity.InhouseActivity"
            android:exported="true"
            android:permission="org.jssec.android.activity.inhouseactivity.MY_PERMISSION" />
```

```
    </application>
</manifest>
```

InhouseActivity.java

```
package org.jssec.android.activity.inhouseactivity;

import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class InhouseActivity extends Activity {

    // In-house Signature Permission
    private static final String MY_PERMISSION = "org.jssec.android.activity.inhouseactivity.MY_PERMISSI
ON";

    // In-house certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of "my company key" in the keystore.
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);

        // *** POINT 6 *** Verify that the in-house signature permission is defined by an in-house applic
ation.
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            Toast.makeText(this, "The in-house signature permission is not declared by in-house applicat
ion.",
                    Toast.LENGTH_LONG).show();
            finish();
            return;
        }

        // *** POINT 7 *** Handle the received intent carefully and securely, even though the intent was
sent from an in-house application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String param = getIntent().getStringExtra("PARAM");
        Toast.makeText(this, String.format("Received param: ¥"%s¥"", param), Toast.LENGTH_LONG).show();
```



```
    }

    public void onReturnResultClick(View view) {

        // *** POINT 8 *** Sensitive information can be returned since the requesting application is in-
house.
        Intent intent = new Intent();
        intent.putExtra("RESULT", "Sensitive Info");
        setResult(RESULT_OK, intent);
        finish();
    }
}
```

SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;

            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
```

```
import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


*** Point9 *** When exporting an APK, sign the APK with the same developer key as the destination application.

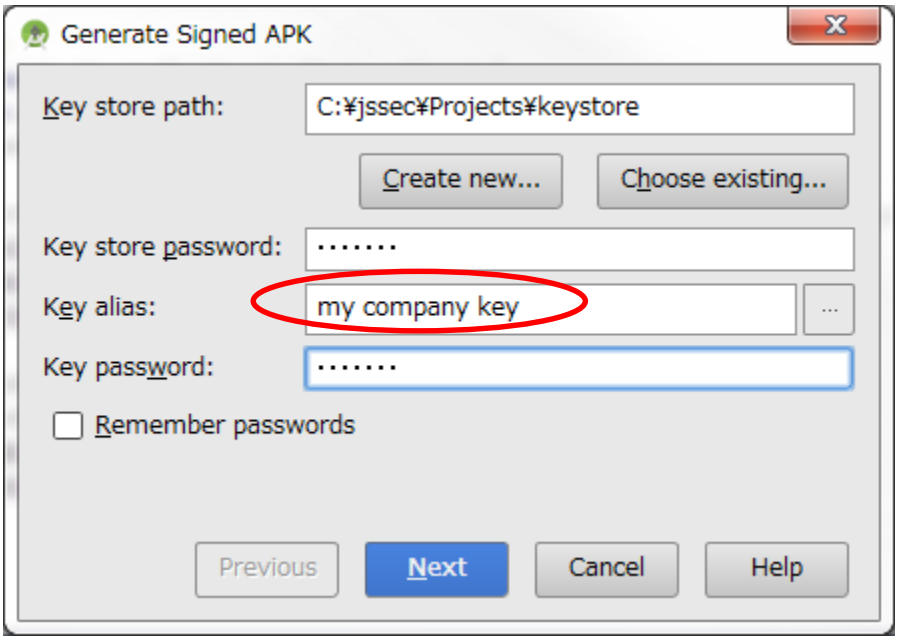


Figure 4.1-2

Sample code for using an In-house Activity is described below.

Points (Using an activity):

10. Declare that you want to use the in-house signature permission.
11. Verify that the in-house signature permission is defined by an in-house application.
12. Verify that the destination application is signed with the in-house certificate.
13. Sensitive information can be sent only by putExtra() since the destination application is in-house.
14. Use explicit intents to call an In-house Activity.
15. Handle the received data carefully and securely, even though the data came from an in-house application.
16. When exporting an APK, sign the APK with the same developer key as the destination application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.activity.inhouseuser" >

    <!-- *** POINT 10 *** Declare to use the in-house signature permission -->
    <uses-permission
        android:name="org.jssec.android.activity.inhouseactivity.MY_PERMISSION" />

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <activity
            android:name="org.jssec.android.activity.inhouseuser.InhouseUserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

InhouseUserActivity.java

```
package org.jssec.android.activity.inhouseuser;

import org.jssec.android.shared.PkgCert;
import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.ActivityNotFoundException;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;
```



```
public class InhouseUserActivity extends Activity {

    // Target Activity information
    private static final String TARGET_PACKAGE =  "org.jssec.android.activity.inhouseactivity";
    private static final String TARGET_ACTIVITY = "org.jssec.android.activity.inhouseactivity.InhouseAc
tivity";

    // In-house Signature Permission
    private static final String MY_PERMISSION = "org.jssec.android.activity.inhouseactivity.MY_PERMISSI
ON";

    // In-house certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of "my company key" in the keystore.
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    private static final int REQUEST_CODE = 1;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }

    public void onUseActivityClick(View view) {

        // *** POINT 11 *** Verify that the in-house signature permission is defined by an in-house appli
cation.
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            Toast.makeText(this, "The in-house signature permission is not declared by in-house applicat
ion.",
                    Toast.LENGTH_LONG).show();
            return;
        }

        // ** POINT 12 *** Verify that the destination application is signed with the in-house certifica
te.
        if (!PkgCert.test(this, TARGET_PACKAGE, myCertHash(this))) {
            Toast.makeText(this, "Target application is not an in-house application.", Toast.LENGTH_LONG
).show();
            return;
        }

        try {
            Intent intent = new Intent();

            // *** POINT 13 *** Sensitive information can be sent only by putExtra() since the destinatio
n application is in-house.
            intent.putExtra("PARAM", "Sensitive Info");
```

```
            // *** POINT 14 *** Use explicit intents to call an In-house Activity.
            intent.setClassName(TARGET_PACKAGE, TARGET_ACTIVITY);
            startActivityForResult(intent, REQUEST_CODE);
        }
        catch (ActivityNotFoundException e) {
            Toast.makeText(this, "Target activity not found.", Toast.LENGTH_LONG).show();
        }
    }

    @Override
    public void onActivityResult(int requestCode, int resultCode, Intent data) {
        super.onActivityResult(requestCode, resultCode, data);

        if (resultCode != RESULT_OK) return;

        switch (requestCode) {
        case REQUEST_CODE:
            String result = data.getStringExtra("RESULT");

            // *** POINT 15 *** Handle the received data carefully and securely,
            // even though the data came from an in-house application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            Toast.makeText(this, String.format("Received result: ¥"%s¥"", result), Toast.LENGTH_LONG).sh
ow();
            break;
        }
    }
}
```

SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;
```



```
            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
```

```
        }
        return hexadecimal.toString();
    }
}
```


*** Point 16 *** When exporting an APK, sign the APK with the same developer key as the destination application.

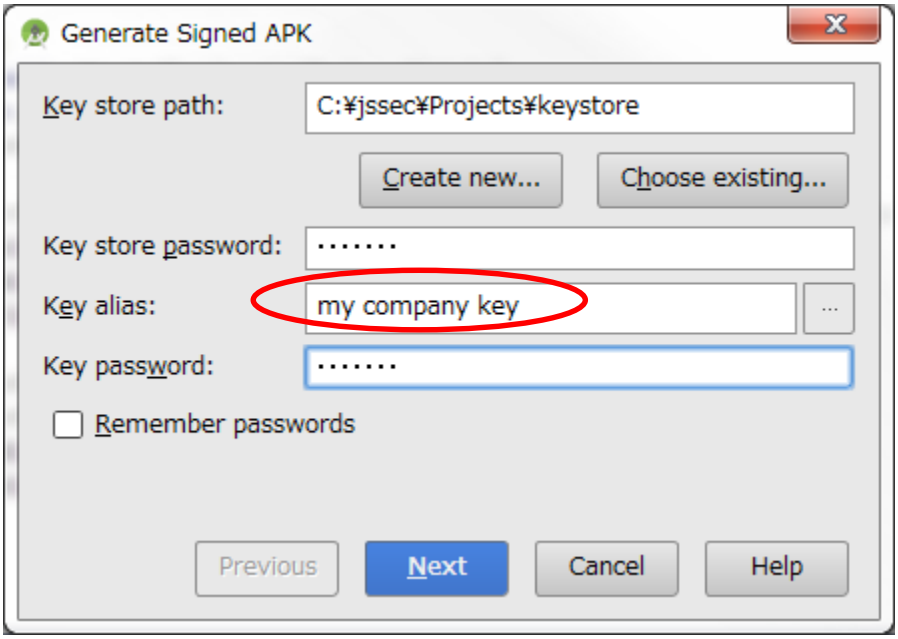


Figure 4.1-3

4.1.2. Rule Book

Be sure to follow the rules below when creating or sending an Intent to an activity.

1.	Activities that are Used Only Internally to the Application Must be Set Private	(Required)
2.	Do Not Specify taskAffinity	(Required)
3.	Do Not Specify launchMode	(Required)
4.	Do Not Set the FLAG_ACTIVITY_NEW_TASK Flag for Intents that Start an Activity	(Required)
5.	Handling the Received Intent Carefully and Securely	(Required)
6.	Use an In-house Defined Signature Permission after Verifying that it is Defined by an In-House Application	(Required)
7.	When Returning a Result, Pay Attention to the Possibility of Information Leakage of that Result from the Destination Application	(Required)
8.	Use the explicit Intents if the destination Activity is predetermined.	(Required)
9.	Handle the Returned Data from a Requested Activity Carefully and Securely	(Required)
10.	Verify the Destination Activity if Linking with Another Company's Application	(Required)
11.	When Providing an Asset Secondhand, the Asset should be Protected with the Same Level of Protection	(Required)
12.	Sending Sensitive Information Should Be Limited as much as possible	(Recommended)

4.1.2.1. Activities that are Used Only Internally to the Application Must be Set Private (Required)

Activities which are only used in a single application are not required to be able to receive any Intents from other applications. Developers often assume that Activities intended to be private will not be attacked but it is necessary to explicitly make these Activities private in order to stop malicious Intents from being received.

AndroidManifest.xml

```
<!-- Private activity -->
<!-- *** POINT 3 *** Explicitly set the exported attribute to false. -->
<activity
    android:name=".PrivateActivity"
    android:label="@string/app_name"
    android:exported="false" />
```

Intent filters should not be set on activities that are only used in a single application. Due to the characteristics of Intent filters, Due to the characteristics of how Intent filters work, even if you intend to send an Intent to a Private Activity internally, if you send the Intent through an Intent filter than you may unintentionally start another Activity. Please see Advanced Topics "4.1.3.1Combining Exported Attributes and Intent Filter Settings (For Activities)" for more details.

AndroidManifest.xml(Not recommended)

```
<!-- Private activity -->
<!-- *** POINT 3 *** Explicitly set the exported attribute to false. -->
<activity
```



```
            android:name=".PictureActivity"
            android:label="@string/picture_name"
            android:exported="false" >
            <intent-filter>
                <action android:name="org.jssec.android.activity.OPEN />
            </intent-filter>
        </activity>
```

4.1.2.2. Do Not Specify taskAffinity (Required)

In Android OS, Activities are managed by tasks. Task names are determined by the affinity that the root Activity has. On the other hand, for Activities other than root Activities, the task to which the Activity belongs is not determined by the Affinity only, but also depends on the Activity's launch mode. Please refer to "4.1.3.4 Root Activity" for more details.

In the default setting, each Activity uses its package name as its affinity. As a result, tasks are allocated according to application, so all Activities in a single application will belong to the same task. To change the task allocation, you can make an explicit declaration for the affinity in the AndroidManifest.xml file or you can set a flag in an Intent sent to an Activity. However, if you change task allocations, there is a risk that another application could read the Intents sent to Activities belonging to another task.

Be sure not to specify android:taskAffinity in the AndroidManifest.xml file and use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

Below is an example AndroidManifest.xml file for creating and using Private Activities.

AndroidManifest.xml

```
    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- Private activity -->
        <!-- *** POINT 1 *** Do not specify taskAffinity -->
        <activity
            android:name=".PrivateActivity"
            android:label="@string/app_name"
            android:exported="false" />
    </application>
```

Please refer to the "Google Android Programming guide"[2], the Google Developer's API Guide "Tasks and Back Stack"[3], "4.1.3.3 Reading Intents Sent to an Activity" and "4.1.3.4 Root Activity" for more

[2] Author Egawa, Fujii, Asano, Fujita, Yamada, Yamaoka, Sano, Takebata, "Google Android Programming Guide", ASCII Media Works, July 2009

[3] http://developer.android.com/guide/components/tasks-and-back-stack.html

details about tasks and affinities.

4.1.2.3. Do Not Specify launchMode (Required)

The Activity launch mode is used to control the settings for creating new tasks and Activity instances when starting an Activity. By default it is set to "standard". In the "standard" setting, new instances are always created when starting an Activity, tasks follow the tasks belonging to the calling Activity, and it is not possible to create a new task. When a new task is created, it is possible for other applications to read the contents of the calling Intent so it is required to use the "standard" Activity launch mode setting when sensitive information is included in an Intent.

The Activity launch mode can be explicitly set in the android:launchMode attribute in the AndroidManifest.xml file, but because of the reason explained above, this should not be set in the Activity declaration and the value should be kept as the default "standard".

AndroidManifest.xml

```
<application
    android:icon="@drawable/ic_launcher"
    android:label="@string/app_name" >

    <!-- Private activity -->
    <!-- *** POINT 2 *** Do not specify launchMode -->
    <activity
        android:name=".PrivateActivity"
        android:label="@string/app_name"
        android:exported="false" />
</application>
```

Please refer to "4.1.3.3 Reading Intents Sent to an Activity" and "4.1.3.4 Root Activity."

4.1.2.4. Do Not Set the FLAG_ACTIVITY_NEW_TASK Flag for Intents that Start an Activity(Required)

The launch mode of an Activity can be changed when executing startActivity() or startActivityForResult() and in some cases a new task may be generated. Therefore it is necessary to not change the launch mode of Activity during execution.

To change the Activity launch mode, set the Intent flags by using setFlags() or addFlags() and use that Intent as an argument to startActivity() or startActivityForResult(). FLAG_ACTIVITY_NEW_TASK is the flag used to create a new task. When the FLAG_ACTIVITY_NEW_TASK is set, a new task will be created if the called Activity does not exist in the background or foreground.
The FLAG_ACTIVITY_MULTIPLE_TASK flag can be set simultaneously with FLAG_ACTIVITY_NEW_TASK. In this case, a new task will always be created. New tasks may be created with either setting so these should not be set with Intents that handle sensitive information.

Example of sending an intent

```
// *** POINT 6 *** Do not set the FLAG_ACTIVITY_NEW_TASK flag for the intent to start an activity.
  Intent intent = new Intent(this, PrivateActivity.class);
  intent.putExtra("PARAM", "Sensitive Info");
```



```
startActivityForResult(intent, REQUEST_CODE);
```

In addition, you may think that there is a way to prevent the contents of an Intent from being read even if a new task was created by explicitly setting the FLAG_ACTIVITY_EXCLUDE_FROM_RECENTS flag. However, even by using this method, the contents can be read by a third party so you should avoid any usage of FLAG_ACTIVITY_NEW_TASK.

Please refer to "4.1.3.1Combining Exported Attributes and Intent Filter Settings (For Activities)" "4.1.3.3 Reading Intents Sent to an Activity" and "4.1.3.4 Root Activity."

4.1.2.5. Handling the Received Intent Carefully and Securely (Required)

Risks differ depending on the types of Activity, but when processing a received Intent data, the first thing you should do is input validation.

Since Public Activities can receive Intents from untrusted sources, they can be attacked by malware. On the other hand, Private Activities will never receive any Intents from other applications directly, but it is possible that a Public Activity in the targeted application may forward a malicious Intent to a Private Activity so you should not assume that Private Activities cannot receive any malicious input. Since Partner Activities and In-house Activities also have the risk of a malicious intent being forwarded to them as well, it is necessary to perform input validation on these Intents as well.

Please refer to "3.2 Handling Input Data Carefully and Securely"

4.1.2.6. Use an In-house Defined Signature Permission after Verifying that it is Defined by an In-House Application (Required)

Make sure to protect your in-house Activities by defining an in-house signature permission when creating the Activity. Since defining a permission in the AndroidManifest.xml file or declaring a permission request does not provide adequate security, please be sure to refer to "5.2.1.2 How to Communicate Between In-house Applications with In-house-defined Signature Permission."

4.1.2.7. When Returning a Result, Pay Attention to the Possibility of Information Leakage of that Result from the Destination Application (Required)

When you use setResult() to return data, the reliability of the destination application will depend on the Activity type. When Public Activities are used to return data, the destination may turn out to be malware in which case that information could be used in a malicious way. For Private and In-house Activities, there is not much need to worry about data being returned to be used maliciously because they are being returned to an application you control. Partner Activities are somewhat in the middle.

As above, when returning data from Activities, you need to pay attention to information leakage from

the destination application.

Example of returning data.

```
      public void onReturnResultClick(View view) {

                // *** POINT 6 *** Information that is granted to be disclosed to a partner application ca
n be returned.
                Intent intent = new Intent();
                intent.putExtra("RESULT", "Sensitive Info");
                setResult(RESULT_OK, intent);
                finish();
      }
```

4.1.2.8. Use the explicit Intents if the destination Activity is predetermined. (Required)

When using an Activity by implicit Intents, the Activity in which the Intent gets sent to is determined by the Android OS. If the Intent is mistakenly sent to malware then Information leakage can occur. On the other hand, when using an Activity by explicit Intents, only the intended Activity will receive the Intent so this is much safer.

Unless it is absolutely necessary for the user to determine which application's Activity the intent should be sent to, you should use explicit intents and specify the destination in advance.

Using an Activity in the same application by an explicit Intent

```
        Intent intent = new Intent(this, PictureActivity.class);
        intent.putExtra("BARCODE", barcode);
        startActivity(intent);
```

Using other applicaion's Public Activity by an explicit Intent

```
        Intent intent = new Intent();
        intent.setClassName(
            "org.jssec.android.activity.publicactivity",
            "org.jssec.android.activity.publicactivity.PublicActivity");
        startActivity(intent);
```

However, even when using another application's Public Activity by explicit Intents, it is possible that the destination Activity could be malware. This is because even if you limit the destination by package name, it is still possible that a malicious application can fake the same package name as the real application. To eliminate this type of risk, it is necessary to consider using a Partner or In-house.

Please refer to "4.1.3.1Combining Exported Attributes and Intent Filter Settings (For Activities)"

4.1.2.9. Handle the Returned Data from a Requested Activity Carefully and Securely (Required)

While the risks differ slightly according to what type of Activity you accessing, when processing Intent data received as a returned value, you always need to perform input validation on the received data.

Public Activities have to accept returned Intents from untrusted sources so when accessing a Public Activity it is possible that, the returned Intents are actually sent by malware. It is often mistakenly thought that all returned Intents from a Private Activity are safe because they are originating from the same application. However, since it is possible that an intent received from an untrusted source is indirectly forwarded, you should not blindly trust the contents of that Intent. Partner and In-house Activities have a risk somewhat in the middle of Private and Public Activities. Be sure to input validate these Activities as well.

Please refer to "3.2 Handling Input Data Carefully and Securely" for more information.

4.1.2.10. Verify the Destination Activity if Linking with Another Company's Application (Required)

Be sure to sure a whitelist when linking with another company's application. You can do this by saving a copy of the company's certificate hash inside your application and checking it with the certificate hash of the destination application. This will prevent a malicious application from being able to spoof Intents. Please refer to sample code section "4.1.1.3 Creating/Using Partner Activities" for the concrete implementation method. For technical details, please refer to "4.1.3.2 Validating the Requesting Application."

4.1.2.11. When Providing an Asset Secondhand, the Asset should be Protected with the Same Level of Protection (Required)

When an information or function asset, which is protected by a permission, is provided to another application secondhand, you need to make sure that it has the same required permissions needed to access the asset. In the Android OS permission security model, only an application that has been granted proper permissions can directly access a protected asset. However, there is a loophole because an application with permissions to an asset can act as a proxy and allow access to an unprivileged application. Substantially this is the same as re-delegating a permission so it is referred to as the "Permission Re-delegation" problem. Please refer to "5.2.3.4 Permission Re-delegation Problem."

4.1.2.12. Sending Sensitive Information Should Be Limited as much as possible (Recommended)

You should not send sensitive information to untrusted parties. Even when you are linking with a specific application, there is still a chance that you unintentionally send an Intent to a different application or that a malicious third party can steal your Intents. Please refer to "4.1.3.5 Log Output When using Activities."

You need to consider the risk of information leakage when sending sensitive information to an Activity. You must assume that all data in Intents sent to a Public Activity can be obtained by a malicious third party. In addition, there is a variety of risks of information leakage when sending Intents to Partner or In-house Activities as well depending on the implementation. Even when sending data to Private Activities, there is a risk that the data in the Intent could be leaked through LogCat. Information in the extras part of the Intent is not output to LogCat so it is best to store sensitive information there.

However, not sending sensitive data in the first place is the only perfect solution to prevent information leakage therefore you should limit the amount of sensitive information being sent as much as possible. When it is necessary to send sensitive information, the best practice is to only send to a trusted Activity and to make sure the information cannot be leaked through LogCat.

In addition, sensitive information should never be sent to the root Activity. Root Activities are Activities that are called first when a task is created. For example, the Activity which is launched from launcher is always the root Activity.

Please refer to "4.1.3.3 Reading Intents Sent to an Activity" and "4.1.3.4 Root Activity" for more details on root Activities.

4.1.3. Advanced Topics

4.1.3.1. Combining Exported Attributes and Intent Filter Settings (For Activities)

We have explained how to implement the four types of Activities in this guidebook: Private Activities, Public Activities, Partner Activities, and In-house Activities. The various combinations of permitted settings for each type of exported attribute defined in the AndroidManifest.xml file and the intent-filter elements are defined in the table below. Please verify the compatibility of the exported attribute and intent-filter element with the Activity you are trying to create.

Table 4.1-2

	Value of exported attribute		
	True	False	Not specified
Intent Filter defined	Public	(Do not Use)	(Do not Use)
Intent Filter Not Defined	Public, Partner, In- house	Private	(Do not Use)

When the exported attribute of an Activity is left unspecified, the question of whether or not the Activity is public is determined by the presence or absence of intent filters for that Activity. [4] However, in this guidebook it is forbidden to set the exported attribute to unspecified. In general, as mentioned previously, it is best to avoid implementations that rely on the default behavior of any given API; moreover, in cases where explicit methods — such as the exported attribute — exist for enabling important security-related settings, it is always a good idea to make use of those methods.

The reason why an undefined intent filter and an exported attribute of false should not be used is that there is a loophole in Android's behavior, and because of how Intent filters work, other application's Activities can be called unexpectedly. The following two figures below show this explanation. Figure 4.1-4 is an example of normal behavior in which a Private Activity (Application A) can be called by an implicit Intent only from the same application. The Intent filter (action = "X") is defined to work only inside Application A, so this is the expected behavior.

[4] If any intent filters are defined, the Activity is public; otherwise it is private. For more information, see https://developer.android.com/guide/topics/manifest/activity-element.html#exported.

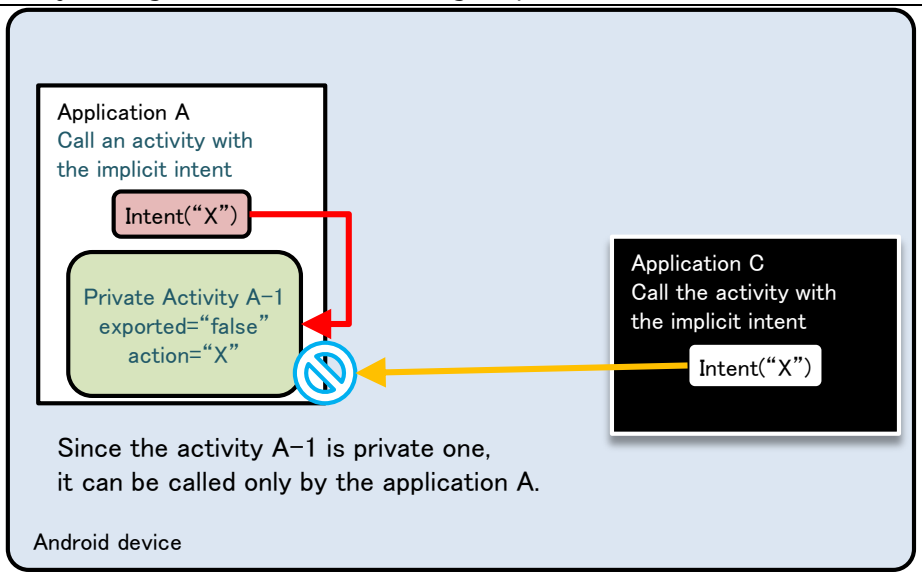


Figure 4.1-4

Figure 4.1-5 below shows a scenario in which the same Intent filter (action="X") is defined in Application B as well as Application A. Application A is trying to call a Private Activity in the same application by sending an implicit Intent, but this time a dialogue box asking the user which application to select is displayed, and the Public Activity B-1 in Application B called by mistake due to the user selection. Due to this loophole, it is possible that sensitive information can be sent to other applications or application may receive an unexpected retuned value.

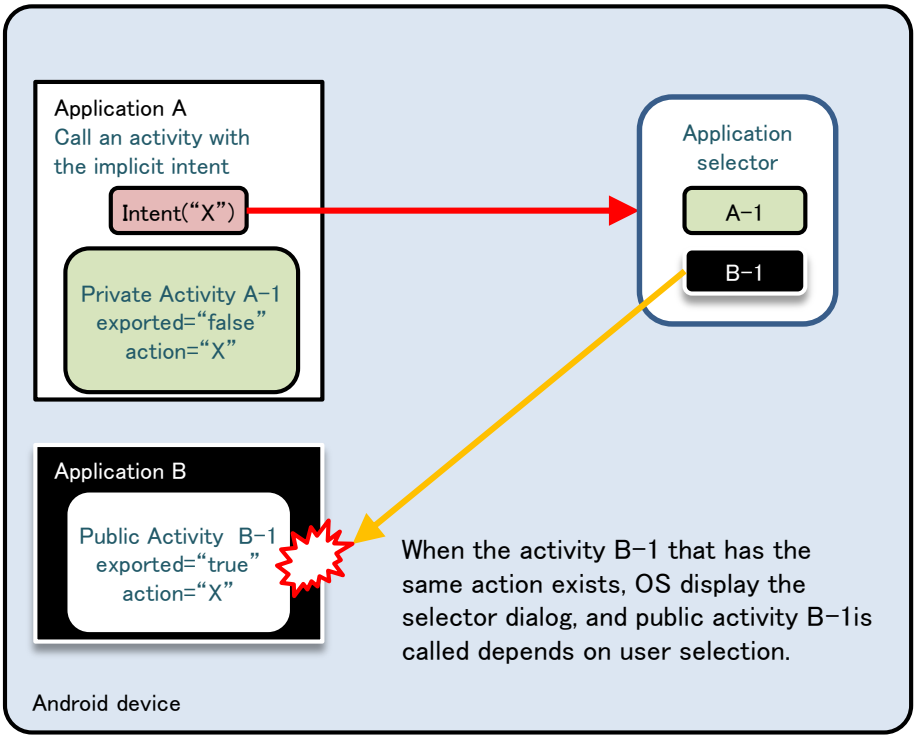


Figure 4.1-5

As shown above, using Intent filters to send implicit Intents to Private Activities may result in unexpected behavior so it is best to avoid this setting. In addition, we have verified that this behavior

does not depend on the installation order of Application A and Application B.

4.1.3.2. Validating the Requesting Application

Here we explain the technical information about how to implement a Partner Activity. Partner applications permit that only particular applications which are registered in a whitelist are allowed access and all other applications are denied. Because applications other than in-house applications also need access permission, we cannot use signature permissions for access control.

Simply speaking, we want to validate the application trying to use the Partner Activity by checking if it is registered in a predefined whitelist and allow access if it is and deny access if it is not. Application validation is done by obtaining the certificate from the application requesting access and comparing its hash with the one in the whitelist.

Some developers may think that it is sufficient to just compare the package name without obtaining the certificate, however, it is easy to spoof the package name of a legitimate application so this is not a good method to check for authenticity. Arbitrarily assignable values should not be used for authentication. On the other hand, because only the application developer has the developer key for signing its certificate, this is a better method for identification. Since the certificate cannot be easily spoofed, unless a malicious third party can steal the developer key, there is a very small chance that malicious application will be trusted. While it is possible to store the entire certificate in the whitelist, it is sufficient to only store the SHA-256 hash value in order to minimize the file size.

There are two restrictions for using this method.

- The requesting application has to use startActivityForResult() instead of startActivity().
- The requesting application can only call from an Activity.

The second restriction is the restriction imposed as a result of the first restriction, so technically there is only a single restriction.
This restriction occurs due to the restriction of Activity.getCallingPackage() which gets the package name of the calling application. Activity.getCallingPackage() returns the package name of source (requesting) application only in case it is called by startActivityForResult(), but unfortunately, when it is called by startActivity(), it only returns null. Because of this, when using the method explained here, the source (requesting) application needs to use startActivityForResult() even if it does not need to obtain a return value. In addition, startActivityForResult() can be used only in Activity classes, so the source (requester) is limited to Activities.

PartnerActivity.java

```
package org.jssec.android.activity.partneractivity;

import org.jssec.android.shared.PkgCertWhitelists;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.Context;
import android.content.Intent;
```

```
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PartnerActivity extends Activity {

    // *** POINT 4 *** Verify the requesting application's certificate through a predefined whitelist.
    private static PkgCertWhitelists sWhitelists = null;
    private static void buildWhitelists(Context context) {
        boolean isdebug = Utils.isDebuggable(context);
        sWhitelists = new PkgCertWhitelists();

        // Register certificate hash value of partner application org.jssec.android.activity.partneruser
.
        sWhitelists.add("org.jssec.android.activity.partneruser", isdebug ?
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255" :
                // Certificate hash value of "partner key" in the keystore.
                "1F039BB5 7861C27A 3916C778 8E78CE00 690B3974 3EB8259F E2627B8D 4C0EC35A");

        // Register the other partner applications in the same way.
    }
    private static boolean checkPartner(Context context, String pkgname) {
        if (sWhitelists == null) buildWhitelists(context);
        return sWhitelists.test(context, pkgname);
    }

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);

        // *** POINT 4 *** Verify the requesting application's certificate through a predefined whitelis
t.
        if (!checkPartner(this, getCallingActivity().getPackageName())) {
            Toast.makeText(this,
                    "Requesting application is not a partner application.",
                    Toast.LENGTH_LONG).show();
            finish();
            return;
        }

        // *** POINT 5 *** Handle the received intent carefully and securely, even though the intent was
sent from a partner application.
        // Omitted, since this is a sample. Refer to "3.2 Handling Input Data Carefully and Securely."
        Toast.makeText(this, "Accessed by Partner App", Toast.LENGTH_LONG).show();
    }

    public void onReturnResultClick(View view) {

        // *** POINT 6 *** Only return Information that is granted to be disclosed to a partner applicati
on.
        Intent intent = new Intent();
        intent.putExtra("RESULT", "Information for partner applications");
        setResult(RESULT_OK, intent);
        finish();
    }
}
```


PkgCertWhitelists.java

```
package org.jssec.android.shared;

import java.util.HashMap;
import java.util.Map;

import android.content.Context;

public class PkgCertWhitelists {
    private Map<String, String> mWhitelists = new HashMap<String, String>();

    public boolean add(String pkgname, String sha256) {
        if (pkgname == null) return false;
        if (sha256 == null) return false;

        sha256 = sha256.replaceAll(" ", "");
        if (sha256.length() != 64) return false;    // SHA-256 -> 32 bytes -> 64 chars
        sha256 = sha256.toUpperCase();
        if (sha256.replaceAll("[0-9A-F]+", "").length() != 0) return false; // found non hex char

        mWhitelists.put(pkgname, sha256);
        return true;
    }

    public boolean test(Context ctx, String pkgname) {
        // Get the correct hash value which corresponds to pkgname.
        String correctHash = mWhitelists.get(pkgname);

        // Compare the actual hash value of pkgname with the correct hash value.
        return PkgCert.test(ctx, pkgname, correctHash);
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
```

```
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```

4.1.3.3. Reading Intents Sent to an Activity

In Android 5.0 (API Level 21) and later, the information retrieved with getRecentTasks() has been limited to the caller's own tasks and possibly some other tasks such as home that are known to not be sensitive. However applications, which support the versions under Android 5.0 (API Level 21), should protect against leaking sensitive information.
The following describes the contents of this problem occurring in Android 5.0 and earlier version.

Intents that are sent to the task's root Activity are added to the task history. A root Activity is the first Activity started in a task. It is possible for any application to read the Intents added to the task history by using the ActivityManager class.

Sample code for reading the task history from an application is shown below. To browse the task history, specify the GET_TASKS permission in the AndroidManifest.xml file.

AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.intent.maliciousactivity" >

    <!-- Use GET_TASKS Permission -->
    <uses-permission android:name="android.permission.GET_TASKS" />

    <application
        android:allowBackup="false"
```



```
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
        <activity
            android:name=".MaliciousActivity"
            android:label="@string/title_activity_main"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

MaliciousActivity.java

```
package org.jssec.android.intent.maliciousactivity;

import java.util.List;
import java.util.Set;

import android.app.Activity;
import android.app.ActivityManager;
import android.content.Intent;
import android.os.Bundle;
import android.util.Log;

public class MaliciousActivity extends Activity {

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.malicious_activity);

        // Get am ActivityManager instance.
        ActivityManager activityManager = (ActivityManager) getSystemService(ACTIVITY_SERVICE);
        // Get 100 recent task info.
        List<ActivityManager.RecentTaskInfo> list = activityManager
                .getRecentTasks(100, ActivityManager.RECENT_WITH_EXCLUDED);
        for (ActivityManager.RecentTaskInfo r : list) {
            // Get Intent sent to root Activity and Log it.
            Intent intent = r.baseIntent;
            Log.v("baseIntent", intent.toString());
            Log.v("  action:", intent.getAction());
            Log.v("  data:", intent.getDataString());
            if (r.origActivity != null) {
                Log.v("  pkg:", r.origActivity.getPackageName() + r.origActivity.getClassName());
            }
            Bundle extras = intent.getExtras();
            if (extras != null) {
                Set<String> keys = extras.keySet();
                for(String key : keys) {
                    Log.v("  extras:", key + "=" + extras.get(key).toString());
                }
            }
        }
    }
```

```
}
```

You can obtain specified entries of the task history by using the getRecentTasks() function of the AcitivityManager class. Information about each task is stored in an instance of the ActivityManager.RecentTaskInfo class, but Intents that were sent to the task's root Activity are stored in its member variable baseIntent. Since the root Activity is the Activity which was started when the task was created, please be sure to not fulfill the following two conditions when calling an Activity.

- A new task is created when the Activity is called.
- The called Activity is the task's root Activity which already exists in the background or foreground.

4.1.3.4. Root Activity

The root Activity is the Activity which is the starting point of a task. In other words, this is the Activity which was launched when task was created. For example, when the default Activity is launched by launcher, this Activity will be the root Activity. According to the Android specifications, the contents of Intents sent to the root Activity can be read from arbitrary applications. So, it is necessary to take countermeasures not to send sensitive information to the root Activity. In this guidebook, the following three rules have been made to avoid a called Activity to become root Activity.

- taskAffinity should not be specified.
- launchMode should not be specified.
- The FLAG_ACTIVITY_NEW_TASK flag should not be set in an Intent sent to an Activity.

We consider the situations that an Activity can become the root Activity below. A called Activity becoming a root Activity depends on the following.

- The launch mode of the called Activity
- The task of a called Activity and its launch mode

First of all, let me explain the "Launch mode of called Activity." Launch mode of Activity can be set by writing android:launchMode in AndroidManifest.xml. When it's not written, it's considered as "standard". In addition, launch mode can be also changed by a flag to set to Intent. Flag "FLAG_ACTIVITY_NEW_TASK" launches Activity by "singleTask" mode.

The launch modes that can be specified are as per below. I'll explain about the relation with the root activity, mainly.

standard

Activity which is called by this mode won't be root, and it belongs to the caller side task. Every time it's called, Instance of Activity is to be generated.

singleTop

This launch mode is the same as "standard", except for that the instance is not generated when

launching an Activity which is displayed in most front side of foreground task.

singleTask

This launch mode determines the task to which the activity would be belonging by Affinity value. When task which is matched with Activity's affinity doesn't exist either in background or in foreground, a new task is generated along with Activity's instance. When task exists, neither of them is to be generated. In the former one, the launched Activity's Instance becomes root.

singleInstance

Same as "singleTask", but following point is different. Only root Activity can belongs to the newly generated task. So instance of Activity which was launched by this mode is always root activity. Now, we need to pay attention to the case that the class name of called Activity and the class name of Activity which is included in a task are different although the task which has the same name of called Activity's affinity already exists.

From as above, we can get to know that Activity which was launched by "singleTask" or "singleInstance" has the possibility to become root. In order to secure the application's safety, it should not be launched by these modes.

Next, I'll explain about "Task of the called Activity and its launch mode". Even if Activity is called by "standard" mode, it becomes root Activity in some cases depends on the task state to which Activity belongs.

For example, think about the case that called Activity's task has being run already in background.
The problem here is the case that Activity Instance of the task is launched by “singleInstance". When the affinity of Activity which was called by "standard" is same with the task, new task is to be generated by the restriction of existing "singleInstance" Activity. However, when class name of each Activity is same, task is not generated and existing activity Instance is to be used. In any cases, that called Activity becomes root Activity.

As per above, the conditions that root Activity is called are complicated, for example it depends on the state of execution. So when developing applications, it's better to contrive that Activity is called by "standard".

As an example of that Intent which is sent to Private Activity is read out form other application, the sample code shows the case that caller side Activity of private Activity is launched by "singleInstance" mode. In this sample code, private activity is launched by "standard" mode, but this private Activity becomes root Activity of new task due the "singleInstance" condition of caller side Activity. At this moment, sensitive information that is sent to Private Activity is recorded task history, so it can be read out from other applications. FYI, both caller side Activity and Private Activity have the same affinity.

AndroidManifest.xml(Not recommended)

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
```

```
    package="org.jssec.android.activity.singleinstanceactivity" >

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- Set the launchMode of the root Activity to "singleInstance". -->
        <!-- Do not use taskAffinity -->
        <activity
            android:name="org.jssec.android.activity.singleinstanceactivity.PrivateUserActivity"
            android:label="@string/app_name"
            android:launchMode="singleInstance"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

        <!-- Private activity -->
        <!-- Set the launchMode to "standard." -->
        <!-- Do not use taskAffinity -->
        <activity
            android:name="org.jssec.android.activity.singleinstanceactivity.PrivateActivity"
            android:label="@string/app_name"
            android:exported="false" />
    </application>
</manifest>
```

Private Activity only returns the results to the received Intent.

PrivateActivity.java

```
package org.jssec.android.activity.singleinstanceactivity;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PrivateActivity extends Activity {

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.private_activity);

        // Handle intent securely, even though the intent sent from the same application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String param = getIntent().getStringExtra("PARAM");
        Toast.makeText(this, String.format("Received param: ¥"%s¥"", param), Toast.LENGTH_LONG).show();
    }

    public void onReturnResultClick(View view) {
        Intent intent = new Intent();
```



```
        intent.putExtra("RESULT", "Sensitive Info");
        setResult(RESULT_OK, intent);
        finish();
    }
}
```

In caller side of Private Activity, Private Activity is launched by "standard" mode without setting flag to Intent.

PrivateUserActivity.java

```
package org.jssec.android.activity.singleinstanceactivity;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class PrivateUserActivity extends Activity {

    private static final int REQUEST_CODE = 1;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.user_activity);
    }

    public void onUseActivityClick(View view) {

        // Start the Private Activity with "standard" lanchMode.
        Intent intent = new Intent(this, PrivateActivity.class);
        intent.putExtra("PARAM", "Sensitive Info");

        startActivityForResult(intent, REQUEST_CODE);
    }

    @Override
    public void onActivityResult(int requestCode, int resultCode, Intent data) {
        super.onActivityResult(requestCode, resultCode, data);

        if (resultCode != RESULT_OK) return;

        switch (requestCode) {
        case REQUEST_CODE:
            String result = data.getStringExtra("RESULT");

            // Handle received result data carefully and securely,
            // even though the data came from the Activity in the same application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            Toast.makeText(this, String.format("Received result: ¥"%s¥"", result), Toast.LENGTH_LONG).sh
ow();
            break;
        }
    }
}
```

4.1.3.5. Log Output When using Activities

When using an activity, the contents of intent are output to LogCat by ActivityManager. The following contents are to be output to LogCat, so in this case, sensitive information should not be included here.

- Destination Package name
- Destination Class name
- URI which is set by Intent#setData()

For example, when an application sent mails, the mail address is unfortunately outputted to LogCat if the application would specify the mail address to URI. So, better to send by setting Extras.

When sending a mail as below, mail address is shown to the logCat.

MainActivity.java
```
// URI is output to the LogCat.
Uri uri = Uri.parse("mailtoest@gmail.com");
Intent intent = new Intent(Intent.ACTION_SENDTO, uri);
startActivity(intent);
```

When using Extras, mail address is no more shown to the logCat.

MainActivity.java
```
// Contents which was set to Extra, is not output to the LogCat.
Uri uri = Uri.parse("mailto:");
Intent intent = new Intent(Intent.ACTION_SENDTO, uri);
intent.putExtra(Intent.EXTRA_EMAIL, new String[] {"test@gmail.com"});
startActivity(intent);
```

However, there are cases where other applications can read the Extras data of intent using ActivityManager#getRecentTasks(). Please refer to "4.1.2.2 Do Not Specify taskAffinity (Required)", "4.1.2.3 Do Not Specify launchMode (Required)" and "4.1.2.4 Do Not Set the FLAG_ACTIVITY_NEW_TASK Flag for Intents that Start an Activity (Required)".

4.1.3.6. Protecting against Fragment Injection in PreferenceActivity

When a class derived from PreferenceActivity is a public Activity, a problem known as *Fragment Injection* [5] may arise. To prevent this problem from arising, it is necessary to override PreferenceActivity.IsValidFragment() and check the validity of its arguments to ensure that the Activity does not handle any Fragments without intention. (For more on the safety of input data, see

[5] For more information on Fragment Injection, consult this URL:
https://securityintelligence.com/new-vulnerability-android-framework-fragment-injection/

Section "3.2 Handling Input Data Carefully and Securely".)

Below we show a sample in which IsValidFragment() has been overridden. Note that, if the source code has been obfuscated, class names and the results of parameter-value comparisons may change. In this case it is necessary to pursue alternative countermeasures.

Example of an overridden isValidFragment() method

```
protected boolean isValidFragment(String fragmentName) {
    // If the source code is obfuscated, we must pursue alternative strategies
    return PreferenceFragmentA.class.getName().equals(fragmentName)
            || PreferenceFragmentB.class.getName().equals(fragmentName)
            || PreferenceFragmentC.class.getName().equals(fragmentName)
            || PreferenceFragmentD.class.getName().equals(fragmentName);
}
```

Note that if the app's targetSdkVersion is 19 or greater, failure to override PreferenceActivity.isValidFragment() will result in a security exception and the termination of the app whenever a Fragment is inserted [when isValidFragment() is called], so in this case overriding PreferenceActivity.isValidFragment() is mandatory.

4.1.3.7. The Autofill framework

The Autofill framework was added in Android 8.0 (API Level 26). Using this framework allows apps to store information entered by users—such as user names, passwords, addresses, phone numbers, and credit cards—and subsequently to retrieve this information as necessary to allow the app to fill in forms automatically. This is a convenient mechanism that reduces data-entry burdens for users; however, because it allows a given app to pass sensitive information such as passwords and credit cards to other apps, it must be handled with appropriate care.

Overview of the framework

2 components

In what follows, we provide an overview of the two components[6] registered by the Autofill framework.

- Apps eligible for Autofill (user apps):
  - Pass view information (text and attributes) to Autofill service; receive information from Autofill service as needed to auto-fill forms.
  - All apps that have Activities are user apps (when in the foreground).

[6] The **user app** and the **Autofill service** may belong to the same package (the same APK file) or to different packages.

- It is possible for all Views of all user apps to be eligible for Autofill. It is also possible to explicitly specify that any given individual view should be ineligible for Autofill.
- It is also possible to restrict an app's use of Autofill to the Autofill service within the same package.

- Services that provide Autofill (Autofill services):
  - Save View information passed by an app (requires user permission); provide an app with information needed for Autofill in a View (candidate lists).
  - The Views eligible for this information saving are determined by the Autofill service. (Within the Autofill framework, by default information on all Views contained in an Activity are passed to the Autofill service.)
  - It is also possible to construct Autofill services provided by third parties.
  - It is possible for several to be present within a single terminal with only the service selected by the user via Settings enabled (None is also a possible selection.)
  - It also possible for a Service to provide a UI to validate users via password entry or other mechanisms to protect the security of the user information handled.

Procedural flowchart for the Autofill framework

Figure 4.1-6 is a flowchart illustrating the procedural flow of interactions among Autofill-related components during Autofill. When triggered by events such as motion of the focus in a user app's View, information on that View (primarily the parent-child relationships and various attributes of the View) is passed via the Autofill framework to the Autofill service selected within Settings. Based on the data it receives, the Autofill service fetches from a database the information (candidate lists) needed for Autofill, then returns this to the framework. The framework displays a candidate list to the user, and the app carries out the Autofill operation using the data selected by the user.

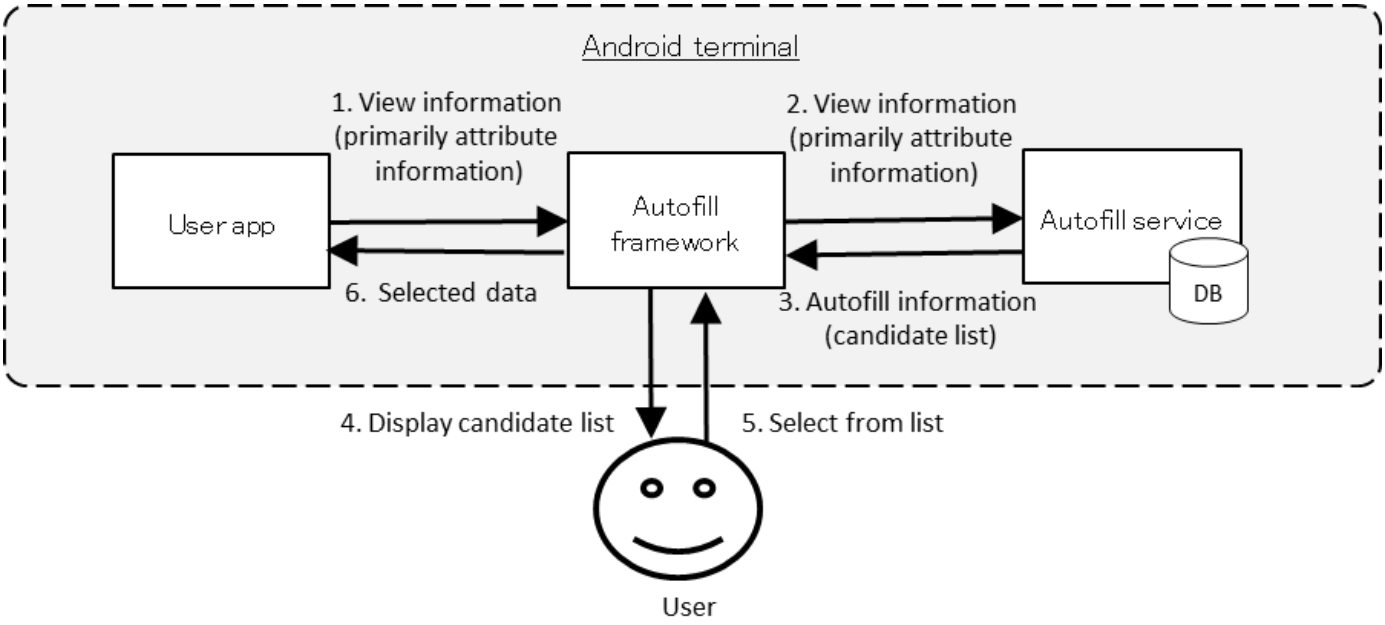


Figure 4.1-6: Procedural flow among components for Autofill

Next, Figure 4.1-7 is a flowchart illustrating the procedural flow for saving user data via Autofill. Upon a triggering event such as when AutofillManager#commit() is called or when an Activity is unfocused, if any Autofilled values for the View have been modified *and* the user has granted permission via the Save Permission dialog box displayed by the Autofill framework, information on the View (including text) is passed via the Autofill framework to the Autofill service selected via Settings, and the Autofill service stores information in the database to complete the procedural sequence.

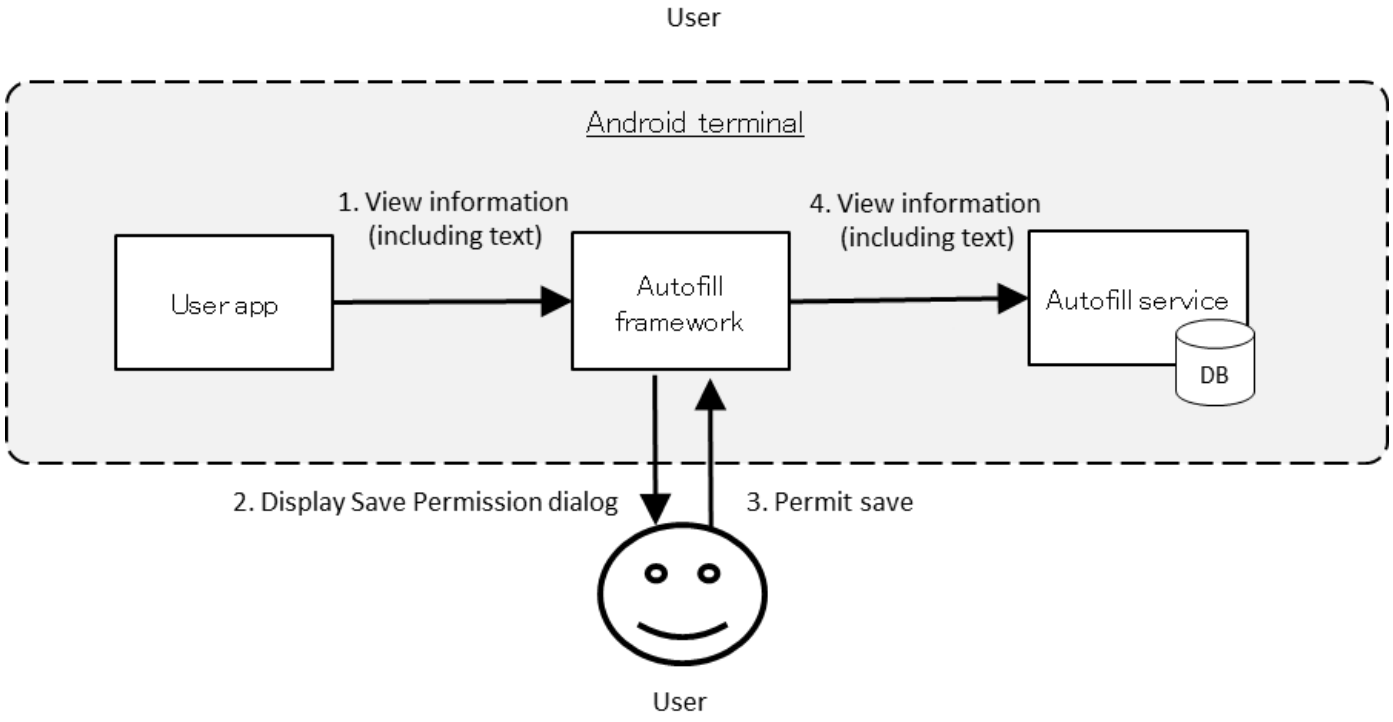


Figure 4.1-7: Procedural flow among components for saving user data

Security concerns for Autofill user apps

As noted in the section "Overview of the framework" above, the security model adopted by the Autofill framework is premised on the assumption that the user configures the Settings to select secure Autofill services and makes appropriate decisions regarding which data to pass to which Autofill service when storing data.

However, if a user unwittingly selects a non-secure Autofill service, there is a possibility that the user may permit the storage of sensitive information that should not be passed to the Autofill service. In what follows we discuss the damage that could result in such a scenario.

When saving information, if the user selects an Autofill service and grants it permission via the Save Permission dialog box, information for all Views contained in the Activity currently displayed by the app in use may be passed to the Autofill service. If the Autofill service is malware, or if other security issues arise—for example, if View information is stored by the Autofill service on an external storage medium or on an insecure cloud service—this could create the risk that information handled by the app might be leaked.

On the other hand, during Autofill, if the user has selected a piece of malware as the Autofill service, values transmitted by the malware may be entered as input. At this point, if the security of the data input is not adequately validated by the app or by the cloud services to which the app sends data, risks of information leakage and/or termination of the app or the service may arise.

Note that, as discussed above in the section *"2 components",* apps with Activities are automatically

eligible for Autofill, and thus all developers of apps with Activities must take the risks described above into account when designing and implementing apps. In what follows we will present countermeasures to mitigate the risks described above we recommend that these be adopted as appropriate based on a consideration of the countermeasures required by an app—referring to "3.1.3 Asset Classification and Protective Countermeasures" and other relevant resources.

Steps to mitigate risk: 1

As discussed above, security within the Autofill framework is ultimately guaranteed only at the user's discretion. For this reason, the range of countermeasures available to apps is somewhat limited. However, there is one way to mitigate the concerns described above: Setting the importantForAutofill attribute for a view to "no" ensures that no View information is passed to the Autofill service (i.e. the View is made ineligible for Autofill), even if the user cannot make appropriate selections or permissions (such as selecting a piece of malware as the Autofill service).[7]

The importantForAutofill attribute may be specified by any of the following methods.

- Set the importantForAutofill attribute in the layout XML
- Call View#setImportantForAutofill()

The values that may be set for this attribute are shown below. Make sure to use values appropriate for the specified range. In particular, note with caution that, when a value is set to "no" for a View, that View will be ineligible for Autofill, but its children *will* remain eligible for Autofill. The default value is "auto."

Value	Name of constant	Eligible for Autofill?	
		Specified View	Child View
"auto"	IMPORTANT_FOR_AUTOFILL_AUTO	Determined by Autofill framework	Determined by Autofill framework
"no"	IMPORTANT_FOR_AUTOFILL_NO	No	Yes
"noExcludeDescendants"	IMPORTANT_FOR_AUTOFILL_NO_EXCLUDE_DESCENDANTS	No	No
"yes"	IMPORTANT_FOR_AUTOFILL_YES	Yes	Yes
"yesExcludeDescendants"	IMPORTANT_FOR_AUTOFILL_YES_EXCLUDE_DESCENDANTS	Yes	No

[7] Even after taking this step, in some cases it may not be possible to avoid the security concerns described above—for example, if the user intentionally uses Autofill. Implementing the steps described in "Steps to mitigate risk: 2" will improve security in these cases.

It is also possible to use AutofillManager#hasEnabledAutofillServices() to restrict the use of Autofill functionality to Autofill services within the same package.

In what follows, we show an example that all Views in an Activity are eligible for Autofill (whether or not a View actually uses Autofill is determined by the Autofill service) only in case that settings have been configured to use a Autofill service within the same package. It is also possible to call View#setImportantForAutofill() for individual Views.

DisableForOtherServiceActivity.java

```
package org.jssec.android.autofillframework.autofillapp;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.view.autofill.AutofillManager;
import android.widget.EditText;
import android.widget.TextView;

import org.jssec.android.autofillframework.R;

public class DisableForOtherServiceActivity extends AppCompatActivity {
    private boolean mIsAutofillEnabled = false;

    private EditText mUsernameEditText;
    private EditText mPasswordEditText;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.disable_for_other_service_activity);

        mUsernameEditText = (EditText)findViewById(R.id.field_username);
        mPasswordEditText = (EditText)findViewById(R.id.field_password);

        findViewById(R.id.button_login).setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                login();
            }
        });
        findViewById(R.id.button_clear).setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                resetFields();
            }
        });
        //Because the floating-toolbar is not supported for this Activity,
        // Autofill may be used by selecting "Automatic Input"
    }

    @Override
    protected void onStart() {
        super.onStart();
    }
```



```
    @Override
    protected void onResume() {
        super.onResume();
        updateAutofillStatus();

        if (!mIsAutofillEnabled) {
            View rootView = this.getWindow().getDecorView();
            //If not using Autofill service within the same package, make all Views ineligible for Autofi
ll
            rootView.setImportantForAutofill(View.IMPORTANT_FOR_AUTOFILL_NO_EXCLUDE_DESCENDANTS);
        } else {
            //If using Autofill service within the same package, make all Views eligible for Autofill
            //View#setImportantForAutofill() may also be called for specific Views
            View rootView = this.getWindow().getDecorView();
            rootView.setImportantForAutofill(View.IMPORTANT_FOR_AUTOFILL_AUTO);
        }
    }
    private void login() {
        String username = mUsernameEditText.getText().toString();
        String password = mPasswordEditText.getText().toString();

        //Validate data obtained from View
        if (!Util.validateUsername(username) || !Util.validatePassword(password)) {
            //appropriate error handling
        }

        //Send username, password to server

        finish();
    }

    private void resetFields() {
        mUsernameEditText.setText("");
        mPasswordEditText.setText("");
    }

    private void updateAutofillStatus() {
        AutofillManager mgr = getSystemService(AutofillManager.class);

        mIsAutofillEnabled = mgr.hasEnabledAutofillServices();

        TextView statusView = (TextView) findViewById(R.id.label_autofill_status);
        String status = "Our autofill service is --.";
        if (mIsAutofillEnabled) {
            status = "autofill service within same package is enabled";
        } else {
            status = "autofill service within same package is disabled";
        }
        statusView.setText(status);
    }
}
```

Steps to mitigate risk: 2

Even in cases where an app has implemented the steps described in the previous section (“Steps to mitigate risk: 1”), the user can forcibly enable the use of Autofill by long-pressing the View, displaying the floating toolbar or a similar control interface, and selecting “Automatic input.” In this

case, information for all Views—including Views for which the importantForAutofill attribute has been set to "no," or for which similar steps have been taken—will be passed to the Autofill service.

It is possible to avoid the risk of information leakage even in circumstances such as these by deleting the "Automatic Input" option from the floating-toolbar menu and other control interfaces; this step is to be carried out in addition to the procedures described in "Steps to mitigate risk: 1"

Sample code for this purpose is shown below.

DisableAutofillActivity.java

```
package org.jssec.android.autofillframework.autofillapp;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.ActionMode;
import android.view.Menu;
import android.view.MenuItem;
import android.view.SubMenu;
import android.view.View;
import android.widget.EditText;

import org.jssec.android.autofillframework.R;

public class DisableAutofillActivity extends AppCompatActivity {

    private EditText mUsernameEditText;
    private EditText mPasswordEditText;

    private ActionMode.Callback mActionModeCallback;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.disable_autofill_activity);

        mUsernameEditText = (EditText) findViewById(R.id.field_username);
        mPasswordEditText = (EditText) findViewById(R.id.field_password);

        findViewById(R.id.button_login).setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                login();
            }
        });
        findViewById(R.id.button_clear).setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                resetFields();
            }
        });
        mActionModeCallback = new ActionMode.Callback() {
            @Override
            public boolean onCreateActionMode(ActionMode mode, Menu menu) {
                removeAutofillFromMenu(menu);
                return true;
            }
```



```
        @Override
        public boolean onPrepareActionMode(ActionMode mode, Menu menu) {
            removeAutofillFromMenu(menu);
            return true;
        }

        @Override
        public boolean onActionItemClicked(ActionMode mode, MenuItem item) {
            return false;
        }

        @Override
        public void onDestroyActionMode(ActionMode mode) {
        }
    };

    //Delete "Automatic Input" from floating-toolbar
    setMenu();
}

void setMenu() {
    if (mActionModeCallback == null) {
        return;
    }
     //Register callback for all editable TextViews contained in Activity
     mUsernameEditText.setCustomInsertionActionModeCallback(mActionModeCallback);
     mPasswordEditText.setCustomInsertionActionModeCallback(mActionModeCallback);
}

//Traverse all menu levels, deleting "Automatic Input" from each
void removeAutofillFromMenu(Menu menu) {
    if (menu.findItem(android.R.id.autofill) != null) {
        menu.removeItem(android.R.id.autofill);
    }

    for (int i=0; i<menu.size(); i++) {
        SubMenu submenu = menu.getItem(i).getSubMenu();
        if (submenu != null) {
            removeAutofillFromMenu(submenu);
        }
    }
}

private void login() {
    String username = mUsernameEditText.getText().toString();
    String password = mPasswordEditText.getText().toString();

    //Validate data obtained from View
    if (!Util.validateUsername(username) || Util.validatePassword(password)) {
        //appropriate error handling
    }

    //Send username, password to server

    finish();
}

private void resetFields() {
    mUsernameEditText.setText("");
```

```
        mPasswordEditText.setText("");
    }

}
```


4.2.1. Sample Code

Creating Broadcast Receiver is required to receive Broadcast. Risks and countermeasures of using Broadcast Receiver differ depending on the type of the received Broadcast.
You can find your Broadcast Receiver in the following judgment flow. The receiving applications cannot check the package names of Broadcast-sending applications that are necessary for linking with the partners. As a result, Broadcast Receiver for the partners cannot be created.

Table 4.2-1 Definition of broadcast receiver types

Type	Definition
Private broadcast receiver	A broadcast receiver that can receive broadcasts only from the same application, therefore is the safest broadcast receiver
Public broadcast receiver	A broadcast receiver that can receive broadcasts from an unspecified large number of applications If the app's targetSDKVersion is 26 or above, then, on terminals running Android 8.0 (API level 26) or later, Broadcast Receivers may not be registered for implicit Broadcast Intents[8]
In-house broadcast receiver	A broadcast receiver that can receive broadcasts only from other In-house applications

[8] As exceptions to this rule, some implicit Broadcast Intents sent by the system may use Broadcast Receivers. For more information, consult the following URL.
https://developer.android.com/guide/components/broadcast-exceptions.html

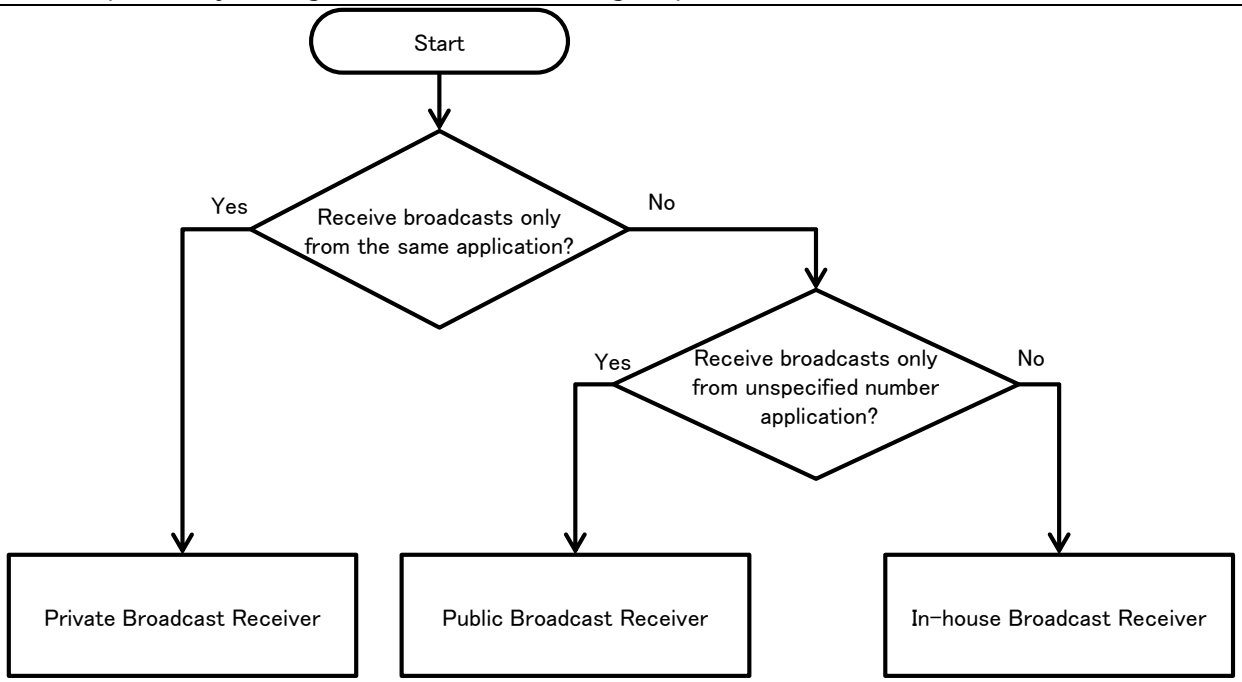


Figure 4.2-1

In addition, Broadcast Receiver can be divided into 2 types based on the definition methods, Static Broadcast Receiver and Dynamic Broadcast Receiver. The differences between them can be found in the following figure. In the sample code, an implementation method for each type is shown. The implementation method for sending applications is also described because the countermeasure for sending information is determined depending on the receivers.

Table 4.2-2

	Definition method	Characteristic
Static Broadcast Receiver	Define by writing <receiver> elements in AndroidManifest.xml	● There is a restriction that some Broadcasts (e.g. ACTION_BATTERY_CHANGED) sent by system cannot be received. ● Broadcast can be received from application's initial boot till uninstallation.
Dynamic Broadcast Receiver	By calling registerReceiver() and unregisterReceiver() in a program, register/unregister Broadcast Receiver dynamically.	● Broadcasts which cannot be received by static Broadcast Receiver can be received. ● The period of receiving Broadcasts can be controlled by the program. For example, Broadcasts can be received only while Activity is on the front side. ● Private Broadcast Receiver cannot be created.

4.2.1.1. Private Broadcast Receiver - Receiving/Sending Broadcasts

Private Broadcast Receiver is the safest Broadcast Receiver because only Broadcasts sent from within the application can be received. Dynamic Broadcast Receiver cannot be registered as Private, so Private Broadcast Receiver consists of only Static Broadcast Receivers.

Points (Receiving Broadcasts):

1. Explicitly set the exported attribute to false.
2. Handle the received intent carefully and securely, even though the intent was sent from within the same application.
3. Sensitive information can be sent as the returned results since the requests come from within the same application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.broadcast.privatereceiver" >

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >

        <!-- Private Broadcast Receiver -->
        <!-- *** POINT 1 *** Explicitly set the exported attribute to false. -->
        <receiver
            android:name=".PrivateReceiver"
            android:exported="false" />

        <activity
            android:name=".PrivateSenderActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

PrivateReceiver.java

```
package org.jssec.android.broadcast.privatereceiver;

import android.app.Activity;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.widget.Toast;

public class PrivateReceiver extends BroadcastReceiver {

    @Override
    public void onReceive(Context context, Intent intent) {
```

```
        // *** POINT 2 *** Handle the received intent carefully and securely,
        // even though the intent was sent from within the same application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String param = intent.getStringExtra("PARAM");
        Toast.makeText(context,
                String.format("Received param: ¥"%s¥"", param),
                Toast.LENGTH_SHORT).show();

        // *** POINT 3 *** Sensitive information can be sent as the returned results since the requests c
ome from within the same application.
        setResultCode(Activity.RESULT_OK);
        setResultData("Sensitive Info from Receiver");
        abortBroadcast();
    }
}
```


The sample code for sending Broadcasts to private Broadcast Receiver is shown below.

Points (Sending Broadcasts):

4. Use the explicit Intent with class specified to call a receiver within the same application.
5. Sensitive information can be sent since the destination Receiver is within the same application.
6. Handle the received result data carefully and securely, even though the data came from the Receiver within the same application.

PrivateSenderActivity.java

```
package org.jssec.android.broadcast.privatereceiver;

import android.app.Activity;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PrivateSenderActivity extends Activity {

    public void onSendNormalClick(View view) {
        // *** POINT 4 *** Use the explicit Intent with class specified to call a receiver within the sam
e application.
        Intent intent = new Intent(this, PrivateReceiver.class);

        // *** POINT 5 *** Sensitive information can be sent since the destination Receiver is within the
 same application.
        intent.putExtra("PARAM", "Sensitive Info from Sender");
        sendBroadcast(intent);
    }

    public void onSendOrderedClick(View view) {
        // *** POINT 4 *** Use the explicit Intent with class specified to call a receiver within the sam
e application.
        Intent intent = new Intent(this, PrivateReceiver.class);

        // *** POINT 5 *** Sensitive information can be sent since the destination Receiver is within the
 same application.
        intent.putExtra("PARAM", "Sensitive Info from Sender");
        sendOrderedBroadcast(intent, null, mResultReceiver, null, 0, null, null);
    }

    private BroadcastReceiver mResultReceiver = new BroadcastReceiver() {
        @Override
        public void onReceive(Context context, Intent intent) {

            // *** POINT 6 *** Handle the received result data carefully and securely,
            // even though the data came from the Receiver within the same application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            String data = getResultData();
            PrivateSenderActivity.this.logLine(
                    String.format("Received result: ¥"%s¥"", data));
        }
    };
```

```
    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView)findViewById(R.id.logview);
    }

    private void logLine(String line) {
        mLogView.append(line);
        mLogView.append("¥n");
    }
}
```


4.2.1.2. Public Broadcast Receiver – Receiving/Sending Broadcasts

Public Broadcast Receiver is the Broadcast Receiver that can receive Broadcasts from unspecified large number of applications, so it's necessary to pay attention that it may receive Broadcasts from malware.

Points (Receiving Broadcasts):

1. Explicitly set the exported attribute to true.
2. Handle the received Intent carefully and securely.
3. When returning a result, do not include sensitive information.

Public Receiver which is the sample code for public Broadcast Receiver can be used both in static Broadcast Receiver and Dynamic Broadcast Receiver.

PublicReceiver.java

```
package org.jssec.android.broadcast.publicreceiver;

import android.app.Activity;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.widget.Toast;

public class PublicReceiver extends BroadcastReceiver {

    private static final String MY_BROADCAST_PUBLIC =
        "org.jssec.android.broadcast.MY_BROADCAST_PUBLIC";

    public boolean isDynamic = false;
    private String getName() {
        return isDynamic ? "Public Dynamic Broadcast Receiver" : "Public Static Broadcast Receiver";
    }

    @Override
    public void onReceive(Context context, Intent intent) {

        // *** POINT 2 *** Handle the received Intent carefully and securely.
        // Since this is a public broadcast receiver, the requesting application may be malware.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        if (MY_BROADCAST_PUBLIC.equals(intent.getAction())) {
            String param = intent.getStringExtra("PARAM");
            Toast.makeText(context,
                    String.format("%s:¥nReceived param: ¥"%s¥"", getName(), param),
                    Toast.LENGTH_SHORT).show();
        }

        // *** POINT 3 *** When returning a result, do not include sensitive information.
        // Since this is a public broadcast receiver, the requesting application may be malware.
        // If no problem when the information is taken by malware, it can be returned as result.
        setResultCode(Activity.RESULT_OK);
        setResultData(String.format("Not Sensitive Info from %s", getName()));
        abortBroadcast();
    }
}
```

Static Broadcast Receive is defined in AndroidManifest.xml. Note with caution that—depending on the terminal version—reception of implicit Broadcast Intents may be restricted, as in「Table 4.2-1」.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.broadcast.publicreceiver" >

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >

        <!-- Public Static Broadcast Receiver -->
        <!-- *** POINT 1 *** Explicitly set the exported attribute to true. -->
        <receiver
            android:name=".PublicReceiver"
            android:exported="true" >
            <intent-filter>
                <action android:name="org.jssec.android.broadcast.MY_BROADCAST_PUBLIC" />
            </intent-filter>
        </receiver>

        <service
            android:name=".DynamicReceiverService"
            android:exported="false" />

        <activity
            android:name=".PublicReceiverActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

In Dynamic Broadcast Receiver, registration/unregistration is executed by calling registerReceiver() or unregisterReceiver() in the program. In order to execute registration/unregistration by button operations, the button is allocated on PublicReceiverActivity. Since the scope of Dynamic Broadcast Receiver Instance is longer than PublicReceiverActivity, it cannot be kept as the member variable of PublicReceiverActivity. In this case, keep the Dynamic Broadcast Receiver Instance as the member variable of DynamicReceiverService, and then start/end DynamicReceiverService from PublicReceiverActivity to register/unregister Dynamic Broadcast Receiver indirectly.

DynamicReceiverService.java

```
package org.jssec.android.broadcast.publicreceiver;

import android.app.Service;
import android.content.Intent;
import android.content.IntentFilter;
```



```
import android.os.IBinder;
import android.widget.Toast;

public class DynamicReceiverService extends Service {

    private static final String MY_BROADCAST_PUBLIC =
        "org.jssec.android.broadcast.MY_BROADCAST_PUBLIC";

    private PublicReceiver mReceiver;

    @Override
    public IBinder onBind(Intent intent) {
        return null;
    }

    @Override
    public void onCreate() {
        super.onCreate();

        // Register Public Dynamic Broadcast Receiver.
        mReceiver = new PublicReceiver();
        mReceiver.isDynamic = true;
        IntentFilter filter = new IntentFilter();
        filter.addAction(MY_BROADCAST_PUBLIC);
        filter.setPriority(1);  // Prioritize Dynamic Broadcast Receiver, rather than Static Broadcast R
eceiver.
        registerReceiver(mReceiver, filter);
        Toast.makeText(this,
                "Registered Dynamic Broadcast Receiver.",
                Toast.LENGTH_SHORT).show();
    }

    @Override
    public void onDestroy() {
        super.onDestroy();

        // Unregister Public Dynamic Broadcast Receiver.
        unregisterReceiver(mReceiver);
        mReceiver = null;
        Toast.makeText(this,
                "Unregistered Dynamic Broadcast Receiver.",
                Toast.LENGTH_SHORT).show();
    }
}
```

PublicReceiverActivity.java

```
package org.jssec.android.broadcast.publicreceiver;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;

public class PublicReceiverActivity extends Activity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
```

```
        setContentView(R.layout.main);
    }

    public void onRegisterReceiverClick(View view) {
        Intent intent = new Intent(this, DynamicReceiverService.class);
        startService(intent);
    }

    public void onUnregisterReceiverClick(View view) {
        Intent intent = new Intent(this, DynamicReceiverService.class);
        stopService(intent);
    }
}
```


Next, the sample code for sending Broadcasts to public Broadcast Receiver is shown. When sending Broadcasts to public Broadcast Receiver, it's necessary to pay attention that Broadcasts can be received by malware.

Points (Sending Broadcasts):

4. Do not send sensitive information.
5. When receiving a result, handle the result data carefully and securely.

PublicSenderActivity.java

```
package org.jssec.android.broadcast.publicsender;

import android.app.Activity;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PublicSenderActivity extends Activity {

    private static final String MY_BROADCAST_PUBLIC =
        "org.jssec.android.broadcast.MY_BROADCAST_PUBLIC";

    public void onSendNormalClick(View view) {
        // *** POINT 4 *** Do not send sensitive information.
        Intent intent = new Intent(MY_BROADCAST_PUBLIC);
        intent.putExtra("PARAM", "Not Sensitive Info from Sender");
        sendBroadcast(intent);
    }

    public void onSendOrderedClick(View view) {
        // *** POINT 4 *** Do not send sensitive information.
        Intent intent = new Intent(MY_BROADCAST_PUBLIC);
        intent.putExtra("PARAM", "Not Sensitive Info from Sender");
        sendOrderedBroadcast(intent, null, mResultReceiver, null, 0, null, null);
    }

    public void onSendStickyClick(View view) {
        // *** POINT 4 *** Do not send sensitive information.
        Intent intent = new Intent(MY_BROADCAST_PUBLIC);
        intent.putExtra("PARAM", "Not Sensitive Info from Sender");
        //sendStickyBroadcast is deprecated at API Level 21
        sendStickyBroadcast(intent);
    }

    public void onSendStickyOrderedClick(View view) {
        // *** POINT 4 *** Do not send sensitive information.
        Intent intent = new Intent(MY_BROADCAST_PUBLIC);
        intent.putExtra("PARAM", "Not Sensitive Info from Sender");
        //sendStickyOrderedBroadcast is deprecated at API Level 21
        sendStickyOrderedBroadcast(intent, mResultReceiver, null, 0, null, null);
    }

    public void onRemoveStickyClick(View view) {
        Intent intent = new Intent(MY_BROADCAST_PUBLIC);
        //removeStickyBroadcast is deprecated at API Level 21
```

```
        removeStickyBroadcast(intent);
    }

    private BroadcastReceiver mResultReceiver = new BroadcastReceiver() {
        @Override
        public void onReceive(Context context, Intent intent) {

            // *** POINT 5 *** When receiving a result, handle the result data carefully and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            String data = getResultData();
            PublicSenderActivity.this.logLine(
                    String.format("Received result: ¥"%s¥"", data));
        }
    };

    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView)findViewById(R.id.logview);
    }

    private void logLine(String line) {
        mLogView.append(line);
        mLogView.append("¥n");
    }
}
```


4.2.1.3. In-house Broadcast Receiver - Receiving/Sending Broadcasts

In-house Broadcast Receiver is the Broadcast Receiver that will never receive any Broadcasts sent from other than in-house applications. It consists of several in-house applications, and it's used to protect the information or functions that in-house application handles.

Points (Receiving Broadcasts):

1. Define an in-house signature permission to receive Broadcasts.
2. Declare to use the in-house signature permission to receive results.
3. Explicitly set the exported attribute to true.
4. Require the in-house signature permission by the Static Broadcast Receiver definition.
5. Require the in-house signature permission to register Dynamic Broadcast Receiver.
6. Verify that the in-house signature permission is defined by an in-house application.
7. Handle the received intent carefully and securely, even though the Broadcast was sent from an in-house application.
8. Sensitive information can be returned since the requesting application is in-house.
9. When Exporting an APK, sign the APK with the same developer key as the sending application.

In-house Receiver which is a sample code of in-house Broadcast Receiver is to be used both in Static Broadcast Receiver and Dynamic Broadcast Receiver.

InhouseReceiver.java

```
package org.jssec.android.broadcast.inhousereceiver;

import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.widget.Toast;

public class InhouseReceiver extends BroadcastReceiver {

    // In-house Signature Permission
    private static final String MY_PERMISSION = "org.jssec.android.broadcast.inhousereceiver.MY_PERMISS
ION";

    // In-house certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of "my company key" in the keystore.
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
```

```
    }

    private static final String MY_BROADCAST_INHOUSE =
        "org.jssec.android.broadcast.MY_BROADCAST_INHOUSE";

    public boolean isDynamic = false;
    private String getName() {
        return isDynamic ? "In-house Dynamic Broadcast Receiver" : "In-house Static Broadcast Receiver";
    }

    @Override
    public void onReceive(Context context, Intent intent) {

        // *** POINT 6 *** Verify that the in-house signature permission is defined by an in-house applic
ation.
        if (!SigPerm.test(context, MY_PERMISSION, myCertHash(context))) {
            Toast.makeText(context, "The in-house signature permission is not declared by in-house appli
cation.",
                    Toast.LENGTH_LONG).show();
            return;
        }

        // *** POINT 7 *** Handle the received intent carefully and securely,
        // even though the Broadcast was sent from an in-house application..
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        if (MY_BROADCAST_INHOUSE.equals(intent.getAction())) {
            String param = intent.getStringExtra("PARAM");
            Toast.makeText(context,
                    String.format("%s:¥nReceived param: ¥"%s¥"", getName(), param),
                    Toast.LENGTH_SHORT).show();
        }

        // *** POINT 8 *** Sensitive information can be returned since the requesting application is in-
house.
        setResultCode(Activity.RESULT_OK);
        setResultData(String.format("Sensitive Info from %s", getName()));
        abortBroadcast();
    }
}
```

Static Broadcast Receiver is to be defined in AndroidManifest.xml.
Note with caution that—depending on the terminal version—reception of implicit Broadcast Intents may be restricted, as in「Table 4.2-1」.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.broadcast.inhousereceiver" >
```



```
    <!-- *** POINT 1 *** Define an in-house signature permission to receive Broadcasts -->
    <permission
        android:name="org.jssec.android.broadcast.inhousereceiver.MY_PERMISSION"
        android:protectionLevel="signature" />

    <!-- *** POINT 2 *** Declare to use the in-house signature permission to receive results. -->
    <uses-permission
        android:name="org.jssec.android.broadcast.inhousesender.MY_PERMISSION" />

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >

        <!-- *** POINT 3 *** Explicitly set the exported attribute to true. -->
        <!-- *** POINT 4 *** Require the in-house signature permission by the Static Broadcast Receiver
definition. -->
        <receiver
            android:name=".InhouseReceiver"
            android:permission="org.jssec.android.broadcast.inhousereceiver.MY_PERMISSION"
            android:exported="true">
            <intent-filter>
                <action android:name="org.jssec.android.broadcast.MY_BROADCAST_INHOUSE" />
            </intent-filter>
        </receiver>

        <service
            android:name=".DynamicReceiverService"
            android:exported="false" />

        <activity
            android:name=".InhouseReceiverActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>
```

Dynamic Broadcast Receiver executes registration/unregistration by calling registerReceiver() or unregisterReceiver() in the program. In order to execute registration/unregistration by the button operations, the button is arranged on InhouseReceiverActivity. Since the scope of Dynamic Broadcast Receiver Instance is longer than InhouseReceiverActivity, it cannot be kept as the member variable of InhouseReceiverActivity. So, keep Dynamic Broadcast Receiver Instance as the member variable of DynamicReceiverService, and then start/end DynamicReceiverService from InhouseReceiverActivity to register/unregister Dynamic Broadcast Receiver indirectly.

InhouseReceiverActivity.java

```
package org.jssec.android.broadcast.inhousereceiver;

import android.app.Activity;
```

```
import android.content.Intent;
import android.os.Bundle;
import android.view.View;

public class InhouseReceiverActivity extends Activity {
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }

    public void onRegisterReceiverClick(View view) {
        Intent intent = new Intent(this, DynamicReceiverService.class);
        startService(intent);
    }

    public void onUnregisterReceiverClick(View view) {
        Intent intent = new Intent(this, DynamicReceiverService.class);
        stopService(intent);
    }
}
```

DynamicReceiverService.java

```
package org.jssec.android.broadcast.inhousereceiver;

import android.app.Service;
import android.content.Intent;
import android.content.IntentFilter;
import android.os.IBinder;
import android.widget.Toast;

public class DynamicReceiverService extends Service {

    private static final String MY_BROADCAST_INHOUSE =
        "org.jssec.android.broadcast.MY_BROADCAST_INHOUSE";

    private InhouseReceiver mReceiver;

    @Override
    public IBinder onBind(Intent intent) {
        return null;
    }

    @Override
    public void onCreate() {
        super.onCreate();

        mReceiver = new InhouseReceiver();
        mReceiver.isDynamic = true;
        IntentFilter filter = new IntentFilter();
        filter.addAction(MY_BROADCAST_INHOUSE);
        filter.setPriority(1);  // Prioritize Dynamic Broadcast Receiver, rather than Static Broadcast R
eceiver.

        // *** POINT 5 *** When registering a dynamic broadcast receiver, require the in-house signature
 permission.
        registerReceiver(mReceiver, filter, "org.jssec.android.broadcast.inhousereceiver.MY_PERMISSION"
, null);
```



```
        Toast.makeText(this,
                "Registered Dynamic Broadcast Receiver.",
                Toast.LENGTH_SHORT).show();
    }

    @Override
    public void onDestroy() {
        super.onDestroy();
        unregisterReceiver(mReceiver);
        mReceiver = null;
        Toast.makeText(this,
                "Unregistered Dynamic Broadcast Receiver.",
                Toast.LENGTH_SHORT).show();
    }
}
```

SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;

            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;
```

```
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


*** Point 9 *** When exporting an APK, sign the APK with the same developer key as the sending application.

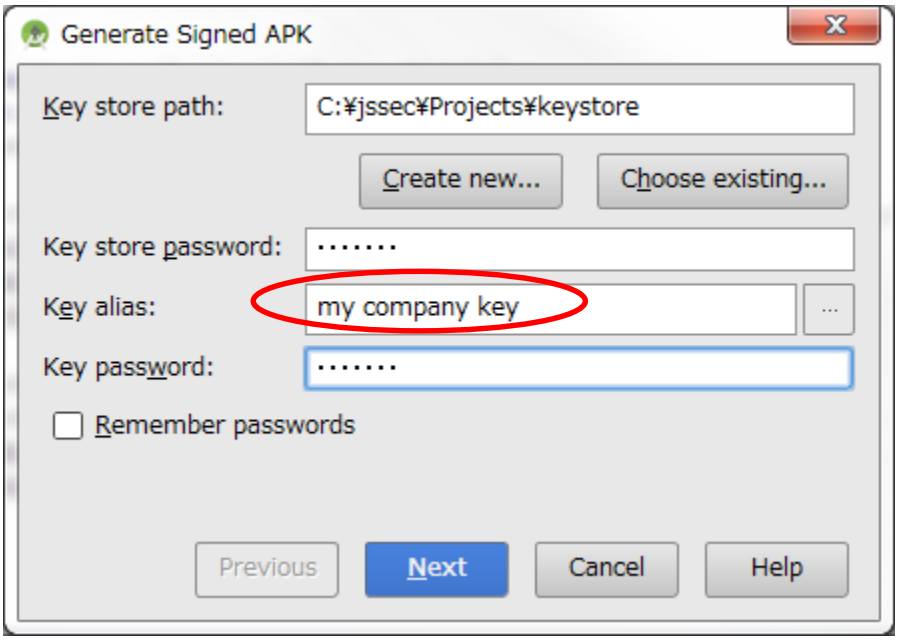


Figure 4.2-2

Next, the sample code for sending Broadcasts to in-house Broadcast Receiver is shown.

Points (Sending Broadcasts):

10. Define an in-house signature permission to receive results.
11. Declare to use the in-house signature permission to receive Broadcasts.
12. Verify that the in-house signature permission is defined by an in-house application.
13. Sensitive information can be returned since the requesting application is the in-house one.
14. Require the in-house signature permission of Receivers.
15. Handle the received result data carefully and securely.
16. When exporting an APK, sign the APK with the same developer key as the destination application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.broadcast.inhousesender" >

    <uses-permission android:name="android.permission.BROADCAST_STICKY"/>

    <!-- *** POINT 10 *** Define an in-house signature permission to receive results. -->
    <permission
        android:name="org.jssec.android.broadcast.inhousesender.MY_PERMISSION"
        android:protectionLevel="signature" />

    <!-- *** POINT 11 *** Declare to use the in-house signature permission to receive Broadcasts. -->
    <uses-permission
        android:name="org.jssec.android.broadcast.inhousereceiver.MY_PERMISSION" />

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >

        <activity
            android:name="org.jssec.android.broadcast.inhousesender.InhouseSenderActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

InhouseSenderActivity.java

```
package org.jssec.android.broadcast.inhousesender;

import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
```



```
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;
import android.widget.Toast;

public class InhouseSenderActivity extends Activity {

    // In-house Signature Permission
    private static final String MY_PERMISSION = "org.jssec.android.broadcast.inhousesender.MY_PERMISSIO
N";

    // In-house certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of "my company key" in the keystore.
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    private static final String MY_BROADCAST_INHOUSE =
        "org.jssec.android.broadcast.MY_BROADCAST_INHOUSE";

    public void onSendNormalClick(View view) {

        // *** POINT 12 *** Verify that the in-house signature permission is defined by an in-house appli
cation.
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            Toast.makeText(this, "The in-house signature permission is not declared by in-house applicat
ion.",
                    Toast.LENGTH_LONG).show();
            return;
        }

        // *** POINT 13 *** Sensitive information can be returned since the requesting application is in
-house.
        Intent intent = new Intent(MY_BROADCAST_INHOUSE);
        intent.putExtra("PARAM", "Sensitive Info from Sender");

        // *** POINT 14 *** Require the in-house signature permission to limit receivers.
        sendBroadcast(intent, "org.jssec.android.broadcast.inhousesender.MY_PERMISSION");
    }

    public void onSendOrderedClick(View view) {

        // *** POINT 12 *** Verify that the in-house signature permission is defined by an in-house appli
cation.
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            Toast.makeText(this, "The in-house signature permission is not declared by in-house applicat
ion.",
                    Toast.LENGTH_LONG).show();
            return;
        }
```

```
        // *** POINT 13 *** Sensitive information can be returned since the requesting application is in
-house.
        Intent intent = new Intent(MY_BROADCAST_INHOUSE);
        intent.putExtra("PARAM", "Sensitive Info from Sender");

        // *** POINT 14 *** Require the in-house signature permission to limit receivers.
        sendOrderedBroadcast(intent, "org.jssec.android.broadcast.inhousesender.MY_PERMISSION",
                mResultReceiver, null, 0, null, null);
    }

    private BroadcastReceiver mResultReceiver = new BroadcastReceiver() {
        @Override
        public void onReceive(Context context, Intent intent) {

            // *** POINT 15 *** Handle the received result data carefully and securely,
            // even though the data came from an in-house application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            String data = getResultData();
            InhouseSenderActivity.this.logLine(String.format("Received result: ¥"%s¥"", data));
        }
    };

    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView)findViewById(R.id.logview);
    }

    private void logLine(String line) {
        mLogView.append(line);
        mLogView.append("¥n");
    }
}
```

SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
```



```
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;

            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
```

```
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```

*** Point 16 *** When exporting an APK, sign the APK with the same developer key as the destination application.

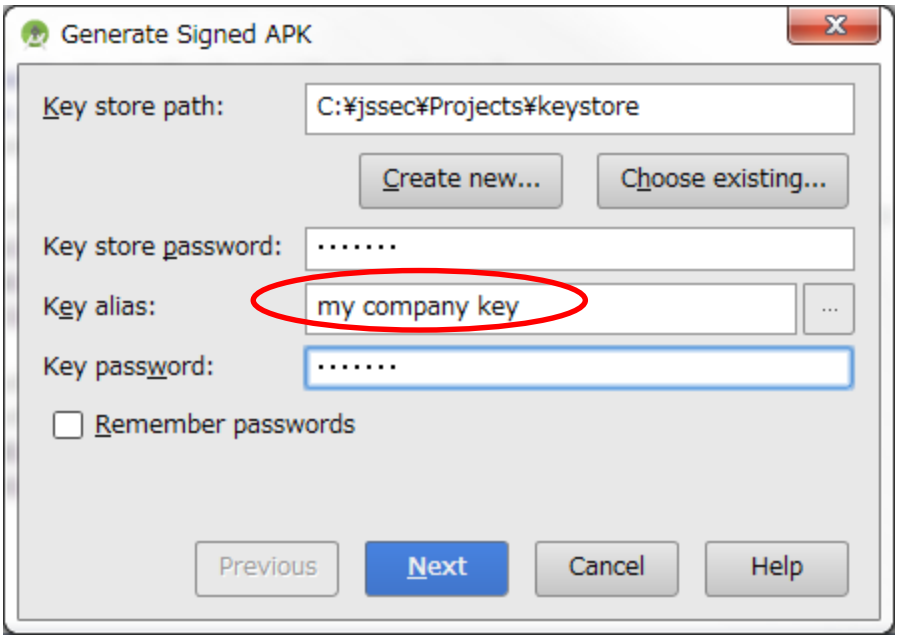


Figure 4.2-3

4.2.2. Rule Book

Follow the rules below to Send or receive Broadcasts.

1.	Broadcast Receiver that Is Used Only in an Application Must Be Set as Private	(Required)
2.	Handle the Received Intent Carefully and Securely	(Required)
3.	Use the In-house Defined Signature Permission after Verifying that it's Defined by an In-house Application	(Required)
4.	When Returning a Result Information, Pay Attention to the Result Information Leakage from the Destination Application	(Required)
5.	When Sending Sensitive Information with a Broadcast, Limit the Receivable Receiver	(Required)
6.	Sensitive Information Must Not Be Included in the Sticky Broadcast	(Required)
7.	Pay Attention that the Ordered Broadcast without Specifying the receiverPermission May Not Be Delivered	(Required)
8.	Handle the Returned Result Data from the Broadcast Receiver Carefully and Securely	(Required)
9.	When Providing an Asset Secondarily, the Asset should be protected with the Same Protection Level	(Required)

4.2.2.1. Broadcast Receiver that Is Used Only in an Application Must Be Set as Private (Required)

Broadcast Receiver which is used only in the application should be set as private to avoid from receiving any Broadcasts from other applications unexpectedly. It will prevent the application function abuse or the abnormal behaviors.

Receiver used only within the same application should not be designed with setting Intent-filter. Because of the Intent-filter characteristics, a public Receiver of other application may be called unexpectedly by calling through Intent-filter even though a private Receiver within the same application is to be called.

AndroidManifest.xml(Not recommended)

```
<!-- Private Broadcast Receiver -->
<!-- *** POINT 1 *** Set the exported attribute to false explicitly. -->
<receiver
    android:name=".PrivateReceiver"
    android:exported="false" >
    <intent-filter>
        <action android:name="org.jssec.android.broadcast.MY_ACTION" />
    </intent-filter>
</receiver>
```

Please refer to "4.2.3.1 Combinations of the exported Attribute and the Intent-filter setting (For Receiver)."

4.2.2.2. Handle the Received Intent Carefully and Securely (Required)

Though risks are different depending on the types of the Broadcast Receiver, firstly verify the safety

of Intent when processing received Intent data.

Since Public Broadcast Receiver receives the Intents from unspecified large number of applications, it may receive malware's attacking Intents. Private Broadcast Receiver will never receive any Intent from other applications directly, but Intent data which a public Component received from other applications may be forwarded to Private Broadcast Receiver. So don't think that the received Intent is totally safe without any qualification. In-house Broadcast Receivers have some degree of the risks, so it also needs to verify the safety of the received Intents.

Please refer to "3.2 Handling Input Data Carefully and Securely"

4.2.2.3. Use the In-house Defined Signature Permission after Verifying that it's Defined by an In-house Application (Required)

In-house Broadcast Receiver which receives only Broadcasts sent by an In-house application should be protected by in-house-defined Signature Permission. Permission definition/Permission request declarations in AndroidManifest.xml are not enough to protecting, so please refer to "5.2.1.2 How to Communicate Between In-house Applications with In-house-defined Signature Permission." ending Broadcasts by specifying in-house-defined Signature Permission to receiverPermission parameter requires verification in the same way.

4.2.2.4. When Returning a Result Information, Pay Attention to the Result Information Leakage from the Destination Application (Required)

The Reliability of the application which returns result information by setResult() varies depending on the types of the Broadcast Receiver. In case of Public Broadcast Receiver, the destination application may be malware, and there may be a risk that the result information is used maliciously. In case of Private Broadcast Receiver and In-house Broadcast Receiver, the result destination is In-house developed application, so no need to mind the result information handling.

Need to pay attention to the result information leakage from the destination application when result information is returned from Broadcast Receivers as above.

4.2.2.5. When Sending Sensitive Information with a Broadcast, Limit the Receivable Receiver (Required)

Broadcast is the created system to broadcast information to unspecified large number of applications or notify them of the timing at once. So, broadcasting sensitive information requires the careful designing for preventing the illicit obtainment of the information by malware.

For broadcasting sensitive information, only reliable Broadcast Receiver can receive it, and other Broadcast Receivers cannot. The following are some examples of Broadcast sending methods.

- The method is to fix the address by Broadcast-sending with an explicit Intent for sending

Broadcasts to the intended reliable Broadcast Receivers only. There are 2 patterns in this method.

- When it's addressed to a Broadcast Receiver within the same application, specify the address by Intent#setClass(Context, Class). Refer to sample code section "4.2.1.1 Private Broadcast Receiver - Receiving/Sending Broadcast" for the concrete code.
- When it's addressed to a Broadcast Receiver in other applications, specify the address by Intent#setClassName(String, String). Confirm the permitted application by comparing the developer key of the APK signature in the destination package with the white list to send Broadcasts. Actually the following method of using implicit Intents is more practical.

- The Method is to send Broadcasts by specifying in-house-defined Signature Permission to receiverPermission parameter and make the reliable Broadcast Receiver declare to use this Signature Permission. Refer to the sample code section "4.2.1.3 In-house Broadcast Receiver - Receiving/Sending Broadcast" for the concrete code. In addition, implementing this Broadcast-sending method needs to apply the rule "4.2.2.3 Use the In-house Defined Signature Permission after Verifying that it's Defined by an In-house Application (Required)."

4.2.2.6. Sensitive Information Must Not Be Included in the Sticky Broadcast (Required)

Usually, the Broadcasts will be disappeared when they are processed to be received by the available Broadcast Receivers. On the other hand, Sticky Broadcasts (hereafter, Sticky Broadcasts including Sticky Ordered Broadcasts), will not be disappeared from the system even when they processed to be received by the available Broadcast Receivers and will be able to be received by registerReceiver(). When Sticky Broadcast becomes unnecessary, it can be deleted anytime arbitrarily with removeStickyBroadcast().

As it's presupposed that Sticky Broadcast is used by the implicit Intent. Broadcasts with specified receiverPermission Parameter cannot be sent. For this reason, information sent via Sticky Broadcasts can be accessed by multiple unspecified apps — including malware — and thus sensitive information must not be sent in this way. Note that Sticky Broadcast is deprecated in Android 5.0 (API Level 21).

4.2.2.7. Pay Attention that the Ordered Broadcast without Specifying the receiverPermission May Not Be Delivered (Required)

Ordered Broadcast without specified receiverPermission Parameter can be received by unspecified large number of applications including malware. Ordered Broadcast is used to receive the returned information from Receiver, and to make several Receivers execute processing one by one. Broadcasts are sent to the Receivers in order of priority. So if the high- priority malware receives Broadcast first and executes abortBroadcast(), Broadcasts won't be delivered to the following Receivers.

4.2.2.8. Handle the Returned Result Data from the Broadcast Receiver Carefully and Securely (Required)

Basically the result data should be processed safely considering the possibility that received results may be the attacking data though the risks vary depending on the types of the Broadcast Receiver

which has returned the result data.

When sender (source) Broadcast Receiver is public Broadcast Receiver, it receives the returned data from unspecified large number of applications. So it may also receive malware's attacking data. When sender (source) Broadcast Receiver is private Broadcast Receiver, it seems no risk. However the data received by other applications may be forwarded as result data indirectly. So the result data should not be considered as safe without any qualification. When sender (source) Broadcast Receiver is In-house Broadcast Receiver, it has some degree of the risks. So it should be processed in a safe way considering the possibility that the result data may be an attacking data.

Please refer to "3.2 Handling Input Data Carefully and Securely"

4.2.2.9. When Providing an Asset Secondarily, the Asset should be protected with the Same Protection Level (Required)

When information or function assets protected by Permission are provided to other applications secondarily, it's necessary to keep the protection standard by claiming the same Permission of the destination application. In the Android Permission security models, privileges are managed only for the direct access to the protected assets from applications. Because of the characteristics, acquired assets may be provided to other applications without claiming Permission which is necessary for protection. This is actually same as re-delegating Permission, as it is called, Permission re-delegation problem. Please refer to "5.2.3.4 Permission Re-delegation Problem."

4.2.3. Advanced Topics

4.2.3.1. Combinations of the exported Attribute and the Intent-filter setting (For Receiver)

Table 4.2-3 represents the permitted combination of export settings and Intent-filter elements when implementing Receivers. The reason why the usage of exported="false" with Intent-filter definition is principally prohibited, is described below.

Table 4.2-3 Usable or not; Combination of exported attribute and intent-filter elements

	Value of exported attribute		
	True	False	Not specified
Intent-filter defined	OK	(Do not Use)	(Do not Use)
Intent Filter Not Defined	OK	OK	(Do not Use)

When the exported attribute of a Receiver is left unspecified, the question of whether or not the Receiver is public is determined by the presence or absence of intent filters for that Receiver.[9] However, in this guidebook it is forbidden to set the exported attribute to unspecified. In general, as mentioned previously, it is best to avoid implementations that rely on the default behavior of any given API; moreover, in cases where explicit methods — such as the exported attribute — exist for enabling important security-related settings, it is always a good idea to make use of those methods.

Public Receivers in other applications may be called unexpectedly even though Broadcasts are sent to the private Receivers within the same applications. This is the reason why specifying exported="false" with Intent-filter definition is prohibited. The following 2 figures show how the unexpected calls occur.

Figure 4.2-4 is an example of the normal behaviors which a private Receiver (application A) can be called by implicit Intent only within the same application. Intent-filter (in the figure, action="X") is defined only in application A, so this is the expected behavior.

[9] If any intent filters are defined then the Receiver is public; otherwise it is private. For more information, see https://developer.android.com/guide/topics/manifest/receiver-element.html#exported.

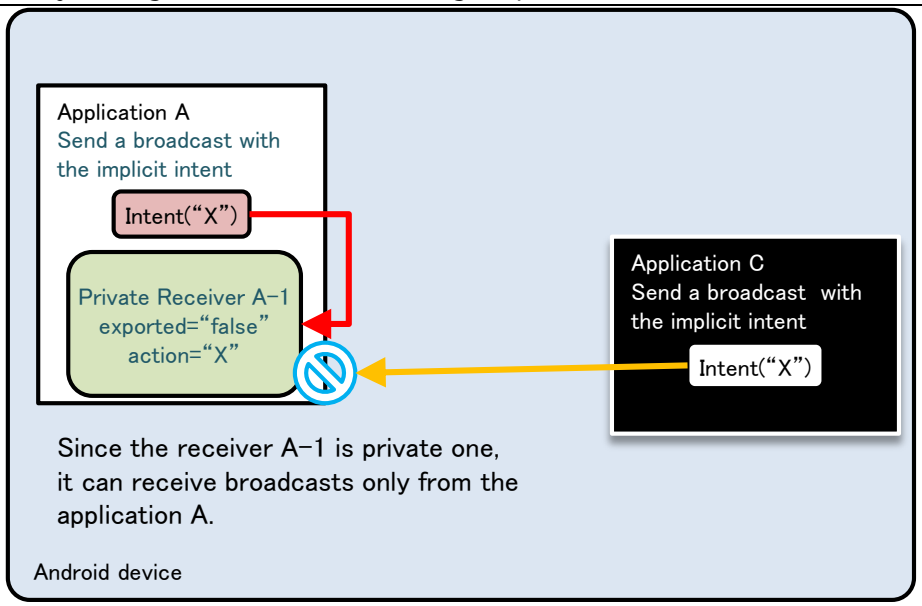


Figure 4.2-4

Figure 4.2-5 is an example that Intent-filter (see action="X" in the figure) is defined in the application B as well as in the application A. First of all, when another application (application C) sends Broadcasts by implicit Intent, they are not received by a private Receiver (A-1) side. So there won't be any security problem. (See the orange arrow marks in the Figure.)
From security point of view, the problem is application A's call to the private Receiver within the same application. When the application A broadcasts implicit Intent, not only Private Receiver within the same application, but also public Receiver (B-1) with the same Intent-filter definition can also receive the Intent. (Red arrow marks in the Figure). In this case, sensitive information may be sent from the application A to B. When the application B is malware, it will cause the leakage of sensitive information. When the Broadcast is Ordered Broadcast, it may receive the unexpected result information.

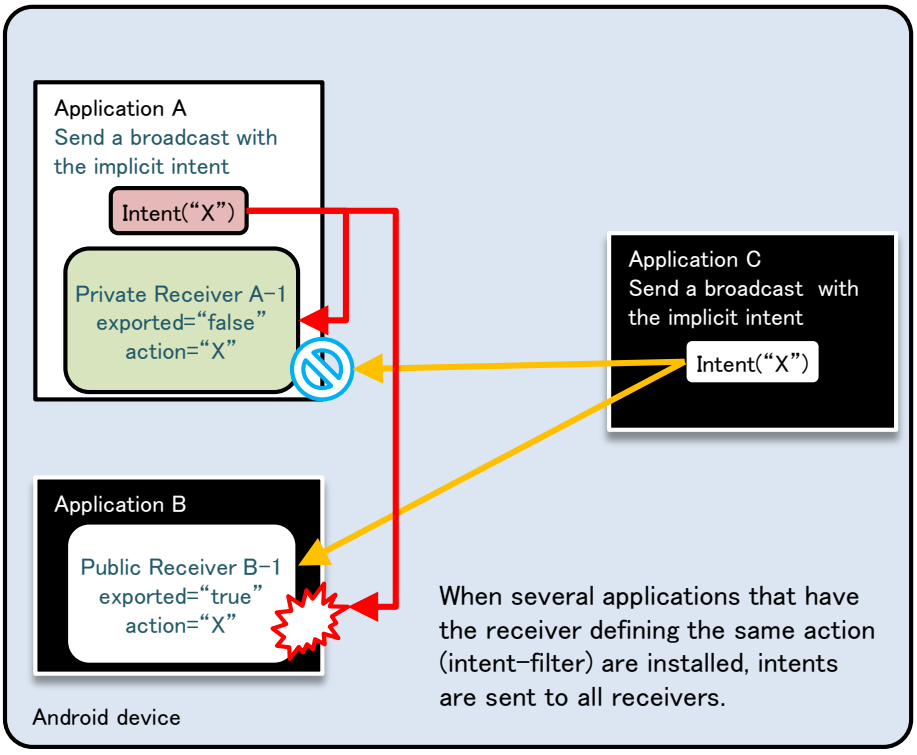


Figure 4.2-5

However, exported="false" with Intent-filter definition should be used when Broadcast Receiver to receive only Broadcast Intent sent by the system is implemented. Other combination should not be used. This is based on the fact that Broadcast Intent sent by the system can be received by exported="false". If other applications send Intent which has same ACTION with Broadcast Intent sent by system, it may cause an unexpected behavior by receiving it. However, this can be prevented by specifying exported="false".

4.2.3.2. Receiver Won't Be Registered before Launching the Application

It is important to note carefully that a Broadcast Receiver defined statically in AndroidManifest.xml will not be automatically enabled upon installation.[10] Apps are able to receive Broadcasts only after they have been launched the first time; thus, it is not possible to use the receipt of a Broadcast after installation as a trigger to initiate operations. However, if the Intent.FLAG_INCLUDE_STOPPED_PACKAGES flag set when sending a Broadcast, that Broadcast will be received even by apps that have not yet been launched for the first time.

4.2.3.3. Private Broadcast Receiver Can Receive the Broadcast that Was Sent by the Same UID Application

Same UID can be provided to several applications. Even if it's private Broadcast Receiver, the Broadcasts sent from the same UID application can be received.

[10] In versions prior to Android 3.0, Receivers were registered automatically simply by installing apps.

However, it won't be a security problem. Since it's guaranteed that applications with the same UID have the consistent developer keys for signing APK. It means that what private Broadcast Receiver receives is only the Broadcast sent from In-house applications.

4.2.3.4. Types and Features of Broadcasts

Regarding Broadcasts, there are 4 types based on the combination of whether it's Ordered or not, and Sticky or not. Based on Broadcast sending methods, a type of Broadcast to send is determined. Note that Sticky Broadcast is deprecated in Android 5.0 (API Level 21).

Table 4.2-4

Type of Broadcast	Method for sending	Ordered?	Sticky?
Normal Broadcast	sendBroadcast()	No	No
Ordered Broadcast	sendOrderedBroadcast()	Yes	No
Sticky Broadcast	sendStickyBroadcast()	No	Yes
Sticky Ordered Broadcast	sendStickyOrderedBroadcast()	Yes	Yes

The feature of each Broad cast is described.

Table 4.2-5

Type of Broadcast	Features for each type of Broadcast
Normal Broadcast	Normal Broadcast disappears when it is sent to receivable Broadcast Receiver. Broadcasts are received by several Broadcast Receivers simultaneously. This is a difference from Ordered Broadcast. Broadcasts are allowed to be received by the particular Broadcast Receivers.
Ordered Broadcast	Ordered Broadcast is characterized by receiving Broadcasts one by one in order with receivable Broadcast Receivers. The higher-priority Broadcast Receiver receives earlier. Broadcasts will disappear when Broadcasts are delivered to all Broadcast Receivers or a Broadcast Receiver in the process calls abortBroadcast(). Broadcasts are allowed to be received by the Broadcast Receivers which declare the specified Permission. In addition, the result information sent from Broadcast Receiver can be received by the sender with Ordered Broadcasts. The Broadcast of SMS-receiving notice (SMS_RECEIVED) is a representative example of Ordered Broadcast.
Sticky Broadcast	Sticky Broadcast does not disappear and remains in the system, and then the application that calls registerReceiver() can receive Sticky Broadcast later. Since Sticky Broadcast is different from other Broadcasts, it will never disappear automatically. So when Sticky Broadcast is not necessary, calling removeStickyBroadcast() explicitly is required to delete Sticky Broadcast. Also, Broadcasts

	cannot be received by the limited Broadcast Receivers with particular Permission. The Broadcast of changing battery-state notice (ACTION_BATTERY_CHANGED) is the representative example of Sticky Broadcast.
Sticky Ordered Broadcast	This is the Broadcast which has both characteristics of Ordered Broadcast and Sticky Broadcast. Same as Sticky Broadcast, it cannot allow only Broadcast Receivers with the particular Permission to receive the Broadcast.

From the Broadcast characteristic behavior point of view, above table is conversely arranged in the following one.

Table 4.2-6

Characteristic behavior of Broadcast	Normal Broadcast	Ordered Broadcast	Sticky Broadcast	Sticky Ordered Broadcast
Limit Broadcast Receivers which can receive Broadcast, by Permission	OK	OK	-	-
Get the results of process from Broadcast Receiver	-	OK	-	OK
Make Broadcast Receivers process Broadcasts in order	-	OK	-	OK
Receive Broadcasts later, which have been already sent	-	-	OK	OK

4.2.3.5. Broadcasted Information May be Output to the LogCat

Basically sending/receiving Broadcasts is not output to LogCat. However, the error log will be output when lacking Permission causes errors in receiver/sender side. Intent information sent by Broadcast is included in the error log, so after an error occurs it's necessary to pay attention that Intent information is displayed in LogCat when Broadcast is sent.

Erorr of lacking Permission in sender side

```
W/ActivityManager(266): Permission Denial: broadcasting Intent { act=org.jssec.android.broadcastreceive
r.creating.action.MY_ACTION } from org.jssec.android.broadcast.sending (pid=4685, uid=10058) requires o
rg.jssec.android.permission.MY_PERMISSION due to receiver org.jssec.android.broadcastreceiver.creating/
org.jssec.android.broadcastreceiver.creating.CreatingType3Receiver
```

Erorr of lacking Permission in receiver side

```
W/ActivityManager(275): Permission Denial: receiving Intent { act=org.jssec.android.broadcastreceiver.c
reating.action.MY_ACTION } to org.jssec.android.broadcastreceiver.creating requires org.jssec.android.p
ermission.MY_PERMISSION due to sender org.jssec.android.broadcast.sending (uid 10158)
```

4.2.3.6. Items to Keep in Mind When Placing an App Shortcut on the Home Screen

In what follows we discuss a number of items to keep in mind when creating a shortcut button for

launching an app from the home screen or for creating URL shortcuts such as bookmarks in web browsers. As an example, we consider the implementation shown below.

Place an app shortcut on the home screen

```
Intent targetIntent = new Intent(this, TargetActivity.class);

// Intent to request shortcut creation
Intent intent = new Intent("com.android.launcher.action.INSTALL_SHORTCUT");

// Specify an Intent to be launched when the shortcut is tapped
intent.putExtra(Intent.EXTRA_SHORTCUT_INTENT, targetIntent);
Parcelable icon = Intent.ShortcutIconResource.fromContext(context, iconResource);
intent.putExtra(Intent.EXTRA_SHORTCUT_ICON_RESOURCE, icon);
intent.putExtra(Intent.EXTRA_SHORTCUT_NAME, title);
intent.putExtra("duplicate", false);

// Use Broadcast to send the system our request for shortcut creation
context.sendBroadcast(intent);
```

In the Broadcast sent by the above code snippet, the receiver is the home-screen app, and it is difficult to identify the package name; one must take care to remember that this is a transmission to a public receiver with an implicit intent. Thus the Broadcast sent by this snippet could be received by any arbitrary app, including malware; for this reason, the inclusion of sensitive information in the Intent may create the risk of a damaging leak of information. It is particularly important to note that, when creating a URL-based shortcut, secret information may be contained in the URL itself.

As countermeasures, it is necessary to follow the points listed in ”4.2.1.2 Public Broadcast Receiver – Receiving/Sending Broadcasts” and to ensure that the transmitted Intent does not contain sensitive information.

Since the interface of ContentResolver and SQLiteDatabase are so much alike, it's often misunderstood that Content Provider is so closely related to SQLiteDatabase. However, actually Content Provider simply provides the interface of inter-application data sharing, so it's necessary to pay attention that it does not interfere each data saving format. To save data in Content Provider, SQLiteDatabase can be used, and other saving formats, such as an XML file format, also can be used. Any data saving process is not included in the following sample code, so please add it if needed.

4.3.1. Sample Code

The risks and countermeasures of using Content Provider differ depending on how that Content Provider is being used. In this section, we have classified 5 types of Content Provider based on how the Content Provider is being used. You can find out which type of Content Provider you are supposed to create through the following chart shown below.

Table 4.3-1 Definition of content provider types

Type	Definition
Private Content Provider	A content provider that cannot be used by another application, and therefore is the safest content provider
Public Content Provider	A content provider that is supposed to be used by an unspecified large number of applications
Partner Content Provider	A content provider that can be used by specific applications made by a trusted partner company.
In-house Content Provider	A content provider that can only be used by other in-house applications
Temporary permit Content Provider	A content provider that is basically private content provider, but permits specific applications to access the particular URI.

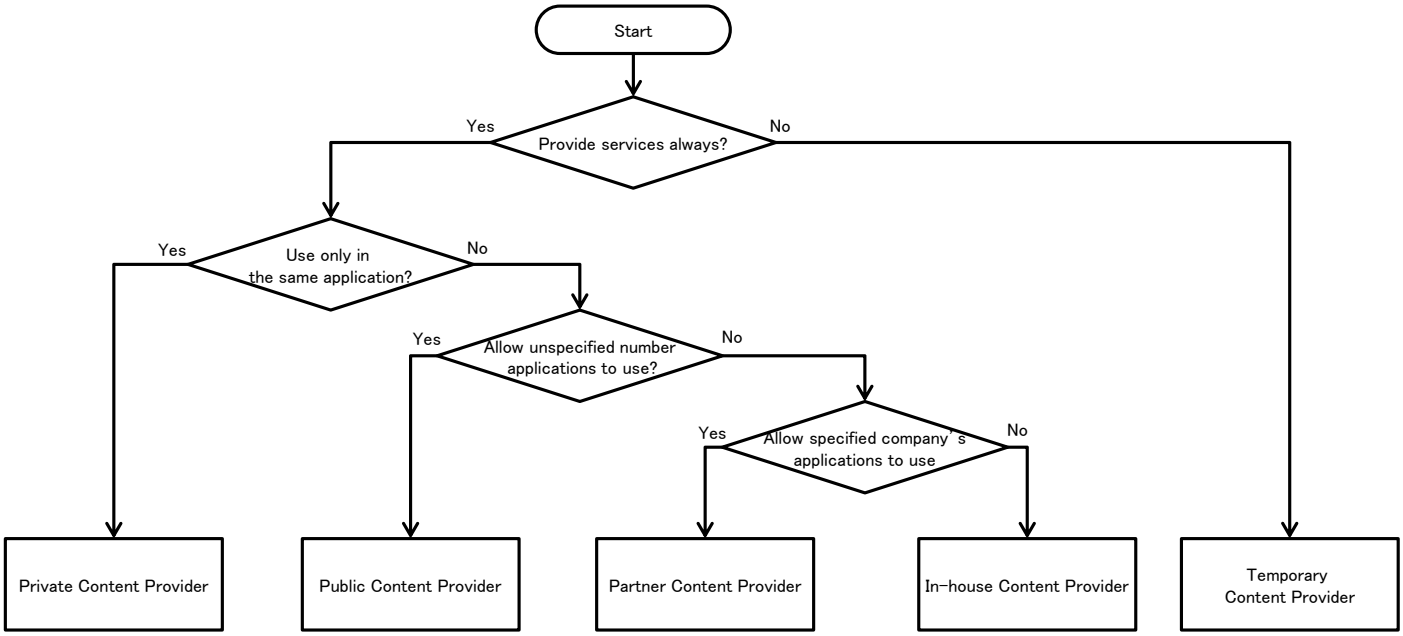


Figure 4.3-1

4.3.1.1. Creating/Using Private Content Providers

Private Content Provider is the Content Provider which is used only in the single application, and the safest Content Provider[11].

Sample code of how to implement a private Content Provider is shown below.

Points (Creating a Content Provider):

1. Explicitly set the exported attribute to false.
2. Handle the received request data carefully and securely, even though the data comes from the same application.
3. Sensitive information can be sent since it is sending and receiving all within the same application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.provider.privateprovider">

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >
        <activity
            android:name=".PrivateUserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

        <!-- *** POINT 1 *** Explicitly set the exported attribute to false. -->
        <provider
            android:name=".PrivateProvider"
            android:authorities="org.jssec.android.provider.privateprovider"
            android:exported="false" />
    </application>
</manifest>
```

PrivateProvider.java

```
package org.jssec.android.provider.privateprovider;

import android.content.ContentProvider;
import android.content.ContentUris;
import android.content.ContentValues;
import android.content.UriMatcher;
import android.database.Cursor;
import android.database.MatrixCursor;
```

[11] However, non-public settings for Content Provider are not functional in Android 2.2 (API Level 8) and previous versions.


```
import android.net.Uri;

public class PrivateProvider extends ContentProvider {

    public static final String AUTHORITY = "org.jssec.android.provider.privateprovider";
    public static final String CONTENT_TYPE = "vnd.android.cursor.dir/vnd.org.jssec.contenttype";
    public static final String CONTENT_ITEM_TYPE = "vnd.android.cursor.item/vnd.org.jssec.contenttype";

    // Expose the interface that the Content Provider provides.
    public interface Download {
        public static final String PATH = "downloads";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }
    public interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }

    // UriMatcher
    private static final int DOWNLOADS_CODE = 1;
    private static final int DOWNLOADS_ID_CODE = 2;
    private static final int ADDRESSES_CODE = 3;
    private static final int ADDRESSES_ID_CODE = 4;
    private static UriMatcher sUriMatcher;
    static {
        sUriMatcher = new UriMatcher(UriMatcher.NO_MATCH);
        sUriMatcher.addURI(AUTHORITY, Download.PATH, DOWNLOADS_CODE);
        sUriMatcher.addURI(AUTHORITY, Download.PATH + "/#", DOWNLOADS_ID_CODE);
        sUriMatcher.addURI(AUTHORITY, Address.PATH, ADDRESSES_CODE);
        sUriMatcher.addURI(AUTHORITY, Address.PATH + "/#", ADDRESSES_ID_CODE);
    }

    // Since this is a sample program,
    // query method returns the following fixed result always without using database.
    private static MatrixCursor sAddressCursor = new MatrixCursor(new String[] { "_id", "city" });
    static {
        sAddressCursor.addRow(new String[] { "1", "New York" });
        sAddressCursor.addRow(new String[] { "2", "Longon" });
        sAddressCursor.addRow(new String[] { "3", "Paris" });
    }
    private static MatrixCursor sDownloadCursor = new MatrixCursor(new String[] { "_id", "path" });
    static {
        sDownloadCursor.addRow(new String[] { "1", "/sdcard/downloads/sample.jpg" });
        sDownloadCursor.addRow(new String[] { "2", "/sdcard/downloads/sample.txt" });
    }

    @Override
    public boolean onCreate() {
        return true;
    }

    @Override
    public String getType(Uri uri) {
        // *** POINT 2 *** Handle the received request data carefully and securely,
        // even though the data comes from the same application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Please refer to "3.2 Handle Input Data Carefully and Securely."
```

```
        // *** POINT 3 *** Sensitive information can be sent since it is sending and receiving all within
the same application.
        // However, the result of getType rarely has the sensitive meaning.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case ADDRESSES_CODE:
            return CONTENT_TYPE;

        case DOWNLOADS_ID_CODE:
        case ADDRESSES_ID_CODE:
            return CONTENT_ITEM_TYPE;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Cursor query(Uri uri, String[] projection, String selection,
            String[] selectionArgs, String sortOrder) {

        // *** POINT 2 *** Handle the received request data carefully and securely,
        // even though the data comes from the same application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
case.
        // Checking for other parameters are omitted here, due to sample.
        // Please refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 3 *** Sensitive information can be sent since it is sending and receiving all within
the same application.
        // It depends on application whether the query result has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case DOWNLOADS_ID_CODE:
            return sDownloadCursor;

        case ADDRESSES_CODE:
        case ADDRESSES_ID_CODE:
            return sAddressCursor;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Uri insert(Uri uri, ContentValues values) {

        // *** POINT 2 *** Handle the received request data carefully and securely,
        // even though the data comes from the same application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
case.
        // Checking for other parameters are omitted here, due to sample.
        // Please refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 3 *** Sensitive information can be sent since it is sending and receiving all within
the same application.
        // It depends on application whether the issued ID has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
```



```
            return ContentUris.withAppendedId(Download.CONTENT_URI, 3);

        case ADDRESSES_CODE:
            return ContentUris.withAppendedId(Address.CONTENT_URI, 4);

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int update(Uri uri, ContentValues values, String selection,
            String[] selectionArgs) {

        // *** POINT 2 *** Handle the received request data carefully and securely,
        // even though the data comes from the same application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
case.
        // Checking for other parameters are omitted here, due to sample.
        // Please refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 3 *** Sensitive information can be sent since it is sending and receiving all within
the same application.
        // It depends on application whether the number of updated records has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return 5;   // Return number of updated records

        case DOWNLOADS_ID_CODE:
            return 1;

        case ADDRESSES_CODE:
            return 15;

        case ADDRESSES_ID_CODE:
            return 1;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int delete(Uri uri, String selection, String[] selectionArgs) {

        // *** POINT 2 *** Handle the received request data carefully and securely,
        // even though the data comes from the same application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
case.
        // Checking for other parameters are omitted here, due to sample.
        // Please refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 3 *** Sensitive information can be sent since it is sending and receiving all within
the same application.
        // It depends on application whether the number of deleted records has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return 10;  // Return number of deleted records

        case DOWNLOADS_ID_CODE:
```

```
            return 1;

        case ADDRESSES_CODE:
            return 20;

        case ADDRESSES_ID_CODE:
            return 1;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }
}
```


Next is an example of Activity which uses Private Content Provider.

Points (Using a Content Provider):

4. Sensitive information can be sent since the destination provider is in the same application.
5. Handle received result data carefully and securely, even though the data comes from the same application.

PrivateUserActivity.java

```
package org.jssec.android.provider.privateprovider;

import android.app.Activity;
import android.database.Cursor;
import android.net.Uri;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PrivateUserActivity extends Activity {

    public void onQueryClick(View view) {

        logLine("[Query]");

        Cursor cursor = null;
        try {
            // *** POINT 4 *** Sensitive information can be sent since the destination provider is in the
 same application.
            cursor = getContentResolver().query(
                    PrivateProvider.Download.CONTENT_URI, null, null, null, null);

            // *** POINT 5 *** Handle received result data carefully and securely,
            // even though the data comes from the same application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            if (cursor == null) {
                logLine("  null cursor");
            } else {
                boolean moved = cursor.moveToFirst();
                while (moved) {
                    logLine(String.format("  %d, %s", cursor.getInt(0), cursor.getString(1)));
                    moved = cursor.moveToNext();
                }
            }
        }
        finally {
            if (cursor != null) cursor.close();
        }
    }

    public void onInsertClick(View view) {

        logLine("[Insert]");

        // *** POINT 4 *** Sensitive information can be sent since the destination provider is in the sam
e application.
        Uri uri = getContentResolver().insert(PrivateProvider.Download.CONTENT_URI, null);
```

```
        // *** POINT 5 *** Handle received result data carefully and securely,
        // even though the data comes from the same application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine("  uri:" + uri);
    }

    public void onUpdateClick(View view) {

        logLine("[Update]");

        // *** POINT 4 *** Sensitive information can be sent since the destination provider is in the sam
e application.
        int count = getContentResolver().update(PrivateProvider.Download.CONTENT_URI, null, null, null);

        // *** POINT 5 *** Handle received result data carefully and securely,
        // even though the data comes from the same application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine(String.format("  %s records updated", count));
    }

    public void onDeleteClick(View view) {

        logLine("[Delete]");

        // *** POINT 4 *** Sensitive information can be sent since the destination provider is in the sam
e application.
        int count = getContentResolver().delete(
                PrivateProvider.Download.CONTENT_URI, null, null);

        // *** POINT 5 *** Handle received result data carefully and securely,
        // even though the data comes from the same application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine(String.format("  %s records deleted", count));
    }

    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView)findViewById(R.id.logview);
    }

    private void logLine(String line) {
        mLogView.append(line);
        mLogView.append("¥n");
    }
}
```


4.3.1.2. Creating/Using Public Content Providers

Public Content Provider is the Content Provider which is supposed to be used by unspecified large number of applications. It's necessary to pay attention that since this doesn't specify clients, it may be attacked and tampered by Malware. For example, a saved data may be taken by select(), a data may be changed by update(), or a fake data may be inserted/deleted by insert()/delete().

In addition, when using a custom Public Content Provider which is not provided by Android OS, it's necessary to pay attention that request parameter may be received by Malware which masquerades as the custom Public Content Provider, and also the attack result data may be sent. Contacts and MediaStore provided by Android OS are also Public Content Providers, but Malware cannot masquerades as them.

Sample code to implement a Public Content Provider is shown below.

Points (Creating a Content Provider):

1. Explicitly set the exported attribute to true.
2. Handle the received request data carefully and securely.
3. When returning a result, do not include sensitive information.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.provider.publicprovider">

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- *** POINT 1 *** Explicitly set the exported attribute to true. -->
        <provider
            android:name=".PublicProvider"
            android:authorities="org.jssec.android.provider.publicprovider"
            android:exported="true" />
    </application>
</manifest>
```

PublicProvider.java

```
package org.jssec.android.provider.publicprovider;

import android.content.ContentProvider;
import android.content.ContentUris;
import android.content.ContentValues;
import android.content.UriMatcher;
import android.database.Cursor;
import android.database.MatrixCursor;
import android.net.Uri;

public class PublicProvider extends ContentProvider {

    public static final String AUTHORITY = "org.jssec.android.provider.publicprovider";
```

```
    public static final String CONTENT_TYPE = "vnd.android.cursor.dir/vnd.org.jssec.contenttype";
    public static final String CONTENT_ITEM_TYPE = "vnd.android.cursor.item/vnd.org.jssec.contenttype";

    // Expose the interface that the Content Provider provides.
    public interface Download {
        public static final String PATH = "downloads";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }
    public interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }

    // UriMatcher
    private static final int DOWNLOADS_CODE = 1;
    private static final int DOWNLOADS_ID_CODE = 2;
    private static final int ADDRESSES_CODE = 3;
    private static final int ADDRESSES_ID_CODE = 4;
    private static UriMatcher sUriMatcher;
    static {
        sUriMatcher = new UriMatcher(UriMatcher.NO_MATCH);
        sUriMatcher.addURI(AUTHORITY, Download.PATH, DOWNLOADS_CODE);
        sUriMatcher.addURI(AUTHORITY, Download.PATH + "/#", DOWNLOADS_ID_CODE);
        sUriMatcher.addURI(AUTHORITY, Address.PATH, ADDRESSES_CODE);
        sUriMatcher.addURI(AUTHORITY, Address.PATH + "/#", ADDRESSES_ID_CODE);
    }

    // Since this is a sample program,
    // query method returns the following fixed result always without using database.
    private static MatrixCursor sAddressCursor = new MatrixCursor(new String[] { "_id", "city" });
    static {
        sAddressCursor.addRow(new String[] { "1", "New York" });
        sAddressCursor.addRow(new String[] { "2", "London" });
        sAddressCursor.addRow(new String[] { "3", "Paris" });
    }
    private static MatrixCursor sDownloadCursor = new MatrixCursor(new String[] { "_id", "path" });
    static {
        sDownloadCursor.addRow(new String[] { "1", "/sdcard/downloads/sample.jpg" });
        sDownloadCursor.addRow(new String[] { "2", "/sdcard/downloads/sample.txt" });
    }

    @Override
    public boolean onCreate() {
        return true;
    }

    @Override
    public String getType(Uri uri) {

        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case ADDRESSES_CODE:
            return CONTENT_TYPE;

        case DOWNLOADS_ID_CODE:
        case ADDRESSES_ID_CODE:
            return CONTENT_ITEM_TYPE;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
```



```
        }
    }

    @Override
    public Cursor query(Uri uri, String[] projection, String selection,
            String[] selectionArgs, String sortOrder) {

        // *** POINT 2 *** Handle the received request data carefully and securely.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 3 *** When returning a result, do not include sensitive information.
        // It depends on application whether the query result has sensitive meaning or not.
        // If no problem when the information is taken by malware, it can be returned as result.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case DOWNLOADS_ID_CODE:
            return sDownloadCursor;

        case ADDRESSES_CODE:
        case ADDRESSES_ID_CODE:
            return sAddressCursor;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Uri insert(Uri uri, ContentValues values) {

        // *** POINT 2 *** Handle the received request data carefully and securely.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 3 *** When returning a result, do not include sensitive information.
        // It depends on application whether the issued ID has sensitive meaning or not.
        // If no problem when the information is taken by malware, it can be returned as result.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return ContentUris.withAppendedId(Download.CONTENT_URI, 3);

        case ADDRESSES_CODE:
            return ContentUris.withAppendedId(Address.CONTENT_URI, 4);

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int update(Uri uri, ContentValues values, String selection,
            String[] selectionArgs) {

        // *** POINT 2 *** Handle the received request data carefully and securely.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
```

```
 case.
       // Checking for other parameters are omitted here, due to sample.
       // Refer to "3.2 Handle Input Data Carefully and Securely."

       // *** POINT 3 *** When returning a result, do not include sensitive information.
       // It depends on application whether the number of updated records has sensitive meaning or not.
       // If no problem when the information is taken by malware, it can be returned as result.
       switch (sUriMatcher.match(uri)) {
       case DOWNLOADS_CODE:
           return 5;   // Return number of updated records

       case DOWNLOADS_ID_CODE:
           return 1;

       case ADDRESSES_CODE:
           return 15;

       case ADDRESSES_ID_CODE:
           return 1;

       default:
           throw new IllegalArgumentException("Invalid URI:" + uri);
       }
   }

   @Override
   public int delete(Uri uri, String selection, String[] selectionArgs) {

       // *** POINT 2 *** Handle the received request data carefully and securely.
       // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
       // Checking for other parameters are omitted here, due to sample.
       // Refer to "3.2 Handle Input Data Carefully and Securely."

       // *** POINT 3 *** When returning a result, do not include sensitive information.
       // It depends on application whether the number of deleted records has sensitive meaning or not.
       // If no problem when the information is taken by malware, it can be returned as result.
       switch (sUriMatcher.match(uri)) {
       case DOWNLOADS_CODE:
           return 10;  // Return number of deleted records

       case DOWNLOADS_ID_CODE:
           return 1;

       case ADDRESSES_CODE:
           return 20;

       case ADDRESSES_ID_CODE:
           return 1;

       default:
           throw new IllegalArgumentException("Invalid URI:" + uri);
       }
   }
}
```


Next is an example of Activity which uses Public Content Provider.

Points (Using a Content Provider):

4. Do not send sensitive information.
5. When receiving a result, handle the result data carefully and securely.

PublicUserActivity.java

```
package org.jssec.android.provider.publicuser;

import android.app.Activity;
import android.content.ContentValues;
import android.content.pm.ProviderInfo;
import android.database.Cursor;
import android.net.Uri;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PublicUserActivity extends Activity {

    // Target Content Provider Information
    private static final String AUTHORITY = "org.jssec.android.provider.publicprovider";
    private interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }

    public void onQueryClick(View view) {

        logLine("[Query]");

        if (!providerExists(Address.CONTENT_URI)) {
            logLine("  Content Provider doesn't exist.");
            return;
        }

        Cursor cursor = null;
        try {
            // *** POINT 4 *** Do not send sensitive information.
            // since the target Content Provider may be malware.
            // If no problem when the information is taken by malware, it can be included in the request.
            cursor = getContentResolver().query(Address.CONTENT_URI, null, null, null, null);

            // *** POINT 5 *** When receiving a result, handle the result data carefully and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            if (cursor == null) {
                logLine("  null cursor");
            } else {
                boolean moved = cursor.moveToFirst();
                while (moved) {
                    logLine(String.format("  %d, %s", cursor.getInt(0), cursor.getString(1)));
                    moved = cursor.moveToNext();
                }
            }
        }
        finally {
            if (cursor != null) cursor.close();
```

```
        }
    }

    public void onInsertClick(View view) {

        logLine("[Insert]");

        if (!providerExists(Address.CONTENT_URI)) {
            logLine("  Content Provider doesn't exist.");
            return;
        }

        // *** POINT 4 *** Do not send sensitive information.
        // since the target Content Provider may be malware.
        // If no problem when the information is taken by malware, it can be included in the request.
        ContentValues values = new ContentValues();
        values.put("city", "Tokyo");
        Uri uri = getContentResolver().insert(Address.CONTENT_URI, values);

        // *** POINT 5 *** When receiving a result, handle the result data carefully and securely.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine("  uri:" + uri);
    }

    public void onUpdateClick(View view) {

        logLine("[Update]");

        if (!providerExists(Address.CONTENT_URI)) {
            logLine("  Content Provider doesn't exist.");
            return;
        }

        // *** POINT 4 *** Do not send sensitive information.
        // since the target Content Provider may be malware.
        // If no problem when the information is taken by malware, it can be included in the request.
        ContentValues values = new ContentValues();
        values.put("city", "Tokyo");
        String where = "_id = ?";
        String[] args = { "4" };
        int count = getContentResolver().update(Address.CONTENT_URI, values, where, args);

        // *** POINT 5 *** When receiving a result, handle the result data carefully and securely.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine(String.format("  %s records updated", count));
    }

    public void onDeleteClick(View view) {

        logLine("[Delete]");

        if (!providerExists(Address.CONTENT_URI)) {
            logLine("  Content Provider doesn't exist.");
            return;
        }

        // *** POINT 4 *** Do not send sensitive information.
        // since the target Content Provider may be malware.
```



```
        // If no problem when the information is taken by malware, it can be included in the request.
        int count = getContentResolver().delete(Address.CONTENT_URI, null, null);

        // *** POINT 5 *** When receiving a result, handle the result data carefully and securely.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine(String.format("  %s records deleted", count));
    }

    private boolean providerExists(Uri uri) {
        ProviderInfo pi = getPackageManager().resolveContentProvider(uri.getAuthority(), 0);
        return (pi != null);
    }

    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView)findViewById(R.id.logview);
    }

    private void logLine(String line) {
        mLogView.append(line);
        mLogView.append("¥n");
    }
}
```

4.3.1.3. Creating/Using Partner Content Providers

Partner Content Provider is the Content Provider which can be used only by the particular applications. The system consists of a partner company's application and In-house application, and it is used to protect the information and features which are handled between a partner application and an In-house application.

Sample code to implement a partner-only Content Provider is shown below.

Points (Creating a Content Provider):

1. Explicitly set the exported attribute to true.
2. Verify if the certificate of a requesting application has been registered in the own white list.
3. Handle the received request data carefully and securely, even though the data comes from a partner application.
4. Information that is granted to disclose to partner applications can be returned.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.provider.partnerprovider">

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- *** POINT 1 *** Explicitly set the exported attribute to true. -->
        <provider
            android:name=".PartnerProvider"
            android:authorities="org.jssec.android.provider.partnerprovider"
            android:exported="true" />
    </application>
</manifest>
```

PartnerProvider.java

```
package org.jssec.android.provider.partnerprovider;

import java.util.List;

import org.jssec.android.shared.PkgCertWhitelists;
import org.jssec.android.shared.Utils;

import android.app.ActivityManager;
import android.app.ActivityManager.RunningAppProcessInfo;
import android.content.ContentProvider;
import android.content.ContentUris;
import android.content.ContentValues;
import android.content.Context;
import android.content.UriMatcher;
import android.database.Cursor;
import android.database.MatrixCursor;
import android.net.Uri;
import android.os.Binder;
```



```
import android.os.Build;

public class PartnerProvider extends ContentProvider {

    public static final String AUTHORITY = "org.jssec.android.provider.partnerprovider";
    public static final String CONTENT_TYPE = "vnd.android.cursor.dir/vnd.org.jssec.contenttype";
    public static final String CONTENT_ITEM_TYPE = "vnd.android.cursor.item/vnd.org.jssec.contenttype";

    // Expose the interface that the Content Provider provides.
    public interface Download {
        public static final String PATH = "downloads";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }
    public interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }

    // UriMatcher
    private static final int DOWNLOADS_CODE = 1;
    private static final int DOWNLOADS_ID_CODE = 2;
    private static final int ADDRESSES_CODE = 3;
    private static final int ADDRESSES_ID_CODE = 4;
    private static UriMatcher sUriMatcher;
    static {
        sUriMatcher = new UriMatcher(UriMatcher.NO_MATCH);
        sUriMatcher.addURI(AUTHORITY, Download.PATH, DOWNLOADS_CODE);
        sUriMatcher.addURI(AUTHORITY, Download.PATH + "/#", DOWNLOADS_ID_CODE);
        sUriMatcher.addURI(AUTHORITY, Address.PATH, ADDRESSES_CODE);
        sUriMatcher.addURI(AUTHORITY, Address.PATH + "/#", ADDRESSES_ID_CODE);
    }

    // Since this is a sample program,
    // query method returns the following fixed result always without using database.
    private static MatrixCursor sAddressCursor = new MatrixCursor(new String[] { "_id", "city" });
    static {
        sAddressCursor.addRow(new String[] { "1", "New York" });
        sAddressCursor.addRow(new String[] { "2", "London" });
        sAddressCursor.addRow(new String[] { "3", "Paris" });
    }
    private static MatrixCursor sDownloadCursor = new MatrixCursor(new String[] { "_id", "path" });
    static {
        sDownloadCursor.addRow(new String[] { "1", "/sdcard/downloads/sample.jpg" });
        sDownloadCursor.addRow(new String[] { "2", "/sdcard/downloads/sample.txt" });
    }

    // *** POINT 2 *** Verify if the certificate of a requesting application has been registered in the
own white list.
    private static PkgCertWhitelists sWhitelists = null;
    private static void buildWhitelists(Context context) {
        boolean isdebug = Utils.isDebuggable(context);
        sWhitelists = new PkgCertWhitelists();

        // Register certificate hash value of partner application org.jssec.android.provider.partneruser
.
        sWhitelists.add("org.jssec.android.provider.partneruser", isdebug ?
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255" :
                // Certificate hash value of "partner key" in the keystore.
                "1F039BB5 7861C27A 3916C778 8E78CE00 690B3974 3EB8259F E2627B8D 4C0EC35A");
```

```
        // Register following other partner applications in the same way.
    }
    private static boolean checkPartner(Context context, String pkgname) {
        if (sWhitelists == null) buildWhitelists(context);
        return sWhitelists.test(context, pkgname);
    }
    // Get the package name of the calling application.
    private String getCallingPackage(Context context) {
        String pkgname;
        if (Build.VERSION.SDK_INT >= Build.VERSION_CODES.KITKAT) {
            pkgname = super.getCallingPackage();
        } else {
            pkgname = null;
            ActivityManager am = (ActivityManager) context.getSystemService(Context.ACTIVITY_SERVICE);
            List<RunningAppProcessInfo> procList = am.getRunningAppProcesses();
            int callingPid = Binder.getCallingPid();
            if (procList != null) {
                for (RunningAppProcessInfo proc : procList) {
                    if (proc.pid == callingPid) {
                        pkgname = proc.pkgList[proc.pkgList.length - 1];
                        break;
                    }
                }
            }
        }
        return pkgname;
    }

    @Override
    public boolean onCreate() {
        return true;
    }

    @Override
    public String getType(Uri uri) {

        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case ADDRESSES_CODE:
            return CONTENT_TYPE;

        case DOWNLOADS_ID_CODE:
        case ADDRESSES_ID_CODE:
            return CONTENT_ITEM_TYPE;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Cursor query(Uri uri, String[] projection, String selection,
            String[] selectionArgs, String sortOrder) {

        // *** POINT 2 *** Verify if the certificate of a requesting application has been registered in t
he own white list.
        if (!checkPartner(getContext(), getCallingPackage(getContext()))) {
            throw new SecurityException("Calling application is not a partner application.");
        }
```



```
        // *** POINT 3 *** Handle the received request data carefully and securely,
        // even though the data comes from a partner application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 4 *** Information that is granted to disclose to partner applications can be returne
d.
        // It depends on application whether the query result can be disclosed or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case DOWNLOADS_ID_CODE:
            return sDownloadCursor;

        case ADDRESSES_CODE:
        case ADDRESSES_ID_CODE:
            return sAddressCursor;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Uri insert(Uri uri, ContentValues values) {

        // *** POINT 2 *** Verify if the certificate of a requesting application has been registered in t
he own white list.
        if (!checkPartner(getContext(), getCallingPackage(getContext()))) {
            throw new SecurityException("Calling application is not a partner application.");
        }

        // *** POINT 3 *** Handle the received request data carefully and securely,
        // even though the data comes from a partner application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 4 *** Information that is granted to disclose to partner applications can be returne
d.
        // It depends on application whether the issued ID has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return ContentUris.withAppendedId(Download.CONTENT_URI, 3);

        case ADDRESSES_CODE:
            return ContentUris.withAppendedId(Address.CONTENT_URI, 4);

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int update(Uri uri, ContentValues values, String selection,
            String[] selectionArgs) {
```

```
        // *** POINT 2 *** Verify if the certificate of a requesting application has been registered in t
he own white list.
        if (!checkPartner(getContext(), getCallingPackage(getContext()))) {
            throw new SecurityException("Calling application is not a partner application.");
        }

        // *** POINT 3 *** Handle the received request data carefully and securely,
        // even though the data comes from a partner application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 4 *** Information that is granted to disclose to partner applications can be returne
d.
        // It depends on application whether the number of updated records has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return 5;   // Return number of updated records

        case DOWNLOADS_ID_CODE:
            return 1;

        case ADDRESSES_CODE:
            return 15;

        case ADDRESSES_ID_CODE:
            return 1;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int delete(Uri uri, String selection, String[] selectionArgs) {

        // *** POINT 2 *** Verify if the certificate of a requesting application has been registered in t
he own white list.
        if (!checkPartner(getContext(), getCallingPackage(getContext()))) {
            throw new SecurityException("Calling application is not a partner application.");
        }

        // *** POINT 3 *** Handle the received request data carefully and securely,
        // even though the data comes from a partner application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 4 *** Information that is granted to disclose to partner applications can be returne
d.
        // It depends on application whether the number of deleted records has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return 10;  // Return number of deleted records

        case DOWNLOADS_ID_CODE:
            return 1;
```



```
        case ADDRESSES_CODE:
            return 20;

        case ADDRESSES_ID_CODE:
            return 1;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }
}
```

Next is an example of Activity which use partner only Content Provider.

Points (Using a Content Provider):

5. Verify if the certificate of the target application has been registered in the own white list.
6. Information that is granted to disclose to partner applications can be sent.
7. Handle the received result data carefully and securely, even though the data comes from a partner application.

PartnerActivity.java

```
package org.jssec.android.provider.partneruser;

import org.jssec.android.shared.PkgCertWhitelists;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.ContentValues;
import android.content.Context;
import android.content.pm.ProviderInfo;
import android.database.Cursor;
import android.net.Uri;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PartnerUserActivity extends Activity {

    // Target Content Provider Information
    private static final String AUTHORITY = "org.jssec.android.provider.partnerprovider";
    private interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }

    // *** POINT 4 *** Verify if the certificate of the target application has been registered in the ow
n white list.
    private static PkgCertWhitelists sWhitelists = null;
    private static void buildWhitelists(Context context) {
        boolean isdebug = Utils.isDebuggable(context);
        sWhitelists = new PkgCertWhitelists();

        // Register certificate hash value of partner application org.jssec.android.provider.partnerprov
ider.
        sWhitelists.add("org.jssec.android.provider.partnerprovider", isdebug ?
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255" :
                // Certificate hash value of "partner key" in the keystore.
                "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA");

        // Register following other partner applications in the same way.
    }
    private static boolean checkPartner(Context context, String pkgname) {
        if (sWhitelists == null) buildWhitelists(context);
        return sWhitelists.test(context, pkgname);
    }

    // Get package name of target content provider.
    private String providerPkgname(Uri uri) {
```



```
        String pkgname = null;
        ProviderInfo pi = getPackageManager().resolveContentProvider(uri.getAuthority(), 0);
        if (pi != null) pkgname = pi.packageName;
        return pkgname;
    }

    public void onQueryClick(View view) {

        logLine("[Query]");

        // *** POINT 4 *** Verify if the certificate of the target application has been registered in the
 own white list.
        if (!checkPartner(this, providerPkgname(Address.CONTENT_URI))) {
            logLine("  The target content provider is not served by partner applications.");
            return;
        }

        Cursor cursor = null;
        try {
            // *** POINT 5 *** Information that is granted to disclose to partner applications can be sen
t.
            cursor = getContentResolver().query(Address.CONTENT_URI, null, null, null, null);

            // *** POINT 6 *** Handle the received result data carefully and securely,
            // even though the data comes from a partner application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            if (cursor == null) {
                logLine("  null cursor");
            } else {
                boolean moved = cursor.moveToFirst();
                while (moved) {
                    logLine(String.format("  %d, %s", cursor.getInt(0), cursor.getString(1)));
                    moved = cursor.moveToNext();
                }
            }
        }
        finally {
            if (cursor != null) cursor.close();
        }
    }

    public void onInsertClick(View view) {

        logLine("[Insert]");

        // *** POINT 4 *** Verify if the certificate of the target application has been registered in the
 own white list.
        if (!checkPartner(this, providerPkgname(Address.CONTENT_URI))) {
            logLine("  The target content provider is not served by partner applications.");
            return;
        }

        // *** POINT 5 *** Information that is granted to disclose to partner applications can be sent.
        ContentValues values = new ContentValues();
        values.put("city", "Tokyo");
        Uri uri = getContentResolver().insert(Address.CONTENT_URI, values);

        // *** POINT 6 *** Handle the received result data carefully and securely,
        // even though the data comes from a partner application.
```

```
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine("  uri:" + uri);
    }

    public void onUpdateClick(View view) {

        logLine("[Update]");

        // *** POINT 4 *** Verify if the certificate of the target application has been registered in the
 own white list.
        if (!checkPartner(this, providerPkgname(Address.CONTENT_URI))) {
            logLine("  The target content provider is not served by partner applications.");
            return;
        }

        // *** POINT 5 *** Information that is granted to disclose to partner applications can be sent.
        ContentValues values = new ContentValues();
        values.put("city", "Tokyo");
        String where = "_id = ?";
        String[] args = { "4" };
        int count = getContentResolver().update(Address.CONTENT_URI, values, where, args);

        // *** POINT 6 *** Handle the received result data carefully and securely,
        // even though the data comes from a partner application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine(String.format("  %s records updated", count));
    }

    public void onDeleteClick(View view) {

        logLine("[Delete]");

        // *** POINT 4 *** Verify if the certificate of the target application has been registered in the
 own white list.
        if (!checkPartner(this, providerPkgname(Address.CONTENT_URI))) {
            logLine("  The target content provider is not served by partner applications.");
            return;
        }

        // *** POINT 5 *** Information that is granted to disclose to partner applications can be sent.
        int count = getContentResolver().delete(Address.CONTENT_URI, null, null);

        // *** POINT 6 *** Handle the received result data carefully and securely,
        // even though the data comes from a partner application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine(String.format("  %s records deleted", count));
    }

    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView)findViewById(R.id.logview);
    }
```



```
    private void logLine(String line) {
        mLogView.append(line);
        mLogView.append("¥n");
    }
}
```

PkgCertWhitelists.java

```
package org.jssec.android.shared;

import java.util.HashMap;
import java.util.Map;

import android.content.Context;

public class PkgCertWhitelists {
    private Map<String, String> mWhitelists = new HashMap<String, String>();

    public boolean add(String pkgname, String sha256) {
        if (pkgname == null) return false;
        if (sha256 == null) return false;

        sha256 = sha256.replaceAll(" ", "");
        if (sha256.length() != 64) return false;    // SHA-256 -> 32 bytes -> 64 chars
        sha256 = sha256.toUpperCase();
        if (sha256.replaceAll("[0-9A-F]+", "").length() != 0) return false; // found non hex char

        mWhitelists.put(pkgname, sha256);
        return true;
    }

    public boolean test(Context ctx, String pkgname) {
        // Get the correct hash value which corresponds to pkgname.
        String correctHash = mWhitelists.get(pkgname);

        // Compare the actual hash value of pkgname with the correct hash value.
        return PkgCert.test(ctx, pkgname, correctHash);
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
```

```
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


4.3.1.4. Creating/Using In-house Content Providers

In-house Content Provider is the Content Provider which prohibits to be used by applications other than In house only applications.

Sample code of how to implement an In house only Content Provider is shown below.

Points (Creating a Content Provider):

1. Define an in-house signature permission.
2. Require the in-house signature permission.
3. Explicitly set the exported attribute to true.
4. Verify if the in-house signature permission is defined by an in-house application.
5. Verify the safety of the parameter even if it's a request from In house only application.
6. Sensitive information can be returned since the requesting application is in-house.
7. When exporting an APK, sign the APK with the same developer key as that of the requesting application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.provider.inhouseprovider">

    <!-- *** POINT 1 *** Define an in-house signature permission -->
    <permission
        android:name="org.jssec.android.provider.inhouseprovider.MY_PERMISSION"
        android:protectionLevel="signature" />

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- *** POINT 2 *** Require the in-house signature permission -->
        <!-- *** POINT 3 *** Explicitly set the exported attribute to true. -->
        <provider
            android:name=".InhouseProvider"
            android:authorities="org.jssec.android.provider.inhouseprovider"
            android:permission="org.jssec.android.provider.inhouseprovider.MY_PERMISSION"
            android:exported="true" />
    </application>
</manifest>
```

InhouseProvider.java

```
package org.jssec.android.provider.inhouseprovider;

import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.content.ContentProvider;
import android.content.ContentUris;
import android.content.ContentValues;
import android.content.Context;
import android.content.UriMatcher;
```

```
import android.database.Cursor;
import android.database.MatrixCursor;
import android.net.Uri;

public class InhouseProvider extends ContentProvider {

    public static final String AUTHORITY = "org.jssec.android.provider.inhouseprovider";
    public static final String CONTENT_TYPE = "vnd.android.cursor.dir/vnd.org.jssec.contenttype";
    public static final String CONTENT_ITEM_TYPE = "vnd.android.cursor.item/vnd.org.jssec.contenttype";

    // Expose the interface that the Content Provider provides.
    public interface Download {
        public static final String PATH = "downloads";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }
    public interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }

    // UriMatcher
    private static final int DOWNLOADS_CODE = 1;
    private static final int DOWNLOADS_ID_CODE = 2;
    private static final int ADDRESSES_CODE = 3;
    private static final int ADDRESSES_ID_CODE = 4;
    private static UriMatcher sUriMatcher;
    static {
        sUriMatcher = new UriMatcher(UriMatcher.NO_MATCH);
        sUriMatcher.addURI(AUTHORITY, Download.PATH, DOWNLOADS_CODE);
        sUriMatcher.addURI(AUTHORITY, Download.PATH + "/#", DOWNLOADS_ID_CODE);
        sUriMatcher.addURI(AUTHORITY, Address.PATH, ADDRESSES_CODE);
        sUriMatcher.addURI(AUTHORITY, Address.PATH + "/#", ADDRESSES_ID_CODE);
    }

    // Since this is a sample program,
    // query method returns the following fixed result always without using database.
    private static MatrixCursor sAddressCursor = new MatrixCursor(new String[] { "_id", "city" });
    static {
        sAddressCursor.addRow(new String[] { "1", "New York" });
        sAddressCursor.addRow(new String[] { "2", "London" });
        sAddressCursor.addRow(new String[] { "3", "Paris" });
    }
    private static MatrixCursor sDownloadCursor = new MatrixCursor(new String[] { "_id", "path" });
    static {
        sDownloadCursor.addRow(new String[] { "1", "/sdcard/downloads/sample.jpg" });
        sDownloadCursor.addRow(new String[] { "2", "/sdcard/downloads/sample.txt" });
    }

    // In-house Signature Permission
    private static final String MY_PERMISSION = "org.jssec.android.provider.inhouseprovider.MY_PERMISSI
ON";

    // In-house certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
```



```
                // Certificate hash value of "my company key" in the keystore.
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    @Override
    public boolean onCreate() {
        return true;
    }

    @Override
    public String getType(Uri uri) {

        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case ADDRESSES_CODE:
            return CONTENT_TYPE;

        case DOWNLOADS_ID_CODE:
        case ADDRESSES_ID_CODE:
            return CONTENT_ITEM_TYPE;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Cursor query(Uri uri, String[] projection, String selection,
            String[] selectionArgs, String sortOrder) {

        // *** POINT 4 *** Verify if the in-house signature permission is defined by an in-house applicat
ion.
        if (!SigPerm.test(getContext(), MY_PERMISSION, myCertHash(getContext()))) {
            throw new SecurityException("The in-house signature permission is not declared by in-house a
pplication.");
        }

        // *** POINT 5 *** Handle the received request data carefully and securely,
        // even though the data came from an in-house application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 6 *** Sensitive information can be returned since the requesting application is in-
house.
        // It depends on application whether the query result has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case DOWNLOADS_ID_CODE:
            return sDownloadCursor;

        case ADDRESSES_CODE:
        case ADDRESSES_ID_CODE:
            return sAddressCursor;

        default:
```

```
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Uri insert(Uri uri, ContentValues values) {

        // *** POINT 4 *** Verify if the in-house signature permission is defined by an in-house applicat
ion.
        if (!SigPerm.test(getContext(), MY_PERMISSION, myCertHash(getContext()))) {
            throw new SecurityException("The in-house signature permission is not declared by in-house a
pplication.");
        }

        // *** POINT 5 *** Handle the received request data carefully and securely,
        // even though the data came from an in-house application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 6 *** Sensitive information can be returned since the requesting application is in-
house.
        // It depends on application whether the issued ID has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return ContentUris.withAppendedId(Download.CONTENT_URI, 3);

        case ADDRESSES_CODE:
            return ContentUris.withAppendedId(Address.CONTENT_URI, 4);

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int update(Uri uri, ContentValues values, String selection,
            String[] selectionArgs) {

        // *** POINT 4 *** Verify if the in-house signature permission is defined by an in-house applicat
ion.
        if (!SigPerm.test(getContext(), MY_PERMISSION, myCertHash(getContext()))) {
            throw new SecurityException("The in-house signature permission is not declared by in-house a
pplication.");
        }

        // *** POINT 5 *** Handle the received request data carefully and securely,
        // even though the data came from an in-house application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 6 *** Sensitive information can be returned since the requesting application is in-
house.
        // It depends on application whether the number of updated records has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return 5;   // Return number of updated records
```



```
        case DOWNLOADS_ID_CODE:
            return 1;

        case ADDRESSES_CODE:
            return 15;

        case ADDRESSES_ID_CODE:
            return 1;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int delete(Uri uri, String selection, String[] selectionArgs) {

        // *** POINT 4 *** Verify if the in-house signature permission is defined by an in-house applicat
ion.
        if (!SigPerm.test(getContext(), MY_PERMISSION, myCertHash(getContext()))) {
            throw new SecurityException("The in-house signature permission is not declared by in-house a
pplication.");
        }

        // *** POINT 5 *** Handle the received request data carefully and securely,
        // even though the data came from an in-house application.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 6 *** Sensitive information can be returned since the requesting application is in-
house.
        // It depends on application whether the number of deleted records has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return 10;  // Return number of deleted records

        case DOWNLOADS_ID_CODE:
            return 1;

        case ADDRESSES_CODE:
            return 20;

        case ADDRESSES_ID_CODE:
            return 1;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }
}
```

SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
```

```
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;

            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
```



```
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```

*** Point 7 *** When exporting an APK, sign the APK with the same developer key as the requesting application.

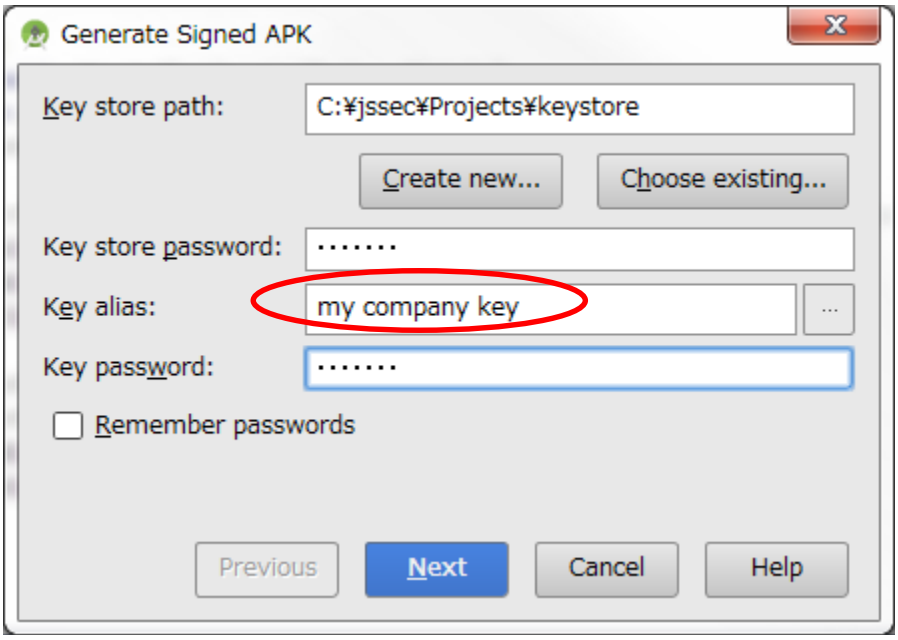


Figure 4.3-2

Next is the example of Activity which uses In house only Content Provider.

Point (Using a Content Provider):

8. Declare to use the in-house signature permission.
9. Verify if the in-house signature permission is defined by an in-house application.
10. Verify if the destination application is signed with the in-house certificate.
11. Sensitive information can be sent since the destination application is in-house one.
12. Handle the received result data carefully and securely, even though the data comes from an in-house application.
13. When exporting an APK, sign the APK with the same developer key as that of the destination application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.provider.inhouseuser">

    <!-- *** POINT 8 *** Declare to use the in-house signature permission. -->
    <uses-permission
        android:name="org.jssec.android.provider.inhouseprovider.MY_PERMISSION" />

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >
        <activity
            android:name=".InhouseUserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

InhouseUserActivity.java

```
package org.jssec.android.provider.inhouseuser;

import org.jssec.android.shared.PkgCert;
import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.ContentValues;
import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.ProviderInfo;
import android.database.Cursor;
import android.net.Uri;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;
```



```
public class InhouseUserActivity extends Activity {

    // Target Content Provider Information
    private static final String AUTHORITY = "org.jssec.android.provider.inhouseprovider";
    private interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }

    // In-house Signature Permission
    private static final String MY_PERMISSION = "org.jssec.android.provider.inhouseprovider.MY_PERMISSI
ON";

    // In-house certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" in the debug.keystore.
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of "my company key" in the keystore.
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    // Get package name of target content provider.
    private static String providerPkgname(Context context, Uri uri) {
        String pkgname = null;
        PackageManager pm = context.getPackageManager();
        ProviderInfo pi = pm.resolveContentProvider(uri.getAuthority(), 0);
        if (pi != null) pkgname = pi.packageName;
        return pkgname;
    }

    public void onQueryClick(View view) {

        logLine("[Query]");

        // *** POINT 9 *** Verify if the in-house signature permission is defined by an in-house applicat
ion.
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            logLine("  The in-house signature permission is not declared by in-house application.");
            return;
        }

        // *** POINT 10 *** Verify if the destination application is signed with the in-house certificat
e.
        String pkgname = providerPkgname(this, Address.CONTENT_URI);
        if (!PkgCert.test(this, pkgname, myCertHash(this))) {
            logLine("  The target content provider is not served by in-house applications.");
            return;
        }

        Cursor cursor = null;
        try {
            // *** POINT 11 *** Sensitive information can be sent since the destination application is in
-house one.
```

```
            cursor = getContentResolver().query(Address.CONTENT_URI, null, null, null, null);

            // *** POINT 12 *** Handle the received result data carefully and securely,
            // even though the data comes from an in-house application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            if (cursor == null) {
                logLine("  null cursor");
            } else {
                boolean moved = cursor.moveToFirst();
                while (moved) {
                    logLine(String.format("  %d, %s", cursor.getInt(0), cursor.getString(1)));
                    moved = cursor.moveToNext();
                }
            }
        }
        finally {
            if (cursor != null) cursor.close();
        }
    }

    public void onInsertClick(View view) {

        logLine("[Insert]");

        // *** POINT 9 *** Verify if the in-house signature permission is defined by an in-house applicat
ion.
        String correctHash = myCertHash(this);
        if (!SigPerm.test(this, MY_PERMISSION, correctHash)) {
            logLine("  The in-house signature permission is not declared by in-house application.");
            return;
        }

        // *** POINT 10 *** Verify if the destination application is signed with the in-house certificat
e.
        String pkgname = providerPkgname(this, Address.CONTENT_URI);
        if (!PkgCert.test(this, pkgname, correctHash)) {
            logLine("  The target content provider is not served by in-house applications.");
            return;
        }

        // *** POINT 11 *** Sensitive information can be sent since the destination application is in-ho
use one.
        ContentValues values = new ContentValues();
        values.put("city", "Tokyo");
        Uri uri = getContentResolver().insert(Address.CONTENT_URI, values);

        // *** POINT 12 *** Handle the received result data carefully and securely,
        // even though the data comes from an in-house application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine("  uri:" + uri);
    }

    public void onUpdateClick(View view) {

        logLine("[Update]");

        // *** POINT 9 *** Verify if the in-house signature permission is defined by an in-house applicat
ion.
```



```
        String correctHash = myCertHash(this);
        if (!SigPerm.test(this, MY_PERMISSION, correctHash)) {
            logLine("  The in-house signature permission is not declared by in-house application.");
            return;
        }

        // *** POINT 10 *** Verify if the destination application is signed with the in-house certificat
e.
        String pkgname = providerPkgname(this, Address.CONTENT_URI);
        if (!PkgCert.test(this, pkgname, correctHash)) {
            logLine("  The target content provider is not served by in-house applications.");
            return;
        }

        // *** POINT 11 *** Sensitive information can be sent since the destination application is in-ho
use one.
        ContentValues values = new ContentValues();
        values.put("city", "Tokyo");
        String where = "_id = ?";
        String[] args = { "4" };
        int count = getContentResolver().update(Address.CONTENT_URI, values, where, args);

        // *** POINT 12 *** Handle the received result data carefully and securely,
        // even though the data comes from an in-house application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine(String.format("  %s records updated", count));
    }

    public void onDeleteClick(View view) {

        logLine("[Delete]");

        // *** POINT 9 *** Verify if the in-house signature permission is defined by an in-house applicat
ion.
        String correctHash = myCertHash(this);
        if (!SigPerm.test(this, MY_PERMISSION, correctHash)) {
            logLine("  The target content provider is not served by in-house applications.");
            return;
        }

        // *** POINT 10 *** Verify if the destination application is signed with the in-house certificat
e.
        String pkgname = providerPkgname(this, Address.CONTENT_URI);
        if (!PkgCert.test(this, pkgname, correctHash)) {
            logLine("  The target content provider is not served by in-house applications.");
            return;
        }

        // *** POINT 11 *** Sensitive information can be sent since the destination application is in-ho
use one.
        int count = getContentResolver().delete(Address.CONTENT_URI, null, null);

        // *** POINT 12 *** Handle the received result data carefully and securely,
        // even though the data comes from an in-house application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        logLine(String.format("  %s records deleted", count));
    }
```

```
    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView)findViewById(R.id.logview);
    }

    private void logLine(String line) {
        mLogView.append(line);
        mLogView.append("¥n");
    }
}
```

SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;

            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```


PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```

*** Point 13 *** When exporting an APK, sign the APK with the same developer key as that of the destination application.

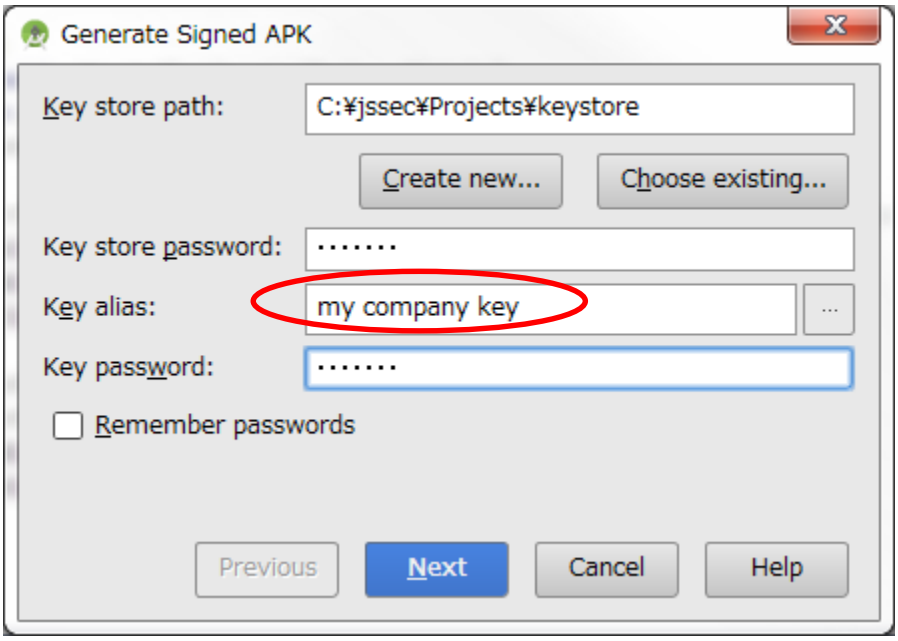


Figure 4.3-3

4.3.1.5. Creating/Using Temporary permit Content Providers

Temporary permit Content Provider is basically a private Content Provider, but this permits the particular applications to access the particular URI. By sending an Intent which special flag is specified to the target applications, temporary access permission is provided to those applications. Contents provider side application can give the access permission actively to other applications, and it can also give access permission passively to the application which claims the temporary access permission.

Sample code of how to implement a temporary permit Content Provider is shown below.

Points (Creating a Content Provider):

1. Explicitly set the exported attribute to false.
2. Specify the path to grant access temporarily with the grant-uri-permission.
3. Handle the received request data carefully and securely, even though the data comes from the application granted access temporarily.
4. Information that is granted to disclose to the temporary access applications can be returned.
5. Specify URI for the intent to grant temporary access.
6. Specify access rights for the intent to grant temporary access.
7. Send the explicit intent to an application to grant temporary access.
8. Return the intent to the application that requests temporary access.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.provider.temporaryprovider">

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <activity
            android:name=".TemporaryActiveGrantActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

        <!-- Temporary Content Provider -->
        <!-- *** POINT 1 *** Explicitly set the exported attribute to false. -->
        <provider
            android:name=".TemporaryProvider"
            android:authorities="org.jssec.android.provider.temporaryprovider"
            android:exported="false" >

            <!-- *** POINT 2 *** Specify the path to grant access temporarily with the grant-uri-permissi
on. -->
            <grant-uri-permission android:path="/addresses" />
```

```
        </provider>

        <activity
            android:name=".TemporaryPassiveGrantActivity"
            android:label="@string/app_name"
            android:exported="true" />
    </application>
</manifest>
```

TemporaryProvider.java

```
package org.jssec.android.provider.temporaryprovider;

import android.content.ContentProvider;
import android.content.ContentUris;
import android.content.ContentValues;
import android.content.UriMatcher;
import android.database.Cursor;
import android.database.MatrixCursor;
import android.net.Uri;

public class TemporaryProvider extends ContentProvider {
    public static final String AUTHORITIY = "org.jssec.android.provider.temporaryprovider";
    public static final String CONTENT_TYPE = "vnd.android.cursor.dir/vnd.org.jssec.contenttype";
    public static final String CONTENT_ITEM_TYPE = "vnd.android.cursor.item/vnd.org.jssec.contenttype";

    // Expose the interface that the Content Provider provides.
    public interface Download {
        public static final String PATH = "downloads";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITIY + "/" + PATH);
    }
    public interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITIY + "/" + PATH);
    }

    // UriMatcher
    private static final int DOWNLOADS_CODE = 1;
    private static final int DOWNLOADS_ID_CODE = 2;
    private static final int ADDRESSES_CODE = 3;
    private static final int ADDRESSES_ID_CODE = 4;
    private static UriMatcher sUriMatcher;
    static {
        sUriMatcher = new UriMatcher(UriMatcher.NO_MATCH);
        sUriMatcher.addURI(AUTHORITIY, Download.PATH, DOWNLOADS_CODE);
        sUriMatcher.addURI(AUTHORITIY, Download.PATH + "/#", DOWNLOADS_ID_CODE);
        sUriMatcher.addURI(AUTHORITIY, Address.PATH, ADDRESSES_CODE);
        sUriMatcher.addURI(AUTHORITIY, Address.PATH + "/#", ADDRESSES_ID_CODE);
    }

    // Since this is a sample program,
    // query method returns the following fixed result always without using database.
    private static MatrixCursor sAddressCursor = new MatrixCursor(new String[] { "_id", "city" });
    static {
        sAddressCursor.addRow(new String[] { "1", "New York" });
        sAddressCursor.addRow(new String[] { "2", "London" });
        sAddressCursor.addRow(new String[] { "3", "Paris" });
    }
    private static MatrixCursor sDownloadCursor = new MatrixCursor(new String[] { "_id", "path" });
```



```
    static {
        sDownloadCursor.addRow(new String[] { "1", "/sdcard/downloads/sample.jpg" });
        sDownloadCursor.addRow(new String[] { "2", "/sdcard/downloads/sample.txt" });
    }

    @Override
    public boolean onCreate() {
        return true;
    }

    @Override
    public String getType(Uri uri) {

        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case ADDRESSES_CODE:
            return CONTENT_TYPE;

        case DOWNLOADS_ID_CODE:
        case ADDRESSES_ID_CODE:
            return CONTENT_ITEM_TYPE;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Cursor query(Uri uri, String[] projection, String selection,
            String[] selectionArgs, String sortOrder) {

        // *** POINT 3 *** Handle the received request data carefully and securely,
        // even though the data comes from the application granted access temporarily.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Please refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 4 *** Information that is granted to disclose to the temporary access applications c
an be returned.
        // It depends on application whether the query result can be disclosed or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
        case DOWNLOADS_ID_CODE:
            return sDownloadCursor;

        case ADDRESSES_CODE:
        case ADDRESSES_ID_CODE:
            return sAddressCursor;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public Uri insert(Uri uri, ContentValues values) {

        // *** POINT 3 *** Handle the received request data carefully and securely,
        // even though the data comes from the application granted access temporarily.
```

```
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Please refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 4 *** Information that is granted to disclose to the temporary access applications c
an be returned.
        // It depends on application whether the issued ID has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return ContentUris.withAppendedId(Download.CONTENT_URI, 3);

        case ADDRESSES_CODE:
            return ContentUris.withAppendedId(Address.CONTENT_URI, 4);

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int update(Uri uri, ContentValues values, String selection,
            String[] selectionArgs) {

        // *** POINT 3 *** Handle the received request data carefully and securely,
        // even though the data comes from the application granted access temporarily.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
        // Please refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 4 *** Information that is granted to disclose to the temporary access applications c
an be returned.
        // It depends on application whether the number of updated records has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return 5;   // Return number of updated records

        case DOWNLOADS_ID_CODE:
            return 1;

        case ADDRESSES_CODE:
            return 15;

        case ADDRESSES_ID_CODE:
            return 1;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }

    @Override
    public int delete(Uri uri, String selection, String[] selectionArgs) {

        // *** POINT 3 *** Handle the received request data carefully and securely,
        // even though the data comes from the application granted access temporarily.
        // Here, whether uri is within expectations or not, is verified by UriMatcher#match() and switch
 case.
        // Checking for other parameters are omitted here, due to sample.
```



```
        // Please refer to "3.2 Handle Input Data Carefully and Securely."

        // *** POINT 4 *** Information that is granted to disclose to the temporary access applications c
an be returned.
        // It depends on application whether the number of deleted records has sensitive meaning or not.
        switch (sUriMatcher.match(uri)) {
        case DOWNLOADS_CODE:
            return 10;  // Return number of deleted records

        case DOWNLOADS_ID_CODE:
            return 1;

        case ADDRESSES_CODE:
            return 20;

        case ADDRESSES_ID_CODE:
            return 1;

        default:
            throw new IllegalArgumentException("Invalid URI:" + uri);
        }
    }
}
```

TemporaryActiveGrantActivity.java

```
package org.jssec.android.provider.temporaryprovider;

import android.app.Activity;
import android.content.ActivityNotFoundException;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class TemporaryActiveGrantActivity extends Activity {

    // User Activity Information
    private static final String TARGET_PACKAGE =  "org.jssec.android.provider.temporaryuser";
    private static final String TARGET_ACTIVITY = "org.jssec.android.provider.temporaryuser.TemporaryUs
erActivity";

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.active_grant);
    }

    // In the case that Content Provider application grants access permission to other application activ
ely.
    public void onSendClick(View view) {
        try {
            Intent intent = new Intent();

            // *** POINT 5 *** Specify URI for the intent to grant temporary access.
            intent.setData(TemporaryProvider.Address.CONTENT_URI);

            // *** POINT 6 *** Specify access rights for the intent to grant temporary access.
            intent.setFlags(Intent.FLAG_GRANT_READ_URI_PERMISSION);
```

```
            // *** POINT 7 *** Send the explicit intent to an application to grant temporary access.
            intent.setClassName(TARGET_PACKAGE, TARGET_ACTIVITY);
            startActivity(intent);

        } catch (ActivityNotFoundException e) {
            Toast.makeText(this, "User Activity not found.", Toast.LENGTH_LONG).show();
        }
    }
}
```

TemporaryPassiveGrantActivity.java

```
package org.jssec.android.provider.temporaryprovider;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;

public class TemporaryPassiveGrantActivity extends Activity {
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.passive_grant);
    }

    // In the case that Content Provider application passively grants access permission
    // to the application that requested Content Provider access.
    public void onGrantClick(View view) {
        Intent intent = new Intent();

        // *** POINT 5 *** Specify URI for the intent to grant temporary access.
        intent.setData(TemporaryProvider.Address.CONTENT_URI);

        // *** POINT 6 *** Specify access rights for the intent to grant temporary access.
        intent.setFlags(Intent.FLAG_GRANT_READ_URI_PERMISSION);

        // *** POINT 8 *** Return the intent to the application that requests temporary access.
        setResult(Activity.RESULT_OK, intent);
        finish();
    }

    public void onCloseClick(View view) {
        finish();
    }
}
```


Next is the example of temporary permit Content Provider.

Points (Using a Content Provider):

9. Do not send sensitive information.
10. When receiving a result, handle the result data carefully and securely.

TemporaryUserActivity.java

```
package org.jssec.android.provider.temporaryuser;

import android.app.Activity;
import android.content.ActivityNotFoundException;
import android.content.Intent;
import android.content.pm.ProviderInfo;
import android.database.Cursor;
import android.net.Uri;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class TemporaryUserActivity extends Activity {

    // Information of the Content Provider's Activity to request temporary content provider access.
    private static final String TARGET_PACKAGE =  "org.jssec.android.provider.temporaryprovider";
    private static final String TARGET_ACTIVITY = "org.jssec.android.provider.temporaryprovider.Tempora
ryPassiveGrantActivity";

    // Target Content Provider Information
    private static final String AUTHORITY = "org.jssec.android.provider.temporaryprovider";
    private interface Address {
        public static final String PATH = "addresses";
        public static final Uri CONTENT_URI = Uri.parse("content://" + AUTHORITY + "/" + PATH);
    }

    private static final int REQUEST_CODE = 1;

    public void onQueryClick(View view) {

        logLine("[Query]");

        Cursor cursor = null;
        try {
            if (!providerExists(Address.CONTENT_URI)) {
                logLine("  Content Provider doesn't exist.");
                return;
            }

            // *** POINT 9 *** Do not send sensitive information.
            // If no problem when the information is taken by malware, it can be included in the request.
            cursor = getContentResolver().query(Address.CONTENT_URI, null, null, null, null);

            // *** POINT 10 *** When receiving a result, handle the result data carefully and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            if (cursor == null) {
                logLine("  null cursor");
            } else {
                boolean moved = cursor.moveToFirst();
                while (moved) {
```

```
                    logLine(String.format("  %d, %s", cursor.getInt(0), cursor.getString(1)));
                    moved = cursor.moveToNext();
                }
            }
        } catch (SecurityException ex) {
            logLine("  Exception:" + ex.getMessage());
        }
        finally {
            if (cursor != null) cursor.close();
        }
    }

    // In the case that this application requests temporary access to the Content Provider
    // and the Content Provider passively grants temporary access permission to this application.
    public void onGrantRequestClick(View view) {
        Intent intent = new Intent();
        intent.setClassName(TARGET_PACKAGE, TARGET_ACTIVITY);
        try {
            startActivityForResult(intent, REQUEST_CODE);
        } catch (ActivityNotFoundException e) {
            logLine("Content Provider's Activity not found.");
        }
    }

    private boolean providerExists(Uri uri) {
        ProviderInfo pi = getPackageManager().resolveContentProvider(uri.getAuthority(), 0);
        return (pi != null);
    }

    private TextView mLogView;

    // In the case that the Content Provider application grants temporary access
    // to this application actively.
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView)findViewById(R.id.logview);
    }

    private void logLine(String line) {
        mLogView.append(line);
        mLogView.append("¥n");
    }
}
```


4.3.2. Rule Book

Be sure to follow the rules below when Implementing or using a content provider.

1.	Content Provider that Is Used Only in an Application Must Be Set as Private (Required)
2.	
3.	Handle the Received Request Parameter Carefully and Securely (Required)
4.	Use an In-house Defined Signature Permission after Verifying that it is Defined by an In-house Application (Required)
5.	When Returning a Result, Pay Attention to the Possibility of Information Leakage of that Result from the Destination Application (Required)
6.	When Providing an Asset Secondarily, the Asset should be Protected with the Same Level of Protection (Required)

And user side should follow the below rules, too.

7.	Handle the Returned Result Data from the Content Provider Carefully and Securely (Required)

4.3.2.1. Content Provider that Is Used Only in an Application Must Be Set as Private (Required)

Content Provider which is used only in a single application is not necessary to be accessed by other applications, and the access which attacks the Content Provider is not often considered by developers. A Content Provider is basically the system to share data, so it's handled as public by default. A Content Provider which is used only in a single application should be set as private explicitly, and it should be a private Content Provider. In Android 2.3.1 (API Level 9) or later, a Content Provider can be set as private by specifying android:exported="false" in provider element.

AndroidManifest.xml

```
<!-- *** POINT 1 *** Set false for the exported attribute explicitly. -->
<provider
    android:name=".PrivateProvider"
    android:authorities="org.jssec.android.provider.privateprovider"
    android:exported="false" />
```

4.3.2.2. Handle the Received Request Parameter Carefully and Securely (Required)

Risks differ depending on the types of Content Providers, but when processing request parameters, the first thing you should do is input validation.

Although each method of a Content Provider has the interface which is supposed to receive the component parameter of SQL statement, actually it simply hands over the arbitrary character string in the system, so it's necessary to pay attention that Contents Provider side needs to suppose the case that unexpected parameter may be provided.

Since Public Content Providers can receive requests from untrusted sources, they can be attacked by

malware. On the other hand, Private Content Providers will never receive any requests from other applications directly, but it is possible that a Public Activity in the targeted application may forward a malicious Intent to a Private Content Provider so you should not assume that Private Content Providers cannot receive any malicious input.
Since other Content Providers also have the risk of a malicious intent being forwarded to them as well, it is necessary to perform input validation on these requests as well.
Please refer to "3.2 Handling Input Data Carefully and Securely"

4.3.2.3. Use an In-house Defined Signature Permission after Verifying that it is Defined by an In-house Application (Required)

Make sure to protect your in-house Content Providers by defining an in-house signature permission when creating the Content Provider. Since defining a permission in the AndroidManifest.xml file or declaring a permission request does not provide adequate security, please be sure to refer to "5.2.1.2 How to Communicate Between In-house Applications with In-house-defined Signature Permission."

4.3.2.4. When Returning a Result, Pay Attention to the Possibility of Information Leakage of that Result from the Destination Application (Required)

In case of query() or insert(), Cursor or Uri is returned to the request sending application as a result information. When sensitive information is included in the result information, the information may be leaked from the destination application. In case of update() or delete(), number of updated/deleted records is returned to the request sending application as a result information. In rare cases, depending on some application specs, the number of updated/deleted records has the sensitive meaning, so please pay attention to this.

4.3.2.5. When Providing an Asset Secondarily, the Asset should be Protected with the Same Level of Protection (Required)

When an information or function asset, which is protected by a permission, is provided to another application secondhand, you need to make sure that it has the same required permissions needed to access the asset. In the Android OS permission security model, only an application that has been granted proper permissions can directly access a protected asset. However, there is a loophole because an application with permissions to an asset can act as a proxy and allow access to an unprivileged application. Substantially this is the same as re-delegating a permission, so it is referred to as the "Permission Re-delegation" problem. Please refer to "5.2.3.4 Permission Re-delegation Problem."

4.3.2.6. Handle the Returned Result Data from the Content Provider Carefully and Securely (Required)

Risks differ depending on the types of Content Provider, but when processing a result data, the first thing you should do is input validation.

In case that the destination Content Provider is a public Content Provider, Malware which masquerades as the public Content Provider may return the attack result data. On the other hand, in case that the destination Content Provider is a private Content Provider, it is less risk because it receives the result data from the same application, but you should not assume that private Content Providers cannot receive any malicious input. Since other Content Providers also have the risk of a malicious data being returned to them as well, it is necessary to perform input validation on that result data as well.

Please refer to "3.2 Handling Input Data Carefully and Securely"

4.4.1. Sample Code

The risks and countermeasures of using Services differ depending on how that Service is being used. You can find out which type of Service you are supposed to create through the following chart shown below. Since the secure coding best practice varies according to how the service is created, we will also explain about the implementation of the Service as well.

Table 4.4-1 Definition of service types

Type	Definition
Private Service	A service that cannot be used another application, and therefore is the safest service.
Public Service	A service that is supposed to be used by an unspecified large number of applications
Partner Service	A service that can only be used by the specific applications made by a trusted partner company.
In-house Service	A service that can only be used by other in-house applications.

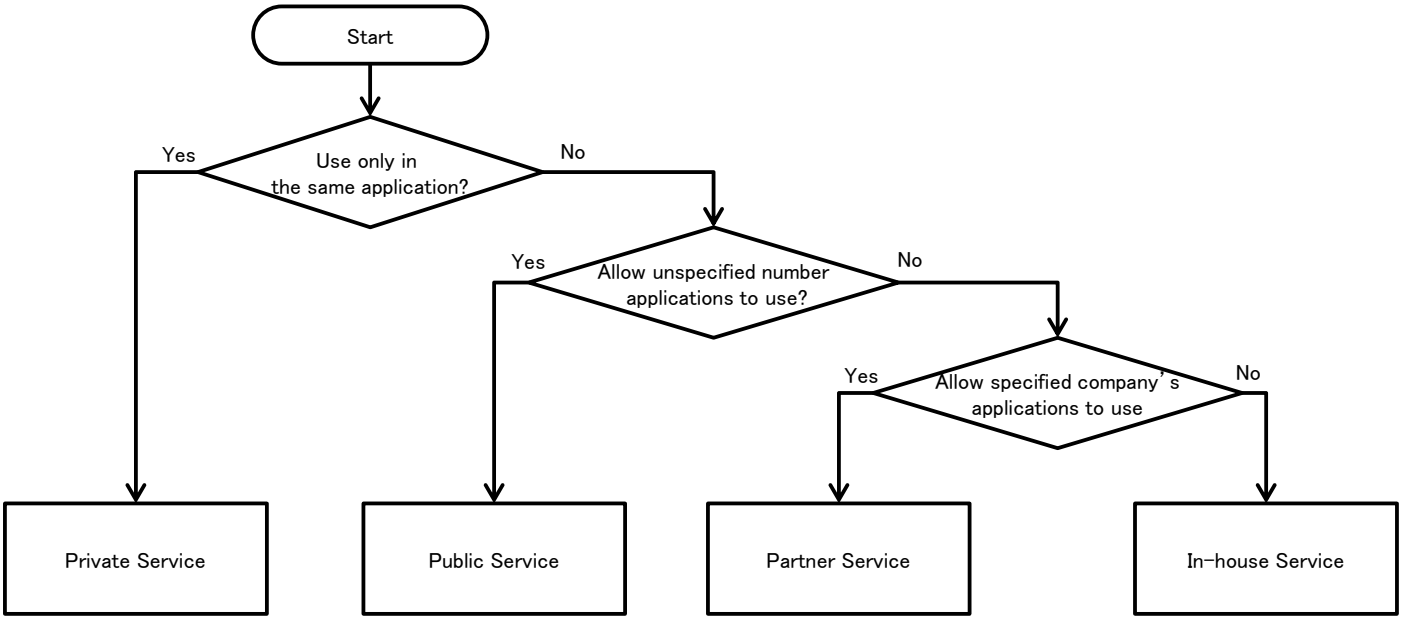


Figure 4.4-1

There are several implementation methods for Service, and you will select the method which matches with the type of Service that you suppose to create. The items of vertical columns in the table show the implementation methods, and these are divided into 5 types. "OK" stands for the possible combination and others show impossible/difficult combinations in the table.

Please refer to "4.4.3.2 How to Implement Service" and Sample code of each Service type (with * mark in a table) for detailed implementation methods of Service.

Table 4.4-2

Category	Private Service	Public Service	Partner Service	In-house Service
startService type	**OK***	OK	-	OK
IntentService type	OK	**OK***	-	OK
local bind type	OK	-	-	-
Messenger bind type	OK	OK	-	**OK***
AIDL bind type	OK	OK	**OK***	OK

Sample code for each security type of Service are shown as below, by using combination of * mark in Table 4.4-2.

4.4.1.1. Creating/Using Private Services

Private Services are Services which cannot be launched by the other applications and therefore it is the safest Service.
When using Private Services that are only used within the application, as long as you use explicit Intents to the class then you do not have to worry about accidently sending it to any other application.

Sample code of how to use the startService type Service is shown below.

Points (Creating a Service):

1. Explicitly set the exported attribute to false.
2. Handle the received intent carefully and securely, even though the intent was sent from the same application.
3. Sensitive information can be sent since the requesting application is in the same application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.service.privateservice" >

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >
        <activity
            android:name=".PrivateUserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

        <!-- Private Service derived from Service class -->
        <!-- *** POINT 1 *** Explicitly set the exported attribute to false. -->
        <service android:name=".PrivateStartService" android:exported="false"/>

        <!-- Private Service derived from IntentService class -->
        <!-- *** POINT 1 *** Explicitly set the exported attribute to false. -->
        <service android:name=".PrivateIntentService" android:exported="false"/>

        </application>

</manifest>
```

PrivateStartService.java

```
package org.jssec.android.service.privateservice;

import android.app.Service;
import android.content.Intent;
```



```
import android.os.IBinder;
import android.widget.Toast;

public class PrivateStartService extends Service {

    // The onCreate gets called only one time when the service starts.
    @Override
    public void onCreate() {
        Toast.makeText(this, "PrivateStartService - onCreate()", Toast.LENGTH_SHORT).show();
    }

    // The onStartCommand gets called each time after the startService gets called.
    @Override
    public int onStartCommand(Intent intent, int flags, int startId) {
        // *** POINT 2 *** Handle the received intent carefully and securely,
        // even though the intent was sent from the same application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String param = intent.getStringExtra("PARAM");
        Toast.makeText(this,
                String.format("PrivateStartService¥nReceived param: ¥"%s¥"", param),
                Toast.LENGTH_LONG).show();

        return Service.START_NOT_STICKY;
    }

    // The onDestroy gets called only one time when the service stops.
    @Override
    public void onDestroy() {
        Toast.makeText(this, "PrivateStartService - onDestroy()", Toast.LENGTH_SHORT).show();
    }

    @Override
    public IBinder onBind(Intent intent) {
        // This service does not provide binding, so return null
        return null;
    }
}
```

Next is sample code for Activity which uses Private Service.

Points (Using a Service):

4. Use the explicit intent with class specified to call a service in the same application.
5. Sensitive information can be sent since the destination service is in the same application.
6. Handle the received result data carefully and securely, even though the data came from a service in the same application.

PrivateUserActivity.java

```
package org.jssec.android.service.privateservice;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;

public class PrivateUserActivity extends Activity {

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.privateservice_activity);
    }

    // --- StartService control ---

    public void onStartServiceClick(View v) {
        // *** POINT 4 *** Use the explicit intent with class specified to call a service in the same app
lication.
        Intent intent = new Intent(this, PrivateStartService.class);

        // *** POINT 5 *** Sensitive information can be sent since the destination service is in the same
 application.
        intent.putExtra("PARAM", "Sensitive information");

        startService(intent);
    }

    public void onStopServiceClick(View v) {
        doStopService();
    }

    @Override
    public void onStop() {
        super.onStop();
        // Stop service if the service is running.
        doStopService();
    }

    private void doStopService() {
        // *** POINT 4 *** Use the explicit intent with class specified to call a service in the same app
lication.
        Intent intent = new Intent(this, PrivateStartService.class);
        stopService(intent);
    }

    // --- IntentService control ---
```



```
    public void onIntentServiceClick(View v) {
        // *** POINT 4 *** Use the explicit intent with class specified to call a service in the same app
lication.
        Intent intent = new Intent(this, PrivateIntentService.class);

        // *** POINT 5 *** Sensitive information can be sent since the destination service is in the same
 application.
        intent.putExtra("PARAM", "Sensitive information");

        startService(intent);
    }
}
```

4.4.1.2. Creating/Using Public Services

Public Service is the Service which is supposed to be used by the unspecified large number of applications. It's necessary to pay attention that it may receive the information (Intent etc.) which was sent by Malware. In case using public Service, It's necessary to pay attention that information(Intent etc.) to send may be received by Malware.

Sample code of how to use the startService type Service is shown below.

Points (Creating a Service):

1. Explicitly set the exported attribute to true.
2. Handle the received intent carefully and securely.
3. When returning a result, do not include sensitive information.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.service.publicservice" >

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >

        <!-- Most standard Service -->
        <!-- *** POINT 1 *** Explicitly set the exported attribute to true. -->
        <service android:name=".PublicStartService" android:exported="true">
            <intent-filter>
                <action android:name="org.jssec.android.service.publicservice.action.startservice" />
            </intent-filter>
        </service>

        <!-- Public Service derived from IntentService class -->
        <!-- *** POINT 1 *** Explicitly set the exported attribute to true. -->
        <service android:name=".PublicIntentService" android:exported="true">
            <intent-filter>
                <action android:name="org.jssec.android.service.publicservice.action.intentservice" />
            </intent-filter>
        </service>

        </application>

</manifest>
```

PublicIntentService.java

```
package org.jssec.android.service.publicservice;

import android.app.IntentService;
import android.content.Intent;
import android.widget.Toast;

public class PublicIntentService extends IntentService{
```



```
    /**
     * Default constructor must be provided when a service extends IntentService class.
     * If it does not exist, an error occurs.
     */
    public PublicIntentService() {
        super("CreatingTypeBService");
    }

    // The onCreate gets called only one time when the Service starts.
    @Override
    public void onCreate() {
        super.onCreate();

        Toast.makeText(this, this.getClass().getSimpleName() + " - onCreate()", Toast.LENGTH_SHORT).show
();
    }

    // The onHandleIntent gets called each time after the startService gets called.
    @Override
    protected void onHandleIntent(Intent intent) {
        // *** POINT 2 *** Handle intent carefully and securely.
        // Since it's public service, the intent may come from malicious application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String param = intent.getStringExtra("PARAM");
        Toast.makeText(this, String.format("Recieved parameter ¥"%s¥"", param), Toast.LENGTH_LONG).show(
);
    }


    // The onDestroy gets called only one time when the service stops.
    @Override
    public void onDestroy() {
        Toast.makeText(this, this.getClass().getSimpleName() + " - onDestroy()", Toast.LENGTH_SHORT).sho
w();
    }

}
```

Next is sample code for Activity which uses Public Service.

Points (Using a Service):

4. Do not send sensitive information.
5. When receiving a result, handle the result data carefully and securely.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.service.publicserviceuser" >

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >
        <activity
            android:name=".PublicUserActivity"
            android:label="@string/app_name"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

    </application>

</manifest>
```

PublicUserActivity.java

```
package org.jssec.android.service.publicserviceuser;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;

public class PublicUserActivity extends Activity {

    // Using Service Info
    private static final String TARGET_PACKAGE = "org.jssec.android.service.publicservice";
    private static final String TARGET_START_CLASS = "org.jssec.android.service.publicservice.PublicSta
rtService";
    private static final String TARGET_INTENT_CLASS = "org.jssec.android.service.publicservice.PublicIn
tentService";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);

        setContentView(R.layout.publicservice_activity);
    }

    // --- StartService control ---

    public void onStartServiceClick(View v) {
```



```
        Intent intent = new Intent("org.jssec.android.service.publicservice.action.startservice");

        // *** POINT 4 *** Call service by Explicit Intent
        intent.setClassName(TARGET_PACKAGE, TARGET_START_CLASS);

        // *** POINT 5 *** Do not send sensitive information.
        intent.putExtra("PARAM", "Not sensitive information");

        startService(intent);
        // *** POINT 6 *** When receiving a result, handle the result data carefully and securely.
        // This sample code uses startService(), so receiving no result.
    }


    public void onStopServiceClick(View v) {
        doStopService();
    }

    // --- IntentService control ---

    public void onIntentServiceClick(View v) {
        Intent intent = new Intent("org.jssec.android.service.publicservice.action.intentservice");

        // *** POINT 4 *** Call service by Explicit Intent
        intent.setClassName(TARGET_PACKAGE, TARGET_INTENT_CLASS);

        // *** POINT 5 *** Do not send sensitive information.
        intent.putExtra("PARAM", "Not sensitive information");

        startService(intent);
    }

    @Override
    public void onStop(){
        super.onStop();
        // Stop service if the service is running.
        doStopService();
    }

    // Stop service
    private void doStopService() {
        Intent intent = new Intent("org.jssec.android.service.publicservice.action.startservice");

        // *** POINT 4 *** Call service by Explicit Intent
        intent.setClassName(TARGET_PACKAGE, TARGET_START_CLASS);

        stopService(intent);
    }
}
```

4.4.1.3. Creating/Using Partner Services

Partner Service is Service which can be used only by the particular applications. System consists of partner company's application and In house application, this is used to protect the information and features which are handled between a partner application and In house application.

Following is an example of AIDL bind type Service.

Points (Creating a Service):

1. Do not define the intent filter and explicitly set the exported attribute to true.
2. Verify that the certificate of the requesting application has been registered in the own white list.
3. Do not (Cannot) recognize whether the requesting application is partner or not by onBind (onStartCommand, onHandleIntent).
4. Handle the received intent carefully and securely, even though the intent was sent from a partner application.
5. Return only information that is granted to be disclosed to a partner application.

In addition, refer to "5.2.1.3 How to Verify the Hash Value of an Application's Certificate" for how to verify the certification hash value of destination application which is specified to white list.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.service.partnerservice.aidl" >

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >

       <!-- Service using AIDL -->
       <!-- *** POINT 1 *** Do not define the intent filter and explicitly set the exported attribute to
true. -->
       <service
           android:name="org.jssec.android.service.partnerservice.aidl.PartnerAIDLService"
           android:exported="true" />
    </application>

</manifest>
```

In this example, 2 AIDL files are to be created. One is for callback interface to give data from Service to Activity. The other one is Interface to give data from Activity to Service and to get information. In addition, package name that is described in AIDL file should be consistent with directory hierarchy in which AIDL file is created, same like package name described in java file.

IExclusiveAIDLServiceCallback.aidl

```
package org.jssec.android.service.exclusiveservice.aidl;

interface IExclusiveAIDLServiceCallback {
```



```
    /**
     * It's called when the value is changed.
     */
    void valueChanged(String info);
}
```

IExclusiveAIDLService.aidl

```
package org.jssec.android.service.exclusiveservice.aidl;

import org.jssec.android.service.exclusiveservice.aidl.IExclusiveAIDLServiceCallback;

interface IExclusiveAIDLService {

    /**
     * Register Callback.
     */
    void registerCallback(IExclusiveAIDLServiceCallback cb);

    /**
     * Get Information
     */
    String getInfo(String param);

    /**
     * Unregister Callback
     */
    void unregisterCallback(IExclusiveAIDLServiceCallback cb);
}
```

PartnerAIDLService.java

```
package org.jssec.android.service.partnerservice.aidl;

import org.jssec.android.shared.PkgCertWhitelists;
import org.jssec.android.shared.Utils;

import android.app.Service;
import android.content.Context;
import android.content.Intent;
import android.os.Handler;
import android.os.IBinder;
import android.os.Message;
import android.os.RemoteCallbackList;
import android.os.RemoteException;
import android.widget.Toast;

public class PartnerAIDLService extends Service {
       private static final int REPORT_MSG = 1;
       private static final int GETINFO_MSG = 2;

    // The value which this service informs to client
    private int mValue = 0;

    // *** POINT 2 *** Verify that the certificate of the requesting application has been registered in
the own white list.
    private static PkgCertWhitelists sWhitelists = null;
    private static void buildWhitelists(Context context) {
        boolean isdebug = Utils.isDebuggable(context);
        sWhitelists = new PkgCertWhitelists();
```

```
        // Register certificate hash value of partner application "org.jssec.android.service.partnerserv
ice.aidluser"
        sWhitelists.add("org.jssec.android.service.partnerservice.aidluser", isdebug ?
                // Certificate hash value of  debug.keystore "androiddebugkey"
                "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255" :
                // Certificate hash value of keystore "partner key"
                "1F039BB5 7861C27A 3916C778 8E78CE00 690B3974 3EB8259F E2627B8D 4C0EC35A");

        // Register other partner applications in the same way
    }

    private static boolean checkPartner(Context context, String pkgname) {
        if (sWhitelists == null) buildWhitelists(context);
        return sWhitelists.test(context, pkgname);
    }

    // Object to register callback
    // Methods which RemoteCallbackList provides are thread-safe.
    private final RemoteCallbackList<IPartnerAIDLServiceCallback> mCallbacks =
        new RemoteCallbackList<IPartnerAIDLServiceCallback>();

    // Handler to send data when callback is called.
    private static class ServiceHandler extends Handler{

        private Context mContext;
        private RemoteCallbackList<IPartnerAIDLServiceCallback> mCallbacks;
        private int mValue = 0;

        public ServiceHandler(Context context, RemoteCallbackList<IPartnerAIDLServiceCallback> callback
, int value){
            this.mContext = context;
            this.mCallbacks = callback;
            this.mValue = value;
        }

        @Override
        public void handleMessage(Message msg) {
            switch (msg.what) {
            case REPORT_MSG: {
                if(mCallbacks == null){
                    return;
                }
                // Start broadcast
                // To call back on to the registered clients, use beginBroadcast().
                // beginBroadcast() makes a copy of the currently registered callback list.
                final int N = mCallbacks.beginBroadcast();
                for (int i = 0; i < N; i++) {
                    IPartnerAIDLServiceCallback target = mCallbacks.getBroadcastItem(i);
                    try {
                        // *** POINT 5 *** Information that is granted to disclose to partner applications
 can be returned.
                        target.valueChanged("Information disclosed to partner application (callback from
Service) No." + (++mValue));

                    } catch (RemoteException e) {
                        // Callbacks are managed by RemoteCallbackList, do not unregister callbacks here.
                        // RemoteCallbackList.kill() unregister all callbacks
                    }
                }
                // finishBroadcast() cleans up the state of a broadcast previously initiated by calling b
```



```
eginBroadcast().
                mCallbacks.finishBroadcast();

                // Repeat after 10 seconds
                sendEmptyMessageDelayed(REPORT_MSG, 10000);
                break;
             }
            case GETINFO_MSG: {
                if(mContext != null) {
                    Toast.makeText(mContext,
                            (String) msg.obj, Toast.LENGTH_LONG).show();
                }
                break;
              }
            default:
                super.handleMessage(msg);
                break;
            } // switch
        }
    }

    protected final ServiceHandler mHandler = new ServiceHandler(this, mCallbacks, mValue);

    // Interfaces defined in AIDL
    private final IPartnerAIDLService.Stub mBinder = new IPartnerAIDLService.Stub() {
        private boolean checkPartner() {
            Context ctx = PartnerAIDLService.this;
            if (!PartnerAIDLService.checkPartner(ctx, Utils.getPackageNameFromUid(ctx, getCallingUid()))
) {
                mHandler.post(new Runnable(){
                    @Override
                    public void run(){
                       Toast.makeText(PartnerAIDLService.this, "Requesting application is not partner app
lication.", Toast.LENGTH_LONG).show();
                    }
                });
                return false;
            }
           return true;
        }
        public void registerCallback(IPartnerAIDLServiceCallback cb) {
            // *** POINT 2 *** Verify that the certificate of the requesting application has been registe
red in the own white list.
          if (!checkPartner()) {
                return;
            }
          if (cb != null) mCallbacks.register(cb);
        }
        public String getInfo(String param) {
            // *** POINT 2 *** Verify that the certificate of the requesting application has been registe
red in the own white list.
            if (!checkPartner()) {
                return null;
            }
            // *** POINT 4 *** Handle the received intent carefully and securely,
            // even though the intent was sent from a partner application
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            Message msg = new Message();
            msg.what = GETINFO_MSG;
```

```
            msg.obj = String.format("Method calling from partner application. Recieved ¥"%s¥"", param);
            PartnerAIDLService.this.mHandler.sendMessage(msg);

            // *** POINT 5 *** Return only information that is granted to be disclosed to a partner appli
cation.
            return "Information disclosed to partner application (method from Service)";
        }

        public void unregisterCallback(IPartnerAIDLServiceCallback cb) {
            // *** POINT 2 *** Verify that the certificate of the requesting application has been registe
red in the own white list.
           if (!checkPartner()) {
               return;
            }

           if (cb != null) mCallbacks.unregister(cb);
        }
    };

    @Override
    public IBinder onBind(Intent intent) {
        // *** POINT 3 *** Verify that the certificate of the requesting application has been registered
in the own white list.
        // So requesting application must be validated in methods defined in AIDL every time.
        return mBinder;
    }

    @Override
    public void onCreate() {
        Toast.makeText(this, this.getClass().getSimpleName() + " - onCreate()", Toast.LENGTH_SHORT).show
();

        // During service is running, inform the incremented number periodically.
        mHandler.sendEmptyMessage(REPORT_MSG);
    }

    @Override
    public void onDestroy() {
        Toast.makeText(this, this.getClass().getSimpleName() + " - onDestroy()", Toast.LENGTH_SHORT).sho
w();

        // Unregister all callbacks
        mCallbacks.kill();

        mHandler.removeMessages(REPORT_MSG);
    }
}
```

PkgCertWhitelists.java

```
package org.jssec.android.shared;

import java.util.HashMap;
import java.util.Map;

import android.content.Context;

public class PkgCertWhitelists {
    private Map<String, String> mWhitelists = new HashMap<String, String>();
```



```
    public boolean add(String pkgname, String sha256) {
        if (pkgname == null) return false;
        if (sha256 == null) return false;

        sha256 = sha256.replaceAll(" ", "");
        if (sha256.length() != 64) return false;    // SHA-256 -> 32 bytes -> 64 chars
        sha256 = sha256.toUpperCase();
        if (sha256.replaceAll("[0-9A-F]+", "").length() != 0) return false; // found non hex char

        mWhitelists.put(pkgname, sha256);
        return true;
    }

    public boolean test(Context ctx, String pkgname) {
        // Get the correct hash value which corresponds to pkgname.
        String correctHash = mWhitelists.get(pkgname);

        // Compare the actual hash value of pkgname with the correct hash value.
        return PkgCert.test(ctx, pkgname, correctHash);
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }
```

```
    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


Next is sample code of Activity which uses partner only Service.

Points (Using a Service):

6. Verify if the certificate of the target application has been registered in the own white list.
7. Return only information that is granted to be disclosed to a partner application.
8. Use the explicit intent to call a partner service.
9. Handle the received result data carefully and securely, even though the data came from a partner application.

ExclusiveAIDLUserActivity.java

```
package org.jssec.android.service.partnerservice.aidluser;

import org.jssec.android.service.partnerservice.aidl.IPartnerAIDLService;
import org.jssec.android.service.partnerservice.aidl.IPartnerAIDLServiceCallback;
import org.jssec.android.shared.PkgCertWhitelists;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.ComponentName;
import android.content.Context;
import android.content.Intent;
import android.content.ServiceConnection;
import android.os.Bundle;
import android.os.Handler;
import android.os.IBinder;
import android.os.Message;
import android.os.RemoteException;
import android.view.View;
import android.widget.Toast;

public class PartnerAIDLUserActivity extends Activity {

    private boolean mIsBound;
    private Context mContext;

    private final static int MGS_VALUE_CHANGED = 1;

    // *** POINT 6 *** Verify if the certificate of the target application has been registered in the ow
n white list.
    private static PkgCertWhitelists sWhitelists = null;
    private static void buildWhitelists(Context context) {
        boolean isdebug = Utils.isDebuggable(context);
        sWhitelists = new PkgCertWhitelists();

        // Register certificate hash value of partner service application "org.jssec.android.service.par
tnerservice.aidl"
        sWhitelists.add("org.jssec.android.service.partnerservice.aidl", isdebug ?
                // Certificate hash value of debug.keystore "androiddebugkey"
                "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255" :
                // Certificate hash value of  keystore "my company key"
                "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA");

        // Register other partner service applications in the same way
    }
    private static boolean checkPartner(Context context, String pkgname) {
        if (sWhitelists == null) buildWhitelists(context);
        return sWhitelists.test(context, pkgname);
```

```
    }

    // Information about destination (requested) partner activity.
    private static final String TARGET_PACKAGE =  "org.jssec.android.service.partnerservice.aidl";
    private static final String TARGET_CLASS = "org.jssec.android.service.partnerservice.aidl.PartnerAI
DLService";

    private static class ReceiveHandler extends Handler{

        private Context mContext;

        public ReceiveHandler(Context context){
            this.mContext = context;
        }

        @Override
        public void handleMessage(Message msg) {
            switch (msg.what) {
                case MGS_VALUE_CHANGED: {
                      String info = (String)msg.obj;
                    Toast.makeText(mContext, String.format("Received ¥"%s¥" with callback.", info), Toast
.LENGTH_SHORT).show();
                    break;
                  }
                default:
                    super.handleMessage(msg);
                    break;
               } // switch
        }
    }

    private final ReceiveHandler mHandler = new ReceiveHandler(this);

    // Interfaces defined in AIDL. Receive notice from service
    private final IPartnerAIDLServiceCallback.Stub mCallback =
        new IPartnerAIDLServiceCallback.Stub() {
            @Override
            public void valueChanged(String info) throws RemoteException {
                Message msg = mHandler.obtainMessage(MGS_VALUE_CHANGED, info);
                mHandler.sendMessage(msg);
            }
    };

    // Interfaces defined in AIDL. Inform service.
    private IPartnerAIDLService mService = null;

    // Connection used to connect with service. This is necessary when service is implemented with bindS
ervice().
    private ServiceConnection mConnection = new ServiceConnection() {

        // This is called when the connection with the service has been established.
        @Override
        public void onServiceConnected(ComponentName className, IBinder service) {
            mService = IPartnerAIDLService.Stub.asInterface(service);

            try{
                // connect to service
                mService.registerCallback(mCallback);

            }catch(RemoteException e){
```



```
                // service stopped abnormally
            }

            Toast.makeText(mContext, "Connected to service", Toast.LENGTH_SHORT).show();
        }

        // This is called when the service stopped abnormally and connection is disconnected.
        @Override
        public void onServiceDisconnected(ComponentName className) {
            Toast.makeText(mContext, "Disconnected from service", Toast.LENGTH_SHORT).show();
        }
    };

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);

        setContentView(R.layout.partnerservice_activity);

        mContext = this;
    }

    // --- StartService control ---

    public void onStartServiceClick(View v) {
        // Start bindService
        doBindService();
    }

    public void onGetInfoClick(View v) {
        getServiceinfo();
    }

    public void onStopServiceClick(View v) {
        doUnbindService();
    }

    @Override
    public void onDestroy() {
        super.onDestroy();
        doUnbindService();
    }

    /**
     * Connect to service
     */
    private void doBindService() {
        if (!mIsBound){
            // *** POINT 6 *** Verify if the certificate of the target application has been registered in
 the own white list.
            if (!checkPartner(this, TARGET_PACKAGE)) {
                Toast.makeText(this, "Destination(Requested) sevice application is not registered in whit
e list.", Toast.LENGTH_LONG).show();
                return;
            }

            Intent intent = new Intent();

            // *** POINT 7 *** Return only information that is granted to be disclosed to a partner appli
cation.
```

```
            intent.putExtra("PARAM", "Information disclosed to partner application");

            // *** POINT 8 *** Use the explicit intent to call a partner service.
            intent.setClassName(TARGET_PACKAGE, TARGET_CLASS);

          bindService(intent, mConnection, Context.BIND_AUTO_CREATE);
          mIsBound = true;
        }
    }

    /**
     * Disconnect service
     */
    private void doUnbindService() {
        if (mIsBound) {
            // Unregister callbacks which have been registered.
            if(mService != null){
                try{
                    mService.unregisterCallback(mCallback);
                }catch(RemoteException e){
                    // Service stopped abnormally
                    // Omitted, since it' s sample.
                }
            }

          unbindService(mConnection);

          Intent intent = new Intent();

        // *** POINT 8 *** Use the explicit intent to call a partner service.
          intent.setClassName(TARGET_PACKAGE, TARGET_CLASS);

          stopService(intent);

          mIsBound = false;
        }
    }

    /**
     * Get information from service
     */
    void getServiceinfo() {
        if (mIsBound && mService != null) {
            String info = null;

            try {
                // *** POINT 7 *** Return only information that is granted to be disclosed to a partner a
pplication.
                info = mService.getInfo("Information disclosed to partner application (method from activi
ty)");
            } catch (RemoteException e) {
                e.printStackTrace();
            }
            // *** POINT 9 *** Handle the received result data carefully and securely,
            // even though the data came from a partner application.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            Toast.makeText(mContext, String.format("Received ¥"%s¥" from service.", info), Toast.LENGTH_
SHORT).show();
         }
```



```
    }
}
```

PkgCertWhitelists.java

```
package org.jssec.android.shared;

import java.util.HashMap;
import java.util.Map;

import android.content.Context;

public class PkgCertWhitelists {
    private Map<String, String> mWhitelists = new HashMap<String, String>();

    public boolean add(String pkgname, String sha256) {
        if (pkgname == null) return false;
        if (sha256 == null) return false;

        sha256 = sha256.replaceAll(" ", "");
        if (sha256.length() != 64) return false;    // SHA-256 -> 32 bytes -> 64 chars
        sha256 = sha256.toUpperCase();
        if (sha256.replaceAll("[0-9A-F]+", "").length() != 0) return false; // found non hex char

        mWhitelists.put(pkgname, sha256);
        return true;
    }

    public boolean test(Context ctx, String pkgname) {
        // Get the correct hash value which corresponds to pkgname.
        String correctHash = mWhitelists.get(pkgname);

        // Compare the actual hash value of pkgname with the correct hash value.
        return PkgCert.test(ctx, pkgname, correctHash);
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }
```

```
    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


4.4.1.4. Creating/Using In-house Services

In-house Services are the Services which are prohibited to be used by applications other than in-house applications. They are used in applications developed internally that want to securely share information and functionality.

Following is an example which uses Messenger bind type Service.

Points (Creating a Service):

1. Define an in-house signature permission.
2. Require the in-house signature permission.
3. Do not define the intent filter and explicitly set the exported attribute to true.
4. Verify that the in-house signature permission is defined by an in-house application.
5. Handle the received intent carefully and securely, even though the intent was sent from an in-house application.
6. Sensitive information can be returned since the requesting application is in-house.
7. When exporting an APK, sign the APK with the same developer key as the requesting application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.service.inhouseservice.messenger" >

    <!-- *** POINT 1 *** Define an in-house signature permission -->
    <permission
        android:name="org.jssec.android.service.inhouseservice.messenger.MY_PERMISSION"
        android:protectionLevel="signature" />

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >

        <!-- Service using Messenger -->
        <!-- *** POINT 2 *** Require the in-house signature permission -->
        <!-- *** POINT 3 *** Do not define the intent filter and explicitly set the exported attribute to
 true. -->
        <service
            android:name="org.jssec.android.service.inhouseservice.messenger.InhouseMessengerService"
            android:exported="true"
            android:permission="org.jssec.android.service.inhouseservice.messenger.MY_PERMISSION" />
    </application>

</manifest>
```

InhouseMessengerService.java

```
package org.jssec.android.service.inhouseservice.messenger;

import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import java.lang.reflect.Array;
```

```
import java.util.ArrayList;
import java.util.Iterator;

import android.app.Service;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.os.Handler;
import android.os.IBinder;
import android.os.Message;
import android.os.Messenger;
import android.os.RemoteException;
import android.widget.Toast;

public class InhouseMessengerService extends Service{
    // In-house signature permission
    private static final String MY_PERMISSION = "org.jssec.android.service.inhouseservice.messenger.MY_
PERMISSION";

    // In-house certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of debug.keystore "androiddebugkey"
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of keystore "my company key"
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }


    // Manage clients(destinations of sending data) in a list
    private ArrayList<Messenger> mClients = new ArrayList<Messenger>();

    // Messenger used when service receive data from client
    private final Messenger mMessenger = new Messenger(new ServiceSideHandler(mClients));

    // Handler which handles message received from client
    private static class ServiceSideHandler extends Handler{

        private ArrayList<Messenger> mClients;

        public ServiceSideHandler(ArrayList<Messenger> clients){
            mClients = clients;
        }

        @Override
        public void handleMessage(Message msg){
            switch(msg.what){
            case CommonValue.MSG_REGISTER_CLIENT:
                // Add messenger received from client
                mClients.add(msg.replyTo);
                break;
            case CommonValue.MSG_UNREGISTER_CLIENT:
                mClients.remove(msg.replyTo);
                break;
```



```
            case CommonValue.MSG_SET_VALUE:
                // Send data to client
                sendMessageToClients(mClients);
                break;
            default:
                super.handleMessage(msg);
               break;
            }
        }
    }

    /**
     * Send data to client
     */
    private static void sendMessageToClients(ArrayList<Messenger> mClients){

        // *** POINT 6 *** Sensitive information can be returned since the requesting application is in-
house.
        String sendValue = "Sensitive information (from Service)";

        // Send data to the registered client one by one.
        // Use iterator to send all clients even though clients are removed in the loop process.
        Iterator<Messenger> ite = mClients.iterator();
        while(ite.hasNext()){
            try {
                Message sendMsg = Message.obtain(null, CommonValue.MSG_SET_VALUE, null);

                Bundle data = new Bundle();
                data.putString("key", sendValue);
                sendMsg.setData(data);

                Messenger next = ite.next();
                next.send(sendMsg);

            } catch (RemoteException e) {
                // If client does not exits, remove it from a list.
                ite.remove();
            }
        }
    }

    @Override
    public IBinder onBind(Intent intent) {

        // *** POINT 4 *** Verify that the in-house signature permission is defined by an in-house applic
ation.
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            Toast.makeText(this, "In-house defined signature permission is not defined by in-house appli
cation.", Toast.LENGTH_LONG).show();
            return null;
        }

        // *** POINT 5 *** Handle the received intent carefully and securely,
        // even though the intent was sent from an in-house application.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String param = intent.getStringExtra("PARAM");
        Toast.makeText(this, String.format("Received parameter ¥"%s¥".", param), Toast.LENGTH_LONG).show
();
```

```
        return mMessenger.getBinder();
    }

    @Override
    public void onCreate() {
        Toast.makeText(this, "Service - onCreate()", Toast.LENGTH_SHORT).show();
    }

    @Override
    public void onDestroy() {
        Toast.makeText(this, "Service - onDestroy()", Toast.LENGTH_SHORT).show();
    }
}
```

SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;

            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
```



```
import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```

*** Point 7 *** When exporting an APK, sign the APK with the same developer key as the requesting application.

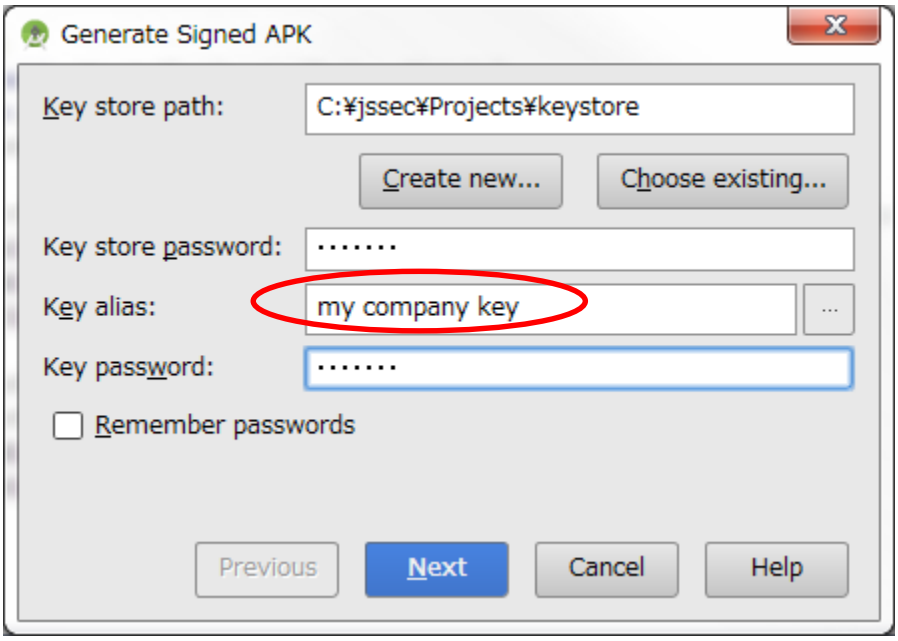


Figure 4.4-2

Next is the sample code of Activity which uses in house only Service.

Points (Using a Service):

8. Declare to use the in-house signature permission.
9. Verify that the in-house signature permission is defined by an in-house application.
10. Verify that the destination application is signed with the in-house certificate.
11. Sensitive information can be sent since the destination application is in-house.
12. Use the explicit intent to call an in-house service.
13. Handle the received result data carefully and securely, even though the data came from an in-house application.
14. When exporting an APK, sign the APK with the same developer key as the destination application.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.service.inhouseservice.messengeruser" >

    <!-- *** POINT 8 *** Declare to use the in-house signature permission.  -->
    <uses-permission
        android:name="org.jssec.android.service.inhouseservice.messenger.MY_PERMISSION" />

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >
        <activity
            android:name="org.jssec.android.service.inhouseservice.messengeruser.InhouseMessengerUserAc
tivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>
```

InhouseMessengerUserActivity.java

```
package org.jssec.android.service.inhouseservice.messengeruser;

import org.jssec.android.shared.PkgCert;
import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.ComponentName;
import android.content.Context;
import android.content.Intent;
import android.content.ServiceConnection;
import android.os.Bundle;
import android.os.Handler;
import android.os.IBinder;
```

```
import android.os.Message;
import android.os.Messenger;
import android.os.RemoteException;
import android.view.View;
import android.widget.Toast;

public class InhouseMessengerUserActivity extends Activity {

    private boolean mIsBound;
    private Context mContext;

    // Destination (Requested) service application information
    private static final String TARGET_PACKAGE =  "org.jssec.android.service.inhouseservice.messenger";
    private static final String TARGET_CLASS = "org.jssec.android.service.inhouseservice.messenger.Inho
useMessengerService";

    // In-house signature permission
    private static final String MY_PERMISSION = "org.jssec.android.service.inhouseservice.messenger.MY_
PERMISSION";

    // In-house certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of debug.keystore "androiddebugkey"
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of keystore "my company key"
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    // Messenger used when this application receives data from service.
    private Messenger mServiceMessenger = null;

    // Messenger used when this application sends data to service.
    private final Messenger mActivityMessenger = new Messenger(new ActivitySideHandler());

    // Handler which handles message received from service
    private class ActivitySideHandler extends Handler {
        @Override
        public void handleMessage(Message msg) {
            switch (msg.what) {
                case CommonValue.MSG_SET_VALUE:
                    Bundle data = msg.getData();
                    String info = data.getString("key");
                    // *** POINT 13 *** Handle the received result data carefully and securely,
                    // even though the data came from an in-house application
                    // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefull
y and Securely."
                    Toast.makeText(mContext, String.format("Received ¥"%s¥" from service.", info),
                            Toast.LENGTH_SHORT).show();
                    break;
                default:
                    super.handleMessage(msg);
            }
        }
```



```
    }

    // Connection used to connect with service. This is necessary when service is implemented with bindS
ervice().
    private ServiceConnection mConnection = new ServiceConnection() {

        // This is called when the connection with the service has been established.
        @Override
        public void onServiceConnected(ComponentName className, IBinder service) {
            mServiceMessenger = new Messenger(service);
            Toast.makeText(mContext, "Connect to service", Toast.LENGTH_SHORT).show();

            try {
                // Send own messenger to service
                Message msg = Message.obtain(null, CommonValue.MSG_REGISTER_CLIENT);
                msg.replyTo = mActivityMessenger;
                mServiceMessenger.send(msg);
            } catch (RemoteException e) {
                // Service stopped abnormally
            }
        }

        // This is called when the service stopped abnormally and connection is disconnected.
        @Override
        public void onServiceDisconnected(ComponentName className) {
            mServiceMessenger = null;
            Toast.makeText(mContext, "Disconnected from service", Toast.LENGTH_SHORT).show();
        }
    };

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);

        setContentView(R.layout.inhouseservice_activity);

        mContext = this;
    }

    // --- StartService control ---

    public void onStartServiceClick(View v) {
        // Start bindService
        doBindService();
    }

    public void onGetInfoClick(View v) {
        getServiceinfo();
    }

    public void onStopServiceClick(View v) {
        doUnbindService();
    }

    @Override
    protected void onDestroy() {
        super.onDestroy();
        doUnbindService();
    }
```

```
    /**
     * Connect to service
     */
    void doBindService() {
        if (!mIsBound){
            // *** POINT 9 *** Verify that the in-house signature permission is defined by an in-house ap
plication.
            if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
                Toast.makeText(this, "In-house defined signature permission is not defined by in-house ap
plication.", Toast.LENGTH_LONG).show();
                return;
            }

            // *** POINT 10 *** Verify that the destination application is signed with the in-house certi
ficate.
            if (!PkgCert.test(this, TARGET_PACKAGE, myCertHash(this))) {
                Toast.makeText(this, "Destination(Requested) service application is not in-house applica
tion.", Toast.LENGTH_LONG).show();
                return;
            }

          Intent intent = new Intent();

            // *** POINT 11 *** Sensitive information can be sent since the destination application is in
-house one.
          intent.putExtra("PARAM", "Sensitive information");

            // *** POINT 12 *** Use the explicit intent to call an in-house service.
          intent.setClassName(TARGET_PACKAGE, TARGET_CLASS);

          bindService(intent, mConnection, Context.BIND_AUTO_CREATE);
          mIsBound = true;
        }
    }

    /**
     * Disconnect service
     */
    void doUnbindService() {
        if (mIsBound) {
            unbindService(mConnection);
            mIsBound = false;
        }
    }

    /**
     * Get information from service
     */
    void getServiceinfo() {
        if (mServiceMessenger != null) {
            try {
                // Request sending information
                Message msg = Message.obtain(null, CommonValue.MSG_SET_VALUE);
                mServiceMessenger.send(msg);
            } catch (RemoteException e) {
                // Service stopped abnormally
            }
         }
    }
}
```


SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;

            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
```

```
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


*** Point14 *** When exporting an APK, sign the APK with the same developer key as the destination application.

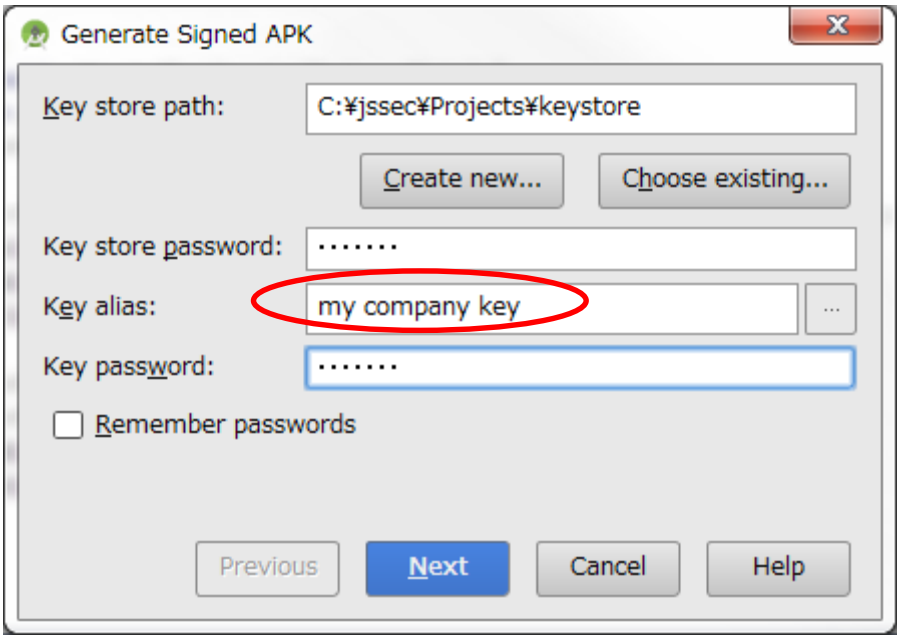


Figure 4.4-3

4.4.2. Rule Book

Implementing or using service, follow the rules below.

1.	Service that Is Used Only in an application, Must Be Set as Private	(Required)
2.	Handle the Received Data Carefully and Securely	(Required)
3.	Use the In-house Defined Signature Permission after Verifying If it's Defined by an In-house Application	(Required)
4.	Do Not Determine Whether the Service Provides its Functions, in onCreate	(Required)
5.	When Returning a Result Information, Pay Attention the Result Information Leakage from the Destination Application	(Required)
6.	Use the Explicit Intent if the Destination Service Is fixed	(Required)
7.	Verify the Destination Service If Linking with the Other Company's Application	(Required)
8.	When Providing an Asset Secondarily, the Asset should be protected with the Same Level Protection	(Required)
9.	Sensitive Information Should Not Be Sent As Much As Possible	(Recommended)

4.4.2.1. Service that Is Used Only in an application, Must Be Set as Private (Required)

Service that is used only in an application (or in same UID) must be set as Private. It avoids the application from receiving Intents from other applications unexpectedly and eventually prevents from damages such as application functions are used or application behavior becomes abnormal.

All you have to do in implementation is set exported attribute false when defining Service in AndroidManifest.xml.

AndroidManifest.xml

```
<!-- Private Service derived from Service class -->
<!-- *** POINT 1 *** Set false for the exported attribute explicitly. -->
<service android:name=".PrivateStartService" android:exported="false"/>
```

In addition, this is a rare case, but do not set Intent Filter when service is used only within the application. The reason is that, due to the characteristics of Intent Filter, public service in other application may be called unexpectedly though you intend to call Private Service within the application.

AndroidManifest.xml(Not recommended)

```
<!-- Private Service derived from Service class -->
<!-- *** POINT 1 *** Set false for the exported attribute explicitly. -->
<service android:name=".PrivateStartService" android:exported="false">
    <intent-filter>
        <action android:name="org.jssec.android.service.OPEN" />
    </intent-filter>
</service>
```


See "4.4.3.1 Combination of Exported Attribute and Intent-filter Setting (In the Case of Service)."

4.4.2.2. Handle the Received Data Carefully and Securely (Required)

Same like Activity, In case of Service, when processing a received Intent data, the first thing you should do is input validation. Also in Service user side, it's necessary to verify the safety of result information from Service. Please refer to "4.1.2.5 Handling the Received Intent Carefully and Securely (Required)" and "4.1.2.9 Handle the Returned Data from a Requested Activity Carefully and Securely (Required)."

In Service, you should also implement calling method and exchanging data by Message carefully.

Please refer to "3.2 Handling Input Data Carefully and Securely"

4.4.2.3. Use the In-house Defined Signature Permission after Verifying If it's Defined by an In-house Application (Required)

Make sure to protect your in-house Services by defining in-house signature permission when creating the Service. Since defining a permission in the AndroidManifest.xml file or declaring a permission request does not provide adequate security, please be sure to refer to "5.2.1.2 How to Communicate Between In-house Applications with In-house-defined Signature Permission."

4.4.2.4. Do Not Determine Whether the Service Provides its Functions, in onCreate (Required)

Security checks such as Intent parameter verification or in-house-defined Signature Permission verification should not be included in onCreate, because when receiving new request during Service is running, process of onCreate is not executed. So, when implementing Service which is started by startService, judgment should be executed by onStartCommand (In case of using IntentService, judgment should be executed by onHandleIntent.) It's also same in the case when implementing Service which is started by bindService, judgment should be executed by onBind.

4.4.2.5. When Returning a Result Information, Pay Attention the Result Information Leakage from the Destination Application (Required)

Depends on types of Service, the reliability of result information destination application (callback receiver side/ Message destination) are different. Need to consider seriously about the information leakage considering the possibility that the destination may be Malware.

See, Activity "4.1.2.7 When Returning a Result, Pay Attention to the Possibility of Information Leakage of that Result from the Destination Application (Required)", for details.

4.4.2.6. Use the Explicit Intent if the Destination Service Is fixed (Required)

When using a Service by implicit Intents, in case the definition of Intent Filter is same, Intent is sent to

the Service which was installed earlier. If Malware with the same Intent Filter defined intentionally was installed earlier, Intent is sent to Malware and information leakage occurs. On the other hand, when using a Service by explicit Intents, only the intended Service will receive the Intent so this is much safer.

There are some other points which should be considered, please refer to "4.1.2.8 Use the explicit Intents if the destination Activity is predetermined. (Required)."

4.4.2.7. Verify the Destination Service If Linking with the Other Company's Application (Required)

Be sure to sure a whitelist when linking with another company's application. You can do this by saving a copy of the company's certificate hash inside your application and checking it with the certificate hash of the destination application. This will prevent a malicious application from being able to spoof Intents. Please refer to sample code section "4.4.1.3 Creating/Using Partner Service" for the concrete implementation method.

4.4.2.8. When Providing an Asset Secondarily, the Asset should be protected with the Same Level Protection (Required)

When an information or function asset, which is protected by permission, is provided to another application secondhand, you need to make sure that it has the same required permissions needed to access the asset. In the Android OS permission security model, only an application that has been granted proper permissions can directly access a protected asset. However, there is a loophole because an application with permissions to an asset can act as a proxy and allow access to an unprivileged application. Substantially this is the same as re-delegating permission so it is referred to as the "Permission Re-delegation" problem. Please refer to "5.2.3.4 Permission Re-delegation Problem."

4.4.2.9. Sensitive Information Should Not Be Sent As Much As Possible (Recommended)

You should not send sensitive information to untrusted parties.

You need to consider the risk of information leakage when exchanging sensitive information with a Service. You must assume that all data in Intents sent to a Public Service can be obtained by a malicious third party. In addition, there is a variety of risks of information leakage when sending Intents to Partner or In-house Services as well depending on the implementation.

Not sending sensitive data in the first place is the only perfect solution to prevent information leakage therefore you should limit the amount of sensitive information being sent as much as possible. When it is necessary to send sensitive information, the best practice is to only send to a trusted Service and to make sure the information cannot be leaked through LogCat

4.4.3. Advanced Topics

4.4.3.1. Combination of Exported Attribute and Intent-filter Setting (In the Case of Service)

We have explained how to implement the four types of Services in this guidebook: Private Services, Public Services, Partner Services, and In-house Services. The various combinations of permitted settings for each type of exported attribute defined in the AndroidManifest.xml file and the intent-filter elements are defined in the table below. Please verify the compatibility of the exported attribute and intent-filter element with the Service you are trying to create.

Table 4.4-3

	Value of exported attribute		
	True	False	Not specified
Intent Filter defined	Public	(Do not Use)	(Do not Use)
Intent Filter Not Defined	Public, Partner, In-house	Private	(Do not Use)

If the exported attribute is not unspecified in a Service, the question of whether or not the Service is public is determined by whether or not intent filters are defined;[12] however, in this guidebook it is forbidden to set a Service's exported attribute to unspecified. In general, as mentioned previously, it is best to avoid implementations that rely on the default behavior of any given API; moreover, in cases where explicit methods exist for configuring important security-related settings such as the exported attribute, it is always a good idea to make use of those methods.

The reason why an undefined intent filter and an exported attribute of false should not be used is that there is a loophole in Android's behavior, and because of how Intent filters work, other application's Services can be called unexpectedly.

Concretely, Android behaves as per below, so it's necessary to consider carefully when application designing.

- When multiple Services define the same content of intent-filter, the definition of Service within application installed earlier is prioritized.
- In case explicit Intent is used, prioritized Service is automatically selected and called by OS.

The system that unexpected call is occurred due to Android's behavior is described in the three figures below. Figure 4.4-4 is an example of normal behavior that Private Service (application A) can be called by implicit Intent only from the same application. Because only application A defines Intent-filter (action="X" in the Figure), it behaves normally. This is the normal behavior.

[12] If any intent filters are defined then the Service is public; otherwise it is private. For more information, see https://developer.android.com/guide/topics/manifest/service-element.html#exported.

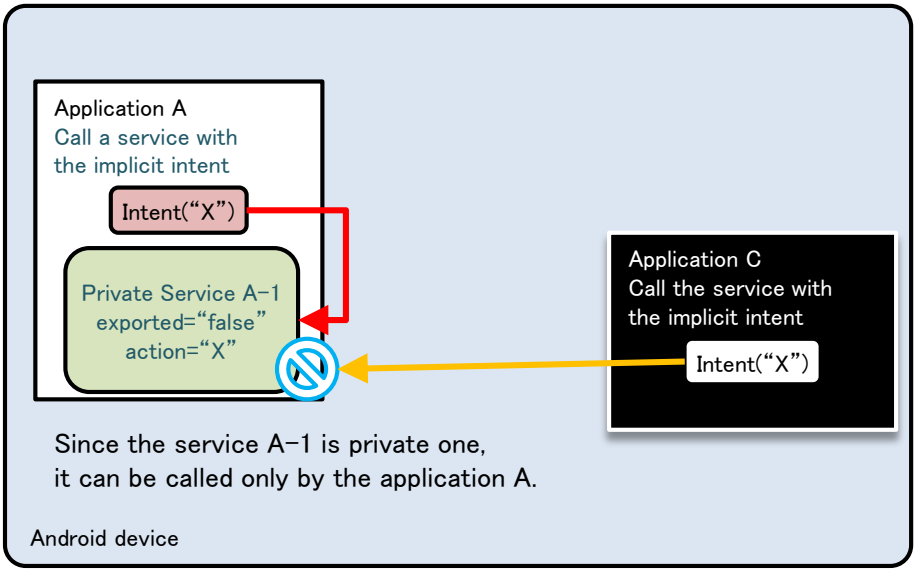


Figure 4.4-4

Figure 4.4-5 and Figure 4.4-6 below show a scenario in which the same Intent filter (action="X") is defined in Application B as well as Application A.

Figure 4.4-5 shows the scenario that applications are installed in the order, application A -> application B. In this case, when application C sends implicit Intent, calling Private Service (A-1) fails. On the other hand, since application A can successfully call Private Service within the application by implicit Intent as expected, there won't be any problems in terms of security (counter-measure for Malware).

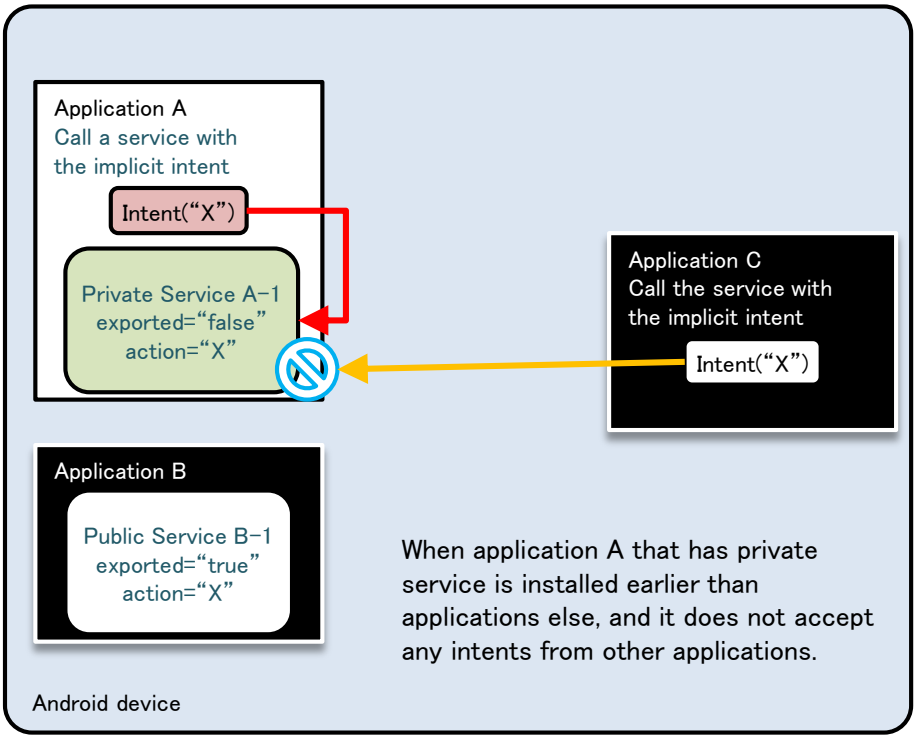


Figure 4.4-5

Figure 4.4-6 shows the scenario that applications are installed in the order, applicationB->applicationA. There is a problem here, in terms of security. It shows an example that applicationA tries to call Private Service within the application by sending implicit Intent, but actually Public Activity (B-1) in application B which was installed earlier, is called. Due to this loophole, it is possible that sensitive information can be sent from applicationA to applicationB. If applicationB is Malware, it will lead the leakage of sensitive information.

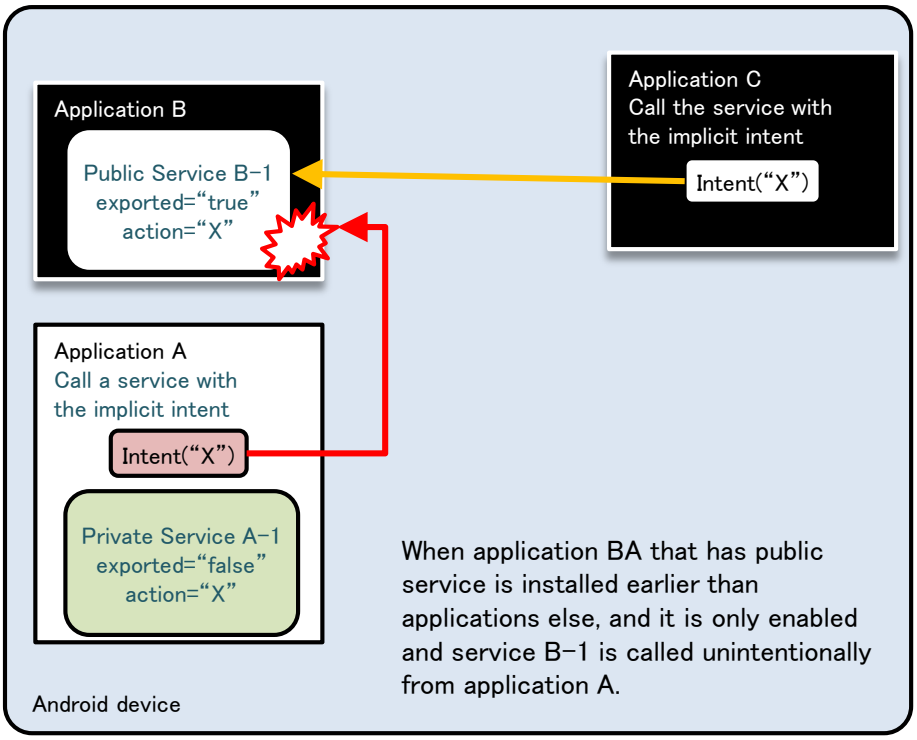


Figure 4.4-6

As shown above, using Intent filters to send implicit Intents to Private Service may result in unexpected behavior so it is best to avoid this setting.

4.4.3.2. How to Implement Service

Because methods for Service implementation are various and should be selected with consideration of security type which is categorized by sample code, each characteristics are briefly explained. It's divided roughly into the case using startService and the case using bindService. And it's also possible to create Service which can be used in both startService and bindService. Following items should be investigated to determine the implementation method of Service.

- Whether to disclose Service to other applications or not (Disclosure of Service)
- Whether to exchange data during running or not (Mutual sending /receiving data)
- Whether to control Service or not (Launch or complete)
- Whether to execute as another process (communication between processes)
- Whether to execute multiple processes in parallel (Parallel process)

Table 4.4-3 shows category of implementation methods and feasibility of each item.
"NG" stands for impossible case or case that another frame work which is different from the provided function is required.

Table 4.4-4 Category of implementation methods for Service

Category	Disclosure of Service	Mutual sending/receiving data	Control Service (Boot /Exit)	Communication between processes	Parallel process
startService type	OK	NG	OK	OK	NG
IntentService type	OK	NG	NG	OK	NG
local bind type	NG	OK	OK	NG	NG
Messenger bind type	OK	OK	OK	OK	NG
AIDL bind type	OK	OK	OK	OK	OK

startService type

This is the most basic Service. This inherits Service class, and executes processes by onStartCommand.

In user side, specify Service by Intent, and call by startService. Because data such as results cannot be returned to source of Intent directly, it should be achieved in combination with another method such as Broadcast. Please refer to "4.4.1.1 Creating/Using Private Service" for the concrete example.

Checking in terms of security should be done by onStartCommand, but it cannot be used for partner only Service since the package name of the source cannot be obtained.

IntentService type

IntentService is the class which was created by inheriting Service. Calling method is same as startService type. Following are characteristics compared with standard service (startService type.)

- Processing Intent is done by onHandleIntent (onStartCommand is not used.)
- It's executed by another thread.
- Process is to be queued.

Call is immediately returned because process is executed by another thread, and process towards Intents is sequentially executed by Queuing system. Each Intent is not processed in parallel, but it is also selectable depending on the product's requirement, as an option to simplify implementation. Since data such as results cannot be returned to source of Intent, it should be achieved in combination with another method such as Broadcast. Please refer to “4.4.1.2 Creating/Using Public Service" for the concrete example of implementation.

Checking in terms of security should be done by onHandleIntent, but it cannot be used for

partner only Service since the package name of the source cannot be obtained.

local bind type

This is a method to implement local Service which works only within the process same as an application. Define the class which was derived from Binder class, and prepare to provide the feature (method) which was implemented in Service to caller side.

From user side, specify Service by Intent and call Service by using bindService. This is the most simple implementation method among all methods of binding Service, but it has limited usages since it cannot be launched by another process and also Service cannot be disclosed. See project "Service PrivateServiceLocalBind" which is included in Sample code, for the concrete implementation example.

From the security point of view, only private Service can be implemented.

Messenger bind type

This is the method to achieve the linking with Service by using Messenger system.

Since Messenger can be given as a Message destination from Service user side, the mutual data exchanging can be achieved comparatively easily. In addition, since processes are to be queued, it has a characteristic that behaves "thread-safely". Parallel process for each process is not possible, but it is also selectable as an option to simplify the implementation depending on the product's requirement. Regarding user side, specify Service by Intent, and call Service by using bindService. See "4.4.1.4 Creating/Using In-house Service" for the concrete implementation example.

Security check in onBind or by Message Handler is necessary, however, it cannot be used for partner only Service since package name of source cannot be obtained.

AIDL bind type

This is a method to achieve linking with Service by using AIDL system. Define interface by AIDL, and provide features that Service has as a method. In addition, call back can be also achieved by implementing interface defined by AIDL in user side, Multi-thread calling is possible, but it's necessary to implement explicitly in Service side for exclusive process.

User side can call Service, by specifying Intent and using bindService. Please refer to "4.4.1.3 Creating/Using Partner Service" for the concrete implementation example.

Security must be checked in onBind for In-house only Service and by each method of interface defined by AIDL for partner only Service.

This can be used for all security types of Service which are described in this Guidebook.

Herein after, some cautions in terms of security when creating/operating database by using SQLite. Main points are appropriate setting of access right to database file, and counter-measures for SQL injection. Database which permits reading/writing database file from outside directly (sharing among multiple applications) is not supposed here, but suppose the usage in backend of Content Provider and in an application itself. In addition, it is recommended to adopt counter-measures mentioned below in case of handling not so much sensitive information, though handling a certain level of sensitive information is supposed here.

4.5.1. Sample Code

4.5.1.1. Creating/Operating Database

When handling database in Android application, appropriate arrangements of database files and access right setting (Setting for denying other application's access) can be achieved by using SQLiteOpenHelper[13]. Here is an example of easy application that creates database when it's launched, and executes searching /adding/changing/deleting data through UI. Sample code is what counter-measure for SQL injection is done, to avoid from incorrect SQL being executed against the input from outside.

[13] As regarding file storing, the absolute file path can be specified as the 2nd parameter (name) of SQLiteOpenHelper constructor. Therefore, need attention that the stored files can be read and written by the other applications if the SD Card path is specified.

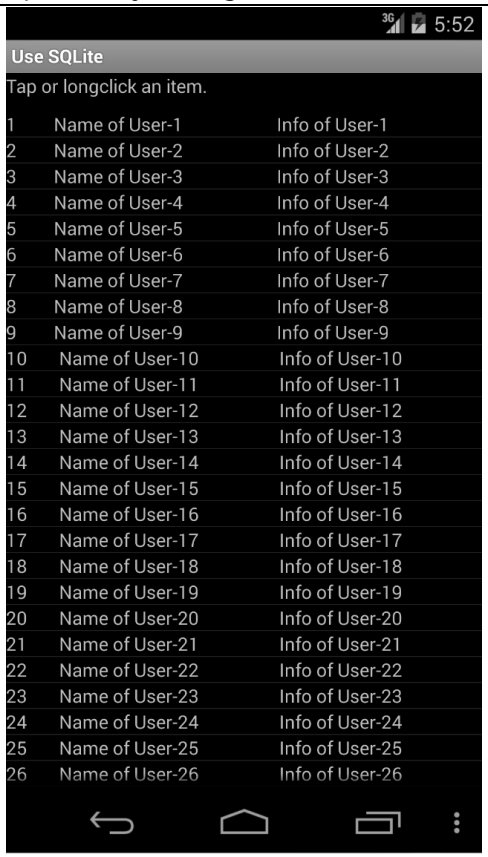


Figure 4.5-1

Points:

1. SQLiteOpenHelper should be used for database creation.
2. Use place holder.
3. Validate the input value according the application requirements.

SampleDbOpenHelper.java

```
package org.jssec.android.sqlite;

import android.content.Context;
import android.database.SQLException;
import android.database.sqlite.SQLiteDatabase;
import android.database.sqlite.SQLiteOpenHelper;
import android.util.Log;
import android.widget.Toast;

public class SampleDbOpenHelper extends SQLiteOpenHelper {
    private SQLiteDatabase          mSampleDb;            //Database to store the data to be handled

    public static SampleDbOpenHelper newHelper(Context context)
    {
        //*** POINT 1 *** SQLiteOpenHelper should be used for database creation.
        return new SampleDbOpenHelper(context);
    }

    public SQLiteDatabase getDb() {
        return mSampleDb;
    }

    //Open DB by Writable mode
```

```
    public void openDatabaseWithHelper() {
        try {
            if (mSampleDb != null && mSampleDb.isOpen()) {
                if (!mSampleDb.isReadOnly())//  Already opened by writable mode
                    return;
                mSampleDb.close();
              }
            mSampleDb  = getWritableDatabase(); //It's opened here.
        } catch (SQLException e) {
            //In case fail to construct database, output to log
            Log.e(mContext.getClass().toString(), mContext.getString(R.string.DATABASE_OPEN_ERROR_MESSAG
E));
            Toast.makeText(mContext, R.string.DATABASE_OPEN_ERROR_MESSAGE, Toast.LENGTH_LONG).show();
        }
    }

    //Open DB by ReadOnly mode.
    public void openDatabaseReadOnly() {
        try {
            if (mSampleDb != null && mSampleDb.isOpen()) {
                if (mSampleDb.isReadOnly())// Already opened by ReadOnly.
                    return;
                mSampleDb.close();
            }
            SQLiteDatabase.openDatabase(mContext.getDatabasePath(CommonData.DBFILE_NAME).getPath(), null
, SQLiteDatabase.OPEN_READONLY);
        } catch (SQLException e) {
            //In case failed to construct database, output to log
            Log.e(mContext.getClass().toString(), mContext.getString(R.string.DATABASE_OPEN_ERROR_MESSAG
E));
            Toast.makeText(mContext, R.string.DATABASE_OPEN_ERROR_MESSAGE, Toast.LENGTH_LONG).show();
        }
    }

    //Database Close
    public void closeDatabase() {
        try {
            if (mSampleDb != null && mSampleDb.isOpen()) {
                mSampleDb.close();
            }
        } catch (SQLException e) {
            //In case failed to construct database, output to log
            Log.e(mContext.getClass().toString(), mContext.getString(R.string.DATABASE_CLOSE_ERROR_MESSA
GE));
            Toast.makeText(mContext, R.string.DATABASE_CLOSE_ERROR_MESSAGE, Toast.LENGTH_LONG).show();
        }
    }

    //Remember Context
    private Context mContext;

    //Table creation command
    private static final String CREATE_TABLE_COMMANDS
            = "CREATE TABLE " + CommonData.TABLE_NAME + " ("
            + "_id INTEGER PRIMARY KEY AUTOINCREMENT, "
            + "idno INTEGER UNIQUE, "
            + "name VARCHAR(" + CommonData.TEXT_DATA_LENGTH_MAX + ") NOT NULL, "
            + "info VARCHAR(" + CommonData.TEXT_DATA_LENGTH_MAX + ")"
            + ");";
```



```
    public SampleDbOpenHelper(Context context) {
        super(context, CommonData.DBFILE_NAME, null, CommonData.DB_VERSION);
        mContext = context;
    }

    @Override
    public void onCreate(SQLiteDatabase db) {
        try {
            db.execSQL(CREATE_TABLE_COMMANDS);  //Execute DB construction command
        } catch (SQLException e) {
            //In case failed to construct database, output to log
            Log.e(this.getClass().toString(), mContext.getString(R.string.DATABASE_CREATE_ERROR_MESSAGE)
);
        }
    }

    @Override
    public void onUpgrade(SQLiteDatabase arg0, int arg1, int arg2) {
        // It's to be executed when database version up. Write processes like data transition.
    }

}
```

DataSearchTask.java (SQLite Database project)

```
package org.jssec.android.sqlite.task;

import org.jssec.android.sqlite.CommonData;
import org.jssec.android.sqlite.DataValidator;
import org.jssec.android.sqlite.MainActivity;
import org.jssec.android.sqlite.R;

import android.database.Cursor;
import android.database.SQLException;
import android.database.sqlite.SQLiteDatabase;
import android.os.AsyncTask;
import android.util.Log;


//Data search task
public class DataSearchTask extends AsyncTask<String, Void, Cursor> {
    private MainActivity    mActivity;
    private SQLiteDatabase      mSampleDB;

    public DataSearchTask(SQLiteDatabase db, MainActivity activity) {
        mSampleDB = db;
        mActivity = activity;
    }

    @Override
    protected Cursor doInBackground(String... params) {
        String  idno = params[0];
        String  name = params[1];
        String  info = params[2];
        String  cols[]  =   {"_id", "idno","name","info"};

        Cursor cur;

        //*** POINT 3 *** Validate the input value according the application requirements.
```

```
        if (!DataValidator.validateData(idno, name, info))
        {
            return null;
        }

        //When all parameters are null, execute all search
        if ((idno == null || idno.length() == 0) &&
                (name == null || name.length() == 0) &&
                (info == null || info.length() == 0) ) {
            try {
                cur = mSampleDB.query(CommonData.TABLE_NAME, cols, null, null, null, null, null);
            } catch (SQLException e) {
                Log.e(DataSearchTask.class.toString(), mActivity.getString(R.string.SEARCHING_ERROR_MESS
AGE));
                return null;
            }
            return cur;
        }

        //When No is specified, execute searching by No
        if (idno != null && idno.length() > 0) {
            String selectionArgs[] = {idno};

            try {
                //*** POINT 2 *** Use place holder.
                cur = mSampleDB.query(CommonData.TABLE_NAME, cols, "idno = ?", selectionArgs, null, null,
 null);
            } catch (SQLException e) {
                Log.e(DataSearchTask.class.toString(), mActivity.getString(R.string.SEARCHING_ERROR_MESS
AGE));
                return null;
            }
            return cur;
        }

        //When Name is specified, execute perfect match search by Name
        if (name != null && name.length() > 0) {
            String selectionArgs[] = {name};
            try {
                //*** POINT 2 *** Use place holder.
                cur = mSampleDB.query(CommonData.TABLE_NAME, cols, "name = ?", selectionArgs, null, null,
 null);
            } catch (SQLException e) {
                Log.e(DataSearchTask.class.toString(), mActivity.getString(R.string.SEARCHING_ERROR_MESS
AGE));
                return null;
            }
            return cur;
        }

        //Other than above, execute partly match searching with the condition of info.
        String argString = info.replaceAll("@", "@@"); //Escape $ in info which was received as input.
        argString = argString.replaceAll("%", "@%"); //Escape % in info which was received as input.
        argString = argString.replaceAll("_", "@_"); //Escape _ in info which was received as input.
        String selectionArgs[] = {argString};

        try {
            //*** POINT 2 *** Use place holder.
            cur = mSampleDB.query(CommonData.TABLE_NAME, cols, "info LIKE '%' || ? || '%' ESCAPE '@'", se
lectionArgs, null, null, null);
```



```
        } catch (SQLException e) {
            Log.e(DataSearchTask.class.toString(), mActivity.getString(R.string.SEARCHING_ERROR_MESSAGE)
);
            return null;
        }
        return cur;
    }

    @Override
    protected void onPostExecute(Cursor resultCur) {
        mActivity.updateCursor(resultCur);
    }
}
```

DataValidator.java

```
package org.jssec.android.sqlite;

public class DataValidator {
    //Validate the Input value
    //validate numeric characters
    public static boolean validateNo(String idno) {
        //null and blank are OK
        if (idno == null || idno.length() == 0) {
           return true;
        }

        //Validate that it's numeric character.
        try {
            if (!idno.matches("[1-9][0-9]*")) {
                //Error if it's not numeric value
                return false;
            }
        } catch (NullPointerException e) {
            //Detected an error
            return false;
        }

        return true;
    }

    // Validate the length of a character string
    public static boolean validateLength(String str, int max_length) {
       //null and blank are OK
       if (str == null || str.length() == 0) {
              return true;
       }

       //Validate the length of a character string is less than MAX
       try {
           if (str.length() > max_length) {
               //When it's longer than MAX, error
               return false;
           }
       } catch (NullPointerException e) {
           //Bug
           return false;
       }
```

```
        return true;
    }

   // Validate the Input value
    public static boolean validateData(String idno, String name, String info) {
        if (!validateNo(idno)) {
            return false;
         }
        if (!validateLength(name, CommonData.TEXT_DATA_LENGTH_MAX)) {
            return false;
         }else if(!validateLength(info, CommonData.TEXT_DATA_LENGTH_MAX)) {
            return false;
         }
        return true;
    }
}
```


4.5.2. Rule Book

Using SQLite, follow the rules below accordingly.

1.	Set DB File Location and Access Right Correctly (Required)
2.	Use Content Provider for Access Control When Sharing DB Data with Other Application (Required)
3.	Place Holder Must Be Used in the Case Handling Variable Parameter during DB Operation. (Required)

4.5.2.1. Set DB File Location and Access Right Correctly (Required)

Considering the protection of DB file data, DB file location and access right setting is the very important elements that need to be considered together.

For example, even if file access right is set correctly, a DB file can be accessed from anybody in case that it is arranged in a location which access right cannot be set, e.g. SD card. And in case that it's arranged in application directory, if the access right is not correctly set, it will eventually allow the unexpected access. Following are some points to be met regarding the correct allocation and access right setting, and the methods to realize them.

About location and access right setting, considering in terms of protecting DB file (data), it's necessary to execute 2 points as per below.

1. Location
   Locate in file path that can be obtained by Context#getDatabasePath(String name), or in some cases, directory that can be obtained by Context#getFilesDir[14].
2. Access right
   Set to MODE_PRIVATE (=it can be accessed only by the application which creates file) mode.

By executing following 2 points, DB file which cannot be accessed by other applications can be created. Here are some methods to execute them.

1. Use SQLiteOpenHelper
2. Use Context#openOrCreateDatabase

When creating DB file, SQLiteDatabase#openOrCreateDatabase can be used. However, when using this method, DB files which can be read out from other applications are created, in some Android smartphone devices. So it is recommended to avoid this method, and using other methods. Each characteristics for the above 2 methods are as per below.

[14] Both methods provide the path under (package) directory which is able to be read and written only by the specified application.

Using SQLiteOpenHelper

When using SQLiteOpenHelper, developers don't need to be worried about many things. Create a class derived from SQLiteOpenHelper, and specify DB name (which is used for file name)[15] to constructer's parameter, then DB file which meets above security requirements, are to be created automatically.

Refer to specific usage method for "4.5.1.1 Creating/Operating Database" for how to use.

Using Context#openOrCreateDatabase

When creating DB by using Context#openOrCreateDatabase method, file access right should be specified by option, in this case specify MODE_PRIVATE explicitly.

Regarding file arrangement, specifying DB name (which is to be used to file name) can be done as same as SQLiteOpenHelper, a file is to be created automatically, in the file path which meets the above mentioned security requirements. However, full path can be also specified, so it's necessary to pay attention that when specifying SD card, even though specifying MODE_PRIVATE, other applications can also access.

Example to execute accsee permission setting to DB explicitly:MainActivity.java

```
public void onCreate(Bundle savedInstanceState) {
       super.onCreate(savedInstanceState);
       setContentView(R.layout.main);

       //Construct database
       try {
          //Create DB by setting MODE_PRIVATE
          db = Context.openOrCreateDatabase("Sample.db",
                                              MODE_PRIVATE, null);
       } catch (SQLException e) {
           //In case failed to construct DB, log output
           Log.e(this.getClass().toString(), getString(R.string.DATABASE_OPEN_ERROR_MESSAGE));
           return;
       }
       //Omit other initial process
    }
```

There are three possible settings for access privileges: MODE_PRIVATE, MODE_WORLD_READABLE, and MODE_WORLD_WRITEABLE. These constants can be specified together by “OR” operator. However, all settings other than MODE_PRIVATE are deprecated in API Level 17 and later versions, and will result in a security exception in API Level 24 and later versions. Even for apps intended for API Level 15 and earlier, it is generally best not to use these flags.[16]

[15] (Undocumented in Android reference) Since the full file path can be specified as the database name in SQLiteOpenHelper implementation, need attention that specifying the place (path) which does not have access control feature (e.g. SD cards) unintentionally.

[16] For more information as to MODE_WORLD_READABLE and MODE_WORLD_WRITEABLE and points of

- MODE_PRIVATE Only creator application can read and write
- MODE_WORLD_READABLE Creator application can read and write, Others can only read in
- MODE_WORLD_WRITEABLE Creator application can read and write, Others can only write in

4.5.2.2. Use Content Provider for Access Control When Sharing DB Data with Other Application (Required)

The method to share DB data with other application is that create DB file as WORLD_READABLE, WORLD_WRITEABLE, to other applications to access directly. However, this method cannot limit applications which access to DB or operations to DB, so data can be read-in or written by unexpected party (application). As a result, it can be considered that some problems may occur in confidentiality or consistency of data, or it may be an attack target of Malware.

As mentioned above, when sharing DB data with other applications in Android, it's strongly recommended to use Content Provider. By using Content Provider, there are some merits, not only the merits from the security point of view which is the access control on DB can be achieved, but also merits from the designing point of view which is DB scheme structure can be hidden into Content Provider.

4.5.2.3. Place Holder Must Be Used in the Case Handling Variable Parameter during DB Operation. (Required)

In the sense that preventing from SQL injection, when incorporating the arbitrary input value to SQL statement, placeholder should be used. There are 2 methods as per below to execute SQL using placeholder.

1. Get SQLiteStatement by using SQLiteDatabase#compileStatement(), and after that place parameter to placeholder by using SQLiteStatement#bindString() or bindLong() etc.
2. When calling execSQL(), insert(), update(), delete(), query(), rawQuery() and replace() in SQLiteDatabese class, use SQL statement which has placeholder.

In addition, when executing SELECT command, by using SQLiteDatabase#compileStatement(), there is a limitation that "only the top 1 element can be obtained as a result of SELECT command," so usages are limited.

In either method, the data content which is given to placeholder is better to be checked in advance according the application requirements. Following is the further explanation for each method.

When Using SQLiteDatabase#compileStatement():

Data is given to placeholder in the following steps.

---

caution regarding their use, see Section “4.6.3.2 Access Permission Setting for the Directory”

1. Get the SQL statement which includes placeholder by using SQLiteDatabase#compileStatement(), as SQLiteStatement.
2. Set the created as SQLiteStatement objects to placeholder by using the method like bindLong() and bindString().
3. Execute SQL by method like execute() of ExecSQLiteStatement object.

Use case of placeholder:DataInsertTask.java (an extra)

```
//Adding data task
public class DataInsertTask extends AsyncTask<String, Void, Void> {
    private MainActivity    mActivity;
    private SQLiteDatabase  mSampleDB;

    public DataInsertTask(SQLiteDatabase db, MainActivity activity) {
        mSampleDB = db;
        mActivity = activity;
    }

    @Override
    protected Void doInBackground(String... params) {
        String  idno = params[0];
        String  name = params[1];
        String  info = params[2];

        //*** POINT 3 *** Validate the input value according the application requirements.
        if (!DataValidator.validateData(idno, name, info))
        {
               return null;
        }
        // Adding data task
        //*** POINT 2 *** Use place holder
        String commandString = "INSERT INTO " + CommonData.TABLE_NAME + " (idno, name, info) VALUES (?,
?, ?)";
        SQLiteStatement sqlStmt = mSampleDB.compileStatement(commandString);
        sqlStmt.bindString(1, idno);
        sqlStmt.bindString(2, name);
        sqlStmt.bindString(3, info);
        try {
            sqlStmt.executeInsert();
        } catch (SQLException e) {
            Log.e(DataInsertTask.class.toString(), mActivity.getString(R.string.UPDATING_ERROR_MESSAGE))
;
        } finally {
               sqlStmt.close();
        }
        return null;
    }

    [...]
}
```

This is a type that SQL statement to be executed as object is created in advance, and parameters are allocated to it. The process to execute is fixed, so there's no room for SQL injection to occur. In addition, there is a merit that process efficiency is enhanced by reutilizing SQLiteStatement object.

In the Case Using Method for Each Process which SQLiteDatabase provides:

There are 2 types of DB operation methods that SQLiteDatabase provides. One is what SQL statement is used, and another is what SQL statement is not used. Methods that SQL statement is used are SQLiteDatabase# execSQL()/rawQuery() and it's executed in the following steps.

1. Prepare SQL statement which includes placeholder.
2. Create data to allocate to placeholder.
3. Send SQL statement and data as parameter, and execute a method for process.

On the other hand, SQLiteDatabase#insert()/update()/delete()/query()/replace() is the method that SQL statement is not used. When using them, data should be sent as per the following steps.

1. In case there's data to insert /update to DB, register to ContentValues.
2. Send ContentValues as parameter, and execute a method for each process (In the following example, SQLiteDatabase#insert())

Use case of metod for each process (SQLiteDatabase#insert())

```
private SQLiteDatabase  mSampleDB;
private void addUserData(String idno, String name, String info) {

  //Validity check of the value(Type, range), escape process
  if (!validateInsertData(idno, name, info)) {
      //If failed to pass the validation, log output
      Log.e(this.getClass().toString(), getString(R.string.VALIDATION_ERROR_MESSAGE));
      return
  }

   //Prepare data to insert
   ContentValues insertValues = new ContentValues();
   insertValues.put("idno", idno);
   insertValues.put("name", name);
   insertValues.put("info", info);

   //Execute Insert
   try {
       mSampleDb.insert("SampleTable", null, insertValues);
   } catch (SQLException e) {
       Log.e(this.getClass().toString(), getString(R.string.DB_INSERT_ERROR_MESSAGE));
       return;
   }
}
```

In this example, SQL command is not directly written, for instead, a method for inserting which SQLiteDatabase provides, is used. SQL command is not directly used, so there's no room for SQL injection in this method, too.

4.5.3. Advanced Topics

4.5.3.1. When Using Wild Card in LIKE Predicate of SQL Statement, Escape Process Should Be Implemented

When using character string which includes wild card (%, _) of LIKE predicate, as input value of place holder, it will work as a wild card unless it is processed properly, so it's necessary to implement escape process in advance according the necessity. It is the case which escape process is necessary that wild card should be used as a single character ("%" or "_").

The actual escape process is executed by using ESCAPE clause as per below sample code.

Example of ESCAPE process in case of using LIKE

```
//Data search task
public class DataSearchTask extends AsyncTask<String, Void, Cursor> {
    private MainActivity       mActivity;
    private SQLiteDatabase     mSampleDB;
    private ProgressDialog     mProgressDialog;

    public DataSearchTask(SQLiteDatabase db, MainActivity activity) {
        mSampleDB = db;
        mActivity = activity;
    }

    @Override
    protected Cursor doInBackground(String... params) {
        String  idno = params[0];
        String  name = params[1];
        String  info = params[2];
        String  cols[]  =   {"_id", "idno","name","info"};

        Cursor cur;

    [...]

        //Execute like search(partly match) with the condition of info
        //Point:Escape process should be performed on characters which is applied to wild card
        String argString = info.replaceAll("@", "@@"); // Escape $ in info which was received as input
        argString = argString.replaceAll("%", "@%"); // Escape % in info which was received as input
        argString = argString.replaceAll("_", "@_"); // Escape _ in info which was received as input
        String selectionArgs[] = {argString};

        try {
            //Point:Use place holder
            cur = mSampleDB.query("SampleTable", cols, "info LIKE '%' || ? || '%' ESCAPE '@'",
                                  selectionArgs, null, null, null);
        } catch (SQLException e) {
            Toast.makeText(mActivity, R.string.SERCHING_ERROR_MESSAGE, Toast.LENGTH_LONG).show();
            return null;
        }
        return cur;
    }

    @Override
    protected void onPostExecute(Cursor resultCur) {
```



```
        mProgressDialog.dismiss();
        mActivity.updateCursor(resultCur);
    }
}
```

4.5.3.2. Use External Input to SQL Command in which Place Holder Cannot Be Used

When executing SQL statement which process targets are DB objects like table creation/deletion etc., placeholder cannot be used for the value of table name. Basically, DB should not be designed using arbitrary character string which was input from outside in case that placeholder cannot be used for the value.

When placeholder cannot be used due to the restriction of specifications or features, whether the Input value is dangerous or not, should be verified before execution, and it's necessary to implement necessary processes.

Basically,

1. When using as character string parameter, escape or quote process for character should be made.
2. When using as numeric value parameter, verify that characters other than numeric value are not included.
3. When using as identifier or command, verify whether characters which cannot be used are not included, along with 1.

should be executed.

Reference: http://www.ipa.go.jp/security/vuln/documents/website_security_sql.pdf (Japanese)

4.5.3.3. Take a Countermeasure that Database Is Not Overwritten Unexpectedly

In case getting instance of DB by SQLiteOpenHelper#getReadableDatabase, getWriteableDatabase, DB is to be opened in readable/WRITEABLE state by using either method[17]. In addition, it's same to Context#openOrCreateDatabase, SQLiteDatabase#openOrCreateDatabase, etc. It means that contents of DB may be overwritten unexpectedly by application operation or by defects in implementation. Basically, it can be supported by the application's spec and range of implementation, but when implementing the function which requires only read in function like application's searching function etc., opening database by read-only, it may lead to simplify designing or inspection and furthermore, lead to enhance application quality, so it's recommended depends on the situation.

[17] getReableDatabase() returns the same object which can be got by getWritableDatabase. This spec is, in case writable object cannot be generated due to disc full etc., it will return Read- only object. (getWritableDatabase() will be execution error under the situation like disc full etc.)

Specifically, open database by specifying OPEN_READONLY to SQLiteDatabase#openDatabase.

Open database by read-only

```
    [...]
    // Open DB(DB should be created in advance)
    SQLiteDatabase db
           = SQLiteDatabase.openDatabase(SQLiteDatabase.getDatabasePath("Sample.db"), null, OPEN_READONL
Y);
```

Reference: http://developer.android.com/reference/android/database/sqlite/SQLiteOpenHelper.html#getReadableDatabase()

4.5.3.4. Verify the Validity of Input/Output Data of DB, According to Application's Requirement

SQLite is the database which is tolerant types, and it can store character type data into columns which is declared as Integer in DB. Regarding data in database, all data including numeric value type is stored in DB as character data of plain text. So searching of character string type, can be executed to Integer type column. (LIKE '%123%' etc.) In addition, the limitation for the value in SQLite (validity verification) is untrustful since data which is longer than limitation can be input in some case, e.g. VARCHAR(100).

So, applications which use SQLite, need to be very careful about this characteristics of DB, and it is necessary take actions according to application requirements, not to store unexpected data to DB or not to get unexpected data. Countermeasures are as per below 2 points.

1. When storing data in database, verify that type and length are matched.
2. When getting the value from database, verify whether data is beyond the supposed type and length, or not.

Following is an example of the code which verifies that the Input value is more than 1.

Verify that the Input value is more than 1 (Extract from MainActivity.java)

```
public class MainActivity extends Activity {

    [...]

    //Process for adding
    private void addUserData(String idno, String name, String info) {
        //Check for No
        if (!validateNo(idno, CommonData.REQUEST_NEW)) {
            return;
        }

        //Inserting data process
        DataInsertTask task = new DataInsertTask(mSampleDbyhis);
        task.execute(idno, name, info);
    }

    [...]
```



```
    private boolean validateNo(String idno, int request) {
        if (idno == null || idno.length() == 0) {
            if (request == CommonData.REQUEST_SEARCH) {
                //When search process, unspecified is considered as OK.
                return true;
            } else {
                //Other than search process, null and blank are error.
                Toast.makeText(this, R.string.IDNO_EMPTY_MESSAGE, Toast.LENGTH_LONG).show();
                return false;
            }
        }

        //Verify that it's numeric character
        try {
            // Value which is more than 1
            if (!idno.matches("[1-9][0-9]*")) {
                //In case of not numeric character, error
                Toast.makeText(this, R.string.IDNO_NOT_NUMERIC_MESSAGE, Toast.LENGTH_LONG).show();
                return false;
            }
        } catch (NullPointerException e) {
            //It never happen in this case
            return false;
        }

        return true;
    }

    [...]
}
```

4.5.3.5. Consideration – the Data Stored into Database

In SQLite implementation, when storing data to file is as per below.

- All data including numeric value type are stored into DB file as character data of plain text.
- When executing data deletion to DB, data itself is not deleted form DB file. (Only deletion mark is added.)
- When updating data, data before updating has not been deleted, and still remains there in DB file.

So, the information which "must have" been deleted may still remain in DB file. Even in this case, take counter-measures according this Guidebook, and when Android security function is enabled, data/file may not be directly accessed by the third party including other applications. However, considering the case that files are picked out by passing through Android's protection system like root privilege is taken, in case the data which gives huge influence on business is stored, data protection which doesn't depend on Android protection system, should be considered.

As above reasons, the important data which is necessary to be protected even when device's root privilege is taken, should not be stored in DB of SQLite, as it is. In case need to store the important data, it's necessary to implement counter-measures, or encrypt overall DB.

When encryption is necessary, there are so many issues that are beyond the range of this Guidebook, like handling the key which is used for encryption or code obfuscation, so as of now it's recommended to consult the specialist when developing an application which handles data that has huge business impact.

Please refer to "4.5.3.6 [Reference] Encrypt SQLite Database (SQLCipher for Android," library which encrypts database is introduced here.

4.5.3.6. [Reference] Encrypt SQLite Database (SQLCipher for Android)

SQLCipher is the SQLite extension that provides encryption of transparent 256 bit AES for database. It is open sourced (BSD license), and maintained/managed by Zetetic LLC. In a world of mobile, SQLCipher is widely used in Nokia/QT, Apple's iOS.

SQLCipher for Android project is aiming to support the standard integrated encryption for SQLite database in Android environment. By creating the standard SQLite's API for SQLCipher, developers can use the encrypted database with the same coding as per usual.

Reference: https://guardianproject.info/code/sqlcipher/

How to Use

Application developers can use SQLCipher by following 3 steps below.

1. Locate sqlcipher.jar, libdatabase_sqlcipher.so, libsqlcipher_android.so and libstlport_shared.so in application's lib directory.
2. Regarding all source files, change all android.database.sqlite.* which is specified by import, to info.guardianproject.database.sqlite.*. In addition, android.database.Cursor can be used as it is.
3. Initialize database in onCreate(), and set password when opening database.

Easy code example

```
SQLiteDatabase.loadLibs(this);                 // First, Initialize library by using context.
SQLiteOpenHelper.getWRITEABLEDatabase(password):  // Parameter is password(Suppose that it's string type and It's got in a secure way.)
```

SQLCipher for Android was version 1.1.0 at the time of writing, and now version 2.0.0 is under developing, and RC4 is disclosed now. In terms of the past usage in Android and stability of API, it's necessary to be verified later, but currently still there's a room to consider as encryption solution of SQLite, which can be used in Android.

Library Structure

The following files which are included as SDK, are necessary, to use SQLCipher.

- assets/icudt46l.zip 2,252KB

It's necessary when icudt46l.dat doesn't exist below /system/usr/icu/ and its earlier version. When icudt46l.dat cannot be found, this zip is unzipped and to be used.

- libs/armeabi/libdatabase_sqlcipher.so 44KB
- libs/armeabi/libsqlcipher_android.so 1,117KB
- libs/armeabi/libstlport_shared.so 555KB
  Native Library. It's read out when SQLCipher's initial load (When calling SQLiteDatabase#loadLibs()).

- libs/commons-codec.jar 46KB
- libs/guava-r09.jar 1,116KB
- libs/sqlcipher.jar 102KB
  Java library which calls Native library. sqlcipher.jar is main. Others are referred from sqlcipher.jar.

Total: about 5.12MB
However, when icudt46l.zip is unzipped, it amounts to around 7MB.

According to Android security designing idea, files are used only for making information persistence and temporary save (cache), and it should be private in principle. Exchanging information between applications should not be direct access to files, but it should be exchanged by inter-application linkage system, like Content Provider or Service. By using this, inter-application access control can be achieved.

Since enough access control cannot be performed on external memory device like SD card etc., so it should be limited to use only when it's necessary by all means in terms of function, like when handling huge size files or transferring information to another location (PC etc.). Basically, files that include sensitive information should not be saved in external memory device. In case sensitive information needs to be saved in a file of external device at any rate, counter-measures like encryption are necessary, but it's not referred here.

4.6.1. Sample Code

As mentioned above, files should be private in principle. However, sometimes files should be read out/written by other applications directly for some reasons. File types which are categorized from the security point of view and comparison are shown in Table 4.6-1. These are categorized into 4 types of files based on the file storage location or access permission to other application. Sample code for each file category is shown below and explanation for each of them are also added there.

Table 4.6-1 File category and comparison from security point of view

File category	Access permission to other application	Storage location	Overview
Private file	NA	In application directory	● Can read and write only in an application ● Sensitive information can be handled. ● File should be this type in principle.
Read out public file	Read out	In application directory	● Other applications and users can read. ● Information that can be disclosed to outside of application is handled.
Read write public file	Read out Write in	In application directory	● Other applications and users can read and write. ● It should not be used from both security and application designing points of view.
External memory device (Read write public)	Read out Write in	External memory device like SD card	● No access control ● Other applications and users can always read/write/delete files. ● Usage should be minimum requirement. ● Comparatively huge size of files can be handled.

4.6.1.1. Using Private Files

This is the case to use files that can be read /written only in the same application, and it is a very safe way to use files. In principle, whether the information stored in the file is public or not, keep files private as much as possible, and when exchanging the necessary information with other applications, it should be done using another Android system (Content Provider, Service.)

Points:

1. Files must be created in application directory.
2. The access privilege of file must be set private mode in order not to be used by other applications.
3. Sensitive information can be stored.
4. Regarding the information to be stored in files, handle file data carefully and securely.

PrivateFileActivity.java

```
package org.jssec.android.file.privatefile;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;

import android.app.Activity;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PrivateFileActivity extends Activity {

    private TextView mFileView;

    private static final String FILE_NAME = "private_file.dat";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.file);

        mFileView = (TextView) findViewById(R.id.file_view);
    }

    /**
     * Create file process
     *
     * @param view
     */
    public void onCreateFileClick(View view) {
        FileOutputStream fos = null;
        try {
            // *** POINT 1 *** Files must be created in application directory.
            // *** POINT 2 *** The access privilege of file must be set private mode in order not to be u
sed by other applications.
            fos = openFileOutput(FILE_NAME, MODE_PRIVATE);
```

```
            // *** POINT 3 *** Sensitive information can be stored.
            // *** POINT 4 *** Regarding the information to be stored in files, handle file data carefull
y and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            fos.write(new String("Not sensotive information (File Activity)¥n").getBytes());
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("PrivateFileActivity", "failed to read file");
        } finally {
            if (fos != null) {
                try {
                    fos.close();
                } catch (IOException e) {
                    android.util.Log.e("PrivateFileActivity", "failed to close file");
                }
            }
        }

        finish();
    }

    /**
     * Read file process
     *
     * @param view
     */
    public void onReadFileClick(View view) {
        FileInputStream fis = null;
        try {
            fis = openFileInput(FILE_NAME);

            byte[] data = new byte[(int) fis.getChannel().size()];

            fis.read(data);

            String str = new String(data);

            mFileView.setText(str);
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("PrivateFileActivity", "failed to read file");
        } finally {
            if (fis != null) {
                try {
                    fis.close();
                } catch (IOException e) {
                    android.util.Log.e("PrivateFileActivity", "failed to close file");
                }
            }
        }
    }

    /**
     * Delete file process
     *
     * @param view
     */
```



```
    public void onDeleteFileClick(View view) {

        File file = new File(this.getFilesDir() + "/" + FILE_NAME);
        file.delete();

        mFileView.setText(R.string.file_view);
    }
}
```

PrivateUserActivity.java

```
package org.jssec.android.file.privatefile;

import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PrivateUserActivity extends Activity {

    private TextView mFileView;

    private static final String FILE_NAME = "private_file.dat";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.user);
        mFileView = (TextView) findViewById(R.id.file_view);
    }

    private void callFileActivity() {
        Intent intent = new Intent();
        intent.setClass(this, PrivateFileActivity.class);

        startActivity(intent);
    }

    /**
     *  Call file Activity process
     *
     * @param view
     */
    public void onCallFileActivityClick(View view) {
        callFileActivity();
    }

    /**
     *  Read file process
     *
     * @param view
     */
    public void onReadFileClick(View view) {
```

```
        FileInputStream fis = null;
        try {
            fis = openFileInput(FILE_NAME);

            byte[] data = new byte[(int) fis.getChannel().size()];

            fis.read(data);

            // *** POINT 4 *** Regarding the information to be stored in files, handle file data carefull
y and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            String str = new String(data);

            mFileView.setText(str);
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("PrivateUserActivity", "failed to read file");
        } finally {
            if (fis != null) {
                try {
                    fis.close();
                } catch (IOException e) {
                    android.util.Log.e("PrivateUserActivity", "failed to close file");
                }
            }
        }
    }

    /**
     * Rewrite file process
     *
     * @param view
     */
    public void onWriteFileClick(View view) {
        FileOutputStream fos = null;
        try {
            // *** POINT 1 *** Files must be created in application directory.
            // *** POINT 2 *** The access privilege of file must be set private mode in order not to be u
sed by other applications.
            fos = openFileOutput(FILE_NAME, MODE_APPEND);

            // *** POINT 3 *** Sensitive information can be stored.
            // *** POINT 4 *** Regarding the information to be stored in files, handle file data carefull
y and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            fos.write(new String("Sensitive information (User Activity)¥n").getBytes());
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("PrivateUserActivity", "failed to read file");
        } finally {
            if (fos != null) {
                try {
                    fos.close();
                } catch (IOException e) {
                    android.util.Log.e("PrivateUserActivity", "failed to close file");
                }
```



```
            }
        }

        callFileActivity();
    }
}
```

4.6.1.2. Using Public Read Only Files

This is the case to use files to disclose the contents to unspecified large number of applications. If you implement by following the below points, it's also comparatively safe file usage method. Note that using the MODE_WORLD_READABLE variable to create a public file is deprecated in API Level 17 and later versions, and will trigger a security exception in API Level 24 and later versions; thus file-sharing methods using Content Provider are preferable.

Points:

1. Files must be created in application directory.
2. The access privilege of file must be set to read only to other applications.
3. Sensitive information must not be stored.
4. Regarding the information to be stored in files, handle file data carefully and securely.

PublicFileActivity.java

```
package org.jssec.android.file.publicfile.readonly;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;

import android.app.Activity;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PublicFileActivity extends Activity {

    private TextView mFileView;

    private static final String FILE_NAME = "public_file.dat";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.file);

        mFileView = (TextView) findViewById(R.id.file_view);
    }

    /**
     * Create file process
     *
     * @param view
     */
    public void onCreateFileClick(View view) {
        FileOutputStream fos = null;
        try {
            // *** POINT 1 *** Files must be created in application directory.
            // *** POINT 2 *** The access privilege of file must be set to read only to other application
s.
            // (MODE_WORLD_READABLE is deprecated API Level 17,
            // don't use this mode as much as possible and exchange data by using ContentProvider().)
```



```
            fos = openFileOutput(FILE_NAME, MODE_WORLD_READABLE);

            // *** POINT 3 *** Sensitive information must not be stored.
            // *** POINT 4 *** Regarding the information to be stored in files, handle file data carefull
y and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            fos.write(new String("Not sensitive information (Public File Activity)¥n")
                    .getBytes());
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("PublicFileActivity", "failed to read file");
        } finally {
            if (fos != null) {
                try {
                    fos.close();
                } catch (IOException e) {
                    android.util.Log.e("PublicFileActivity", "failed to close file");
                }
            }
        }

        finish();
    }

    /**
     * Read file process
     *
     * @param view
     */
    public void onReadFileClick(View view) {
        FileInputStream fis = null;
        try {
            fis = openFileInput(FILE_NAME);

            byte[] data = new byte[(int) fis.getChannel().size()];

            fis.read(data);

            String str = new String(data);

            mFileView.setText(str);
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("PublicFileActivity", "failed to read file");
        } finally {
            if (fis != null) {
                try {
                    fis.close();
                } catch (IOException e) {
                    android.util.Log.e("PublicFileActivity", "failed to close file");
                }
            }
        }
    }

    /**
     * Delete file process
```

```
     *
     * @param view
     */
    public void onDeleteFileClick(View view) {

        File file = new File(this.getFilesDir() + "/" + FILE_NAME);
        file.delete();

        mFileView.setText(R.string.file_view);
    }
}
```

PublicUserActivity.java

```
package org.jssec.android.file.publicuser.readonly;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;

import android.app.Activity;
import android.content.ActivityNotFoundException;
import android.content.Context;
import android.content.Intent;
import android.content.pm.PackageManager.NameNotFoundException;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class PublicUserActivity extends Activity {

    private TextView mFileView;

    private static final String TARGET_PACKAGE = "org.jssec.android.file.publicfile.readonly";
    private static final String TARGET_CLASS = "org.jssec.android.file.publicfile.readonly.PublicFileAc
tivity";

    private static final String FILE_NAME = "public_file.dat";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.user);
        mFileView = (TextView) findViewById(R.id.file_view);
    }

    private void callFileActivity() {
        Intent intent = new Intent();
        intent.setClassName(TARGET_PACKAGE, TARGET_CLASS);

        try {
            startActivity(intent);
        } catch (ActivityNotFoundException e) {
            mFileView.setText("(File Activity does not exist)");
        }
    }
```



```
    /**
     * Call file Activity process
     *
     * @param view
     */
    public void onCallFileActivityClick(View view) {
        callFileActivity();
    }

    /**
     * Read file process
     *
     * @param view
     */
    public void onReadFileClick(View view) {
        FileInputStream fis = null;
        try {
            File file = new File(getFilesPath(FILE_NAME));
            fis = new FileInputStream(file);

            byte[] data = new byte[(int) fis.getChannel().size()];

            fis.read(data);

            // *** POINT 4 *** Regarding the information to be stored in files, handle file data carefull
y and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            String str = new String(data);

            mFileView.setText(str);
        } catch (FileNotFoundException e) {
            android.util.Log.e("PublicUserActivity", "no file");
        } catch (IOException e) {
            android.util.Log.e("PublicUserActivity", "failed to read file");
        } finally {
            if (fis != null) {
                try {
                    fis.close();
                } catch (IOException e) {
                    android.util.Log.e("PublicUserActivity", "failed to close file");
                }
            }
        }
    }

    /**
     * Rewrite file process
     *
     * @param view
     */
    public void onWriteFileClick(View view) {
        FileOutputStream fos = null;
        boolean exception = false;
        try {
            File file = new File(getFilesPath(FILE_NAME));
            // Fail to write in. FileNotFoundException occurs.
            fos = new FileOutputStream(file, true);

            fos.write(new String("Not sensitive information (Public User Activity)¥n")
```

```
                    .getBytes());
        } catch (IOException e) {
            mFileView.setText(e.getMessage());
            exception = true;
        } finally {
            if (fos != null) {
                try {
                    fos.close();
                } catch (IOException e) {
                    exception = true;
                }
            }
        }

        if (!exception)
            callFileActivity();
    }

    private String getFilesPath(String filename) {
        String path = "";

        try {
            Context ctx = createPackageContext(TARGET_PACKAGE,
                    Context.CONTEXT_RESTRICTED);
            File file = new File(ctx.getFilesDir(), filename);
            path = file.getPath();
        } catch (NameNotFoundException e) {
            android.util.Log.e("PublicUserActivity", "no file");
        }
        return path;
    }
}
```


4.6.1.3. Using Public Read/Write Files

This is the usage of the file which permits read-write access to unspecified large number of application.

Unspecified large number of application can read and write, means that needless to say. Malware can also read and write, so the credibility and safety of data will be never guaranteed. In addition, even in case of not malicious intention, data format in file or timing to write in cannot be controlled. So this type of file is almost not practical in terms of functionality.

As above, it's impossible to use read-write files safely from both security and application designing points of view, so using read-write files should be avoided.

Point:

1. Must not create files that be allowed to read/write access from other applications.

4.6.1.4. Using Eternal Memory (Read Write Public) Files

This is the case when storing files in an external memory like SD card. It's supposed to be used when storing comparatively huge information (placing file which was downloaded from Web), or when bring out the information to outside (backup etc.)

"External memory file (Read Write public)" has the equal characteristics with "Read Write public file" to unspecified large number of applications. In addition, it has the equal characteristics with "Read Write public file" to applications which declares to use android.permission.WRITE_EXTERNAL_STORAGE Permission. So, the usage of "External memory file (Read Write public) file" should be minimized as less as possible.

A Backup file is most probably created in an external memory device as Android application's customary practice. However, as mentioned as above, files in an external memory have the risk that is tampered/ deleted by other applications including malware. Hence, in applications which output backup, some contrivances to minimize risks in terms of application spec or designing like displaying a caution "Copy Backup files to the safety location like PC etc., a.s.a.p.", are necessary.

Points:

1. Sensitive information must not be stored.
2. Files must be stored in the unique directory per application.
3. Regarding the information to be stored in files, handle file data carefully and securely.
4. Writing file by the requesting application should be prohibited as the specification.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.file.externalfile" >

    <!-- declare android.permission.WRITE_EXTERNAL_STORAGE permission to write to the external strage --
>
    <!-- In Android 4.4 (API Level 19) and later, the application, which read/write only files in its sp
ecific
    directories on external storage media, need not to require the permission and it should declare
    the maxSdkVersion -->
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"
        android:maxSdkVersion="18"/>

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >
        <activity
            android:name=".ExternalFileActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
```



```
        </activity>
    </application>
</manifest>
```

ExternalFileActivity.java

```
package org.jssec.android.file.externalfile;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;

import android.app.Activity;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class ExternalFileActivity extends Activity {

    private TextView mFileView;

    private static final String TARGET_TYPE = "external";

    private static final String FILE_NAME = "external_file.dat";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.file);

        mFileView = (TextView) findViewById(R.id.file_view);
    }

    /**
     * Create file process
     *
     * @param view
     */
    public void onCreateFileClick(View view) {
        FileOutputStream fos = null;
        try {
            // *** POINT 1 *** Sensitive information must not be stored.
            // *** POINT 2 *** Files must be stored in the unique directory per application.
            File file = new File(getExternalFilesDir(TARGET_TYPE), FILE_NAME);
            fos = new FileOutputStream(file, false);

            // *** POINT 3 *** Regarding the information to be stored in files, handle file data carefull
y and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            fos.write(new String("Non-Sensitive Information(ExternalFileActivity)¥n")
                    .getBytes());
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("ExternalFileActivity", "failed to read file");
        } finally {
```

```
            if (fos != null) {
                try {
                    fos.close();
                } catch (IOException e) {
                    android.util.Log.e("ExternalFileActivity", "failed to close file");
                }
            }
        }

        finish();
    }

    /**
     * Read file process
     *
     * @param view
     */
    public void onReadFileClick(View view) {
        FileInputStream fis = null;
        try {
            File file = new File(getExternalFilesDir(TARGET_TYPE), FILE_NAME);
            fis = new FileInputStream(file);

            byte[] data = new byte[(int) fis.getChannel().size()];

            fis.read(data);

            // *** POINT 3 *** Regarding the information to be stored in files, handle file data carefull
y and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            String str = new String(data);

            mFileView.setText(str);
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("ExternalFileActivity", "failed to read file");
        } finally {
            if (fis != null) {
                try {
                    fis.close();
                } catch (IOException e) {
                    android.util.Log.e("ExternalFileActivity", "failed to close file");
                }
            }
        }
    }

    /**
     * Delete file process
     *
     * @param view
     */
    public void onDeleteFileClick(View view) {

        File file = new File(getExternalFilesDir(TARGET_TYPE), FILE_NAME);
        file.delete();

        mFileView.setText(R.string.file_view);
```



```
    }
}
```

Sample code for use

ExternalFileUser.java

```
package org.jssec.android.file.externaluser;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.IOException;

import android.app.Activity;
import android.app.AlertDialog;
import android.content.ActivityNotFoundException;
import android.content.Context;
import android.content.DialogInterface;
import android.content.Intent;
import android.content.pm.PackageManager.NameNotFoundException;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class ExternalUserActivity extends Activity {

    private TextView mFileView;

    private static final String TARGET_PACKAGE = "org.jssec.android.file.externalfile";
    private static final String TARGET_CLASS = "org.jssec.android.file.externalfile.ExternalFileActivit
y";
    private static final String TARGET_TYPE = "external";

    private static final String FILE_NAME = "external_file.dat";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.user);
        mFileView = (TextView) findViewById(R.id.file_view);
    }

    private void callFileActivity() {
        Intent intent = new Intent();
        intent.setClassName(TARGET_PACKAGE, TARGET_CLASS);

        try {
            startActivity(intent);
        } catch (ActivityNotFoundException e) {
            mFileView.setText("(File Activity does not exist)");
        }
    }

    /**
     * Call file Activity process
     *
     * @param view
     */
    public void onCallFileActivityClick(View view) {
```

```
        callFileActivity();
    }

    /**
     * Read file process
     *
     * @param view
     */
    public void onReadFileClick(View view) {
        FileInputStream fis = null;
        try {
            File file = new File(getFilesPath(FILE_NAME));
            fis = new FileInputStream(file);

            byte[] data = new byte[(int) fis.getChannel().size()];

            fis.read(data);

            // *** POINT 3 *** Regarding the information to be stored in files, handle file data carefull
y and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            String str = new String(data);

            mFileView.setText(str);
        } catch (FileNotFoundException e) {
            mFileView.setText(R.string.file_view);
        } catch (IOException e) {
            android.util.Log.e("ExternalUserActivity", "failed to read file");
        } finally {
            if (fis != null) {
                try {
                    fis.close();
                } catch (IOException e) {
                    android.util.Log.e("ExternalUserActivity", "failed to close file");
                }
            }
        }
    }

    /**
     * Rewrite file process
     *
     * @param view
     */
    public void onWriteFileClick(View view) {

        // *** POINT 4 *** Writing file by the requesting application should be prohibited as the specifi
cation.
        // Application should be designed supposing malicious application may overwrite or delete file.

        final AlertDialog.Builder alertDialogBuilder = new AlertDialog.Builder(
                this);
        alertDialogBuilder.setTitle("POINT 4");
        alertDialogBuilder.setMessage("Do not write in calling appllication.");
        alertDialogBuilder.setPositiveButton("OK",
                new DialogInterface.OnClickListener() {

                    @Override
                    public void onClick(DialogInterface dialog, int which) {
```



```
                    callFileActivity();
                }
            });

        alertDialogBuilder.create().show();

    }

    private String getFilesPath(String filename) {
        String path = "";

        try {
            Context ctx = createPackageContext(TARGET_PACKAGE,
                    Context.CONTEXT_IGNORE_SECURITY);
            File file = new File(ctx.getExternalFilesDir(TARGET_TYPE), filename);
            path = file.getPath();
        } catch (NameNotFoundException e) {
            android.util.Log.e("ExternalUserActivity", "no file");
        }
        return path;
    }
}
```

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.file.externaluser" >

    <!-- In Android 4.0.3 (API Level 14) and later, the permission for reading external storages
    has been defined and the application should decalre that it requires the permission.
    In fact in Android 4.4 (API Level 19) and later, that must be declared to read other directories
    than the package specific directories. -->
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >
        <activity
            android:name=".ExternalUserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

4.6.2. Rule Book

Handling files follow the rules below.

1.	File Must Be Created as a Private File in Principle	(Required)
2.	Must Not Create Files that Be Allowed to Read/Write Access from Other Applications	(Required)
3.	Using Files Stored in External Device (e.g. SD Card) Should Be Requisite Minimum	(Required)
4.	Application Should Be Designed Considering the Scope of File	(Required)

4.6.2.1. File Must Be Created as a Private File in Principle (Required)

As mentioned in "4.6 Handling Files" and "4.6.1.3 Using Public Read/Write File," regardless of the contents of the information to be stored, files should be set private, in principle. From Android security designing point of view, exchanging information and its access control should be done in Android system like Content Provider and Service, etc., and in case there's a reason that is impossible, it should be considered to be substituted by file access permission as alternative method.

Please refer to sample code of each file type and following rule items.

4.6.2.2. Must Not Create Files that Be Allowed to Read/Write Access from Other Applications (Required)

As mentioned in "4.6.1.3 Using Public Read/Write File," when permitting other applications to read/write files, information stored in files cannot be controlled. So, sharing information by using read/write public files should not be considered from both security and function/designing points of view.

4.6.2.3. Using Files Stored in External Device (e.g. SD Card) Should Be Requisite Minimum(Required)

As mentioned in "4.6.1.4 Using Eternal Memory (Read Write Public) File," storing files in external memory device like SD card, leads to holding the potential problems from security and functional points of view. On the other hand, SD card can handle files which have longer scope, compared with application directory, and this is the only one storage that can be always used to bring out the data to outside of application. So, there may be many cases that cannot help using it, depends on application's spec.

When storing files in external memory device, considering unspecified large number of applications and users can read/write/delete files, so it's necessary that application is designed considering the points as per below as well as the points mentioned in sample code.

- Sensitive information should not be saved in a file of external memory device, in principle.
- In case sensitive information is saved in a file of external memory device, it should be encrypted.
- In case saving in a file of external memory device information that will be trouble if it's tampered by other application or users, it should be saved with electrical signature.

- When reading in files in external memory device, use data after verifying the safety of data to read in.
- Application should be designed supposing that files in external memory device can be always deleted.

Please refer to "4.6.2.4 Application Should Be Designed Considering the Scope of File (Required)."

4.6.2.4. Application Should Be Designed Considering the Scope of File (Required)

Data saved in application directory is deleted by the following user operations. It's consistent with the application's scope, and it's distinctive that it's shorter than the scope of application.

- Uninstalling application.
- Delete data and cache of each application (Setting > Apps > select target application.)

Files that were saved in external memory device like SD card, it's distinctive that the scope of the file is longer than the scope of the application. In addition, the following situations are also necessary to be considered.

- File deletion by user
- Pick off/replace/unmount SD card
- File deletion by Malware

As mentioned above, since scope of files are different depends on the file saving location, not only from the viewpoint to protect sensitive information, but also form view point to achieve the right behavior as application, it's necessary to select the file save location.

4.6.3. Advanced Topics

4.6.3.1. File Sharing Through File Descriptor

There is a method to share files through file descriptor, not letting other applications access to public files. This method can be used in Content Provider and in Service. Opponent application can read/write files through file descriptors which are got by opening private files in Content Provider or in Service.

Comparison between the file sharing method of direct access by other applications and the file sharing method via file descriptor, is as per below Table 4.6-2. Variation of access permission and range of applications that are permitted to access, can be considered as merits. Especially, from security point of view, this is a great merit that, applicaions that are permitted to accesss can be controlled in detail.

Table 4.6-2 Comparison of inter-application file sharing method

File sharing method	Variation or access permission setting	Range of applications that are permitted to access
File sharing that permits other applications to access files directly	Read in Write in Read in + Write in	Give all applications access permissions equally
File sharing through file descriptor	Read in Write in Only add Read in + Write in Read in + Only add	Can control whether to give access permission or not, to application which try to access individually and temporarily, to Content Provider or Service

This is common in both of above file sharing methods, when giving write permission for files to other applications, integrity of file contents are difficult to be guaranteed. When several applications write in in parallel, there's a risk that data structure of file contents are destroyed, and application doesn't work normally. So, in sharing files with other applications, giving only read only permission is preferable.

Herein below an implementation example of file sharing by Content Provider and its sample code, are published.

Point

1. The source application is In house application, so sensitive information can be saved.
2. Even if it's a result from In house only Content Provider application, verify the safety of the result data.

InhouseProvider.java

```
package org.jssec.android.file.inhouseprovider;

import java.io.File;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;

import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.content.ContentProvider;
import android.content.ContentValues;
import android.content.Context;
import android.database.Cursor;
import android.net.Uri;
import android.os.ParcelFileDescriptor;

public class InhouseProvider extends ContentProvider {

    private static final String FILENAME = "sensitive.txt";

    // In-house signature permission
    private static final String MY_PERMISSION = "org.jssec.android.file.inhouseprovider.MY_PERMISSION";

    // In-house certificate hash value
    private static String sMyCertHash = null;

    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of  debug.keystore "androiddebugkey"
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of  keystore "my company key"
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    @Override
    public boolean onCreate() {
        File dir = getContext().getFilesDir();
        FileOutputStream fos = null;
        try {
            fos = new FileOutputStream(new File(dir, FILENAME));
            // *** POINT 1 *** The source application is In house application, so sensitive information c
an be saved.
            fos.write(new String("Sensitive information").getBytes());

        } catch (IOException e) {
            android.util.Log.e("InhouseProvider", "failed to read file");
        } finally {
            try {
                fos.close();
            } catch (IOException e) {
                android.util.Log.e("InhouseProvider", "failed to close file");
            }
        }
```

```
        return true;
    }

    @Override
    public ParcelFileDescriptor openFile(Uri uri, String mode)
            throws FileNotFoundException {

        // Verify that in-house-defined signature permission is defined by in-house application.
        if (!SigPerm
                .test(getContext(), MY_PERMISSION, myCertHash(getContext()))) {
            throw new SecurityException(
                    "In-house-defined signature permission is not defined by in-house application.");
        }

        File dir = getContext().getFilesDir();
        File file = new File(dir, FILENAME);

        // Always return read-only, since this is sample
        int modeBits = ParcelFileDescriptor.MODE_READ_ONLY;
        return ParcelFileDescriptor.open(file, modeBits);
    }

    @Override
    public String getType(Uri uri) {
        return "";
    }

    @Override
    public Cursor query(Uri uri, String[] projection, String selection,
            String[] selectionArgs, String sortOrder) {
        return null;
    }

    @Override
    public Uri insert(Uri uri, ContentValues values) {
        return null;
    }

    @Override
    public int update(Uri uri, ContentValues values, String selection,
            String[] selectionArgs) {
        return 0;
    }

    @Override
    public int delete(Uri uri, String selection, String[] selectionArgs) {
        return 0;
    }
}
```

InhouseUserActivity.java

```
package org.jssec.android.file.inhouseprovideruser;

import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.IOException;
```



```
import org.jssec.android.shared.PkgCert;
import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.ProviderInfo;
import android.net.Uri;
import android.os.Bundle;
import android.os.ParcelFileDescriptor;
import android.view.View;
import android.widget.TextView;

public class InhouseUserActivity extends Activity {

    // Content Provider information of destination (requested provider)
    private static final String AUTHORITY = "org.jssec.android.file.inhouseprovider";

    // In-house signature permission
    private static final String MY_PERMISSION = "org.jssec.android.file.inhouseprovider.MY_PERMISSION";

    // In-house certificate hash value
    private static String sMyCertHash = null;

    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of  debug.keystore "androiddebugkey"
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of  keystore "my company key"
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    // Get package name of destination (requested) content provider.
    private static String providerPkgname(Context context, String authority) {
        String pkgname = null;
        PackageManager pm = context.getPackageManager();
        ProviderInfo pi = pm.resolveContentProvider(authority, 0);
        if (pi != null)
            pkgname = pi.packageName;
        return pkgname;
    }

    public void onReadFileClick(View view) {

        logLine("[ReadFile]");

        // Verify that in-house-defined signature permission is defined by in-house application.
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            logLine("  In-house-defined signature permission is not defined by in-house application.");
            return;
        }

        // Verify that the certificate of destination (requested) content provider application is in-hou
se certificate.
```

```
        String pkgname = providerPkgname(this, AUTHORITY);
        if (!PkgCert.test(this, pkgname, myCertHash(this))) {
            logLine("  Destination (Requested) Content Provider is not in-house application.");
            return;
        }

        // Only the information which can be disclosed to in-house only content provider application, ca
n be included in a request.
        ParcelFileDescriptor pfd = null;
        try {
            pfd = getContentResolver().openFileDescriptor(
                    Uri.parse("content://" + AUTHORITY), "r");
        } catch (FileNotFoundException e) {
            android.util.Log.e("InhouseUserActivity", "no file");
        }

        if (pfd != null) {
            FileInputStream fis = new FileInputStream(pfd.getFileDescriptor());

            if (fis != null) {
                try {
                    byte[] buf = new byte[(int) fis.getChannel().size()];
                    fis.read(buf);
                    // *** POINT 2 *** Handle received result data carefully and securely,
                    // even though the data came from in-house applications.
                    // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefull
y and Securely."
                    logLine(new String(buf));
                } catch (IOException e) {
                    android.util.Log.e("InhouseUserActivity", "failed to read file");
                } finally {
                    try {
                        fis.close();
                    } catch (IOException e) {
                        android.util.Log.e("ExternalFileActivity", "failed to close file");
                    }
                }
            }
            try {
                pfd.close();
            } catch (IOException e) {
                android.util.Log.e("ExternalFileActivity", "failed to close file descriptor");
            }

        } else {
            logLine("  null file descriptor");
        }
    }

    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        mLogView = (TextView) findViewById(R.id.logview);
    }

    private void logLine(String line) {
        mLogView.append(line);
```



```
        mLogView.append("¥n");
    }
}
```

4.6.3.2. Access Permission Setting for the Directory

Herein above, security considerations are explained, focusing on files. It's also necessary to consider the security for directory which is a file container. Herein below, security considerations of access permission setting for directory are explained.

In Android, there are some methods to get/create subdirectory in application directory. The major ones are as per below Table 4.6-3.

Table 4.6-3 Methods to get/create subdirectory in application directory

	Specify access permission to other application	Deletion by user
Context#getFilesDir()	Impossible (Only execution permission)	"Setting" > "Apps" > select target application > "Clear data"
Context#getCacheDir()	Impossible (Only execution permission)	"Setting" > "Apps" > select target application > "Clear cache" It can be deleted by "Clear data," too
Context#getDir(String name, int MODE)	Following can be specified to MODE MODE_PRIVATE MODE_WORLD_READABLE MODE_WORLD_WRITEABLE	"Setting" > "Apps" > select target application > "Clear data"

Here especially what needs to pay attention is access permission setting by Context#getDir(). As explained in file creation, basically directory also should be set private from the security designing point of view. When sharing information depends on access permission setting, there may be an unexpected side effect, so other methods should be taken as information sharing.

MODE_WORLD_READABLE

This is a flag to give all applications read-only permission to directory. So all applications can get file list and individual file attribute information in the directory. Because secret files may not be placed in these directories, in general this flag must not be used.[18]

MODE_WORLD_WRITEABLE

This flag gives other applications write permission to directory. All applications can

[18] MODE_WORLD_READABLE and MODE_WORLD_WRITEABLE are deprecated in API Level17 and later versions, and in API Level 24 and later versions their use will trigger a security exception.

create/move[19]/rename/delete files in the directory. These operations has no relation with access permission setting (Read/Write/Execute) of file itself, so it's necessary to pay attention that operations can be done only with write permission to directory. This flag allows other apps to delete or replace files arbitrarily, so in general it must not be used.[18]

Regarding Table 4.6-3 "Deletion by User," refer to "4.6.2.4 Application Should Be Designed Considering the Scope of File (Required)."

4.6.3.3. Access Permission Setting for Shared Preference and Database File

Shared Preference and database also consist of files. Regarding access permission setting what are explained for files are applied here. Therefore, both Shared Preference and database, should be created as private files same like files, and sharing contents should be achieved by the Android's inter-application linkage system.

Herein below, the usage example of Shared Preference is shown. Shared Preference is crated as private file by MODE_PRIVATE.

Example of setting access restriction to Shared Preference file.

```
import android.content.SharedPreferences;
import android.content.SharedPreferences.Editor;

       Ommision of a passage

       // Get Shared Preference . (If there's no Shared Preference, it's to be created.)
       // Point:Basically, specify MODE_PRIVATE mode.
       SharedPreferences preference = getSharedPreferences(
              PREFERENCE_FILE_NAME, MODE_PRIVATE);

       // Example of writing preference which value is charcter string
       Editor editor = preference.edit();
       editor.putString("prep_key", "prep_value");// key:"prep_key", value:"prep_value"
       editor.commit();
```

Please refer to "4.5 Using SQLite" for database.

4.6.3.4. Specification Change regarding External Storage Access in Android 4.4 (API Level 19) and later

The specification regarding External Storage Access has been changed to the followings since Android 4.4 (API Level 19).

(1) In the case that the application needs read/write to its specific directories on external storage media, the WRITE_EXTERNAL_STORAGE/READ_EXTERNAL_STORAGE permissions need not to be declared with <uses-permission>. (Changed)

(2) In the case that the application needs read files on other directories than its specific directories

[19] Files cannot be moved over mount point (e.g. from internal storage to external storage). Therefore, moving the protected files from internal storage to external storage cannot be happened.

on external storage media, the READ_EXTERNAL_STORAGE permission needs to be declared with <uses-permission>. (Changed)

(3) In the case that the application needs to write files on other directories than its specific directories on the primary external storage media, the WRITE_EXTERNAL_STORAGE permission needs to be declared with <uses-permission>.

(4) The application cannot write files on other directories than its specific directories on the secondary external storage media.

In that specification, whether the permission requisitions are needed is determined according to the version of Android OS. So in the case that the application supports the versions including Android 4.3 and 4.4, it could lead to a pleasant situation that the application requires the unnecessary permission of users. Therefore, applications just corresponding to the paragraph (1) is recommended to use the maxSdkVersion attribute of <uses-permission> like the below.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.file.externaluser" >

    <!-- In Android 4.0.3 (API Level 14) and later, the permission for reading external storages
    has been defined and the application should decalre that it requires the permission.
    In fact in Android 4.4 (API Level 19) and later, that must be declared to read other directories
    than the package specific directories. -->
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >
        <activity
            android:name=".ExternalUserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

4.6.3.5. Revised specifications in Android 7.0 (API Level 24) for accessing specific directories on external storage media

On devices running Android 7.0 (API Level 24) or later, a new API known as Scoped Directory Access API has been introduced. Scoped Directory Access allows the application to access to specific directories on external storage media without permission.

Within Scoped Directory Access, a directory defined in the Environment class is passed as a

parameter to the StorageVolume#createAccessIntent method to create an Intent. By sending this Intent via startActivityForResult, you can enable a situation in which a dialog box requesting access permission appears on the terminal screen, and—if the user grants permission—the specified directories on each storage volume become accessible.

Table 4.6-4 Directories that may be accessed via Scoped Directory Access

DIRECTORY_MUSIC	Standard location for general music files
DIRECTORY_PODCASTS	Standard directory for podcasts
DIRECTORY_RINGTONES	Standard directory for ringtones
DIRECTORY_ALARMS	Standard directory for alarms
DIRECTORY_NOTIFICATIONS	Standard directory for notifications
DIRECTORY_PICTURES	Standard directory for pictures
DIRECTORY_MOVIES	Standard directory for movies
DIRECTORY_DOWNLOADS	Standard directory for user-downloaded files
DIRECTORY_DCIM	Standard directory for image/video files produced by cameras
DIRECTORY_DOCUMENTS	Standard directory for user-created documents

If the location to be accessed by an app lies within one of the above directories, and if the app is running on an Android 7.0 or later device, the use of Scoped Directory Access is recommended for the following reasons. For apps that must continue to support pre-Android 7.0 devices, see the sample code in the AndroidManifest listed in Section “4.6.3.4Specification Change regarding External Storage Access in Android 4.4 (API Level 19) and later”.

- When a Permission is granted to access external storage, the app is able to access directories other than its intended destination.
- Using Storage Access Framework to require users to choose accessible directories results in a cumbersome procedure in which the user must configure a selector on each access. Also, when access to the root directory of an external storage is granted, the entirety of that storage becomes accessible.

4.7. Using Browsable Intent

Android application can be designed to launch from browser corresponding with a webpage link. This functionality is called 'Browsable Intent.' By specifying URI scheme in Manifest file, an application responds the transition to the link (user tap etc.) which has its URI scheme, and the application is launched with the link as a parameter.

In addition, the method to launch the corresponding application from browser by using URI scheme is supported not only in Android but also in iOS and other platforms, and this is generally used for the linkage between Web application and external application, etc. For example, following URI scheme is defined in Twitter application or Facebook application, and the corresponding applications are launched from the browser both in Android and in iOS.

Table 4.7-1

URI scheme	Corresponding application
fb://	Facebook
twitter://	Twitter

It seems very convenient function considering the linkage and convenience, but there are some risks that this function is abused by a malicious third party. What can be supposed are as follows, they abuse application functions by preparing a malicious Web site with a link in which URL has incorrect parameter, or they get information which is included in URL by cheating a smartphone owner into installing the Malware which responds the same URI scheme.

There are some points to be aware when using 'Browsable Intent' against these risks.

4.7.1. Sample Code

Sample codes of an application which uses 'Browsable Intent' are shown below.

Points:

1. (Webpage side) Sensitive information must not be included.
2. Handle the URL parameter carefully and securely.

Starter.html

```
<html>
    <body>
        <!-- *** POINT 1 *** Sensitive information must not be included -->
        <!-- Character strings to be passed as URL parameter, should be UTF-8 and URI encoded. -->
        <a href="secure://jssec?user=user_id"> Login </a>
    </body>
</html>
```

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.browsableintent" >
```

```
    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:allowBackup="false" >
        <activity
            android:name=".BrowsableIntentActivity"
            android:label="@string/title_activity_browsable_intent"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>

            <intent-filter>
                <action android:name="android.intent.action.VIEW" />
                // Accept implicit Intent
                <category android:name="android.intent.category.DEFAULT" />
                // Accept Browsable intent
                <category android:name="android.intent.category.BROWSABLE" />
                // Accept URI 'secure://jssec'
                <data android:scheme="secure" android:host="jssec"/>
            </intent-filter>
        </activity>
    </application>

</manifest>
```

BrowsableIntentActivity.java

```
package org.jssec.android.browsableintent;

import android.app.Activity;
import android.content.Intent;
import android.net.Uri;
import android.os.Bundle;
import android.widget.TextView;

public class BrowsableIntentActivity extends Activity {

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_browsable_intent);

        Intent intent = getIntent();
        Uri uri = intent.getData();
        if (uri != null) {
            // Get UserID which is passed by URI parameter
            // *** POINT 2 *** Handle the URL parameter carefully and securely.
            // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Se
curely."
            String userID = "User ID = " +  uri.getQueryParameter("user");
            TextView tv = (TextView)findViewById(R.id.text_userid);
            tv.setText(userID);
        }
    }
}
```


4.7.2. Rule Book

Follow rules listed below when using "Browsable Intent".

1.	(Webpage side) Sensitive Information Must Not Be Included in Parameter of Corresponding Link (Required)
2.	Handle the URL Parameter Carefully and Securely (Required)

4.7.2.1. (Webpage side) Sensitive Information Must Not Be Included in Parameter of Corresponding Link (Required)

When tapping the link in browser, an intent which has a URL value in its data (It can be retrieve by Intent#getData) is issued, and an application which has a corresponding Intent Filter is launched from Android system.

At this moment, when there are several applications which Intent Filter is set to receive the same URI scheme, application selection dialogue is shown in the same way as normal launch by implicit Intent, and an application which user selected is launched. In case that a Malware is listed in the selection of application selection dialogue, there is a risk that user may launch the Malware by mistake and parameters in URL are sent to Malware.

As per above, it is necessary to avoid from include sensitive information directly in URL parameter as it is for creating general Webpage link since all parameters which are included in Webpage link URL can be given to Malware.

Example that User ID and Password are included in URL

```
insecure://sample/login?userID=12345&password=abcdef
```

In addition, there is a risk that user may launch a Malware and input password to it when it is defined in specs that password input is executed in an application after being launched by 'Browsable Intent', even if the URL parameter includes only non-sensitive information like User ID. So it should be considered that specs like a whole Login process is completed within application side. It must be kept in mind when designing an application and a service that launching application by 'Browsable Intent' is equivalent to launching by implicit Intent and there is no guarantee that a valid application is launched.

4.7.2.2. Handle the URL Parameter Carefully and Securely (Required)

URL parameters which are sent to an application are not always from a legitimate Web page, since a link which is matched with URI scheme can be made by not only developers but anyone. In addition, there is no method to verify whether the URL parameter is sent from a valid Web page or not.

So it is necessary to verify safety of a URL parameter before using it, e.g. check if an unexpected value is included or not.

4.8. Outputting Log to LogCat

There's a logging mechanism called LogCat in Android, and not only system log information but also application log information are also output to LogCat. Log information in LogCat can be read out from other application in the same device[20], so the application which outputs sensitive information to Logcat, is considered that it has the vulnerability of the information leakage. The sensitive information should not be output to LogCat.

From a security point of view, in release version application, it's preferable that any log should not be output. However, even in case of release version application, log is output for some reasons in some cases. In this chapter, we introduce some ways to output messages to LogCat in a safe manner even in a release version application. Along with this explanation, please refer to "4.8.3.1 Two Ways of Thinking for the Log Outputting in Release version application."

4.8.1. Sample Code

Herein after, the method to control the Log output to LogCat by ProGuard in release version application. ProGuard is one of the optimization tools which automatically delete the unnecessary code like unused methods, etc.

There are five types of log output methods, Log.e(), Log.w(), Log.i(), Log.d(), Log.v(), in android.util.Log class. Regarding log information, intentionally output log information (hereinafter referred to as the Operation log information) should be distinguished from logging which is inappropriate for a release version application such as debug log (hereinafter referred to as the Development log information). It's recommended to use Log.e()/w()/i() for outputting operation log information, and to use Log.d()/v() for outputting development log. Refer to "4.8.3.2 Selection Standards of Log Level and Log Output Method" for the details of proper usage of five types of log output methods, in addition, also refer to "4.8.3.3 DEBUG Log and VERBOSE Log Are Not Always Deleted Automatically."

Here's an example of how to use LogCat in a safe manner. This example includes Log.d() and Log.v() for outputting debug log. If the application is for release, these two methods would be deleted automatically. In this sample code, ProGuard is used to automatically delete code blocks where Log.d()/v() is called.

[20] The log information output to LogCat can be read by applications that declare using READ_LOGS permission. However, in Android 4.1 and later, log information that is output by other application cannot be read. But smartphone user can read every log information output to logcat through ADB.

Points:

1. Sensitive information must not be output by Log.e()/w()/i(), System.out/err.
2. Sensitive information should be output by Log.d()/v() in case of need.
3. The return value of Log.d()/v() should not be used (with the purpose of substitution or comparison).
4. When you build an application for release, you should bring the mechanism that automatically deletes inappropriate logging method like Log.d() or Log.v() in your code.
5. An APK file for the (public) release must be created in release build configurations.

ProGuardActivity.java

```
package org.jssec.android.log.proguard;

import android.app.Activity;
import android.os.Bundle;
import android.util.Log;

public class ProGuardActivity extends Activity {

    final static String LOG_TAG = "ProGuardActivity";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_proguard);

        // *** POINT 1 *** Sensitive information must not be output by Log.e()/w()/i(), System.out/err.
        Log.e(LOG_TAG, "Not sensitive information (ERROR)");
        Log.w(LOG_TAG, "Not sensitive information (WARN)");
        Log.i(LOG_TAG, "Not sensitive information (INFO)");

        // *** POINT 2 *** Sensitive information should be output by Log.d()/v() in case of need.
        // *** POINT 3 *** The return value of Log.d()/v()should not be used (with the purpose of substit
ution or comparison).
        Log.d(LOG_TAG, "sensitive information (DEBUG)");
        Log.v(LOG_TAG, "sensitive information (VERBOSE)");
    }
}
```

proguard-project.txt

```
# prevent from changing class name and method name etc.
-dontobfuscate

# *** POINT 4 *** In release build, the build configurations in which Log.d()/v() are deleted automatica
lly should be constructed.
-assumenosideeffects class android.util.Log {
    public static int d(...);
    public static int v(...);
}
```

*** Point 5 *** An APK file for the (public) release must be created in release build configurations.

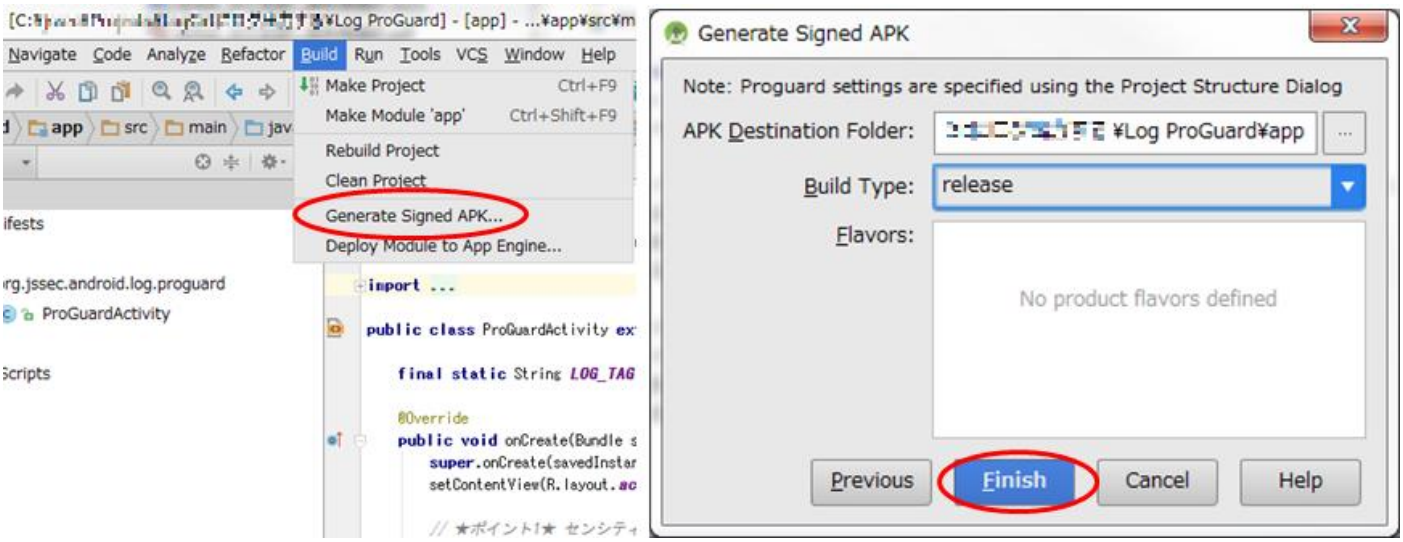


Figure 4.8-1 How to create release version application

The difference of LogCat output between development version application (debug build) and release version application (release build) are shown in below Figure 4.8-2.

Development version application (Debug build)

LogCat Search Console

Search for messages. Accepts Java regexes. Prefix with pid:, app:, tag

Level	Tag	Text
E	ProGuardActivity	Not sensitive information (ERROR)
W	ProGuardActivity	Not sensitive information (WARN)
I	ProGuardActivity	Not sensitive information (INFO)
D	ProGuardActivity	sensitive information (DEBUG)
V	ProGuardActivity	sensitive information (VERBOSE)

Release version application (Release build)

LogCat Search Console

Search for messages. Accepts Java regexes. Prefix with pid:, app:, tag

Level	Tag	Text
E	ProGuardActivity	Not sensitive information (ERROR)
W	ProGuardActivity	Not sensitive information (WARN)
I	ProGuardActivity	Not sensitive information (INFO)

Figure 4.8-2 Difference of LogCat output
between development version application and release version application

4.8.2. Rule Book

When you output log messages, follow the rules below.

1.	Sensitive Information Must Not Be Included in Operation Log Information (Required)
2.	Construct the Build System to Auto-delete Codes which Output Development Log Information When Build for the Release (Recommended)
3.	Use Log.d()/v() Method When Outputting Throwable Object (Recommended)
4.	Use Only Methods of the android.util.Log Class for the Log Output (Recommended)

4.8.2.1. Sensitive Information Must Not Be Included in Operation Log Information (Required)

Log which was output to LogCat can be read out from other applications, so sensitive information like user's login information should not be output by release version application. It's necessary not to write code which outputs sensitive information to log during development, or it's necessary to delete all of such codes before release.

To follow this rule, first, not to include sensitive information in operation log information. In addition, it's recommended to construct the system to delete code which outputs sensitive information when build for release. Please refer to "4.8.2.2 Construct the Build System to Auto-delete Codes which Output Development Log Information When Build for the Release (Recommended)."

4.8.2.2. Construct the Build System to Auto-delete Codes which Output Development Log Information When Build for the Release (Recommended)

When application development, sometimes it's preferable if sensitive information is output to log for checking the process contents and for debugging, for example the interim operation result in the process of complicated logic, information of program's internal state, communication data structure of communication protocol. It doesn't matter to output the sensitive information as debug log during developing, in this case, the corresponding log output code should be deleted before release, as mentioned in "4.8.2.1 Sensitive Information Must Not Be Included in Operation Log Information (Required)."

To delete surely the code which outputs development log information when release builds, the system which executes code deletion automatically by using some tools, should be constructed. ProGuard, which was described in "4.8.1 Sample Code," can work for this method. As described below, there are some noteworthy points on deleting code by ProGuard. Here it's supposed to apply the system to applications which output development log information by either of Log.d()/v(), based on "4.8.3.2 Selection Standards of Log Level and Log Output Method."

ProGuard deletes unnecessary code like unused methods, automatically. By specifying Log.d()/v() as parameter of -assumenosideeffects option, call for Log.d(), Log.v() are granted as unnecessary code, and those are to be deleted.

By specifying -assumenosideeffects to Log.d()/v(), make it auto-deletion target

```
-assumenosideeffects class android.util.Log {
    public static int d(...);
    public static int v(...);
}
```

In case using this auto deletion system, pay attention that Log.v()/d() code is not deleted when using returned value of Log.v(), Log.d(), so returned value of Log.v(), Log.d(), should not be used. For example, Log.v() is not deleted in the next examination code.

Examination code which Log.v() that is specifeied to be deleted is not deketed

```
int i = android.util.Log.v("tag", "message");
System.out.println(String.format("Log.v() returned %d. ", i));  //Use the returned value of Log.v() for examination
```

If you'd like to reuse source code, you should keep the consistency of the project environment including ProGuard settings. For example, source code that presupposes Log.d() and Log.v() are deleted automatically by above ProGuard setting. If using this source code in another project which ProGuard is not set, Log.d() and Log.v() are not to be deleted, so there's a risk that the sensitive information may be leaked. When reusing source code, the consistency of project environment including ProGuard setting should be secured.

4.8.2.3. Use Log.d()/v() Method When Outputting Throwable Object (Recommended)

As mentioned in "4.8.1 Sample Code" and "4.8.3.2 Selection Standards of Log Level and Log Output Method," sensitive information should not be output to log through Log.e()/w()/i(). On the other hand, in order that a developer wants to output the details of program abnormality to log, when exception occurs, stack trace is output to LogCat by Log.e(..., Throwable tr)/w(..., Throwable tr)/i(..., Throwable tr), in some cases. However, sensitive information may sometimes be included in the stack trace because it shows detail internal structure of the program. For example, when SQLiteException is output as it is, what type of SQL statement is issued is clarified, so it may give the clue for SQL injection attack. Therefore, it's recommended that use only Log.d()/Log.v() methods, when outputting throwable object.

4.8.2.4. Use Only Methods of the android.util.Log Class for the Log Output (Recommended)

You may output log by System.out/err to verify the application's behavior whether it works as expected or not, during development. Of course, log can be output to LogCat by print()/println() method of System.out/err, but it's strongly recommended to use only methods of android.util.Log class, by the following reasons.

When outputting log, generally, use the most appropriate output method properly based on the urgency of the information, and control the output. For example, categories like serious error, caution, simple application's information notice, etc. are to be used. However, in this case, information which needs to be output at the time of release (operation log information) and information which may include the sensitive information (development log information) are output

by the same method. So, it may happen that when delete code which outputs sensitive information, it's in danger that some deletion are dropped by oversight.

Along with this, when using android.util.Log and System.out/err for log output, compared with using only android.util.Log, what needs to be considered will increase, so it's in danger that some mistakes may occur, like some deletion are dropped by oversight.

To decrease risk of above mentioned mistakes occurrence, it's recommended to use only methods of android.util.Log class.

4.8.3. Advanced Topics

4.8.3.1. Two Ways of Thinking for the Log Outputting in Release version application

There are two ways of thinking for log output in release version application. One is any log should never be output, and another is necessary information for later analysis should be output as log. It's favorable that any log should never be output in release version application from the security point of view, but sometimes, log is output even in release version application for various reasons. Each way of thinking is described as per below.

The former is "Any log should never be output," this is because outputting log in release version application is not so much valuable, and there is a risk to leak sensitive information. This comes from there's no method for developers to collect log information of the release version application in Android application operation environment, which is different from many Web application operation environments. Based on this thinking, the logging codes are used only in development phase, and all the logging codes are deleted on building release version application.

The latter is "necessary information should be output as log for the later analysis," as a final option to analyze application bugs in customer support, in case of any questions or doubt to your customer support. Based on this idea, as introduced above, it is necessary to prepare the system that prevent human errors and bring it in your project because if you don't have the system you have to keep in mind to avoid logging the sensitive information in release version application.

For more details about logging method, refer to the following document.

> Code Style Guidebook for Contributors / Log Sparingly
> http://source.android.com/source/code-style.html#log-sparingly

4.8.3.2. Selection Standards of Log Level and Log Output Method

There are five levels of log level (ERROR, WARN, INFO, DEBUG, VERBOSE) are defined in android.util.Log class in Android. You should select the most appropriate method when using the android.util.Log class to output log messages according to Table 4.8-1 which shows the selection standards of logging levels and methods.

Table 4.8-1 Selection standards of log levels and log output method

Log level	Method	Log information to be output	Cautions for application release
ERROR	`Log.e()`	Log information which is output when application is in a fatal state.	Log information as per left may be referred by users, so it could be output both in development version application and in release version application. Therefore, sensitive information should not be output in these levels.
WARN	`Log.w()`	Log information which is output when application faces the unexpected serious situation.	
INFO	`Log.i()`	Other than above, log information which is output to notify any	

		remarkable changes or results in application state.	
DEBUG	`Log.d()`	Program's internal state information which needs to be output temporarily for analyzing the cause of specific bug when developing application.	Log information as per left is only for application developers. Therefore, this type of information should not be output in case of release version application.
VERBOSE	`Log.v()`	Log information which is not applied to any of above. Log information which application developer outputs for many purposes, is applied this. For example, in case of outputting server communication data to dump.	

For more details about logging method, refer to the following document.

> Code Style Guidebook for Contributors / Log Sparingly
> http://source.android.com/source/code-style.html#log-sparingly

4.8.3.3. DEBUG Log and VERBOSE Log Are Not Always Deleted Automatically

The following is quoted from the developer reference of android.util.Log class[21].

The order in terms of verbosity, from least to most is ERROR, WARN, INFO, DEBUG, VERBOSE. Verbose should never be compiled into an application except during development. Debug logs are compiled in but stripped at runtime. Error, warning and info logs are always kept.

After reading the above texts, some developers might have misunderstood the Log class behavior as per below.

- Log.v() call is not compiled when release build, VERBOSE log is never output.
- Log.v() call is compiled, but DEBUG log is never output when execution.

However, logging methods never behave in above ways, and all messages are output regardless of whether it is compiled with debug mode or release mode. If you read the document carefully, you will be able to realize that the gist of the document is not about the behavior of logging methods but basic policies for logging.

In this chapter, we introduced the sample code to get the expected result as described above by

[21] http://developer.android.com/reference/android/util/Log.html

using ProGuard.

4.8.3.4. Remove Sensitive Information from Assembly

If you build the following code with ProGuard for the purpose of deleting Log.d() method, it is necessary to remember that ProGuard keeps the statement that construct the string for logging message (the first line of the code) even though it remove the statement of calling Log.d() method (the second line of the code).

```
    String debug_info = String.format("%s:%s", "Sensitive information1", "Sensitive information2");
    if (BuildConfig.DEBUG) android.util.Log.d(TAG, debug_info);
```

The following disassembly shows the result of release build of the code above with ProGuard. Actually, there's no Log.d() call process, but you can see that character string consistence definition like "Sensitive information1" and calling process of String#format() method, are not deleted and still remaining there.

```
    const-string v1, "%s:%s"
    const/4 v2, 0x2
    new-array v2, v2, [Ljava/lang/Object;
    const/4 v3, 0x0
    const-string v4, "Sensitive information 1"
    aput-object v4, v2, v3
    const/4 v3, 0x1
    const-string v4, "Sensitive information 2"
    aput-object v4, v2, v3
    invoke-static {v1, v2}, Ljava/lang/String;->format(Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang
/String;
    move-result-object v0
```

Actually, it's not easy to find the particular part that disassembled APK file and assembled log output information as above. However, in some application which handles the very confidential information, this type of process should not be remained in APK file in some cases.

You should implement your application like below to avoid such a consequence of remaining the sensitive information in bytecode. In release build, the following codes are deleted completely by the compiler optimization.

```
    if (BuildConfig.DEBUG) {
        String debug_info = String.format("%s:%s", " Snsitive information 1", "Sensitive information 2")
;
        if (BuildConfig.DEBUG) android.util.Log.d(TAG, debug_info);
    }
```

Besides, ProGuard cannot remove the log message of the following code ("result:" + value).

```
    Log.d(TAG, "result:" + value);
```

In this case, you can solve the problem in the following manner.


```
    if (BuildConfig.DEBUG) Log.d(TAG, "result:" + value);
```

4.8.3.5. The Contents of Intent Is Output to LogCat

When using Activity, it's necessary to pay attention, since ActivityManager outputs the content of Intent to LogCat. Refer to "4.1.3.5 Log Output When using Activities."

4.8.3.6. Restrain Log which Is Output to System.out/err

System.out/err method outputs all messages to LogCat. Android could send some messages to System.out/err even if developers did not use these methods in their code, for example, in the following cases, Android sends stack trace to System.err method.

- When using Exception#printStackTrace()
- When it's output to System.err implicitly
  (When the exception is not caught by application, it's given to Exception#printStackTrace() by the system.)

You should handle errors and exceptions appropriately since the stack trace includes the unique information of the application.

We introduce a way of changing default output destination of System.out/err. The following code redirects the output of System.out/err method to nowhere when you build a release version application. However, you should consider whether this redirection does not cause a malfunction of application or system because the code temporarily overwrites the default behavior of System.out/err method. Furthermore, this redirection is effective only to your application and is worthless to system processes.

OutputRedirectApplication.java

```
package org.jssec.android.log.outputredirection;

import java.io.IOException;
import java.io.OutputStream;
import java.io.PrintStream;

import android.app.Application;

public class OutputRedirectApplication extends Application {

    // PrintStream which is not output anywhere
    private final PrintStream emptyStream = new PrintStream(new OutputStream() {
        public void write(int oneByte) throws IOException {
            // do nothing
        }
    });

    @Override
    public void onCreate() {
        // Redirect System.out/err to PrintStream which doesn't output anywhere, when release build.
```

```
        // Save original stream of System.out/err
        PrintStream savedOut = System.out;
        PrintStream savedErr = System.err;

        // Once, redirect System.out/err to PrintStream which doesn't output anywhere
        System.setOut(emptyStream);
        System.setErr(emptyStream);

        // Restore the original stream only when debugging. (In release build, the following 1 line is de
leted byProGuard.)
        resetStreams(savedOut, savedErr);
    }

    // All of the following methods are deleted byProGuard when release.
    private void resetStreams(PrintStream savedOut, PrintStream savedErr) {
        System.setOut(savedOut);
        System.setErr(savedErr);
    }
}
```

AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.log.outputredirection" >

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:name=".OutputRedirectApplication"
        android:allowBackup="false" >
        <activity
            android:name=".LogActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

proguard-project.txt

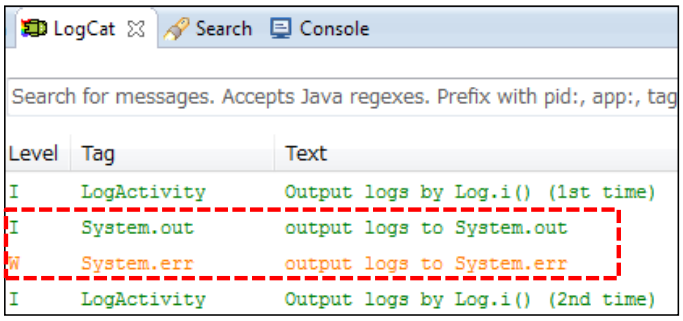
```
# Prevent from changing class name and method name, etc
-dontobfuscate

# In release build, delete call from Log.d()/v() automatically.
-assumenosideeffects class android.util.Log {
    public static int d(...);
    public static int v(...);
}

# In release build, delete resetStreams() automatically.
-assumenosideeffects class org.jssec.android.log.outputredirection.OutputRedirectApplication {
    private void resetStreams(...);
}
```


The difference of LogCat output between development version application (debug build) and release version application (release build) are shown as per below Figure 4.8-3.

Development version application (Debug build)



Release version application (Release build)

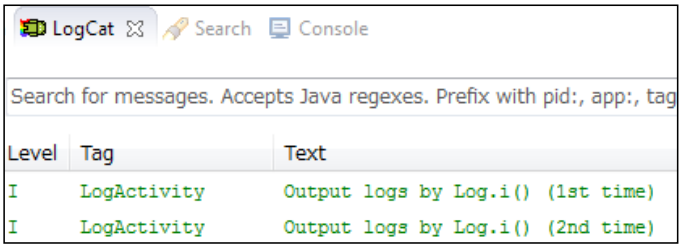


Figure 4.8-3 Difference of System.out/err in LogCat output, between development application and release application

WebView enables your application to integrate HTML/JavaScript content.

4.9.1. Sample Code

We need to take proper action, depending on what we'd like to show through WebView although we can easily show web site and html file by it. And also we need to consider risk from WebView's remarkable function; such as JavaScript-Java object bind.

Especially what we need to pay attention is JavaScript. (Please note that JavaScript is disabled as default. And we can enable it by WebSettings#setJavaScriptEnabled()). With enabling JavaScript, there is potential risk that malicious third party can get device information and operate your device.

The following is principle for application with WebView[22]:

(1) You can enable JavaScript if the application uses contents which are managed in house.
(2) You should NOT enable JavaScript other than the above case.

Figure 4.9-1 shows flow chart to choose sample code according to content characteristic.

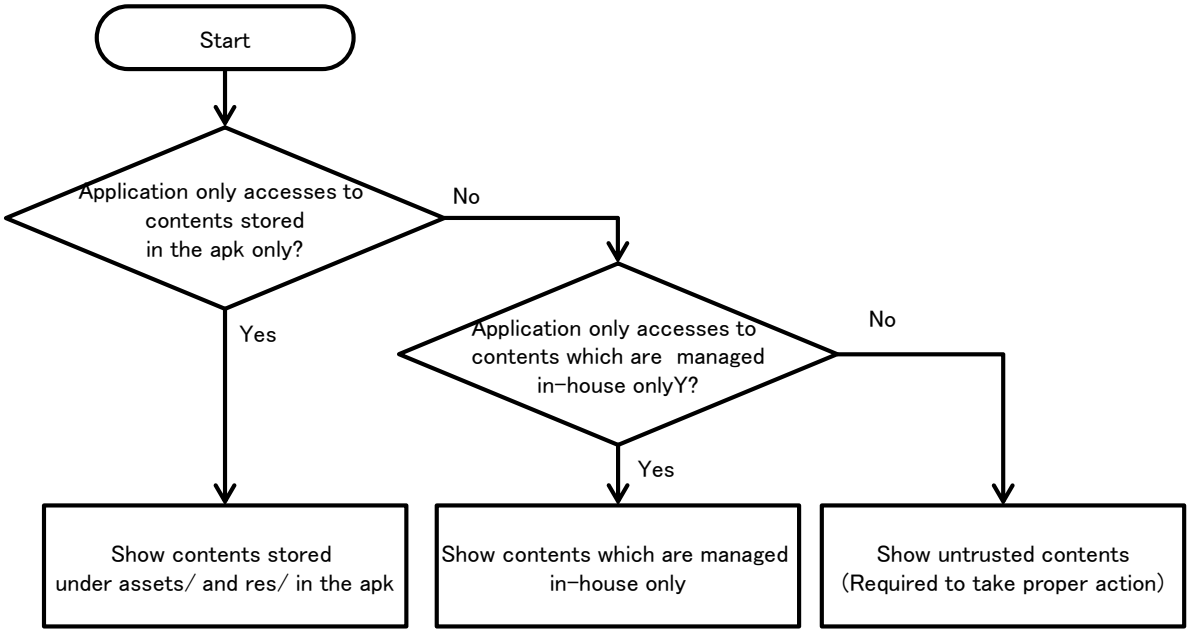


Figure 4.9-1 Flow Figure to select Sample code of WebView

[22]Strictly speaking, you can enable JavaScript if we can say the content is safe. If the contents are managed in house, the contents should be guaranteed of security. And the company can secure them. In other words, we need to have business representation's decision to enable JavaScript for other company's contents. The contents which are developed by trusted partner might have security guarantee. But there is still potential risk. Therefore the decision is needed by responsible person.

4.9.1.1. Show Only Contents Stored under assets/res Directory in the APK

You can enable JavaScript if your application shows only contents stored under assets/ and res/ directory in apk.

The following sample code shows how to use WebView to show contents stored under assets/ and res/.

Points:

1. Disable to access files (except files under assets/ and res/ in apk).
2. You may enable JavaScript.

WebViewAssetsActivity.java

```
package org.jssec.webview.assets;

import android.app.Activity;
import android.os.Bundle;
import android.webkit.WebSettings;
import android.webkit.WebView;

public class WebViewAssetsActivity extends Activity {
    /**
     * Show contents in assets
     */
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        WebView webView = (WebView) findViewById(R.id.webView);
        WebSettings webSettings = webView.getSettings();

        // *** POINT 1 *** Disable to access files (except files under assets/ and res/ in this apk)
        webSettings.setAllowFileAccess(false);

        // *** POINT 2 *** Enable JavaScript (Optional)
        webSettings.setJavaScriptEnabled(true);

        // Show contents which were stored under assets/ in this apk
        webView.loadUrl("file:///android_asset/sample/index.html");
    }
}
```

4.9.1.2. Show Only Contents which Are Managed In-house

You can enable JavaScript to show only contents which are managed in-house only if your web service and your Android application can take proper actions to secure both of them.

- Web service side actions:

As Figure 4.9-2 shows, your web service can only refer to contents which are managed in-house. In addition, the web service is needed to take appropriate security action. Because there is potential risk if contents which your web service refers to may have risk; such as malicious attack code injection, data manipulation, etc.

Please refer to "4.9.2.1 Enable JavaScript Only If Contents Are Managed In-house (Required)."

- Android application side actions:

Using HTTPS, the application should establish network connection to your managed web service only if the certification is trusted.

The following sample code is an activity to show contents which are managed in-house.

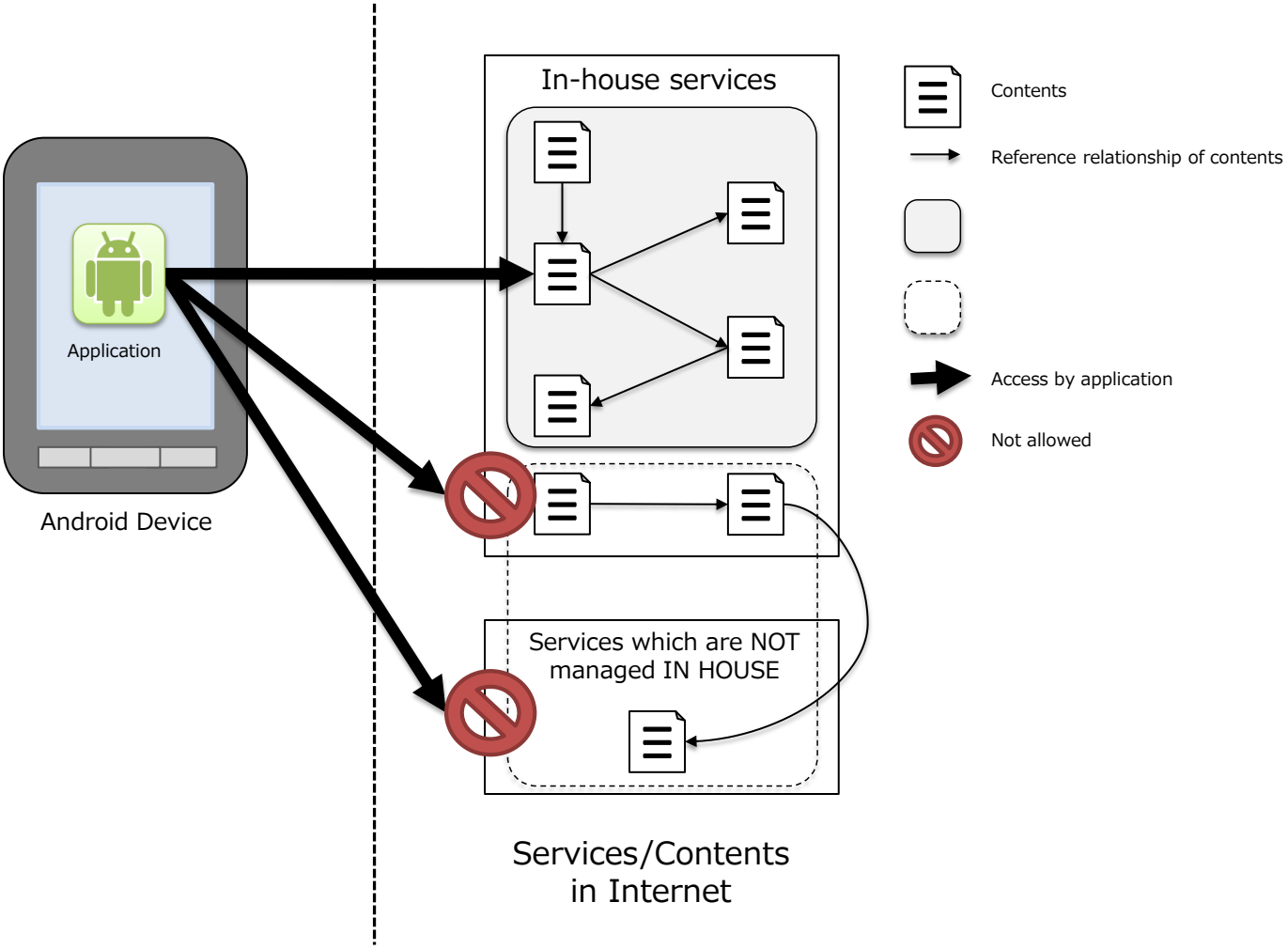


Figure 4.9-2 Accessible contents and Non-accessible contents from application

Points:

1. Handle SSL error from WebView appropriately.
2. (Optional) Enable JavaScript of WebView.
3. Restrict URLs to HTTPS protocol only.
4. Restrict URLs to in-house.

WebViewTrustedContentsActivity.java

```
package org.jssec.webview.trustedcontents;

import android.app.Activity;
import android.app.AlertDialog;
import android.content.DialogInterface;
import android.net.http.SslCertificate;
import android.net.http.SslError;
import android.os.Bundle;
import android.webkit.SslErrorHandler;
import android.webkit.WebView;
import android.webkit.WebViewClient;

import java.text.SimpleDateFormat;

public class WebViewTrustedContentsActivity extends Activity {
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
        WebView webView = (WebView) findViewById(R.id.webView);

        webView.setWebViewClient(new WebViewClient() {
            @Override
            public void onReceivedSslError(WebView view,
                    SslErrorHandler handler, SslError error) {
                // *** POINT 1 *** Handle SSL error from WebView appropriately
                // Show SSL error dialog.
                AlertDialog dialog = createSslErrorDialog(error);
                dialog.show();

                // *** POINT 1 *** Handle SSL error from WebView appropriately
                // Abort connection in case of SSL error
                // Since, there may be some defects in a certificate like expiration of validity,
                // or it may be man-in-the-middle attack.
                handler.cancel();
            }
        });

        // *** POINT 2 *** Enable JavaScript (optional)
        // in case to show contents which are managed in house.
        webView.getSettings().setJavaScriptEnabled(true);

        // *** POINT 3 *** Restrict URLs to HTTPS protocol only
        // *** POINT 4 *** Restrict URLs to in-house
        webView.loadUrl("https://url.to.your.contents/");
    }

    private AlertDialog createSslErrorDialog(SslError error) {
        // Error message to show in this dialog
        String errorMsg = createErrorMessage(error);
        // Handler for OK button
```

```
        DialogInterface.OnClickListener onClickOk = new DialogInterface.OnClickListener() {
            @Override
            public void onClick(DialogInterface dialog, int which) {
                setResult(RESULT_OK);
            }
        };
        // Create a dialog
        AlertDialog dialog = new AlertDialog.Builder(
                WebViewTrustedContentsActivity.this).setTitle("SSL connection error")
                .setMessage(errorMsg).setPositiveButton("OK", onClickOk)
                .create();
        return dialog;
    }

    private String createErrorMessage(SslError error) {
        SslCertificate cert = error.getCertificate();
        SimpleDateFormat dateFormat = new SimpleDateFormat("yyyy/MM/dd HH:mm:ss");
        StringBuilder result = new StringBuilder()
        .append("The site's certification is NOT valid. Connection was disconnected.¥n¥nError:¥n");
        switch (error.getPrimaryError()) {
        case SslError.SSL_EXPIRED:
            result.append("The certificate is no longer valid.¥n¥nThe expiration date is ")
            .append(dateFormat.format(cert.getValidNotAfterDate()));
            return result.toString();
        case SslError.SSL_IDMISMATCH:
            result.append("Host name doesn't match. ¥n¥nCN=")
            .append(cert.getIssuedTo().getCName());
            return result.toString();
        case SslError.SSL_NOTYETVALID:
            result.append("The certificate isn't valid yet.¥n¥nIt will be valid from ")
            .append(dateFormat.format(cert.getValidNotBeforeDate()));
            return result.toString();
        case SslError.SSL_UNTRUSTED:
            result.append("Certificate Authority which issued the certificate is not reliable.¥n¥nCertif
icate Authority¥n")
            .append(cert.getIssuedBy().getDName());
            return result.toString();
        default:
            result.append("Unknown error occured. ");
            return result.toString();

        }
    }

}
```


4.9.1.3. Show Contents which Are Not Managed In-house

Don't enable JavaScript if your application shows contents which are not managed in house because there is potential risk to access to malicious content.

The following sample code is an activity to show contents which are not managed in-house.

This sample code shows contents specified by URL which user inputs through address bar. Please note that JavaScript is disabled and connection is aborted when SSL error occurs. The error handling is the same as "4.9.1.2 Show Only Contents which Are Managed In-house" for the details of HTTPS communication. Please refer to "5.4 Communicating via HTTPS" for the details also.

Points:

1. Handle SSL error from WebView appropriately.
2. Disable JavaScript of WebView.

WebViewUntrustActivity.java

```
package org.jssec.webview.untrust;

import android.app.Activity;
import android.app.AlertDialog;
import android.content.DialogInterface;
import android.graphics.Bitmap;
import android.net.http.SslCertificate;
import android.net.http.SslError;
import android.os.Bundle;
import android.view.View;
import android.webkit.SslErrorHandler;
import android.webkit.WebView;
import android.webkit.WebViewClient;
import android.widget.Button;
import android.widget.EditText;

import java.text.SimpleDateFormat;

public class WebViewUntrustActivity extends Activity {
    /*
     * Show contents which are NOT managed in-house (Sample program works as a simple browser)
     */

    private EditText textUrl;
    private Button buttonGo;
    private WebView webView;

    // Activity definition to handle any URL request
    private class WebViewUnlimitedClient extends WebViewClient {

        @Override
        public boolean shouldOverrideUrlLoading(WebView webView, String url) {
            webView.loadUrl(url);
            textUrl.setText(url);
            return true;
        }
```

```
        // Start reading Web page
        @Override
        public void onPageStarted(WebView webview, String url, Bitmap favicon) {
            buttonGo.setEnabled(false);
            textUrl.setText(url);
        }

        // Show SSL error dialog
        // And abort connection.
        @Override
        public void onReceivedSslError(WebView webview,
                SslErrorHandler handler, SslError error) {

            // *** POINT 1 *** Handle SSL error from WebView appropriately
            AlertDialog errorDialog = createSslErrorDialog(error);
            errorDialog.show();
            handler.cancel();
            textUrl.setText(webview.getUrl());
            buttonGo.setEnabled(true);
        }

        // After loading Web page, show the URL in EditText.
        @Override
        public void onPageFinished(WebView webview, String url) {
            textUrl.setText(url);
            buttonGo.setEnabled(true);
        }
    }

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);

        webView = (WebView) findViewById(R.id.webview);
        webView.setWebViewClient(new WebViewUnlimitedClient());

        // *** POINT 2 *** Disable JavaScript of WebView
        // Explicitly disable JavaScript even though it is disabled by default.
        webView.getSettings().setJavaScriptEnabled(false);

        webView.loadUrl(getString(R.string.texturl));
        textUrl = (EditText) findViewById(R.id.texturl);
        buttonGo = (Button) findViewById(R.id.go);
    }

    public void onClickButtonGo(View v) {
        webView.loadUrl(textUrl.getText().toString());
    }

    private AlertDialog createSslErrorDialog(SslError error) {
        // Error message to show in this dialog
        String errorMsg = createErrorMessage(error);
        // Handler for OK button
        DialogInterface.OnClickListener onClickOk = new DialogInterface.OnClickListener() {
            @Override
            public void onClick(DialogInterface dialog, int which) {
                setResult(RESULT_OK);
            }
        };
```



```
        // Create a dialog
        AlertDialog dialog = new AlertDialog.Builder(
                WebViewUntrustActivity.this).setTitle("SSL connection error")
                .setMessage(errorMsg).setPositiveButton("OK", onClickOk)
                .create();
        return dialog;
    }

    private String createErrorMessage(SslError error) {
        SslCertificate cert = error.getCertificate();
        SimpleDateFormat dateFormat = new SimpleDateFormat("yyyy/MM/dd HH:mm:ss");
        StringBuilder result = new StringBuilder()
        .append("The site's certification is NOT valid. Connection was disconnected.¥n¥nError:¥n");
        switch (error.getPrimaryError()) {
        case SslError.SSL_EXPIRED:
            result.append("The certificate is no longer valid.¥n¥nThe expiration date is ")
            .append(dateFormat.format(cert.getValidNotAfterDate()));
            return result.toString();
        case SslError.SSL_IDMISMATCH:
            result.append("Host name doesn't match. ¥n¥nCN=")
            .append(cert.getIssuedTo().getCName());
            return result.toString();
        case SslError.SSL_NOTYETVALID:
            result.append("The certificate isn't valid yet.¥n¥nIt will be valid from ")
            .append(dateFormat.format(cert.getValidNotBeforeDate()));
            return result.toString();
        case SslError.SSL_UNTRUSTED:
            result.append("Certificate Authority which issued the certificate is not reliable.¥n¥nCertif
icate Authority¥n")
            .append(cert.getIssuedBy().getDName());
            return result.toString();
        default:
            result.append("Unknown error occured. ");
            return result.toString();
        }
    }
}
```

4.9.2. Rule Book

Comply with following rule when you need to use WebView.

1.	Enable JavaScript Only If Contents Are Managed In-house	(Required)
2.	Use HTTPS to Communicate to Servers which Are Managed In-house	(Required)
3.	Disable JavaScript to Show URLs Which Are Received through Intent, etc.	(Required)
4.	Handle SSL Error Properly	(Required)

4.9.2.1. Enable JavaScript Only If Contents Are Managed In-house (Required)

What we have to pay attention on WebView is whether we enable the JavaScript or not. As principle, we can only enable the JavaScript only IF the application will access to services which are managed in-house. And you must not enable the JavaScript if there is possibility to access services which are not managed in-house.

Services managed In-house

In case that application accesses contents which are developed IN HOUSE and are distributed through servers which are managed IN HOUSE, we can say that the contents are ONLY modified by your company. In addition, it is also needed that each content refers to only contents stored in the servers which have proper security.

In this scenario, we can enable JavaScript on the WebView. Please refer to "4.9.1.2 Show Only Contents which Are Managed In-house" also.

And you can also enable JavaScript if your application shows only contents stored under assets/ and res/ directory in the apk. Please refer to "4.9.1.1 Show Only Contents Stored under assets/res Directory" also.

Services unmanaged in-house

You must NOT think you can secure safety on contents which are NOT managed IN HOUSE. Therefore you have to disable JavaScript. Please refer to "4.9.1.3 Show Contents which Are Not Managed In-house."

In addition, you have to disable JavaScript if the contents are stored in external storage media; such as microSD because other application can modify the contents.

4.9.2.2. Use HTTPS to Communicate to Servers which Are Managed In-house (Required)

You have to use HTTPS to communicate to servers which are managed in-house because there is potential risk of spoofing the services by malicious third party.

Please refer to both "4.9.2.4 Handle SSL Error Properly (Required)," and "5.4 Communicating via HTTPS".

4.9.2.3. Disable JavaScript to Show URLs Which Are Received through Intent, etc. (Required)

Don't enable JavaScript if your application needs to show URLs which are passed from other application as Intent, etc. Because there is potential risk to show malicious web page with malicious JavaScript.

Sample code in the section "4.9.1.2 Show Only Contents which Are Managed In-house," uses fixed value URL to show contents which are managed in-house, to secure safety.

If you need to show URL which is received from Intent, etc., you have to confirm that URL is in managed URL in-house. In short, the application has to check URL with white list which is regular expression, etc. In addition, it should be HTTPS.

4.9.2.4. Handle SSL Error Properly (Required)

You have to terminate the network communication and inform error notice to user when SSL error happens on HTTPS communication.

SSL error shows invalid server certification risk or MTIM (man-in-the-middle attack) risk. Please note that WebView has NO error notice mechanism regarding SSL error. Therefore your application has to show the error notice to inform the risk to the user. Please refer to sample code in the section of "4.9.1.2 Show Only Contents which Are Managed In-house," and "4.9.1.3 Show Contents which Are Not Managed In-house".

In addition, your application MUST terminate the communication with the error notice.
In other words, you MUST NOT do following.

- Ignore the error to keep the transaction with the service.
- Retry HTTP communication instead of HTTPS.

Please refer to the detail described in "5.4 Communicating via HTTPS".

WebView's default behavior is to terminate the communication in case of SSL error. Therefore what we need to add is to show SSL error notice. And then we can handle SSL error properly.

4.9.3. Advanced Topics

4.9.3.1. Vulnerability caused by addJavascriptInterface() at Android versions 4.1 or earlier

Android versions under 4.2（API Level 17） have a vulnerability caused by addJavascriptInterface(), which could allow attackers to call native Android methods (Java) via JavaScript on WebView.

As explained in "4.9.2.1 Enable JavaScript Only If Contents Are Managed In-house (Required)", JavaScript must not be enabled if the services could access services out of in-house control.

In Android 4.2（API Level 17） or later, the measure of the vulnerability has been taken to limit access from JavaScript to only methods with @JavascriptInterface annotation on Java source codes instead of all methods of Java objects injected. However it is necessary to disable JavaScript if the services could access services out of in-house control as mentioned in "4.9.2.1".

4.9.3.2. Issue caused by file scheme

In case of using WebView with default settings, all files that the app has access rights can be accessed to by using the file scheme in web pages regardless of the page origins. For example, a malicious web page could access the files stored in the app's private directory by sending a request to the uri of a private file of the app with the file scheme.

A countermeasure is to disable JavaScript as explained in "4.9.2.1 Enable JavaScript Only If Contents Are Managed In-house (Required)" if the services could access services out of in-house control. Doing that is to protect against sending the malicious file scheme request.

Also in case of Android 4.1 (API Level 16) or later, setAllowFileAccessFromFileURLs() and setAllowUniversalAccessFromFileURLs() can be used to limit access via the file scheme.

Disabling the file scheme

```
webView = (WebView) findViewById(R.id.webview);
webView.setWebViewClient(new WebViewUnlimitedClient());
WebSettings settings = webView.getSettings();
settings.setAllowUniversalAccessFromFileURLs(false);
settings.setAllowFileAccessFromFileURLs(false);
```

4.9.3.3. Specifying a Sender Origin When Using Web Messaging

Android 6.0 (API Level 23) adds an API for realizing HTML5 Web Messaging. Web Messaging is a framework defined in HTML5 for sending and receiving data between different browsing contexts.[23]

The postWebMessage() method added to the WebView class is a method for processing data

[23] http://www.w3.org/TR/webmessaging/

transmissions via the Cross-domain messaging protocol defined by Web Messaging.

This method sends a message object—specified by its first parameter—from the browsing context that has been read into WebView; however, in this case it is necessary to specify the origin of the sender as the second parameter. If the specified origin[24] does not agree with the origin in the sender context, the message will not be sent. By placing restrictions on the sender origin in this way, this mechanism aims to prevent the passing of messages to unintended senders.

However, it is important to note that wildcards may be specified as the origin in the postWebMessage() method.[25] If wildcards are specified, the sender origin of the message is not checked, and the message may be sent from any arbitrary origin. In a situation in which malicious content has been read into WebView, various types of harm or damage may result if important messages are sent without origin restrictions. Thus, when using WebView for Web messaging, it is best to specify explicitly a specific origin in the postWebMessage() method.

[24] An "origin" is a URL scheme together with a host name and port number. For the detailed definition see http://tools.ietf.org/html/rfc6454.

[25] Note that Uri.EMPTY and Uri.parse("") function as wildcards (at the time of writing the September 1, 2016 version).

Android offers the Notification feature for sending messages to end users. Using a Notification causes a region known as a status bar to appear on the screen, inside which you may display icons and messages.

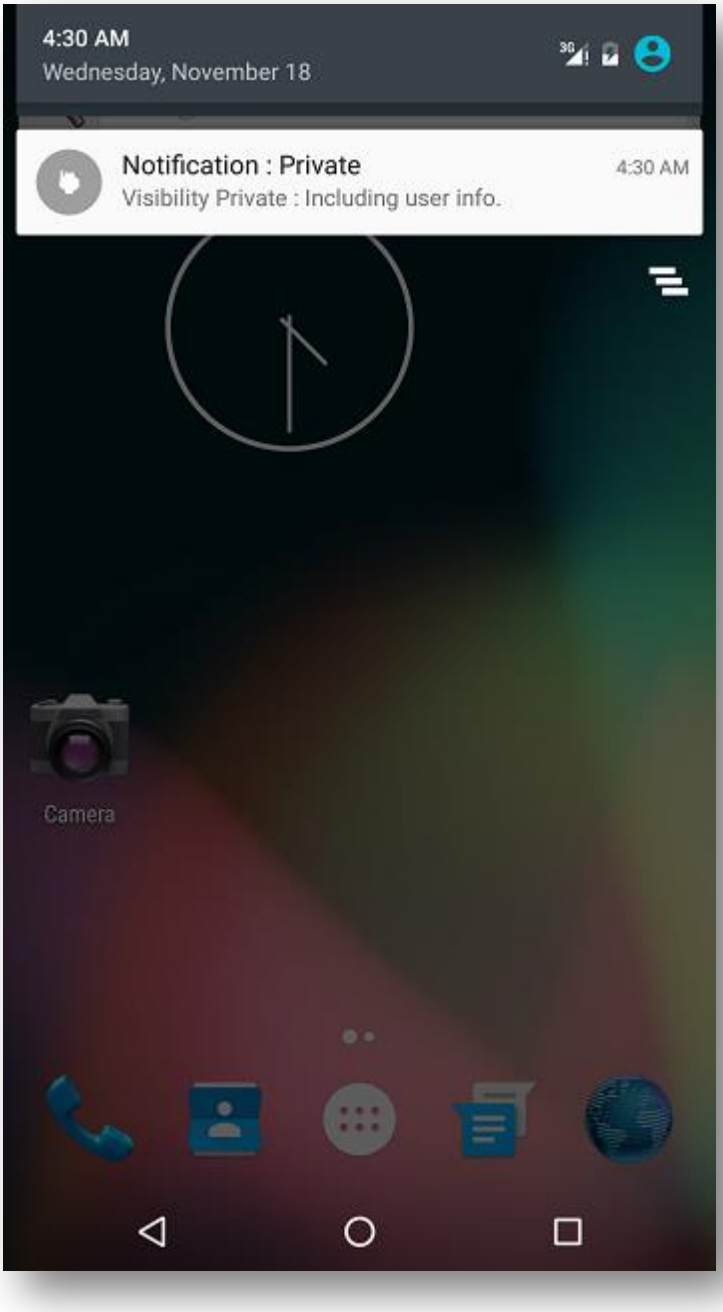


Figure 4.10-1 An example of a Notification

The communication functionality of Notifications is enhanced in Android 5.0 (API Level 21) to allow messages to be displayed via Notifications even when the screen is locked, depending on user and application settings. However, incorrect use of Notifications runs the risk that private information—which should only be shown to the terminal user herself—may be seen by third parties. For this reason, this functionality must be implemented with careful attention paid to privacy and

security.

The possible values for the Visibility option and the corresponding behavior of Notifications is summarized in the following table.

Visibility value	Behavior of Notifications
Public	Notifications are displayed on all locked screens.
Private	Notifications are displayed on all locked screens; however, on locked screens that have been password-protected (secure locks), fields such as the title and text of the Notification are hidden (replaced by publicly-releasable messages in which private information is hidden).
Secret	Notifications are not displayed on locked screens that are protected by passwords or other security measures (secure locks). (Notifications are displayed on locked screens that do not involve secure locks.)

4.10.1. Sample Code

When a Notification contains private information regarding the terminal user, a message from which the private information has been excluded must be prepared and added to be displayed in the event of a locked screen.

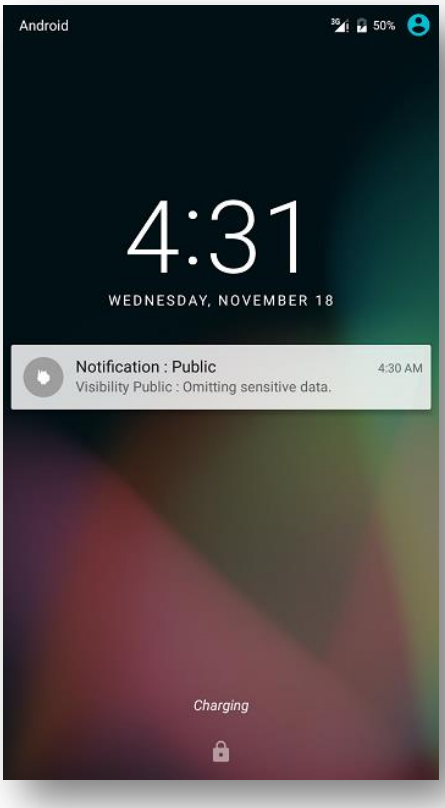


Figure 4.10-2 A notification on a locked screen

Sample code illustrating the proper use of Notifications for messages containing private data is shown below.

Points:

1. When using Notifications for messages containing private data, prepare a version of the Notification that is suitable for public display (to be displayed when the screen is locked).
2. Do not include private information in Notifications prepared for public display (displayed when the screen is locked).
3. Explicitly set Visibility to Private when creating Notifications.
4. When Visibility is set to Private, Notifications may contain private information.

VisibilityPrivateNotificationActivity.java

```
package org.jssec.notification.visibilityPrivate;

import android.app.Activity;
import android.app.Notification;
import android.app.NotificationManager;
import android.content.Context;
import android.os.Build;
import android.os.Bundle;
import android.view.View;

public class VisibilityPrivateNotificationActivity extends Activity {
    /**
     * Display a private Notification
     */
    private final int mNotificationId = 0;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
    }

    public void onSendNotificationClick(View view) {
        // *** POINT 1 *** When preparing a Notification that includes private information, prepare an a
dditional Noficiation for public display (displayed when the screen is locked).
        Notification.Builder publicNotificationBuilder = new Notification.Builder(this).setContentTitle
("Notification : Public");

        if (Build.VERSION.SDK_INT >= 21)
            publicNotificationBuilder.setVisibility(Notification.VISIBILITY_PUBLIC);
        // *** POINT 2 *** Do not include private information in Notifications prepared for public displ
ay (displayed when the screen is locked).
        publicNotificationBuilder.setContentText("Visibility Public : Omitting sensitive data.");
        publicNotificationBuilder.setSmallIcon(R.drawable.ic_launcher);
        Notification publicNotification = publicNotificationBuilder.build();

        // Construct a Notification that includes private information.
        Notification.Builder privateNotificationBuilder = new Notification.Builder(this).setContentTitl
e("Notification : Private");

        // *** POINT 3 *** Explicitly set Visibility to Private when creating Notifications.
        if (Build.VERSION.SDK_INT >= 21)
            privateNotificationBuilder.setVisibility(Notification.VISIBILITY_PRIVATE);
```



```
        // *** POINT 4 *** When Visibility is set to Private, Notifications may contain private informat
ion.
        privateNotificationBuilder.setContentText("Visibility Private : Including user info.");
        privateNotificationBuilder.setSmallIcon(R.drawable.ic_launcher);
        // When creating a Notification with Visibility=Private, we also create and register a separate
Notification with Visibility=Public for public display.
        if (Build.VERSION.SDK_INT >= 21)
            privateNotificationBuilder.setPublicVersion(publicNotification);

        Notification privateNotification = privateNotificationBuilder.build();
        //Although not implemented in this sample code, in many cases
        //Notifications will use setContentIntent(PendingIntent intent)
        //to ensure that an Intent is transmission when Notification
        //is clicked. In this case, it is necessary to take steps--depending
        //on the type of component being called--to ensure that the Intent
        //in question is called by safe methods (for example, by explicitly
        //using Intent). For information on safe methods for calling various
        //types of component, see the following sections.
        //4.1. Creating and using Activities
        //4.2. Sending and receiving Broadcasts
        //4.4. Creating and using Services

        NotificationManager notificationManager = (NotificationManager) this.getSystemService(Context.N
OTIFICATION_SERVICE);
        notificationManager.notify(mNotificationId, privateNotification);
    }
}
```

4.10.2. Rule Book

When creating Notification, the following rules must be observed.

1.	Regardless of the Visibility setting, Notifications must not contain sensitive information (although private information is an exception)
2.	Notifications with Visibility=Public must not contain private information (Required)
3.	For Notifications that contain private information, Visibility must be explicitly set to Private or Secret (Required)
4.	When using Notifications with Visibility=Private, create an additional Notification with Visibility=Public for public display (Recommended)

4.10.2.1. Regardless of the Visibility setting, Notifications must not contain sensitive information (although private information is an exception) (Required)

On terminals using Android4.3 (API Level 18) or later, users can use the Settings window to grant apps permission to read Notifications. Apps granted this permission will be able to read all information in Notifications; for this reason, sensitive information must not be included in Notifications. (However, private information may be included in Notifications depending on the Visibility setting).

Information contained in Notifications may generally not be read by apps other than the app that sent the Notification. However, users may explicitly grant permission to certain user-selected apps to read all information in Notifications. Because only apps that have been granted user permission may read information in Notifications, there is nothing problematic about including private information on the user within the Notification. On the other hand, if sensitive information other than the user's private information (for example, secret information known only to the app developers) is include in a Notification, the user herself may attempt to read the information contained in the Notification and may grant applications permission to view this information as well; thus the inclusion of sensitive information other than private user information is problematic.

For specific methods and conditions, see Section “4.10.3.1 On User-granted Permission to View Notifications”.

4.10.2.2. Notifications with Visibility=Public must not contain private information (Required)

When sending Notifications with Visibility=Public, private user information must not be included in the Notification. When a Notifications has the setting Visibility=Public, the information in the Notification is displayed even when the screen is locked. This is because such Notifications carry the risk that private information might be seen and stolen by a third party in physical proximity to the terminal.

VisibilityPrivateNotificationActivity.java

```
        // Prepare a Notification for public display (to be displayed on locked screens) that does not co
ntain sensitive information
Notification.Builder publicNotificationBuilder = new Notification.Builder(this).setContentTitle("Notifi
cation : Public");

        publicNotificationBuilder.setVisibility(Notification.VISIBILITY_PUBLIC);
        // Do not include private information in Notifications for public display (to be displayed on lo
cked screens)
        publicNotificationBuilder.setContentText("Visibility Public: sending notification without sensit
ive information ");
        publicNotificationBuilder.setSmallIcon(R.drawable.ic_launcher);
```

4.10.2.3. For Notifications that contain private information, Visibility must be explicitly set to Private or Secret (Required)

Terminals using Android 5.0 (API Level 21) or later will display Notifications even when the screen is locked. Thus, when the Notification contains private information, its Visibility flag should be set explicitly to Private or Secret. This is to protect against the risk of private information contained in a Notification being displayed on a locked screen.

At present, the default value of Visibility is set to Private for Notifications, so the aforementioned risk will only arise if this flag is explicitly changed to Public. However, the default value of Visibility may change in the future; for this reason, and also for the purpose of clearly communicating one's intentions at all times when handling information, it is mandatory to set Visibility=Private explicitly for Notifications that contain private information.

VisibilityPrivateNotificationActivity.java

```
        // Create a Notification that includes private information
        Notification.Builder priavteNotificationBuilder = new Notification.Builder(this).setContentTitl
e("Notification : Private");

        // *** POINT *** Explicitly set Visibility=Private when creating the Notification
        priavteNotificationBuilder.setVisibility(Notification.VISIBILITY_PRIVATE);
```

Typical examples of private information include emails sent to the user, the user's location data, and other items listed in Section “5.5 Handling privacy data".

On terminals using Android4.3 (API Level 18) or later, users can use the Settings window to grant apps permission to read Notifications. Apps granted this permission will be able to read all information in Notifications; for this reason, sensitive information other than private user information must not be included in Notifications.

4.10.2.4. When using Notifications with Visibility=Private, create an additional Notification with Visibility=Public for public display (Recommended)

When communicating information via a Notification with Visibility=Private, it is desirable to create simultaneously an additional Notification, for public display, with Visibility=Public; this is to restrict

the information displayed on locked screens.

If a public-display Notification is not registered together with a Visibility=Private notification, a default message prepared by the operating system will be displayed when the screen is locked. Thus there is no security problem in this case. However, for the purpose of clearly communicating one's intentions at all times when handling information, it is recommended that a public-display Notification be explicitly created and registered.

VisibilityPrivateNotificationActivity.java

```
        // Create a Notification that contains private information
        Notification.Builder privateNotificationBuilder = new Notification.Builder(this).setContentTitl
e("Notification : Private");

        // *** POINT *** Explicitly set Visibility=Private when creating the Notification
        if (Build.VERSION.SDK_INT >= 21)
            privateNotificationBuilder.setVisibility(Notification.VISIBILITY_PUBLIC);
        // *** POINT *** Notifications with Visibility=Private may include private information
        privateNotificationBuilder.setContentText("Visibility Private : Including user info.");
        privateNotificationBuilder.setSmallIcon(R.drawable.ic_launcher);
        // When creating a Notification with Visibility=Private, simultaneously create and register a pu
blic-display Notification with Visibility=Public
        if (Build.VERSION.SDK_INT >= 21)
            privateNotificationBuilder.setPublicVersion(publicNotification);
```


4.10.3. Advanced Topics

4.10.3.1. On User-granted Permission to View Notifications

As noted above in Section "4.10.2.1 Regardless of the Visibility setting, Notifications must not contain sensitive information (although private information is an exception) ", on terminals using Android 4.3 (API Level 18) or later, certain user-selected apps that have been granted user permission may read information in all Notifications.

However, in order for an app to be eligible to receive this user permission, the app must implement a Service derived from NotificationListenerService.

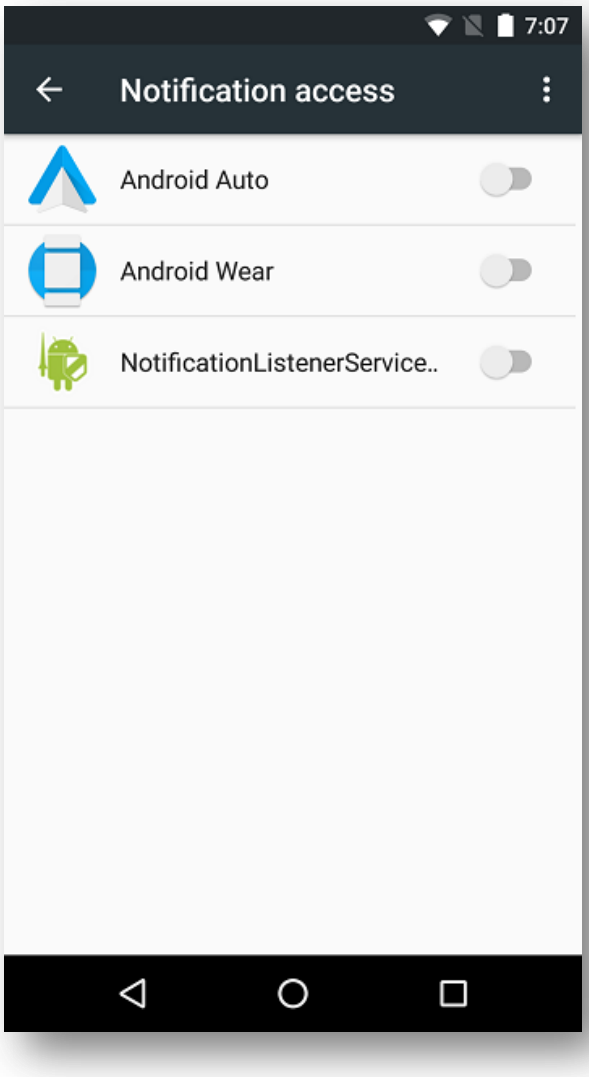


Figure 4.10-3 The Access to Notifications window, from which Notification read controls may be configured

The following sample code illustrates the use of NotificationListenerService.

AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.notification.notificationListenerService">

     <application
         android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >
         <service android:name=".MyNotificationListenerService"
             android:label="@string/app_name"
             android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
             <intent-filter>
                 <action android:name=
                     "android.service.notification.NotificationListenerService" />
             </intent-filter>
         </service>
     </application>
</manifest>
```

MyNotificationListenerService.java

```
package org.jssec.notification.notificationListenerService;

import android.app.Notification;
import android.service.notification.NotificationListenerService;
import android.service.notification.StatusBarNotification;
import android.util.Log;

public class MyNotificationListenerService extends NotificationListenerService {
    @Override
    public void onNotificationPosted(StatusBarNotification sbn) {
        // Notification is posted.
        outputNotificationData(sbn, "Notification Posted : ");
    }

    @Override
    public void onNotificationRemoved(StatusBarNotification sbn) {
        // Notification is deleted.
        outputNotificationData(sbn, "Notification Deleted : ");
    }

    private void outputNotificationData(StatusBarNotification sbn, String prefix) {
        Notification notification = sbn.getNotification();
        int notificationID = sbn.getId();
        String packageName = sbn.getPackageName();
        long PostTime = sbn.getPostTime();

        String message = prefix + "Visibility :" + notification.visibility + " ID : " + notificationID;
        message += " Package : " + packageName + " PostTime : " + PostTime;

        Log.d("NotificationListen", message);
    }
}
```

As discussed above, by using NotificationListenerService to obtain user permission it is possible to read Notifications. However, because the information contained in Notifications frequently includes private information on the terminal, care is required in handling such information.

5. How to use Security Functions

There are various security functions prepared in Android, like encryption, digital signature and permission etc. If these security functions are not used correctly, security functions don't work efficiently and loophole will be prepared. This chapter will explain how to use the security functions properly.

5.1. Creating Password Input Screens

5.1.1. Sample Code

When creating password input screen, some points to be considered in terms of security, are described here. Only what is related to password input is mentioned, here. Regarding how to save password, another articles is planned to be published is future edition.

Figure 5.1-1

Points:

1. The input password should be mask displayed (Display with *)
2. Provide the option to display the password in a plain text.
3. Alert a user that displaying password in a plain text has a risk.

Points: When handling the last Input password, pay attention the following points along with the above points.

4. In the case there is the last input password in an initial display, display the fixed digit numbers of black dot as dummy in order not that the digits number of last password is guessed.
5. When the dummy password is displayed and the "Show password" button is pressed, clear the last input password and provide the state for new password input.
6. When last input password is displayed with dummy, in case user tries to input password, clear the last input password and treat new user input as a new password.

password_activity.xml

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
    android:layout_width="fill_parent"
    android:layout_height="fill_parent"
    android:orientation="vertical"
    android:padding="10dp" >

    <!-- Label for password item -->
    <TextView
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:text="@string/password" />

    <!-- Label for password item -->
    <!-- *** POINT 1 *** The input password must be masked (Display with black dot) -->
    <EditText
        android:id="@+id/password_edit"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:hint="@string/hint_password"
        android:inputType="textPassword" />

    <!-- *** POINT 2 *** Provide the option to display the password in a plain text -->
    <CheckBox
        android:id="@+id/password_display_check"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:text="@string/display_password" />

    <!-- *** POINT 3 *** Alert a user that displaying password in a plain text has a risk. -->
    <TextView
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:text="@string/alert_password" />

    <!-- Cancel/OK button -->
    <LinearLayout
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_marginTop="50dp"
        android:gravity="center"
        android:orientation="horizontal" >

        <Button
            android:layout_width="0dp"
            android:layout_height="wrap_content"
            android:layout_weight="1"
```



```
            android:onClick="onClickCancelButton"
            android:text="@android:string/cancel" />

        <Button
            android:layout_width="0dp"
            android:layout_height="wrap_content"
            android:layout_weight="1"
            android:onClick="onClickOkButton"
            android:text="@android:string/ok" />
    </LinearLayout>
</LinearLayout>
```

Implementation for 3 methods which are located at the bottom of PasswordActivity.java, should be adjusted depends on the purposes.

- private String getPreviousPassword()
- private void onClickCancelButton(View view)
- private void onClickOkButton(View view)

PasswordActivity.java

```
package org.jssec.android.password.passwordinputui;

import android.app.Activity;
import android.os.Bundle;
import android.text.Editable;
import android.text.InputType;
import android.text.TextWatcher;
import android.view.View;
import android.view.WindowManager;
import android.widget.CheckBox;
import android.widget.CompoundButton;
import android.widget.CompoundButton.OnCheckedChangeListener;
import android.widget.EditText;
import android.widget.Toast;

public class PasswordActivity extends Activity {

    // Key to save the state
    private static final String KEY_DUMMY_PASSWORD = "KEY_DUMMY_PASSWORD";

    // View inside Activity
    private EditText mPasswordEdit;
    private CheckBox mPasswordDisplayCheck;

    // Flag to show whether password is dummy display or not
    private boolean mIsDummyPassword;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.password_activity);
        // Set Disabling Screen Capture
        getWindow().addFlags(WindowManager.LayoutParams.FLAG_SECURE);

        // Get View
        mPasswordEdit = (EditText) findViewById(R.id.password_edit);
```

```
        mPasswordDisplayCheck = (CheckBox) findViewById(R.id.password_display_check);

        // Whether last Input password exist or not.
        if (getPreviousPassword() != null) {
            // *** POINT 4 *** In the case there is the last input password in an initial display,
            // display the fixed digit numbers of black dot as dummy in order not that the digits number
of last password is guessed.

            // Display should be dummy password.
            mPasswordEdit.setText("**********");
            // To clear the dummy password when inputting password, set text change listener.
            mPasswordEdit.addTextChangedListener(new PasswordEditTextWatcher());
            // Set dummy password flag
            mIsDummyPassword = true;
        }

        // Set a listner to change check state of password display option.
        mPasswordDisplayCheck
                .setOnCheckedChangeListener(new OnPasswordDisplayCheckedChangeListener());
    }

    @Override
    public void onSaveInstanceState(Bundle outState) {
        super.onSaveInstanceState(outState);

        // Unnecessary when specifying not to regenerate Activity by the change in screen aspect ratio.
        // Save Activity state
        outState.putBoolean(KEY_DUMMY_PASSWORD, mIsDummyPassword);
    }

    @Override
    public void onRestoreInstanceState(Bundle savedInstanceState) {
        super.onRestoreInstanceState(savedInstanceState);

        // Unnecessary when specifying not to regenerate Activity by the change in screen aspect ratio.
        // Restore Activity state
        mIsDummyPassword = savedInstanceState.getBoolean(KEY_DUMMY_PASSWORD);
    }

    /**
     * Process in case password is input
     */
    private class PasswordEditTextWatcher implements TextWatcher {

        public void beforeTextChanged(CharSequence s, int start, int count,
                int after) {
            // Not used
        }

        public void onTextChanged(CharSequence s, int start, int before,
                int count) {
            // *** POINT 6 *** When last Input password is displayed as dummy, in the case an user tries
to input password,
            // Clear the last Input password, and treat new user input as new password.
            if (mIsDummyPassword) {
                // Set dummy password flag
                mIsDummyPassword = false;
                // Trim space
                CharSequence work = s.subSequence(start, start + count);
                mPasswordEdit.setText(work);
```



```
                // Cursor position goes back the beginning, so bring it at the end.
                mPasswordEdit.setSelection(work.length());
            }
        }

        public void afterTextChanged(Editable s) {
            // Not used
        }

    }

    /**
     * Process when check of password display option is changed.
     */
    private class OnPasswordDisplayCheckedChangeListener implements
            OnCheckedChangeListener {

        public void onCheckedChanged(CompoundButton buttonView,
                boolean isChecked) {
            // *** POINT 5 ***  When the dummy password is displayed and the "Show password" button is pr
essed,
            // clear the last input password and provide the state for new password input.
            if (mIsDummyPassword && isChecked) {
                // Set dummy password flag
                mIsDummyPassword = false;
                // Set password empty
                mPasswordEdit.setText(null);
            }

            // Cursor position goes back the beginning, so memorize the current cursor position.
            int pos = mPasswordEdit.getSelectionStart();

            // *** POINT 2 *** Provide the option to display the password in a plain text
            // Create InputType
            int type = InputType.TYPE_CLASS_TEXT;
            if (isChecked) {
                // Plain display when check is ON.
                type |= InputType.TYPE_TEXT_VARIATION_VISIBLE_PASSWORD;
            } else {
                // Masked display when check is OFF.
                type |= InputType.TYPE_TEXT_VARIATION_PASSWORD;
            }

            // Set InputType to password EditText
            mPasswordEdit.setInputType(type);

            // Set cursor position
            mPasswordEdit.setSelection(pos);
        }

    }

    // Implement the following method depends on application

    /**
     * Get the last Input password
     *
     * @return Last Input password
     */
    private String getPreviousPassword() {
```

```
        // When need to restore the saved password, return password character string
        // For the case password is not saved, return null
        return "hirake5ma";
    }

    /**
     * Process when cancel button is clicked
     *
     * @param view
     */
    public void onClickCancelButton(View view) {
        // Close Activity
        finish();
    }

    /**
     * Process when OK button is clicked
     *
     * @param view
     */
    public void onClickOkButton(View view) {
        // Execute necessary processes like saving password or using for authentication

        String password = null;

        if (mIsDummyPassword) {
            // When dummy password is displayed till the final moment, grant last iInput password as fixe
d password.
            password = getPreviousPassword();
        } else {
            // In case of not dummy password display, grant the user input password as fixed password.
            password = mPasswordEdit.getText().toString();
        }

        // Display password by Toast
        Toast.makeText(this, "password is ¥"" + password + "¥"",
                Toast.LENGTH_SHORT).show();

        // Close Activity
        finish();
    }
}
```


5.1.2. Rule Book

Follow the below rules when creating password input screen.

1.	Provide the Mask Display Feature, If the Password Is Entered	(Required)
2.	Provide the Option to Display Password in a Plain Text	(Required)
3.	Mask the Password when Activity Is Launched	(Required)
4.	When Displaying the Last Input Password, Dummy Password Must Be Displayed	(Required)

5.1.2.1. Provide the Mask Display Feature, If the Password Is Entered (Required)

Smartphone is often used in crowded places like in a train or in a bus, and the risk that password is peeked by someone. So the function to mask display password is necessary as an application spec.

There are two ways to display the EditText as password: specifying this statically in the layout XML, or specifying this dynamically by switching the display from a program. The former is achieved by specifying “textPassword” for the android:inputType attribute or by using android:password attribute. The latter is achieved by using the setInputType() method of the EditText class to add InputType.TYPE_TEXT_VARIATION_PASSWORD to its input type.

Sample code of each of them is shown below.

Masking password in layout XML.

password_activity.xml

```
<!—Password input item -->
<!—Set true for the android:password attribute -->
<EditText
    android:id="@+id/password_edit"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content"
    android:hint="@string/hint_password"
    android:password="true" />
```

Masking password in Activity.

PasswordActivity.java

```
    // Set password display type
    // Set TYPE_TEXT_VARIATION_PASSWORD for InputType.
    EditText passwordEdit = (EditText) findViewById(R.id.password_edit);
    int type = InputType.TYPE_CLASS_TEXT
            | InputType.TYPE_TEXT_VARIATION_PASSWORD;
    passwordEdit.setInputType(type);
```

5.1.2.2. Provide the Option to Display Password in a Plain Text (Required)

Password input in Smartphone is done by touch panel input, so compared with keyboard input in PC, miss input may be easily happened. Because of the inconvenience of inputting, user may use the simple password, and it makes more dangerous. In addition, when there's a policy like account is locked due the several times of password input failure, it's necessary to avoid from miss input as much as possible. As a solution of these problems, by preparing an option to display password in a plain text, user can use the safe password.

However, when displaying password in a plain text, it may be sniffed, so when using this option. It's necessary to call user cautions for sniffing from behind. In addition, in case option to display in a plain text is implemented, it's also necessary to prepare the system to auto cancel the plain text display like setting the time of plain display. The restrictions for password plain text display are published in another article in future edition. So, the restrictions for password plain text display are not included in sample code.

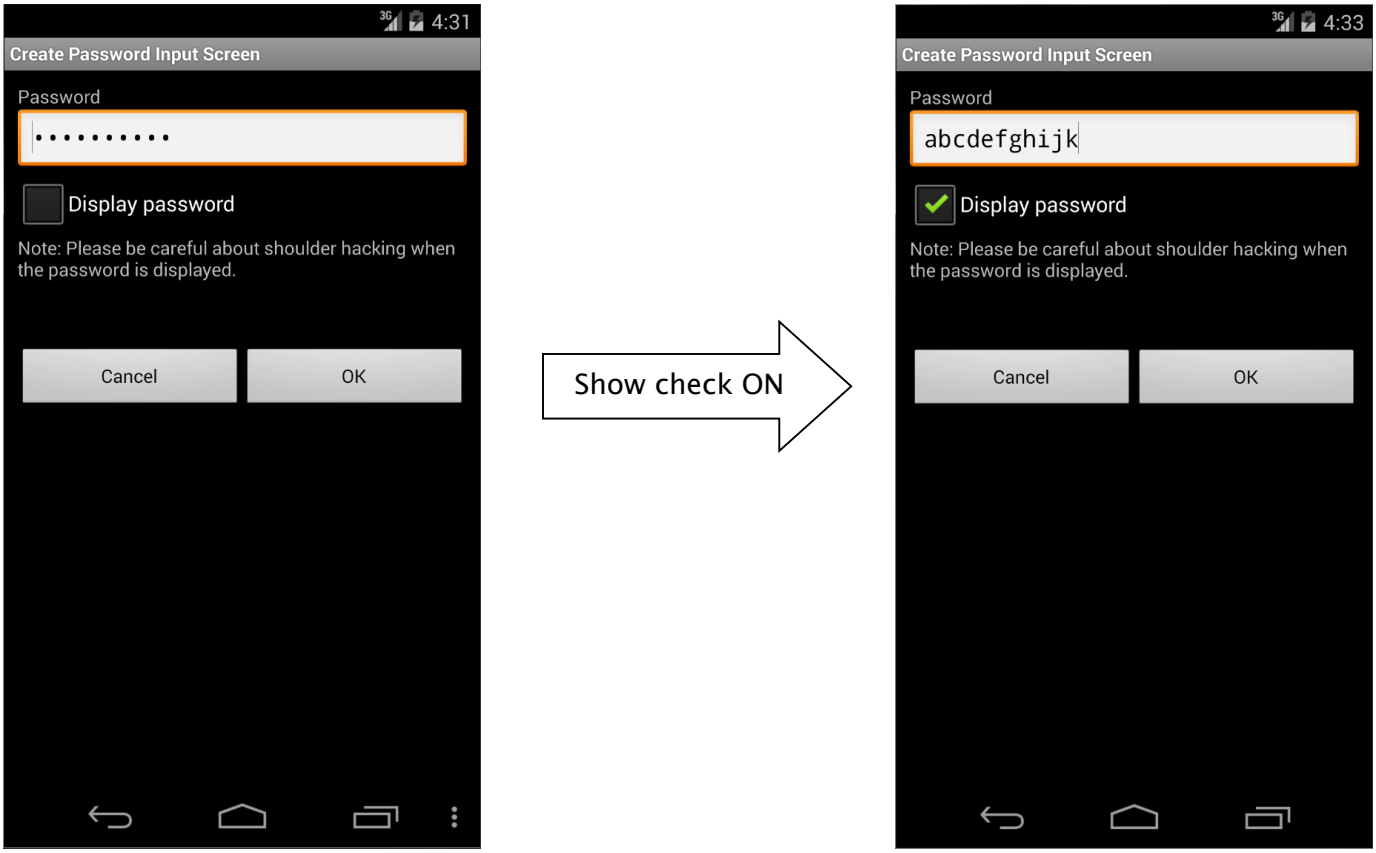


Figure 5.1-2

By specifying InputType of EditText, mask display and plain text display can be switched.

PasswordActivity.java

```
    /**
     * Process when check of password display option is changed.
     */
    private class OnPasswordDisplayCheckedChangeListener implements
            OnCheckedChangeListener {
```



```
        public void onCheckedChanged(CompoundButton buttonView,
                boolean isChecked) {
            // *** POINT 5 ***  When the dummy password is displayed and the "Show password" button is pr
essed,
            // Clear the last input password and provide the state for new password input.
            if (mIsDummyPassword && isChecked) {
                // Set dummy password flag
                mIsDummyPassword = false;
                // Set password empty
                mPasswordEdit.setText(null);
            }

            // Cursor position goes back the beginning, so memorize the current cursor position.
            int pos = mPasswordEdit.getSelectionStart();

            // *** POINT 2 *** Provide the option to display the password in a plain text
            // Create InputType
            int type = InputType.TYPE_CLASS_TEXT;
            if (isChecked) {
                // Plain display when check is ON.
                type |= InputType.TYPE_TEXT_VARIATION_VISIBLE_PASSWORD;
            } else {
                // Masked display when check is OFF.
                type |= InputType.TYPE_TEXT_VARIATION_PASSWORD;
            }

            // Set InputType to password EditText
            mPasswordEdit.setInputType(type);

            // Set cursor position
            mPasswordEdit.setSelection(pos);
        }

    }
```

5.1.2.3. Mask the Password when Activity Is Launched (Required)

To prevent it from a password peeping out, the default value of password display option, should be set OFF, when Activity is launched. The default value should be always defined as safer side, basically.

5.1.2.4. When Displaying the Last Input Password, Dummy Password Must Be Displayed(Required)

When specifying the last input password, not to give the third party any hints for password, it should be displayed as dummy with the fixed digits number of mask characters (* etc.). In addition, in the case pressing "Show password" when dummy display, clear password and switch to plain text display mode. It can help to suppress the risk that the last input password is sniffed low, even if the device is passed to a third person like when it's stolen. FYI, In case of dummy display and when a user tries to input password, dummy display should be cancelled, it necessary to turn the normal input state.

When displaying the last Input password, display dummy password.

PasswordActivity.java

```
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.password_activity);

        // Get View
        mPasswordEdit = (EditText) findViewById(R.id.password_edit);
        mPasswordDisplayCheck = (CheckBox) findViewById(R.id.password_display_check);

        // Whether last Input password exist or not.
        if (getPreviousPassword() != null) {
            // *** POINT 4 *** In the case there is the last input password in an initial display,
               // display the fixed digit numbers of black dot as dummy in order not that the digits numb
er of last password is guessed.

            // Display should be dummy password.
            mPasswordEdit.setText("**********");
            // To clear the dummy password when inputting password, set text change listener.
            mPasswordEdit.addTextChangedListener(new PasswordEditTextWatcher());
            // Set dummy password flag
            mIsDummyPassword = true;
        }

        [...]

    }

    /**
     * Get the last input password.
     *
     * @return the last input password
     */
    private String getPreviousPassword() {
        // To restore the saved password, return the password character string.
        // For the case password is not saved, return null.
        return "hirake5ma";
    }
```

In the case of dummy display, when password display option is turned ON, clear the displayed contents.

PasswordActivity.java

```
    /**
     * Process when check of password display option is changed.
     */
    private class OnPasswordDisplayCheckedChangeListener implements
            OnCheckedChangeListener {

        public void onCheckedChanged(CompoundButton buttonView,
                boolean isChecked) {
            // *** POINT 5 ***  When the dummy password is displayed and the "Show password" button is pr
essed,
               // Clear the last input password and provide the state for new password input.
            if (mIsDummyPassword && isChecked) {
                // Set dummy password flag
                mIsDummyPassword = false;
                // Set password empty
```



```
            mPasswordEdit.setText(null);
        }

        [...]

    }

}
```

In case of dummy display, when user tries to input password, clear dummy display.

PasswordActivity.java

```
    // Key to save the state
    private static final String KEY_DUMMY_PASSWORD = "KEY_DUMMY_PASSWORD";

    [...]

    // Flag to show whether password is dummy display or not.
    private boolean mIsDummyPassword;

    @Override
    public void onCreate(Bundle savedInstanceState) {

        [...]

        // Whether last Input password exist or not.
        if (getPreviousPassword() != null) {
            // *** POINT 4 *** In the case there is the last input password in an initial display,
            // display the fixed digit numbers of black dot as dummy in order not that the digits number
of last password is guessed.

            // Display should be dummy password.
            mPasswordEdit.setText("**********");
            // To clear the dummy password when inputting password, set text change listener.
            mPasswordEdit.addTextChangedListener(new PasswordEditTextWatcher());
            // Set dummy password flag
            mIsDummyPassword = true;
        }

        [...]

    }

    @Override
    public void onSaveInstanceState(Bundle outState) {
        super.onSaveInstanceState(outState);

        // Unnecessary when specifying not to regenerate Activity by the change in screen aspect ratio.
        // Save Activity state
        outState.putBoolean(KEY_DUMMY_PASSWORD, mIsDummyPassword);
    }

    @Override
    public void onRestoreInstanceState(Bundle savedInstanceState) {
        super.onRestoreInstanceState(savedInstanceState);

        // Unnecessary when specifying not to regenerate Activity by the change in screen aspect ratio.
        // Restore Activity state
```

```
        mIsDummyPassword = savedInstanceState.getBoolean(KEY_DUMMY_PASSWORD);
    }

    /**
     * Process when inputting password.
     */
    private class PasswordEditTextWatcher implements TextWatcher {

        public void beforeTextChanged(CharSequence s, int start, int count,
                int after) {
            // Not used
        }

        public void onTextChanged(CharSequence s, int start, int before,
                int count) {
            // *** POINT 6 *** When last Input password is displayed as dummy, in the case an user tries
to input password,
                // Clear the last Input password, and treat new user input as new password.
            if (mIsDummyPassword) {
                // Set dummy password flag
                mIsDummyPassword = false;
                // Trim space
                CharSequence work = s.subSequence(start, start + count);
                mPasswordEdit.setText(work);
                // Cursor position goes back the beginning, so bring it at the end.
                mPasswordEdit.setSelection(work.length());
            }
        }

        public void afterTextChanged(Editable s) {
            // Not used
        }

    }
```


5.1.3. Advanced Topics

5.1.3.1. Login Process

The representative example of where password input is required is login process. Here are some Points that need cautions in Login process.

Error message when login fail

In login process, need to input 2 information which is ID(account) and password. When login failure, there are 2 cases. One is ID doesn't exist. Another is ID exists but password is incorrect. If either of these 2 cases is distinguished and displayed in a login failure message, attackers can guess whether the specified ID exists or not. To stop this kind of guess, these 2 cases should not be specified in login failure message, and this message should be displayed as per below.

Message example: Login ID or password is incorrect.

Auto Login function

There is a function to perform auto login by omitting login ID/password input in the next time and later, after successful login process has been completed once. Auto login function can omit the complicated input. So the convenience will increase, but on the other hand, when a Smartphone is stolen, the risk which is maliciously being used by the third party, will follow.

Only the use when damages caused by the malicious third party is somehow acceptable, or only in the case enough security measures can be taken, auto login function can be used. For example, in the case of online banking application, when the device is operated by the third party, financial damage may be caused. So in this case, security measures are necessary along with auto login function. There are some possible counter-measures, like [Require re-inputting password just before financial process like payment process occurs], [When setting auto login, call a user for enough attentions and prompt user to secure device lock], etc. When using auto login, it's necessary to investigate carefully considering the convenience and risks along with the assumed counter measures.

5.1.3.2. Changing Password

When changing the password which was once set, following input items should be prepared on the screen.

- Current password
- New password
- New password (confirmation)

When auto login function is introduced, there are possibilities that third party can use an application. In that case, to avoid from changing password unexpectedly, it's necessary to require the current password input. In addition, to decrease the risk of getting into unserviceable state due to miss

inputting new password, it's necessary to require new password input 2 times.

5.1.3.3. Regarding "Make passwords visible" Setting

There is a setting in Android's setting menu, called "Make passwords visible." In case of Android 4.4, it's shown as below.

```
Setting > Security > Make passwords visible
```

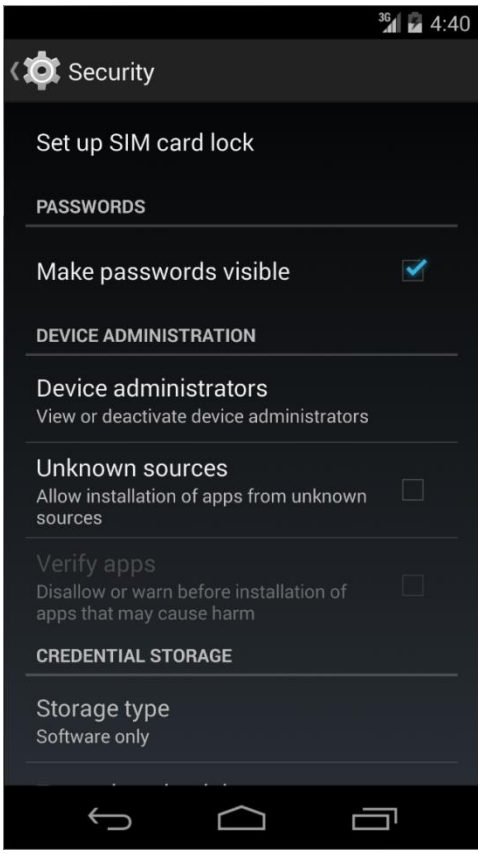


Figure 5.1-3

When turning ON "Make passwords visible" setting, the last input character is displayed in a plain text. After the certain time (about 2 seconds) passed, or after inputting the next character, the characters which was displayed in a plain text is masked. When turning OFF, it's masked right after inputting. This setting affects overall system, and it's applied to all applications which use password display function of EditText.

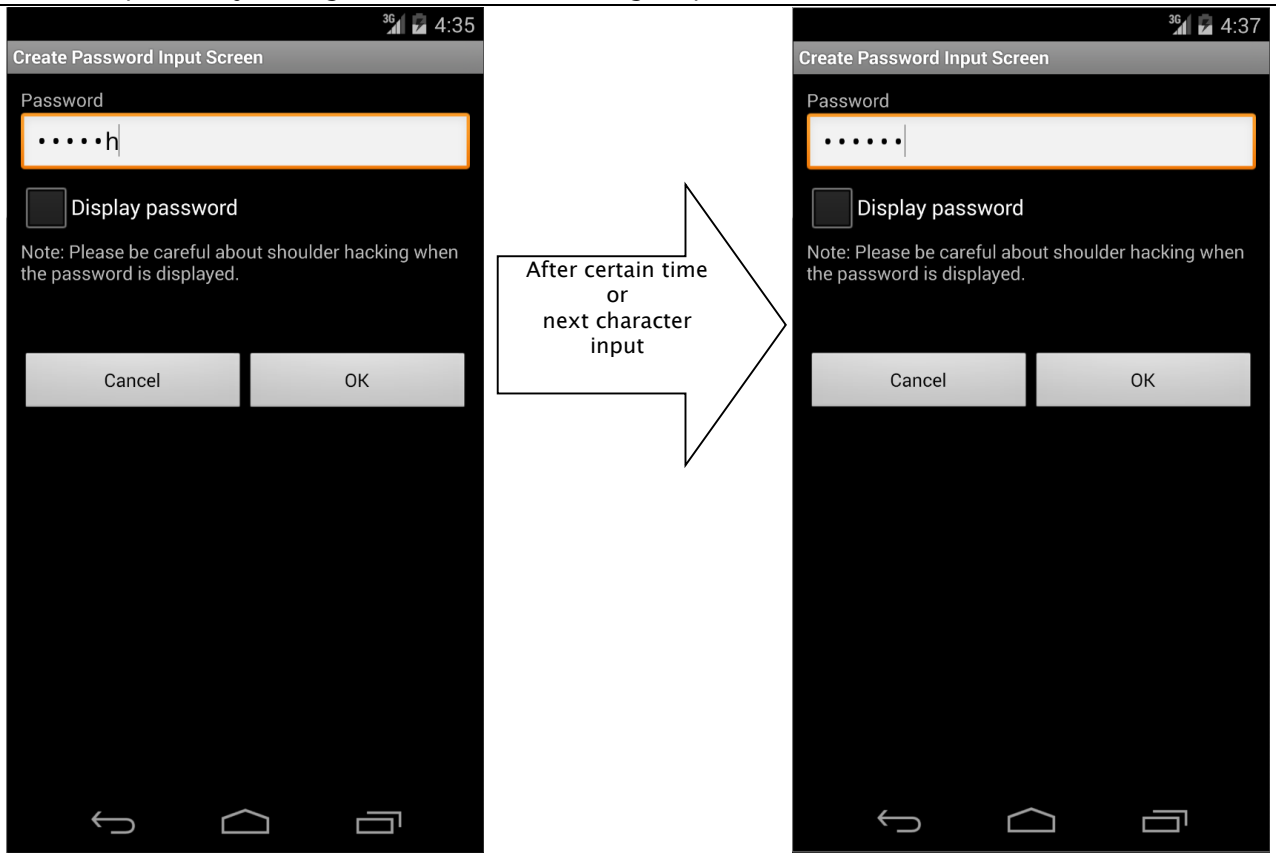


Figure 5.1-4

5.1.3.4. Disabling Screen Shot

In password input screens, passwords could be displayed in the clear on the screens. In such screens as handle personal information, they could be leaked from screenshot files stored on external storage if the screenshot function is stayed enable as default. Thus it is recommended to disable the screenshot function for such screens as password input screens. The screenshot can be disabled by appending the following code.

PasswordActivity.java

```
@Override
public void onCreate(Bundle saveInstanceState) {
[...]
        Window window = getWindow();
        window.addFlags(WindowManager.LayoutParams.FLAG_SECURE);

        setContentView(R.layout.passwordInputScreen);
[...]
```

5.2. Permission and Protection Level

There are four types of Protection Level within permission and they consist of normal, dangerous, signature, and signatureOrSystem. Depending on the Protection Level, permission is referred to as normal permission, dangerous permission, signature permission, or signatureOrSystem permission. In the following sections, such names are used.

5.2.1. Sample Code

5.2.1.1. How to Use System Permissions of Android OS

Android OS has a security mechanism called "permission" that protects its user's assets such as contacts and a GPS feature from a malware. When an application seeks access to such information and/or features, which are protected under Android OS, the application needs to explicitly declare a permission in order to access them. When an application, which has declared a permission that needs user's consent to be used, is installed, the following confirmation screen appears[26].

[26] In Android 6.0 (API Level 23) and later, the granting or refusal of user permissions does not occur when an app is installed, but instead at runtime when then app requests permissions. For more details, see Section "5.2.1.4 Methods for using Dangerous Permissions in Android 6.0 and later" and Section "5.2.3.6 Modifications to the Permission model specifications in Android versions 6.0 and later".

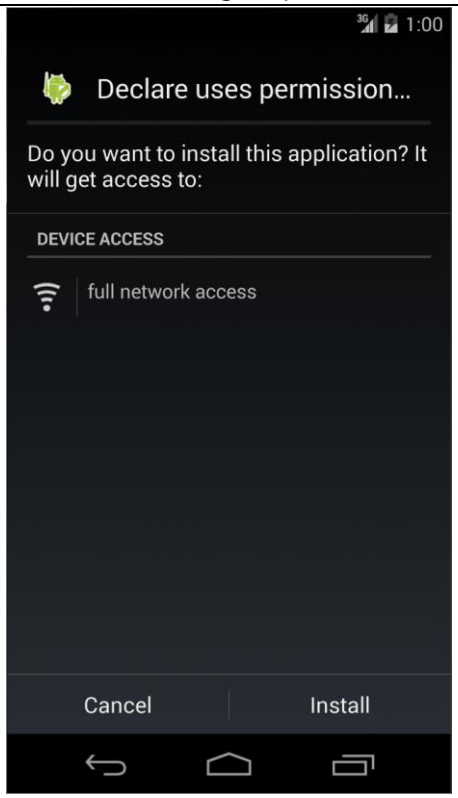


Figure 5.2-1

From this confirmation screen, a user is able to know which types of features and/or information an application is trying to access. If the behavior of an application is trying to access features and/or information that are clearly unnecessary, then there is a high possibility that the application is a malware. Hence, as your application is not suspected to be a malware, declarations of permission to use needs to be minimized.

Points:

1. Declare a permission used in an application with uses-permission.
2. Do not declare any unnecessary permissions with uses-permission.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.permission.usespermission" >

    <!-- *** POINT 1 *** Declare a permission used in an application with uses-permission -->
    <!-- Permission to access Internet -->
    <uses-permission android:name="android.permission.INTERNET"/>

    <!-- *** POINT 2 *** Do not declare any unnecessary permissions with uses-permission -->
    <!-- If declaring to use Permission that is unnecessary for application behaviors, it gives users a
sense of distrust. -->

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >
        <activity
            android:name=".MainActivity"
```

```
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>
```


5.2.1.2. How to Communicate Between In-house Applications with In-house-defined Signature Permission

Besides system permissions defined by Android OS, an application can define its own permissions as well. If using an in-house-defined permission (it is an in-house-defined signature permission to be more precise), you can build a mechanism where only communications between in-house applications is permitted. By providing the composite function based on inter-application communication between multiple in-house applications, the applications get more attractive and your business could get more profitable by selling them as series. It is a case of using in-house-defined signature permission.

The sample application "In-house-defined Signature Permission (UserApp)" launches the sample application "In-house-defined Signature Permission (ProtectedApp)" with Context.startActivity() method. Both applications need to be signed with the same developer key. If keys for signing them are different, the UserApp sends no Intent to the ProtectedApp, and the ProtectedApp processes no Intent received from the UserApp. Furthermore, it prevents malwares from circumventing your own signature permission using the matter related to the installation order as explained in the Advanced Topic section.

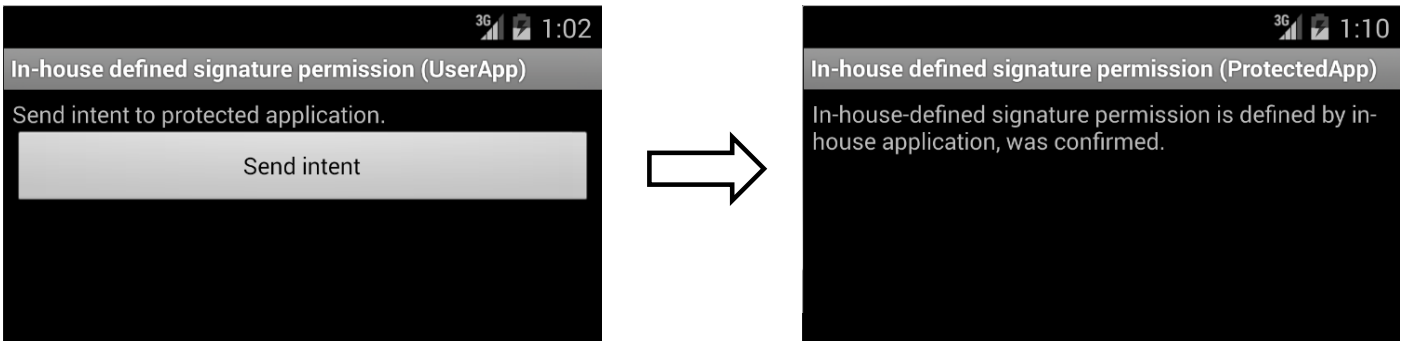


Figure 5.2-2

Points: Application Providing Component

1. Define a permission with protectionLevel="signature".
2. For a component, enforce the permission with its permission attribute.
3. If the component is an activity, you must define no intent-filter.
4. At run time, verify if the signature permission is defined by itself on the program code.
5. When exporting an APK, sign the APK with the same developer key that applications using the component use.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.permission.protectedapp" >

    <!-- *** POINT 1 *** Define a permission with protectionLevel="signature" -->
    <permission
```

```
        android:name="org.jssec.android.permission.protectedapp.MY_PERMISSION"
        android:protectionLevel="signature" />

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- *** POINT 2 *** For a component, enforce the permission with its permission attribute -->
        <activity
            android:name=".ProtectedActivity"
            android:exported="true"
            android:label="@string/app_name"
            android:permission="org.jssec.android.permission.protectedapp.MY_PERMISSION" >

            <!-- *** POINT 3 *** If the component is an activity, you must define no intent-filter -->
        </activity>
    </application>
</manifest>
```

ProtectedActivity.java

```
package org.jssec.android.permission.protectedapp;

import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.Context;
import android.os.Bundle;
import android.widget.TextView;

public class ProtectedActivity extends Activity {

    // In-house Signature Permission
    private static final String MY_PERMISSION = "org.jssec.android.permission.protectedapp.MY_PERMISSIO
N";

    // Hash value of in-house certificate
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" of debug.keystore
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of "my company key" of keystore
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    private TextView mMessageView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
```



```
        mMessageView = (TextView) findViewById(R.id.messageView);

        // *** POINT 4 *** At run time, verify if the signature permission is defined by itself on the pr
ogram code
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            mMessageView.setText("In-house defined signature permission is not defined by in-house appli
cation.");
            return;
        }

        // *** POINT 4 *** Continue processing only when the certificate matches
        mMessageView.setText("In-house-defined signature permission is defined by in-house application,
was confirmed.");
    }
}
```

SigPerm.java

```
package org.jssec.android.shared;

import android.content.Context;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.PermissionInfo;

public class SigPerm {

    public static boolean test(Context ctx, String sigPermName, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, sigPermName));
    }

    public static String hash(Context ctx, String sigPermName) {
        if (sigPermName == null) return null;
        try {
            // Get the package name of the application which declares a permission named sigPermName.
            PackageManager pm = ctx.getPackageManager();
            PermissionInfo pi;
            pi = pm.getPermissionInfo(sigPermName, PackageManager.GET_META_DATA);
            String pkgname = pi.packageName;

            // Fail if the permission named sigPermName is not a Signature Permission
            if (pi.protectionLevel != PermissionInfo.PROTECTION_SIGNATURE) return null;

            // Return the certificate hash value of the application which declares a permission named sig
PermName.
            return PkgCert.hash(ctx, pkgname);

        } catch (NameNotFoundException e) {
            return null;
        }
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


*** Point 5 *** When exporting an APK, sign the APK with the same developer key that applications using the component have used.

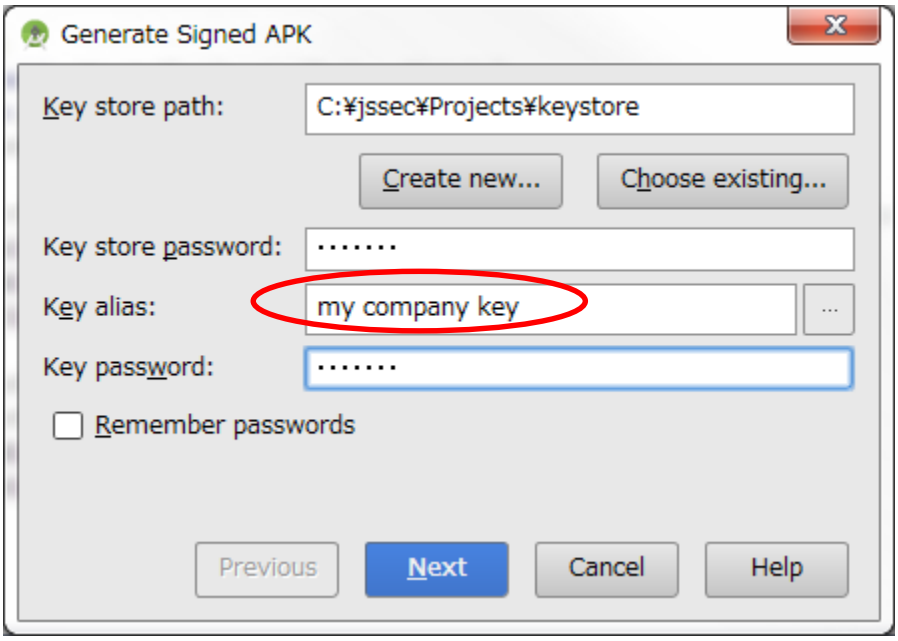


Figure 5.2-3

Points: Application Using Component

6. The same signature permission that the application uses must not be defined.
7. Declare the in-house permission with uses-permission tag.
8. Verify if the in-house signature permission is defined by the application that provides the component on the program code.
9. Verify if the destination application is an in-house application.
10. Use an explicit intent when the destination component is an activity.
11. When exporting an APK, sign the APK with the same developer key that the destination application uses.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.permission.userapp" >

    <!-- *** POINT 6 *** The same signature permission that the application uses must not be defined -->

    <!-- *** POINT 7 *** Declare the in-house permission with uses-permission tag -->
    <uses-permission
        android:name="org.jssec.android.permission.protectedapp.MY_PERMISSION" />

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >
        <activity
            android:name=".UserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
```

```
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
</application>
</manifest>
```

UserActivity.java

```
package org.jssec.android.permission.userapp;

import org.jssec.android.shared.PkgCert;
import org.jssec.android.shared.SigPerm;
import org.jssec.android.shared.Utils;

import android.app.Activity;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;

public class UserActivity extends Activity {

    // Requested (Destination) application's Activity information
    private static final String TARGET_PACKAGE  = "org.jssec.android.permission.protectedapp";
    private static final String TARGET_ACTIVITY = "org.jssec.android.permission.protectedapp.ProtectedA
ctivity";

    // In-house Signature Permission
    private static final String MY_PERMISSION = "org.jssec.android.permission.protectedapp.MY_PERMISSIO
N";

    // Hash value of in-house certificate
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" of debug.keystore.
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of "my company key" of keystore.
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }

    public void onSendButtonClicked(View view) {

        // *** POINT 8 *** Verify if the in-house signature permission is defined by the application that
 provides the component on the program code.
```



```
        if (!SigPerm.test(this, MY_PERMISSION, myCertHash(this))) {
            Toast.makeText(this, "In-house-defined signature permission is not defined by In house appli
cation.", Toast.LENGTH_LONG).show();
            return;
        }

        // *** POINT 9 *** Verify if the destination application is an in-house application.
        if (!PkgCert.test(this, TARGET_PACKAGE, myCertHash(this))) {
            Toast.makeText(this, "Requested (Destination) application is not in-house application.", Toa
st.LENGTH_LONG).show();
            return;
        }

        // *** POINT 10 *** Use an explicit intent when the destination component is an activity.
        try {
            Intent intent = new Intent();
            intent.setClassName(TARGET_PACKAGE, TARGET_ACTIVITY);
            startActivity(intent);
        } catch(Exception e) {
            Toast.makeText(this,
                    String.format("Exception occurs:%s", e.getMessage()),
                    Toast.LENGTH_LONG).show();
        }
    }
}
```

PkgCertWhitelists.java

```
package org.jssec.android.shared;

import java.util.HashMap;
import java.util.Map;

import android.content.Context;

public class PkgCertWhitelists {
    private Map<String, String> mWhitelists = new HashMap<String, String>();

    public boolean add(String pkgname, String sha256) {
        if (pkgname == null) return false;
        if (sha256 == null) return false;

        sha256 = sha256.replaceAll(" ", "");
        if (sha256.length() != 64) return false;    // SHA-256 -> 32 bytes -> 64 chars
        sha256 = sha256.toUpperCase();
        if (sha256.replaceAll("[0-9A-F]+", "").length() != 0) return false; // found non hex char

        mWhitelists.put(pkgname, sha256);
        return true;
    }

    public boolean test(Context ctx, String pkgname) {
        // Get the correct hash value which corresponds to pkgname.
        String correctHash = mWhitelists.get(pkgname);

        // Compare the actual hash value of pkgname with the correct hash value.
        return PkgCert.test(ctx, pkgname, correctHash);
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```


*** Point 11 *** When generating an APK by [Build] -> [Generate Signed APK], sign the APK with the same developer key that the destination application uses.

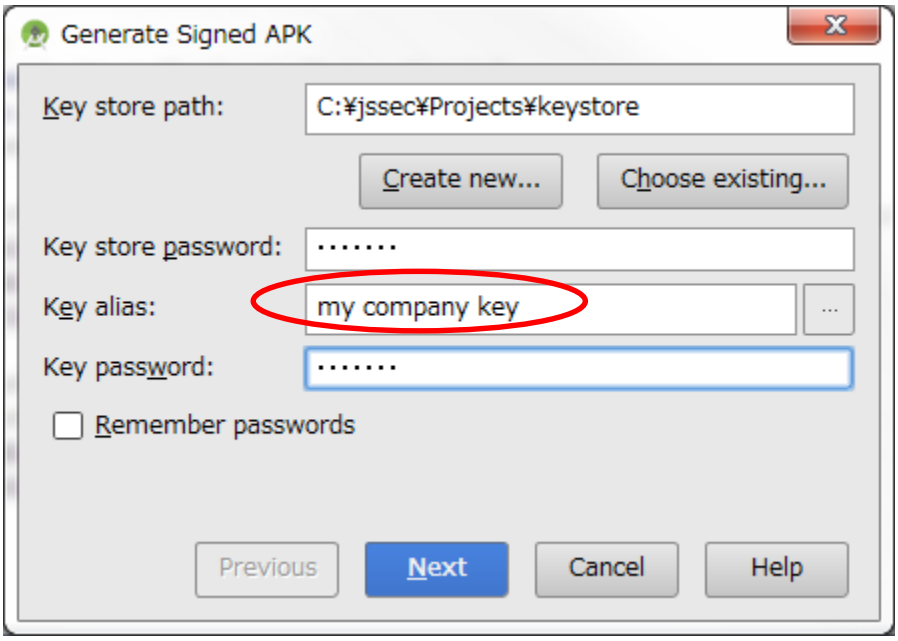


Figure 5.2-4

5.2.1.3. How to Verify the Hash Value of an Application's Certificate

We will provide an explanation on how to verify the hash value of an application's certificate that appears at different points in this Guidebook. Strictly speaking, the hash value means "the SHA256 hash value of the public key certificate for the developer key used to sign the APK."

How to verify it with Keytool

Using a program called keytool that is bundled with JDK, you can get the hash value (also known as certificate fingerprint) of a public key certificate for the developer key. There are various hash methods such as MD5, SHA1, and SHA256 due to the differences in hash algorithm. However, considering the security strength of the encryption bit length, this Guidebook recommends the use of SHA256. Unfortunately, the keytool bundled to JDK6 that is used in Android SDK does not support SHA256 for calculating hash values. Therefore, it is necessary to use the keytool that is bundled to JDK7 or later.

Example of outputting the content of a debugging certicate of an Android through a keytool

```
> keytool -list -v -keystore < keystore file > -storepass < password >

Type of keystore: JKS
Keystore provider: SUN

One entry is included in a keystore

Other name: androiddebugkey
Date of creation: 2012/01/11
Entry type: PrivateKeyEntry
Length of certificate chain: 1
Certificate[1]:
Owner: CN=Android Debug, O=Android, C=US
Issuer: CN=Android Debug, O=Android, C=US
Serial number: 4f0cef98
Start date of validity period: Wed Jan 11 11:10:32 JST 2012 End date: Fri Jan 03 11:10:32 JST 2042
Certificate fingerprint:
        MD5:  9E:89:53:18:06:B2:E3:AC:B4:24:CD:6A:56:BF:1E:A1
        SHA1: A8:1E:5D:E5:68:24:FD:F6:F1:ED:2F:C3:6E:0F:09:A3:07:F8:5C:0C
        SHA256: FB:75:E9:B9:2E:9E:6B:4D:AB:3F:94:B2:EC:A1:F0:33:09:74:D8:7A:CF:42:58:22:A2:56:85:1B:0F
:85:C6:35
        Signatrue algorithm name: SHA1withRSA
        Version: 3


*******************************************
*******************************************
```

How to Verify it with JSSEC Certificate Hash Value Checker

Without installing JDK7 or later, you can easily verify the certificate hash value by using JSSEC Certificate Hash Value Checker.

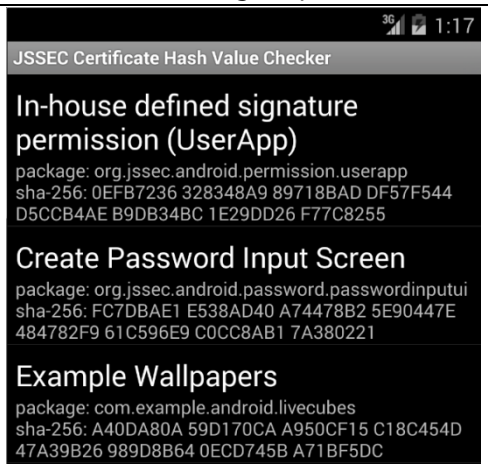


Figure 5.2-5

This is an Android application that displays a list of certificate hash values of applications which are installed in the device. In the Figure above, the 64-character hexadecimal notation string that is shown on the right of "sha-256" is the certificate hash value. The sample code folder, "JSSEC CertHash Checker" that comes with this Guidebook is the set of source codes. If you would like, you can compile the codes and use it.

5.2.1.4. Methods for using Dangerous Permissions in Android 6.0 and later

Android 6.0 (API Level 23) incorporates modified specifications that are relevant to the implementation of apps---specifically, to the times at which apps are granted permission.

Under the Permission model of Android 5.1 (API Level 22) and earlier versions (See section "5.2.3.6 Modifications to the Permission model specifications in Android versions 6.0 and later"), all Permissions declared by an app are granted to that app at the time of installation. However, in Android 6.0 and later versions, app developers must explicitly implement apps in such a way that, for Dangerous Permissions, the app requests Permission at appropriate times. When an app requests a Permission, a confirmation window like that shown below is displayed to the Android OS user, requesting a decision from the user as to whether or not to grant the Permission in question. If the user allows the use of the Permission, the app may execute whatever operations require that Permission.

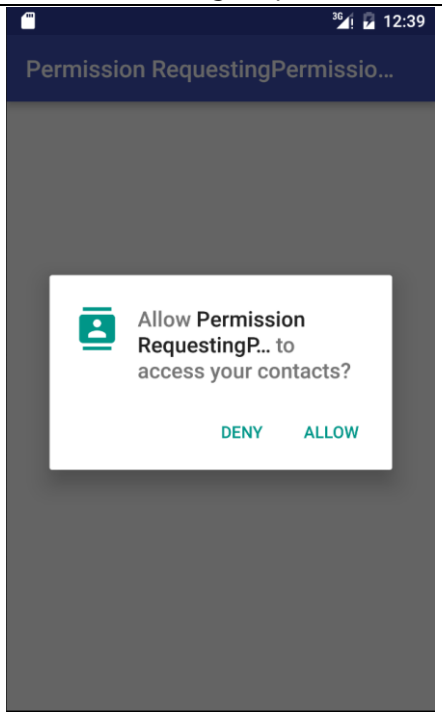


Figure 5.2-6

The specifications are also modified regarding the units in which Permissions are granted. Previously, all Permissions were granted simultaneously; in Android 6.0 (API Level 23) and later versions, Permissions are granted by Permission Group. In Android 8.0 (API Level 26) and later versions, Permissions are granted individually. In conjunction with this modification, users are now shown individual confirmation windows for each Permission, allowing users to make more flexible decisions regarding the granting or refusal of Permissions. App developers must revisit the specifications and design of their apps with full consideration paid to the possibility that Permissions may be refused.

For details on the Permission model in Android 6.0 and later, see Section ”5.2.3.6 Modifications to the Permission model specifications in Android versions 6.0 and later”.

Points:

1. Apps declare the Permissions they will use
2. Do not declare the use of unnecessary Permissions
3. Check whether or not Permissions have been granted to the app
4. Request Permissions (open a dialog to request permission from users)
5. Implement appropriate behavior for cases in which the use of a Permission is refused

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.permission.permissionrequestingpermissionatruntime" >

    <!-- *** POINT 1 *** Apps declare the Permissions they will use -->
    <!-- Permission to read information on contacts (Protection Level: dangerous) -->
    <uses-permission android:name="android.permission.READ_CONTACTS" />

    <!-- *** POINT 2 *** Do not declare the use of unnecessary Permissions -->
```



```
    <application
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:supportsRtl="true"
        android:theme="@style/AppTheme" >
        <activity
            android:name=".MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity
            android:name=".ContactListActivity"
            android:exported="false">
        </activity>
    </application>

</manifest>
```

MainActivity.java

```
package org.jssec.android.permission.permissionrequestingpermissionatruntime;

import android.Manifest;
import android.content.Intent;
import android.content.pm.PackageManager;
import android.os.Bundle;
import android.support.v4.app.ActivityCompat;
import android.support.v4.content.ContextCompat;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.Button;
import android.widget.Toast;

public class MainActivity extends AppCompatActivity implements View.OnClickListener {
    private static final int REQUEST_CODE_READ_CONTACTS = 0;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        Button button = (Button)findViewById(R.id.button);
        button.setOnClickListener(this);
    }

    @Override
    public void onClick(View v) {
        readContacts();
    }

    private void readContacts() {
        // *** POINT 3 *** Check whether or not Permissions have been granted to the app
        if (ContextCompat.checkSelfPermission(getApplicationContext(), Manifest.permission.READ_CONTACT
S) != PackageManager.PERMISSION_GRANTED) {
```

```
            // Permission was not granted
            // *** POINT 4 *** Request Permissions (open a dialog to request permission from users)
            ActivityCompat.requestPermissions(this, new String[]{Manifest.permission.READ_CONTACTS}, REQ
UEST_CODE_READ_CONTACTS);
        } else {
            // Permission was previously granted
            showContactList();
        }
    }

    // A callback method that receives the result of the user's selection
    @Override
    public void onRequestPermissionsResult(int requestCode, String[] permissions, int[] grantResults) {
        switch (requestCode) {
            case REQUEST_CODE_READ_CONTACTS:
                if (grantResults.length > 0 && grantResults[0] == PackageManager.PERMISSION_GRANTED) {
                    // Permissions were granted; we may execute operations that use contact information
                    showContactList();
                } else {
                    // Because the Permission was denied, we may not execute operations that use contact
information
                    // *** POINT 5 *** Implement appropriate behavior for cases in which the use of a Perm
ission is refused
                    Toast.makeText(this, String.format("Use of contact is not allowed."), Toast.LENGTH_LO
NG).show();
                }
                return;
        }
    }

    // Show contact list
    private void showContactList() {
        // Launch ContactListActivity
        Intent intent = new Intent();
        intent.setClass(getApplicationContext(), ContactListActivity.class);
        startActivity(intent);
    }
}
```


5.2.2. Rule Book

Be sure to follow the rules below when using in-house permission.

1.	System Dangerous Permissions of Android OS Must Only Be Used for Protecting User Assets (Required)
2.	Your Own Dangerous Permission Must Not Be Used (Required)
3.	Your Own Signature Permission Must Only Be Defined on the Provider-side Application (Required)
4.	Verify If the In-house-defined Signature Permission Is Defined by an In-house Application (Required)
5.	Your Own Normal Permission Should Not Be Used (Recommended)
6.	The String for Your Own Permission Name Should Be of an Extent of the Package Name of Application (Recommended)

5.2.2.1. System Dangerous Permissions of Android OS Must Only Be Used for Protecting User Assets (Required)

Since the use of your own dangerous permission is not recommended (please refer to "5.2.2.2 Your Own Dangerous Permission Must Not Be Used (Required)", we will proceed on the premise of using system dangerous permission of Android OS.

Unlike the other three types of permissions, dangerous permission has a feature that requires the user's consent to the grant of the permission to the application. When installing an application on a device that has declared a dangerous permission to use, the following screen will be displayed. Subsequently, the user is able to know what level of permission (dangerous permission and normal permission) the application is trying to use. When the user taps "install," the application will be granted the permission and then it will be installed.

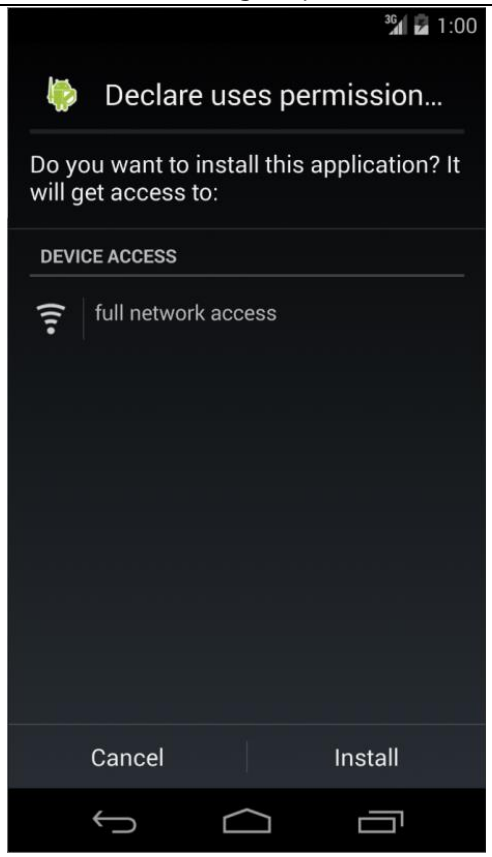


Figure 5.2-7

An application can handle user assets and assets that the developer wants to protect. We must be aware that dangerous permission can protect only user assets because the user is just who the granting of permission is entrusted to. On the other hand, assets that the developer wants to protect cannot be protected by the method above.

For example, suppose that an application has a Component that communicates only with an In-house application, it doesn't permit the access to the Component from any applications of the other companies, and it is implemented that it's protected by dangerous permission. When a user grants permission to an application of another company based on the user's judgment, in-house assets that need to be protected may be exploited by the application granted. In order to provide protection for in-house assets in such cases, we recommend the usage of in-house-defined signature permission.

5.2.2.2. Your Own Dangerous Permission Must Not Be Used (Required)

Even when in-house-defined Dangerous Permission is used, the screen prompt "Asking for the Allowance of Permission from User" is not displayed in some cases. This means that at times the feature that asks for permission based on the judgment of a user, which is the characteristic of Dangerous Permission, does not function. Accordingly, the Guidebook will make the rule "In-house -defined dangerous permission must not be used."

In order to explain it, we assume two types of applications. The first type of application defines an in-house dangerous permission, and it is an application that makes a Component, which is protected by this permission, public. We call this ProtectedApp. The other is another application which we call AttackerApp and it tries to exploit the Component of ProtectedApp. Also we assume that the

AttackerApp not only declares the permission to use it, but also defines the same permission.

AttackerApp can use the Component of a ProtectedApp without the consent of a user in the following cases:

1. When the user installs the AttackerApp, the installation will be completed without the screen prompt that asks for the user to grant the application the dangerous permission.
2. Similarly, when the user installs the ProtectedApp, the installation will be completed without any special warnings.
3. When the user launches the AttackerApp afterwards, the AttackerApp can access the Component of the ProtectedApp without being detected by the user, which can potentially lead to damage.

The cause of this case is explained in the following. When the user tries to install the AttackerApp first, the permission that has been declared for usage with uses-permission is not defined on the particular device yet. Finding no error, Android OS will continue the installation. Since the user consent for dangerous permission is required only at the time of installation, an application that has already been installed will be handled as if it has been granted permission. Accordingly, if the Component of an application which is installed later is protected with the dangerous permission of the same name, the application which was installed beforehand without the user permission will be able to exploit the Component.

Furthermore, since the existence of system dangerous permissions defined by Android OS is guaranteed when an application is installed, the user verification prompt will be displayed every time an application with uses-permission is installed. This problem arises only in the case of self-defined dangerous permission.

At the time of this writing, no viable method to protect the access to the Component in such cases has been developed yet. Therefore, your own dangerous permission must not be used.

5.2.2.3. Your Own Signature Permission Must Only Be Defined on the Provider-side Application (Required)

As demonstrated in, "5.2.1.2 How to Communicate Between In-house Applications with In-house-defined Signature Permission," the security can be assured by checking the signature permission at the time of executing inter-communications between In-house applications. When using this mechanism, the definition of the permission whose Protection Level is signature must be written in AndroidManifest.xml of the provider-side application that has the Component, but the user-side application must not define the signature permission.
This rule is applied to signatureOrSystem Permission as well.

The reason for this is as follows.

We assume that there are multiple user-side applications that have been installed prior to the provider-side application and every user-side application not only has required the signature permission that the provider-side application has defined, but also has defined the same permission. Under these circumstances, all user-side applications will be able to access the provider-side application just after the provider-side application is installed. Subsequently, when the user-side application that was installed first is uninstalled, the definition of the permission also will be deleted

and then the permission will turn out to be undefined. As a result, the remaining user-side applications will be unable to access to the provider-side application.

In this manner, when the user-side application defines a self-defined permission, it can unexpectedly turn out the permission to be undefined. Therefore, only the provider-side application providing the Component that needs to be protected should define the permission, and defining the permission on the user-side must be avoided.

By doing as mentioned just above, the self-defined permission will be applied by Android OS at the time of the installation of the provider-side application, and the permission will turn out to be undefined at the time of the uninstallation of the application. Therefore, since the existence of the permission's definition always corresponds to that of the provider-side application, it is possible to provide an appropriate Component and protect it. Please be aware that this argument stands because regarding in-house-defined signature permission the user-side application is granted the permission regardless of the installation order of applications in inter-communication[27].

5.2.2.4. Verify If the In-house-defined Signature Permission Is Defined by an In-house Application (Required)

Actuality, you cannot say to be secure enough only by declaring a signature permission through AnroidManifest.xml and protecting the Component with the permission. For the details of this issue, please refer to, "5.2.3.1 Characteristics of Android OS that Avoids Self-defined Signature Permission and Its Counter-measures" in the Advanced Topics section.

The following are the steps for using in-house-defined signature permission securely and correctly.

First, write as the followings in AndroidManifest.xml:

1. Define an in-house signature permission in the AndroidManifest.xml of the provider-side application. (definition of permission)
   Example: <permission android:name="xxx" android:protectionLevel="signature" />
2. Enforce the permission with the permission attribute of the Component to be protected in the AndroidManifest.xml of the provider-side application. (enforcement of permission)
   Example: <activity android:permission="xxx" ... >...</activity>
3. Declare the in-house-defined signature permission with the uses-permission tag in the AndroidManifest.xml of every user-side application to access the Component to be protected. (declaration of using permission)
   Example: <uses-permission android:name="xxx" />

Next, implement the followings in the source code.

4. Before processing a request to the Component, first verify that the in-house-defined signature permission has been defined by an in-house application. If not, ignore the request. (protection in the provider-side component)

[27] If using normal/dangerous permission, the permission will not be granted the user-side application if the user-side application is installed before the provider-side application, the permission remains undefined. Therefore, the Component cannot be accessed even after the provider-side application has been installed.

5. Before accessing the Component, first verify that the in-house-defined signature permission has been defined by an in-house application. If not, do not access the Component (protection in the user-side component).

Lastly, execute the following with the Signing function of Android Studio.

6. Sign APKs of all inter-communicating applications with the same developer key.

Here, for specific points on how to implement "Verify that the in-house-defined signature permission has been defined by an In house application", please refer to "5.2.1.2 How to Communicate Between In-house Applications with In-house-defined Signature Permission".

This rule is applied to signatureOrSystem Permission as well.

5.2.2.5. Your Own Normal Permission Should Not Be Used (Recommended)

An application can use a normal permission just by declaring it with uses-permission in AndroidManifest.xml. Therefore, you cannot use a normal permission for the purpose of protecting a Component from a malware installed.

Furthermore, in the case of inter-application communication with self-defined normal permission, whether an application can be granted the permission depends on the order of installation. For example, when you install an application (user-side) that has declared to use a normal permission prior to another application (provider-side) that possesses a Component which has defined the permission, the user-side application will not be able to access the Component protected with the permission even if the provider-side application is installed later.

As a way to prevent the loss of inter-application communication due to the order of installation, you may think of defining the permission in every application in the communication. By this way, even if a user-side application has been installed prior to the provider-side application, all user-side applications will be able to access the provider-side application. However, it will create a situation that the permission is undefined when the user-side application installed first is uninstalled. As a result, even if there are other user-side applications, they will not be able to gain access to the provider-side application.

As stated above, there is a concern of damaging the availability of an application, thus your own normal permission should not be used.

5.2.2.6. The String for Your Own Permission Name Should Be of an Extent of the Package Name of Application (Recommended)

When multiple applications define permissions under the same name, the Protection Level that has been defined by an application installed first will be applied. Protection by signature permission will not be available in the case that the application installed first defines a normal permission and the application installed later defines a signature permission under the same name. Even in the absence of malicious intent, a conflict of permission names among multiple applications could cause behavior s of any applications as an unintended Protection Level. To prevent such accidents, it is

recommended that a permission name extends (starts with) the package name of the application defining the permission as below.

```
(package name).permission.(identifying string)
```

For example, the following name would be preferred when defining a permission of READ access for the package of org.jssec.android.sample.

```
org.jssec.android.sample.permission.READ
```


5.2.3. Advanced Topics

5.2.3.1. Characteristics of Android OS that Avoids Self-defined Signature Permission and Its Counter-measures

Self-defined signature permission is a permission that actualizes inter-application communication between the applications signed with the same developer key. Since a developer key is a private key and must not be public, there is a tendency to use signature permission for protection only in cases where in-house applications communicate with each other.

First, we will describe the basic usage of self-defined signature permission that is explained in the Developer Guide (http://developer.android.com/guide/topics/security/security.html) of Android. However, as it will be explained later, there are problems with regard to the avoidance of permission. Consequently, counter-measures that are described in this Guidebook are necessary.

The followings are the basic usage of self-defined Signature Permission.

1. Define a self-defined signature permission in the AndroidManifest.xml of the provider-side application. (definition of permission)
   Example: <permission android:name="xxx" android:protectionLevel="signature" />
2. Enforce the permission with the permission attribute of the Component to be protected in the AndroidManifest.xml of the provider-side application. (enforcement of permission)
   Example: <activity android:permission="xxx" ... >...</activity>
3. Declare the self-defined signature permission with the uses-permission tag in the AndroidManifest.xml of every user-side application to access the Component to be protected. (declaration of using permission)
   Example: <uses-permission android:name="xxx" />
4. Sign APKs of all inter-communicating applications with the same developer key.

Actually, if the following conditions are fulfilled, this approach will create a loophole to avoid signature permission from being performed.

For the sake of explanation, we call an application that is protected by self-defined signature permission as ProtectedApp, and AttackerApp for an application that has been signed by a different developer key from the ProtectedApp. What a loophole to avoid signature permission from being performed means is, despite the mismatch of the signature for AttackerApp, it is possible to gain access to the Component of ProtectedApp.

Condition 1. An AttackerApp also defines a normal permission (strictly speaking, signature permission is also acceptable) under the same name as the signature permission which has been defined by the ProtectedApp.
   Example: <permission android:name=" xxx" android:protectionLevel="normal" />
Condition 2. The AttackerApp declares the self-defined normal permission with uses-permission.
   Example: <uses-permission android:name="xxx" />
Condition 3. The AttackerApp has installed on the device prior to the ProtectedApp.

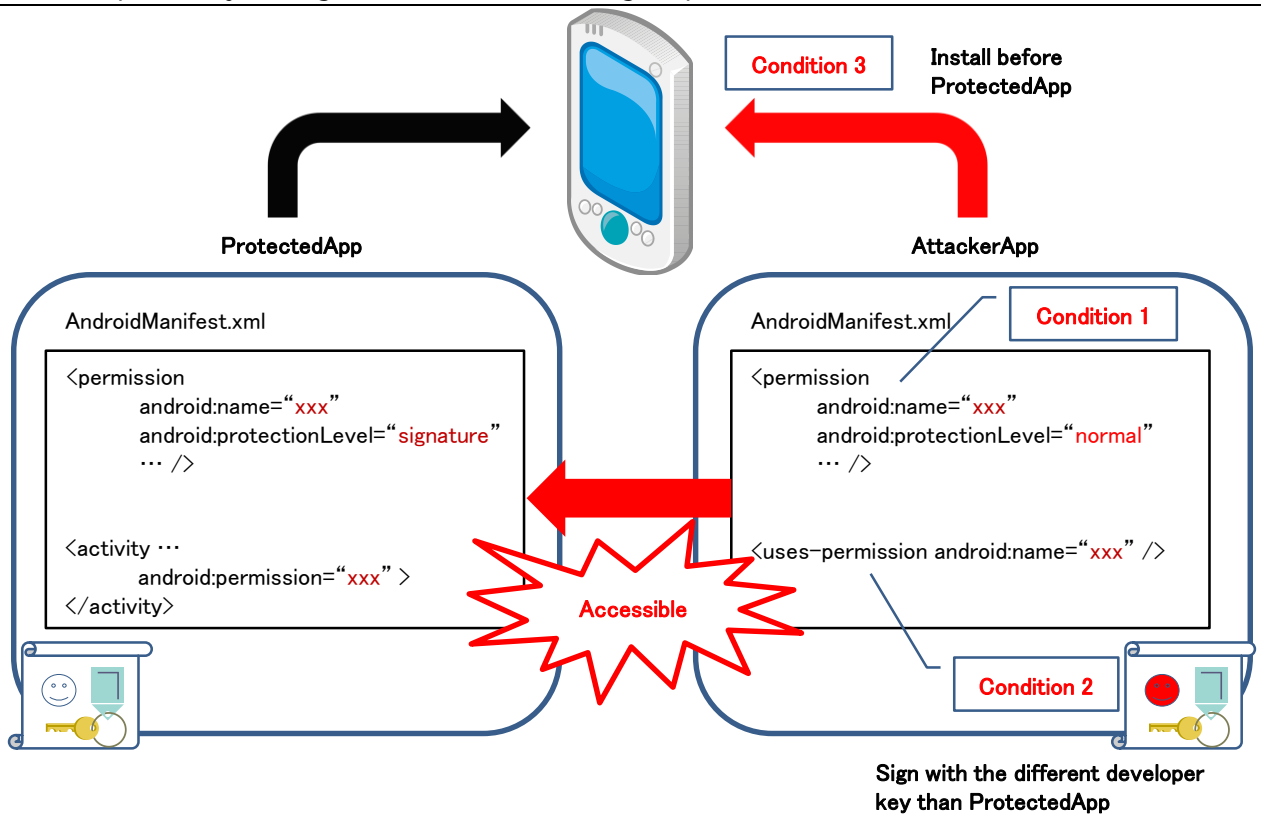


Figure 5.2-8

The permission name that is necessary to meet Condition 1 and Condition 2 can easily be known by an attacker taking AndroidManifest.xml out from an APK file. The attacker also could satisfy Condition 3 with a certain amount of effort (e.g. deceiving a user).

There is a risk of self-defined signature permission to evade protection if only the basic usage is adopted, and a counter-measure to prevent such loopholes is needed. Specifically, you could find how to solve the above-mentioned issues by using the method described in "5.2.2.4 Verify If the In-house-defined Signature Permission Is Defined by an In-house Application".

5.2.3.2. Falsification of AndroidManifest.xml by a User

We have already touched on the case that a Protection Level of self-defined permission could be changed as not intended. To prevent malfunctioning due to such cases, it has been needed to implement some sort of counter-measures on the source-code side of Java. From the viewpoint of AndroidManifest.xml falsification, we will talk about the counter-measures to be taken on the source-code side. We will demonstrate a simple case of installation that can detect falsifications. However, please note that these counter-measures are little effective against professional hackers who falsify with criminal intent.

This section is about the falsification of an application and users with malicious intent. Although this is originally outside of the scope of a Guidebook, from the fact that this is related to Permission and the tools for such falsification are provided in public as Android applications, we decided to mention it as "Simple counter-measures against amateur hackers".

It must be remembered that applications that can be installed from market are applications that can

be falsified without root privilege. The reason is that applications that can rebuild and sign APK files with altered AndroidManifest.xml are distributed. By using these applications, anyone can delete any permission from applications they have installed.

As an example, there seems to be cases of rebuilding APKs with different signatures altering AndroidManifest.xml with INTERNET permission removed to render advertising modules attached in applications as useless. There are some users who praise these types of tools due to the fact that no personal information is leaked anywhere. As these ads which are attached in applications stop functioning, such actions cause monetary damage for developers who are counting on ad revenue. And it is believed that most of the users don't have any compunction.

In the following code, we show an instance of implementation that an application that has declared INTERNET permission with uses-permission verifies if INTERNET permission is described in the AndroidManifest.xml of itself at run time.

```
public class CheckPermissionActivity extends Activity {

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);

        // Acquire Permission defined in AndroidManifest.xml
        List<String> list = getDefinedPermissionList();

        // Detect falsification
        if( checkPermissions(list) ){
            // OK
            Log.d("dbg", "OK.");
        }else{
            Log.d("dbg", "manifest file is stale.");
            finish();
        }
    }

    /**
     * Acquire Permission through list that was defined in AndroidManifest.xml
     * @return
     */
    private List<String> getDefinedPermissionList(){
        List<String> list = new ArrayList<String>();
        list.add("android.permission.INTERNET");
        return list;
    }

    /**
     * Verify that Permission has not been changed Permission
     * @param permissionList
     * @return
     */
    private boolean checkPermissions(List<String> permissionList){
        try {
            PackageInfo packageInfo = getPackageManager().getPackageInfo(
                    getPackageName(), PackageManager.GET_PERMISSIONS);
            String[] permissionArray = packageInfo.requestedPermissions;
            if (permissionArray != null) {
```

```
                for (String permission : permissionArray) {
                    if(! permissionList.remove(permission)){
                        // Unintended Permission has been added
                        return false;
                    }
                }
            }

            if(permissionList.size() == 0){
                // OK
                return true;
            }

        } catch (NameNotFoundException e) {
        }

        return false;
    }
}
```

5.2.3.3. Detection of APK Falsification

We explained about detecting the falsification of permissions by a user in "5.2.3.2 Falsification of AndroidManifest.xml by a User". However, the falsification of applications is not limited to permission only, and there are many other cases where applications are appropriated without any changes in the source code. For example, it is a case where they distribute other developers' applications (falsified) in the market as if they were their own applications just by replacing resources to their own. Here, we will show a more generic method to detect the falsification of an APK file.

In order to falsify an APK, it is needed to decode the APK file into folders and files, modify their contents, and then rebuild them into a new APK file. Since the falsifier does not have the key of the original developer, he would have to sign the new APK file with his own key. As the falsification of an APK inevitably brings with a change in signature (certificate), it is possible to detect whether an APK has been falsified at run time by comparing the certificate in the APK and the developer's certificate embedded in the source code as below.

The following is a sample code. Also, a professional hacker will be able to easily circumvent the detection of falsification if this implementation example is used as it is. Please apply this sample code to your application by being aware that this is a simple implementation example.

Points:

1. Verify that an application's certificate belongs to the developer before major processing is started.

SignatureCheckActivity.java

```
package org.jssec.android.permission.signcheckactivity;

import org.jssec.android.shared.PkgCert;
import org.jssec.android.shared.Utils;

import android.app.Activity;
```



```
import android.content.Context;
import android.os.Bundle;
import android.widget.Toast;

public class SignatureCheckActivity extends Activity {
    // Self signed certificate hash value
    private static String sMyCertHash = null;
    private static String myCertHash(Context context) {
        if (sMyCertHash == null) {
            if (Utils.isDebuggable(context)) {
                // Certificate hash value of "androiddebugkey" of debug.
                sMyCertHash = "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
            } else {
                // Certificate hash value of "my company key" of keystore
                sMyCertHash = "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
            }
        }
        return sMyCertHash;
    }

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);

        // *** POINT 1 *** Verify that an application's certificate belongs to the developer before majo
r processing is started
        if (!PkgCert.test(this, this.getPackageName(), myCertHash(this))) {
            Toast.makeText(this, "Self-sign match  NG", Toast.LENGTH_LONG).show();
            finish();
            return;
        }
        Toast.makeText(this, "Self-sign match  OK", Toast.LENGTH_LONG).show();
    }
}
```

PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
```

```
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```

5.2.3.4. Permission Re-delegation Problem

An application must declare to use permission when accessing contacts or GPS with its information and features that are protected by Android OS. When the permission required is granted, the permission is delegated to the application and the application would be able to access the information and features protected with the permission.

Depending on how the program is designed, the application to which has been delegated (granted) the permission is able to acquire data that is protected with the permission. Furthermore, the application can offer another application the protected data without enforcing the same permission. This is nothing less than permission-less application to access data that is protected by permission. This is virtually the same thing as re-delegating the permission, and this is referred to the Permission Re-delegation Problem. Accordingly, the specification of the permission mechanism of Android only is able to manage permission of direct access from an application to protected data.

A specific example is shown in Figure 5.2-9. The application in the center shows that an application which has declared android.permission.READ_CONTACTS to use it reads contacts and then stores them into its own database. The Permission Re-delegation Problem occurs when information that has been stored is offered to another application without any restriction via Content Provider.

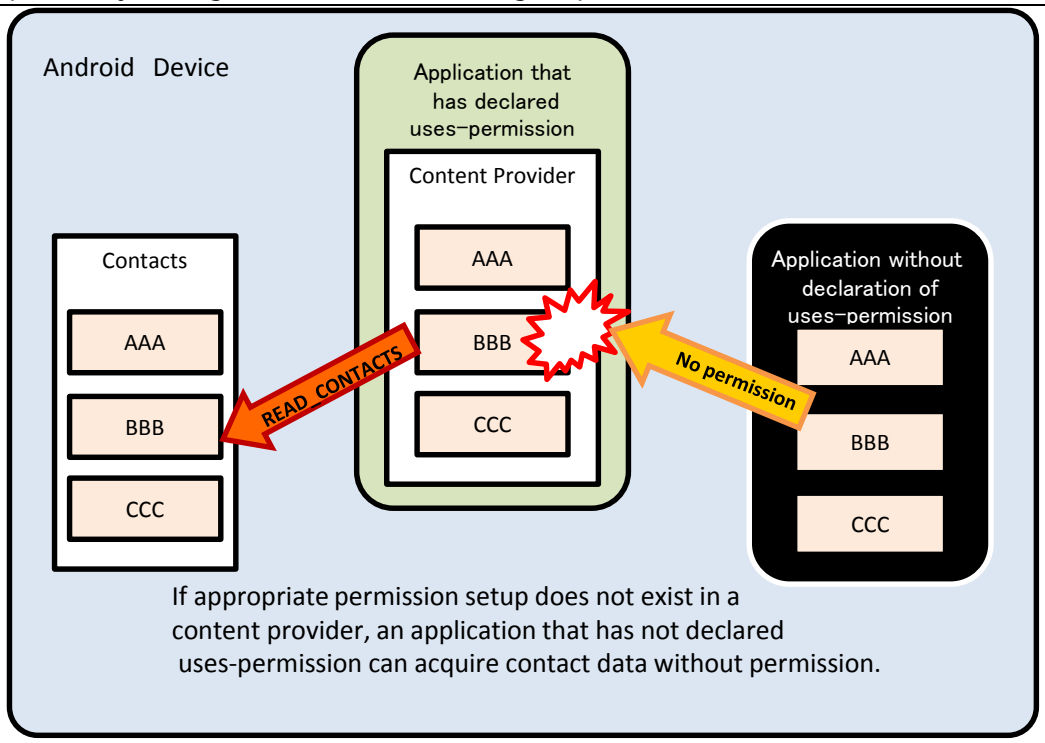


Figure 5.2-9 An Application without Permission Acquires Contacts

As a similar example, an application that has declared android.permission.CALL_PHONE to use it receives a phone number (maybe input by a user) from another application that has not declared the same permission. If that number is being called without the verification of a user, then also there is the Permission Re-delegation Problem.

There are cases where the secondary provision of another application with nearly-intact information asset or functional asset acquired with the permission is needed. In those cases, the provider-side application must demand the same permission for the provision in order to maintain the original level of protection. Also, in the case of only providing a portion of information asset as well as functional asset in a secondary fashion, an appropriate amount of protection is necessary in accordance with the degree of damage that is incurred when a portion of that information or functional asset is exploited. We can use protective measures such as demanding permission as similar to the former, verifying user consent, and setting up restrictions for target applications by using "4.1.1.1 Creating/Using Private Activities," or "4.1.1.4 Creating/Using In-house Activities" etc.

Such Permission Re-delegation Problem is not only limited to the issue of the Android permission. For an Android application, it is generic that the application acquires necessary information/functions from different applications, networks, and storage media. And in many cases, some permissions as well as restrictions are needed to access them. For example, if the provider source is an Android application, it is the permission, if it is a network, then it is the log-in, and if it is a storage media, there will be access restrictions. Therefore, such measures need to be implemented for an application after carefully considering as information/functions are not used in the contrary manner of the user's intention. This is especially important at the time of providing acquired information/functions to another application in a secondary manner or transferring to networks or storage media. Depending on the necessity, you have to enforce permission or restrict usage like the Android permission. Asking for the user's consent is part of the solution.

In the following code, we demonstrate a case where an application that acquires a list from the contact database by using READ_CONTACTS permission enforces the same READ_CONTACTS permission on the information destination source.

Point

1. Enforce the same permission that the provider does.

AndroidManifest.xml

```
<?xml version="1.0" encofing="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.permission.transferpermission"
    android:versionCode="1"
    android:versionName="1.0" >

    <uses-sdk
        android:minSdkVersion="8" />
    <uses-permission android:name="android.permission.READ_CONTACTS"/>

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
        <activity
            android:name=".TransferPermissionActivity"
            android:label="@string/title_activity_transfer_permission" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

        <provider
            android:name=".TransferPermissionContentProvider"
            <!-- *** Point1 *** Enforce the same permission that the provider does. -->
            android:authorities="org.jssec.android.permission.transferpermission"
            android:enabled="true"
            android:exported="true"
            android:readPermission="android.permission.READ_CONTACTS" >
        </provider>
    </application>

</manifest>
```

When an application enforces multiple permissions, the above method will not solve it. By using Context#checkCallingPermission() or PackageManager#checkPermission() from the source code, verify whether the invoker application has declared all permissions with uses-permission in the Manifest.

In the case of an Activity

```
public void onCreate(Bundle savedInstanceState) {
[...]
      if (checkCallingPermission("android.permission.READ_CONTACTS") == PackageManager.PERMISSION_GRANT
ED
       && checkCallingPermission("android.permission.WRITE_CONTACTS") == PackageManager.PERMISSION_GRAN
TED) {
               // Processing during the time when an invoker is correctly declaring to use
```



```
                return;
        }
        finish();
}
```

5.2.3.5. Signature check mechanism for custom permissions (Android 5.0 and later)

In versions of Android 5.0 (API Level 21) and later, the application which defines its own custom permissions cannot be installed if the following conditions are met.

Cond 1. Another application which defines its own permission with the same name has already installed on the device.
Cond 2. The applications are signed with different keys

When both an application with the protected function (Component) and an application using the function define their own permission with the same name and are signed with the same key, the above mechanism will protect against installation of other company's applications which define their own custom permission with the same name. However, as mentioned in "5.2.2.3 Your Own Signature Permission Must Only Be Defined on the Provider-side Application (Required)", that mechanism won't work well for checking if a custom permission is defined by your own company because the permission could be undefined without your intent by uninstalling applications when plural applications define the same permission.

To sum it up, also in versions of Android 5.0 (API Level 21) and later, you are required to comply with the two rules, "5.2.2.3 Your Own Signature Permission Must Only Be Defined on the Provider-side Application (Required)" and "5.2.2.4 Verify If the In-house-defined Signature Permission Is Defined by an In-house Application (Required)" when your application defines your own Signature Permission.

.

5.2.3.6. Modifications to the Permission model specifications in Android versions 6.0 and later

Android 6.0 (API Level 23) introduces modified specifications for the Permission model that affect both the design and specifications of apps. In this section we offer an overview of the Permission model in Android 6.0 and later. We also describe modifications made in Android 8.0 and later.

The timing of permission grants and refusals

In cases where an app declares use of permissions requiring user confirmation (Dangerous Permissions) [see Section "5.2.2.1 System Dangerous Permissions of Android OS Must Only Be Used for Protecting User Assets (Required)"], the specifications for Android 5.1 (API level 22) and earlier versions called for a list of such permissions to be displayed when the app is installed, and the user must grant all permissions for the installation to proceed. At this point, all permissions declared by the app (including permissions other than Dangerous Permissions) were granted to the app; once these permissions were granted to the app, they remained in effect until the app was uninstalled from the terminal.

However, in the specifications for Android 6.0 and later versions, the granting of permissions takes place when an app is executed. The granting of permissions, and user confirmation of permissions, does not take place when the app is installed. When an app executes a procedure that requires Dangerous Permissions, it is necessary to check whether or not those permissions have been granted to the app in advance; if not, a confirmation window must be displayed in Android OS to request permission from the user.[28] If the user grants permission from the confirmation window, the permissions are granted to the app. However, permissions granted to an app by a user (Dangerous Permissions) may be revoked at any time via the Settings menu (Figure 5.2-10). For this reason, appropriate procedures must be implemented to ensure that apps cause no irregular behavior even in situations in which they cannot access needed information or functionality because permission has not been granted.

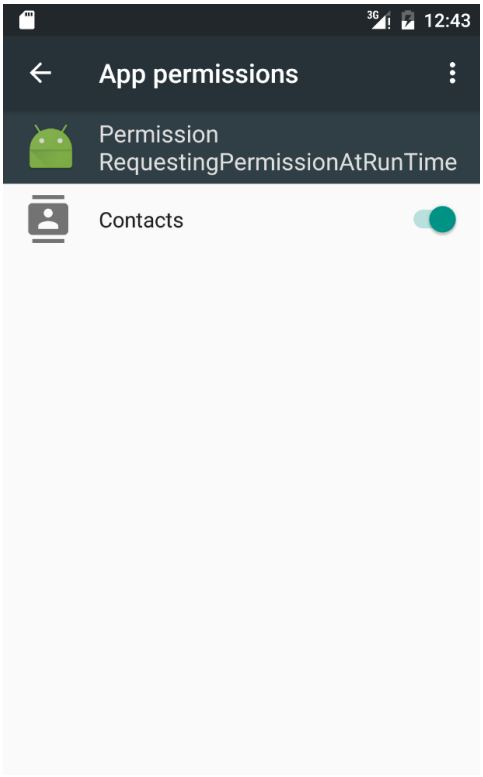


Figure 5.2-10

Units of permission grants and refusals

Multiple Permissions may be grouped together into what is known as a Permission Group based on their functions and type of information relevant to them. For example, the Permission android.permission.READ_CALENDAR, which is required to read calendar information, and the Permission android.permission.WRITE_CALENDAR, which is required to write calendar information, are both affiliated with the Permission Group named android.permission-group.CALENDAR.

[28] Because Normal Permissions and Signature Permissions are automatically granted by Android OS, there is no need to obtain user confirmation for these permissions.

In the Permission model for Android 6.0 (API Level 23) and later, privileges are granted or denied at the block-unit level of the Permission Group, as shown here. However, developers must be careful to note that the block unit may vary depending on the combination of OS and SDK (see below).

- For terminals running Android 6.0 (API Level 23) or later and app targetSdkVersion: 23~25
  If android.permission.READ_CALENDAR and android.permission.WRITE_CALENDAR are listed in the Manifest, then when the app is launched a request for android.permission.READ_CALENDAR is issued; if the user grants this permission, Android OS determines that both android.permission.READ_CALENDAR and android.permission.WRITE_CALENDAR are permitted for use and thus grants the permission.

- For terminals running Android 8.0 (API Level 26) or later and app targetSdkVersion 26 and above:
  Only requested Permissions are granted. Thus, even if android.permission.READ_CALENDAR and android.permission.WRITE_CALENDAR are both listed, if only android.permission.READ_CALENDAR has been requested and granted by the user, then only android.permission.READ_CALENDAR will be granted. Thereafter, if android.permission.WRITE_CALENDAR is requested, the permission will be granted immediately with no dialog box shown to the user.[29]

Also, in contrast to the granting of permissions, cancelling of permissions from the settings menu is carried out at the block-unit level of the Permission Group on Android 8.0 or later.
For more information on the classification of Permission Groups, see the Developer Reference (http://developer.android.com/intl/ja/guide/topics/security/permissions.html#perm-groups).

The affected range of the revised specifications

Cases in which apps require Permission requests at runtime are restricted to situations in which the terminal is running Android 6.0 or later and the app's targetSDKVersion is 23 or higher. If the terminal is running Android 5.1 or earlier, or if the app's targetSDKVersion was 23 or lower, permissions are requested and granted altogether at the time of installation, as was traditionally the case. However, if the terminal is running Android 6.0 or later, then—even if the app's targetSDKVersion is below 23—permissions that were granted by the user at installation may be revoked by the user at any time. This creates the possibility of unintended irregular app termination. Developers must either comply immediately with the modified specifications or set the maxSDKVersion of their app to 22 or earlier to ensure that the app cannot be installed on terminals running Android 6.0 (API Level 23) or later(Table 5.2-1).

Table 5.2-1

Terminal Android OS	App targetSDKVersion	Times at which app is	User has control over

[29] In this case as well, the app must declare usage of both android.permission.READ_CALENDAR and android.permission.WRITE_CALENDAR.

Version		granted permissions	permissions?
≧8.0	≧26	App execution (granted individually)	Yes
	＜26	App execution (granted by Permission Group)	Yes
	＜23	App installation	Yes (rapid response required)
≧6.0	≧23	App execution (granted by Permission Group)	Yes
	＜23	App installation	Yes (rapid response required)
≦5.1	≧23	App installation	No
	＜23	App installation	No

However, it should be noted that the effect of maxSdkVersion is limited. When the value of maxSdkVersion is set 22 or earlier, Android 6.0 (API Level 23) and later of the devices are no longer listed as an installable device of the target application in Google Play. On the other hand, because the value of maxSdkVersion is not checked in the marketplace other than Google Play, it may be possible to install the target application in the Android 6.0 (API Level 23) or later.
Because the effect of maxSdkVersion is limited, and further Google does not recommend the use of maxSdkVersion, it is recommended that developers comply immediately with the modified specifications.

In Android 6.0 and later versions, permissions for the following network communications have their Protection Level changed from Dangerous to Normal. Thus, even if apps declare the use of these Permissions, there is no need to acquire explicit permission from the user, and hence the modified specification has no impact in this case.

- android.permission.BLUETOOTH
- android.permission.BLUETOOTH_ADMIN
- android.permission.CHANGE_WIFI_MULTICAST_STATE
- android.permission.CHANGE_WIFI_STATE
- android.permission.CHANGE_WIMAX_STATE
- android.permission.DISABLE_KEYGUARD
- android.permission.INTERNET
- android.permission.NFC

5.3. Add In-house Accounts to Account Manager

Account Manager is the Android OS's system which centrally manages account information (account name, password) which is necessary for applications to access to online service and authentication token. A user needs to register the account information to Account Manager in advance, and when an application tries to access to online service, Account Manager will automatically provide application authentication token after getting user's permission. The advantage of Account Manager is that an application doesn't need to handle the extremely sensitive information, password.

The structure of account management function which uses Account Manager is as per below Figure 5.3-1. "Requesting application" is the application which accesses the online service, by getting authentication token, and this is above mentioned application. On the other hand, "Authenticator application" is function extension of Account Manager, and by providing Account Manager of an object called Authenticator, as a result Account Manager can manage centrally the account information and authentication token of the online service. Requesting application and Authenticator application don't need to be the separate ones, so these can be implemented as a single application.

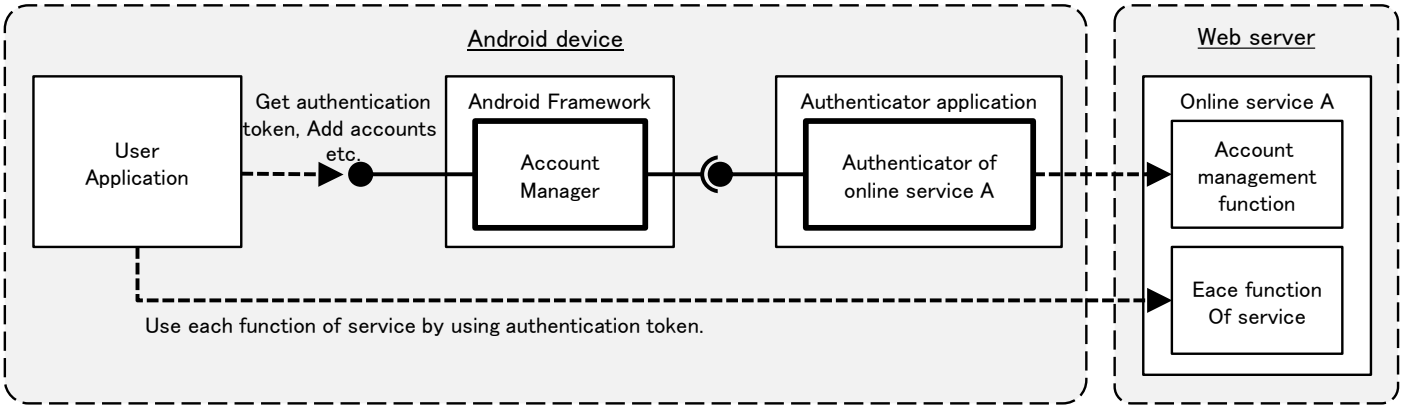


Figure 5.3-1 Configuration of account management function which uses Account Manager

Originally, the developer's signature key of user application (requesting application) and Authenticator application can be the different ones. However, only in Android 4.0.x devices, there's an Android Framework bug, and when the signature key of user application and Authenticator application are different, exception occurs in user application, and in-house account cannot be used. The following sample code does not implement any workarounds against this defect. Please refer to "5.3.3.2 Exception Occurs When Signature Keys of User Application and Authenticator Application Are Different, in Android 4.0.x" for details.

5.3.1. Sample Code

"5.3.1.1 Creating In-house account" is prepared as a sample of Authenticator application, and "5.3.1.2 Using In-house Account" is prepared as a sample of requesting application. In sample code set which is distributed in JSSEC's Web site, each of them is corresponded to AccountManager Authenticator and AccountManager User.

5.3.1.1. Creating In-house accounts

Here is the sample code of Authenticator application which enables Account Manager to use the in-house account. There is no Activity which can be launched from home screen in this application. Please pay attention that it's called indirectly via Account Manager from another sample code "5.3.1.2 Using In-house Account."

Points:

1. The service that provides an authenticator must be private.
2. The login screen activity must be implemented in an authenticator application.
3. The login screen activity must be made as a public activity.
4. The explicit intent which the class name of the login screen activity is specified must be set to KEY_INTENT.
5. Sensitive information (like account information or authentication token) must not be output to the log.
6. Password should not be saved in Account Manager.
7. HTTPS should be used for communication between an authenticator and the online services.

Service which gives Account Manager IBinder of Authenticator is defined in AndroidManifest.xml. Specify resource XML file which Authenticator is written, by meta-data.

AccountManager Authenticator/AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.accountmanager.authenticator"
    xmlns:tools="http://schemas.android.com/tools">

    <!-- Necessary Permission to implement Authenticator -->
    <uses-permission android:name="android.permission.GET_ACCOUNTS" />
    <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS" />

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- Service which gives IBinder of Authenticator to AccountManager -->
        <!-- *** POINT 1 *** The service that provides an authenticator must be private. -->
        <service
            android:name=".AuthenticationService"
            android:exported="false" >
            <!-- intent-filter and meta-data are usual pattern. -->
            <intent-filter>
                <action android:name="android.accounts.AccountAuthenticator" />
            </intent-filter>
            <meta-data
                android:name="android.accounts.AccountAuthenticator"
                android:resource="@xml/authenticator" />
        </service>

        <!-- Activity for for login screen which is displayed when adding an account -->
        <!-- *** POINT 2 *** The login screen activity must be implemented in an authenticator applicati
on. -->
```



```
        <!-- *** POINT 3 *** The login screen activity must be made as a public activity. -->
        <activity
            android:name=".LoginActivity"
            android:exported="true"
            android:label="@string/login_activity_title"
            android:theme="@android:style/Theme.Dialog"
            tools:ignore="ExportedActivity" />
    </application>

</manifest>
```

Define Authenticator by XML file. Specify account type etc. of in-house account.

res/xml/authenticator.xml

```
<account-authenticator xmlns:android="http://schemas.android.com/apk/res/android"
    android:accountType="org.jssec.android.accountmanager"
    android:icon="@drawable/ic_launcher"
    android:label="@string/label"
    android:smallIcon="@drawable/ic_launcher"
    android:customTokens="true" />
```

Service which gives Authenticator's Instance to AccountManager. Easy implementation which returns Instance of JssecAuthenticator class that is Authenticator implemented in this sample by onBind(), is enough.

AuthenticationService.java

```
package org.jssec.android.accountmanager.authenticator;

import android.app.Service;
import android.content.Intent;
import android.os.IBinder;

public class AuthenticationService extends Service {

    private JssecAuthenticator mAuthenticator;

    @Override
    public void onCreate() {
        mAuthenticator = new JssecAuthenticator(this);
    }

    @Override
    public IBinder onBind(Intent intent) {
        return mAuthenticator.getIBinder();
    }
}
```

JssecAuthenticator is the Authenticator which is implemented in this sample. It inherits AbstractAccountAuthenticator, and all abstract methods are implemented. These methods are called by Account Manager. At addAccount() and at getAuthToken(), the intent for launching LoginActivity to get authentication token from online service are returned to Account Manager.

JssecAuthenticator.java

```
package org.jssec.android.accountmanager.authenticator;

import android.accounts.AbstractAccountAuthenticator;
import android.accounts.Account;
import android.accounts.AccountAuthenticatorResponse;
import android.accounts.AccountManager;
import android.accounts.NetworkErrorException;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;

public class JssecAuthenticator extends AbstractAccountAuthenticator {

    public static final String JSSEC_ACCOUNT_TYPE = "org.jssec.android.accountmanager";
    public static final String JSSEC_AUTHTOKEN_TYPE = "webservice";
    public static final String JSSEC_AUTHTOKEN_LABEL = "JSSEC Web Service";
    public static final String RE_AUTH_NAME = "reauth_name";

    protected final Context mContext;

    public JssecAuthenticator(Context context) {
        super(context);
        mContext = context;
    }

    @Override
    public Bundle addAccount(AccountAuthenticatorResponse response, String accountType,
            String authTokenType, String[] requiredFeatures, Bundle options)
            throws NetworkErrorException {

        AccountManager am = AccountManager.get(mContext);
        Account[] accounts = am.getAccountsByType(JSSEC_ACCOUNT_TYPE);
        Bundle bundle = new Bundle();
        if (accounts.length > 0) {
            // In this sample code, when an account already exists, consider it as an error.
            bundle.putString(AccountManager.KEY_ERROR_CODE, String.valueOf(-1));
            bundle.putString(AccountManager.KEY_ERROR_MESSAGE,
                    mContext.getString(R.string.error_account_exists));
        } else {
            // *** POINT 2 *** The login screen activity must be implemented in an authenticator applicat
ion.
            // *** POINT 4 *** The explicit intent which the class name of the login screen activity is s
pecified must be set to KEY_INTENT.
            Intent intent = new Intent(mContext, LoginActivity.class);
            intent.putExtra(AccountManager.KEY_ACCOUNT_AUTHENTICATOR_RESPONSE, response);

            bundle.putParcelable(AccountManager.KEY_INTENT, intent);
        }
        return bundle;
    }

    @Override
```



```
    public Bundle getAuthToken(AccountAuthenticatorResponse response, Account account,
            String authTokenType, Bundle options) throws NetworkErrorException {

        Bundle bundle = new Bundle();
        if (accountExist(account)) {
            // *** POINT 4 *** KEY_INTENT must be given an explicit intent that is specified the class na
me of the login screen activity.
            Intent intent = new Intent(mContext, LoginActivity.class);
            intent.putExtra(RE_AUTH_NAME, account.name);
            intent.putExtra(AccountManager.KEY_ACCOUNT_AUTHENTICATOR_RESPONSE, response);
            bundle.putParcelable(AccountManager.KEY_INTENT, intent);
        } else {
            // When the specified account doesn't exist, consider it as an error.
            bundle.putString(AccountManager.KEY_ERROR_CODE, String.valueOf(-2));
            bundle.putString(AccountManager.KEY_ERROR_MESSAGE,
                    mContext.getString(R.string.error_account_not_exists));
        }
        return bundle;
    }

    @Override
    public String getAuthTokenLabel(String authTokenType) {
        return JSSEC_AUTHTOKEN_LABEL;
    }

    @Override
    public Bundle confirmCredentials(AccountAuthenticatorResponse response, Account account,
            Bundle options) throws NetworkErrorException {
        return null;
    }

    @Override
    public Bundle editProperties(AccountAuthenticatorResponse response, String accountType) {
        return null;
    }

    @Override
    public Bundle updateCredentials(AccountAuthenticatorResponse response, Account account,
            String authTokenType, Bundle options) throws NetworkErrorException {
        return null;
    }

    @Override
    public Bundle hasFeatures(AccountAuthenticatorResponse response, Account account,
            String[] features) throws NetworkErrorException {
        Bundle result = new Bundle();
        result.putBoolean(AccountManager.KEY_BOOLEAN_RESULT, false);
        return result;
    }

    private boolean accountExist(Account account) {
        AccountManager am = AccountManager.get(mContext);
        Account[] accounts = am.getAccountsByType(JSSEC_ACCOUNT_TYPE);
        for (Account ac : accounts) {
            if (ac.equals(account)) {
                return true;
            }
        }
        return false;
    }
```

```
}
```

This is Login activity which sends an account name and password to online service, and perform login authentication, and as a result, get an authentication token. It's displayed when adding a new account or when getting authentication token again. It's supposed that the actual access to online service is implemented in WebService class.

LoginActivity.java

```
package org.jssec.android.accountmanager.authenticator;

import org.jssec.android.accountmanager.webservice.WebService;

import android.accounts.Account;
import android.accounts.AccountAuthenticatorActivity;
import android.accounts.AccountManager;
import android.content.Intent;
import android.os.Bundle;
import android.text.InputType;
import android.text.TextUtils;
import android.util.Log;
import android.view.View;
import android.view.Window;
import android.widget.EditText;

public class LoginActivity extends AccountAuthenticatorActivity {
    private static final String TAG = AccountAuthenticatorActivity.class.getSimpleName();
    private String mReAuthName = null;
    private EditText mNameEdit = null;
    private EditText mPassEdit = null;

    @Override
    public void onCreate(Bundle icicle) {
        super.onCreate(icicle);

        // Display alert icon
        requestWindowFeature(Window.FEATURE_LEFT_ICON);
        setContentView(R.layout.login_activity);
        getWindow().setFeatureDrawableResource(Window.FEATURE_LEFT_ICON,
                android.R.drawable.ic_dialog_alert);

        // Find a widget in advance
        mNameEdit = (EditText) findViewById(R.id.username_edit);
        mPassEdit = (EditText) findViewById(R.id.password_edit);

        // *** POINT 3 *** The login screen activity must be made as a public activity, and suppose the a
ttack access from other application.
        // Regarding external input, only RE_AUTH_NAME which is String type of Intent#extras, are handle
d.
        // This external input String is passed toextEdit#setText(), WebService#login(),new Account(),
        // as a parameter,it's verified that there's no problem if any character string is passed.
        mReAuthName = getIntent().getStringExtra(JssecAuthenticator.RE_AUTH_NAME);
        if (mReAuthName != null) {
            // Since LoginActivity is called with the specified user name, user name should not be editab
le.
            mNameEdit.setText(mReAuthName);
            mNameEdit.setInputType(InputType.TYPE_NULL);
            mNameEdit.setFocusable(false);
            mNameEdit.setEnabled(false);
```



```
        }
    }

    // It's executed when login button is pressed.
    public void handleLogin(View view) {
        String name = mNameEdit.getText().toString();
        String pass = mPassEdit.getText().toString();

        if (TextUtils.isEmpty(name) || TextUtils.isEmpty(pass)) {
            // Process when the inputed value is incorrect
            setResult(RESULT_CANCELED);
            finish();
        }

        // Login to online service based on the inpputted account information.
        WebService web = new WebService();
        String authToken = web.login(name, pass);
        if (TextUtils.isEmpty(authToken)) {
            // Process when authentication failed
            setResult(RESULT_CANCELED);
            finish();
        }

        // Process when login was successful, is as per below.

        // *** POINT 5 *** Sensitive information (like account information or authentication token) must
 not be output to the log.
        Log.i(TAG, "WebService login succeeded");


        if (mReAuthName == null) {
            // Register accounts which logged in successfully, to aAccountManager
            // *** POINT 6 *** Password should not be saved in Account Manager.
            AccountManager am = AccountManager.get(this);
            Account account = new Account(name, JssecAuthenticator.JSSEC_ACCOUNT_TYPE);
            am.addAccountExplicitly(account, null, null);
            am.setAuthToken(account, JssecAuthenticator.JSSEC_AUTHTOKEN_TYPE, authToken);
            Intent intent = new Intent();
            intent.putExtra(AccountManager.KEY_ACCOUNT_NAME, name);
            intent.putExtra(AccountManager.KEY_ACCOUNT_TYPE,
                    JssecAuthenticator.JSSEC_ACCOUNT_TYPE);
            setAccountAuthenticatorResult(intent.getExtras());
            setResult(RESULT_OK, intent);
        } else {
            // Return authentication token
            Bundle bundle = new Bundle();
            bundle.putString(AccountManager.KEY_ACCOUNT_NAME, name);
            bundle.putString(AccountManager.KEY_ACCOUNT_TYPE,
                    JssecAuthenticator.JSSEC_ACCOUNT_TYPE);
            bundle.putString(AccountManager.KEY_AUTHTOKEN, authToken);
            setAccountAuthenticatorResult(bundle);
            setResult(RESULT_OK);
        }
        finish();
    }
}
```

Actually, WebService class is dummy implementation here, and this is the sample implementation

which supposes authentication is always successful, and fixed character string is returned as an authentication token.

WebService.java

```
package org.jssec.android.accountmanager.webservice;

public class WebService {

    /**
     * Suppose to access to account managemnet function of online service.
     *
     * @param username Account name character string
     * @param password password character string
     * @return Return authentication token
     */
    public String login(String username, String password) {
        // *** POINT 7 *** HTTPS should be used for communication between an authenticator and the online
 services.
        // Actually, communication process with servers is implemented here, but Omit here, since this i
s a sample.
        return getAuthToken(username, password);
    }

    private String getAuthToken(String username, String password) {
        // In fact, get the value which uniqueness and impossibility of speculation are guaranteed by th
e server,
        // but the fixed value is returned without communication here, since this is sample.
        return "c2f981bda5f34f90c0419e171f60f45c";
    }
}
```


5.3.1.2. Using In-house Accounts

Here is the sample code of an application which adds an in-house account and gets an authentication token. When another sample application "5.3.1.1 Creating In-house account" is installed in a device, in-house account can be added or authentication token can be got. "Access request" screen is displayed only when the signature keys of both applications are different.

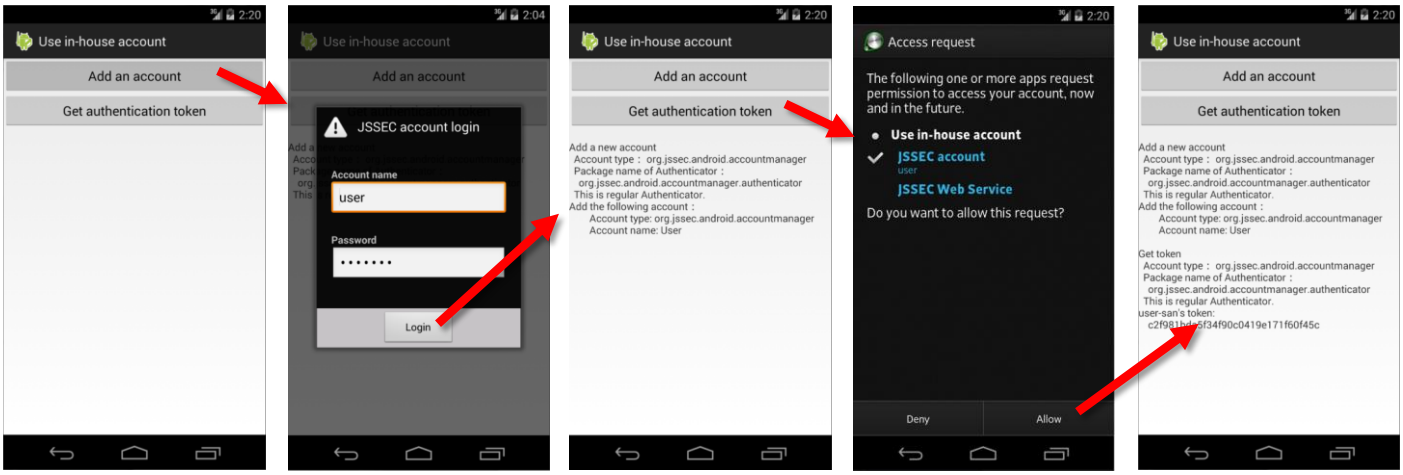


Figure 5.3-2 Behavior screen of sample application AccountManager User

Point:

1. Execute the account process after verifying if the authenticator is regular one.

AndroidManifest.xml of AccountManager user application. Declare to use necessary Permission. Refer to "5.3.3.1 Usage of Account Manager and Permission" for the necessary Permission.

AccountManager User/AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.accountmanager.user" >

    <uses-permission android:name="android.permission.GET_ACCOUNTS" />
    <uses-permission android:name="android.permission.MANAGE_ACCOUNTS" />
    <uses-permission android:name="android.permission.USE_CREDENTIALS" />

    <application
        android:allowBackup="false"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
        <activity
            android:name=".UserActivity"
            android:label="@string/app_name"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
```

```
</manifest>
```

Activity of user application. When tapping the button on the screen, either addAccount() or getAuthToken() is to be executed. Authenticator which corresponds to the specific account type may be fake in some cases, so pay attention that the account process is started after verifying that the Authenticator is regular one.

UserActivity.java

```
package org.jssec.android.accountmanager.user;

import java.io.IOException;

import org.jssec.android.shared.PkgCert;
import org.jssec.android.shared.Utils;

import android.accounts.Account;
import android.accounts.AccountManager;
import android.accounts.AccountManagerCallback;
import android.accounts.AccountManagerFuture;
import android.accounts.AuthenticatorDescription;
import android.accounts.AuthenticatorException;
import android.accounts.OperationCanceledException;
import android.app.Activity;
import android.content.Context;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;

public class UserActivity extends Activity {

    // Information of the Authenticator to be used
    private static final String JSSEC_ACCOUNT_TYPE = "org.jssec.android.accountmanager";
    private static final String JSSEC_TOKEN_TYPE = "webservice";
    private TextView mLogView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.user_activity);

        mLogView = (TextView)findViewById(R.id.logview);
    }

    public void addAccount(View view) {
        logLine();
        logLine("Add a new account");

        // *** POINT 1 *** Execute the account process after verifying if the authenticator is regular on
e.
        if (!checkAuthenticator()) return;

        AccountManager am = AccountManager.get(this);
        am.addAccount(JSSEC_ACCOUNT_TYPE, JSSEC_TOKEN_TYPE, null, null, this,
                new AccountManagerCallback<Bundle>() {
                    @Override
                    public void run(AccountManagerFuture<Bundle> future) {
```



```
                    try {
                        Bundle result = future.getResult();
                        String type = result.getString(AccountManager.KEY_ACCOUNT_TYPE);
                        String name = result.getString(AccountManager.KEY_ACCOUNT_NAME);
                        if (type != null && name != null) {
                            logLine("Add the following accounts:");
                            logLine("  Account type: %s", type);
                            logLine("  Account name: %s", name);
                        } else {
                            String code = result.getString(AccountManager.KEY_ERROR_CODE);
                            String msg = result.getString(AccountManager.KEY_ERROR_MESSAGE);
                            logLine("The account cannot be added");
                            logLine("  Error code %s: %s", code, msg);
                        }
                    } catch (OperationCanceledException e) {
                    } catch (AuthenticatorException e) {
                    } catch (IOException e) {
                    }
                }
            },
            null);
    }

    public void getAuthToken(View view) {
        logLine();
        logLine("Get token");

        // *** POINT 1 *** After checking that the Authenticator is the regular one, execute account proc
ess.
        if (!checkAuthenticator()) return;

        AccountManager am = AccountManager.get(this);
        Account[] accounts = am.getAccountsByType(JSSEC_ACCOUNT_TYPE);
        if (accounts.length > 0) {
            Account account = accounts[0];
            am.getAuthToken(account, JSSEC_TOKEN_TYPE, null, this,
                    new AccountManagerCallback<Bundle>() {
                        @Override
                        public void run(AccountManagerFuture<Bundle> future) {
                            try {
                                Bundle result = future.getResult();
                                String name = result.getString(AccountManager.KEY_ACCOUNT_NAME);
                                String authtoken = result.getString(AccountManager.KEY_AUTHTOKEN);
                                logLine("%s-san's token:", name);
                                if (authtoken != null) {
                                    logLine("    %s", authtoken);
                                } else {
                                    logLine("    Couldn't get");
                                }
                            } catch (OperationCanceledException e) {
                                logLine("  Exception: %s",e.getClass().getName());
                            } catch (AuthenticatorException e) {
                                logLine("  Exception: %s",e.getClass().getName());
                            } catch (IOException e) {
                                logLine("  Exception: %s",e.getClass().getName());
                            }
                        }
                    }, null);
        } else {
            logLine("Account is not registered.");
```

```
        }
    }

    // *** POINT 1 *** Verify that Authenticator is regular one.
    private boolean checkAuthenticator() {
        AccountManager am = AccountManager.get(this);
        String pkgname = null;
        for (AuthenticatorDescription ad : am.getAuthenticatorTypes()) {
            if (JSSEC_ACCOUNT_TYPE.equals(ad.type)) {
                pkgname = ad.packageName;
                break;
            }
        }

        if (pkgname == null) {
            logLine("Authenticator cannot be found.");
            return false;
        }

        logLine("  Account type: %s", JSSEC_ACCOUNT_TYPE);
        logLine("  Package name of Authenticator: ");
        logLine("    %s", pkgname);

        if (!PkgCert.test(this, pkgname, getTrustedCertificateHash(this))) {
            logLine("  It's not regular Authenticator(certificate is not matched.)");
            return false;
        }

        logLine("  This is regular Authenticator.");
        return true;
    }

    // Certificate hash value of regular Authenticator application
    // Certificate hash value can be checked in sample applciation JSSEC CertHash Checker
    private String getTrustedCertificateHash(Context context) {
        if (Utils.isDebuggable(context)) {
            // Certificate hash value of  debug.keystore "androiddebugkey"
            return "0EFB7236 328348A9 89718BAD DF57F544 D5CCB4AE B9DB34BC 1E29DD26 F77C8255";
        } else {
            // Certificate hash value of  keystore "my company key"
            return "D397D343 A5CBC10F 4EDDEB7C A10062DE 5690984F 1FB9E88B D7B3A7C2 42E142CA";
        }
    }

    private void log(String str) {
        mLogView.append(str);
    }

    private void logLine(String line) {
        log(line + "¥n");
    }

    private void logLine(String fmt, Object... args) {
        logLine(String.format(fmt, args));
    }

    private void logLine() {
        log("¥n");
    }
}
```


PkgCert.java

```
package org.jssec.android.shared;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

import android.content.Context;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.content.pm.Signature;

public class PkgCert {

    public static boolean test(Context ctx, String pkgname, String correctHash) {
        if (correctHash == null) return false;
        correctHash = correctHash.replaceAll(" ", "");
        return correctHash.equals(hash(ctx, pkgname));
    }

    public static String hash(Context ctx, String pkgname) {
        if (pkgname == null) return null;
        try {
            PackageManager pm = ctx.getPackageManager();
            PackageInfo pkginfo = pm.getPackageInfo(pkgname, PackageManager.GET_SIGNATURES);
            if (pkginfo.signatures.length != 1) return null;    // Will not handle multiple signatures.
            Signature sig = pkginfo.signatures[0];
            byte[] cert = sig.toByteArray();
            byte[] sha256 = computeSha256(cert);
            return byte2hex(sha256);
        } catch (NameNotFoundException e) {
            return null;
        }
    }

    private static byte[] computeSha256(byte[] data) {
        try {
            return MessageDigest.getInstance("SHA-256").digest(data);
        } catch (NoSuchAlgorithmException e) {
            return null;
        }
    }

    private static String byte2hex(byte[] data) {
        if (data == null) return null;
        final StringBuilder hexadecimal = new StringBuilder();
        for (final byte b : data) {
            hexadecimal.append(String.format("%02X", b));
        }
        return hexadecimal.toString();
    }
}
```

5.3.2. Rule Book

Follow the rules below when implementing Authenticator application.

1.	Service that Provides Authenticator Must Be Private (Required)
2.	Login Screen Activity Must Be Implemented by Authenticator Application (Required)
3.	The Login Screen Activity Must Be Made as a Public Activity and Suppose Attack Accesses by Other Applications (Required)
4.	Provide KEY_INTENT with Explicit Intent with the Specified Class Name of Login Screen Activity (Required)
5.	Sensitive Information (like Account Information and Authentication Token) Must Not Be Output to the Log (Required)
6.	Password Should Not Be Saved in Account Manager (Recommended)
7.	HTTPS Should Be Used for Communication Between an Authenticator and the Online Service (Required)

Follow the rules below when implementing user application.

8.	Account Process Should Be Executed after verifying if the Authenticator is the regular one (Required)

5.3.2.1. Service that Provides Authenticator Must Be Private (Required)

It's presupposed that the Service which provides with Authenticator is used by Account Manager, and it should not be accessed by other applications. So, by making it Private Service, it can exclude accesses by other applications. In addition, Account Manager runs with system privilege, so Account Manager can access even if it's private Service.

5.3.2.2. Login Screen Activity Must Be Implemented by Authenticator Application (Required)

Login screen for adding a new account and getting the authentication token should be implemented by Authenticator application. Own Login screen should not be prepared in user application side. As mentioned at the beginning of this article, [The advantage of AccountManager is that the extremely sensitive information/password is not necessarily to be handled by application.], If login screen is prepared in user application side, password is handled by user application, and its design becomes what is beyond the policy of Account Manager.

By preparing login screen by Authenticator application, who can operate login screen is limited only the device's user. It means that there's no way to attack the account for malicious applications by attempting to login directly, or by creating an account.

5.3.2.3. The Login Screen Activity Must Be Made as a Public Activity and Suppose Attack Accesses by Other Applications (Required)

Login screen Activity is the system launched by the user application's p. In order that the login screen Activity is displayed even when the signature keys of user application and Authenticator application are different, login screen Activity should be implemented as Public Activity.

What login screen Activity is public Activity means, that there's a chance that it may be launched by malicious applications. Never trust on any input data. Hence, it's necessary to take the counter-measures mentioned in "3.2 Handling Input Data Carefully and Securely"

5.3.2.4. Provide KEY_INTENT with Explicit Intent with the Specified Class Name of Login Screen Activity (Required)

When Authenticator needs to open login screen Activity, Intent which launches login screen Activity is to be given in the Bundle that is returned to Account Manager, by KEY_INTENT. The Intent to be given, should be the explicit Intent which specifies class name of login screen Activity. If an *implicit* Intent is given, the framework may attempt to launch an Activity *other* than the Activity prepared by the Authenticator app for the login window. On Android 4.4 (API Level 19) and later versions, this may cause the app to crash; on earlier versions it may cause unintended Activities prepared by other apps to be launched.

On Android 4.4(API Level 19) and later versions, if the signature of an app launched by an intent given by the framework via KEY_INTENT does not match the signature of the Authenticator app, a SecurityException is generated; in this case, there is no risk that a false login screen will be launched; however, there is a possibility that the ordinary screen will be able to launch and the user's normal use of the app will be obstructed. On versions prior to Android 4.4(API Level 19), there is a risk that a false login screen prepared by a malicious app will be launched, and thus that the user may input passwords and other authentication information to the malicious app.

5.3.2.5. Sensitive Information (like Account Information and Authentication Token) Must Not Be Output to the Log (Required)

Applications which access to online service sometimes face a trouble like it cannot access to online service successfully. The causes of unsuccessful access are various, like lack in network environment arrangement, mistakes in implementing communication protocol, lack of Permission, authentication error, etc. A common implementation is that a program outputs the detailed information to log, so that developer can analyze the cause of a problem later.

Sensitive information like password or authentication token should not be output to log. Log information can be read from other applications, so it may become the cause of information leakage. Also, account names should not be output to log, if it could be lead the damage of leakage.

5.3.2.6. Password Should Not Be Saved in Account Manager (Recommended)

Two of authentication information, password and authentication token, can be saved in an account to be register to AccountManager. This information is to be stored in accounts.db under the following directories, in a plain text (i.e. without encryption).

- Android 4.1 or earlier
  /data/system/accounts.db
- Android 4.2 to Android 6.0
  /data/system/0/accounts.db or /data/system/<UserId>/accounts.db
- Android 7.0 or later
  /data/system_ce/0/accounts_ce.db

Note: Because multiuser functionality is supported on Android 4.2 and later versions, this has been changed to save the content to a user-specific directory. Also, because Android 7.0 and later versions support Direct Boot, the database file is divided into two parts: one file that handles data while locked (/data/system_de/0/accounts_de_db) and a separate file that handles data while unlocked (/data/system_ce/0/accounts_ce.db) Under ordinary circumstances, authentication information is stored in the latter database file.

Root privileges or system privileges are required to read the content of these database files, so they cannot be read on commercial Android terminals. If Android OS contains any vulnerabilities that allow attackers to acquire root privileges or system privileges, this would leave the authentication information stored in accounts.db exposed to risk.

To read in the contents of accounts.db, either root privilege or system privilege is required, and it cannot be read from the marketed Android devices. In the case there is any vulnerability in Android OS, which root privilege or system privilege may be taken over by attackers, authentication information which is saved in accounts.db will be on the edge of the risk.

The Authentication application, which is introduced in this article, is designed to save authentication token in AccountManager without saving user password. When accessing to online service continuously in a certain period, generally the expiration period of authentication token is extended, so the design that password is not saved is enough in most cases.

In general, valid date of authentication token is shorter than password, and it's characteristic that it can be disabled anytime. In case, authentication token is leaked, it can be disabled, so authentication token is comparatively safer, compared with password. In the case authentication token is disabled, user can input the password again to get a new authentication token.

If disabling password when it's leaked, user cannot use online service any more. In this case, it requires call center support etc., and it will take huge cost. Hence, it's better to avoid from the design to save password in AccountManager. In case, the design to save password cannot be avoided, high level of reverse engineering counter-measures like encrypting password and obfuscating the key of

that encryption, should be taken.

5.3.2.7. HTTPS Should Be Used for Communication Between an Authenticator and the Online Service (Required)

Password or authentication token is so called authentication information, and if it's taken over by the third party, the third party can masquerade as the valid user. Since Authenticator sends/receives these types of authentication information with online service, reliable encrypted communication method like an HTTPS should be used.

5.3.2.8. Account Process Should Be Executed after verifying if the Authenticator is the regular one (Required)

In the case there are several Authenticators which the same account type is defined in a device, Authenticator which was installed earlier becomes valid. So, when the own Authenticator was installed later, it's not to be used.

If the Authenticator which was installed earlier, is the malware's masquerade, account information inputted by user may be taken over by malware. User application should verify the account type which performs account operation, whether the regular Authenticator is allocated to it or not, before executing account operation.

Whether the Authenticator which is allocated to one account type is regular one or not, can be verified by checking whether the certificate hash value of the package of Authenticator matches with pre-confirmed valid certificate hash value. If the certificate hash values are found to be not matched, a measure to prompt user to uninstall the package which includes the unexpected Authenticator allocated to that account type, is preferable.

5.3.3. Advanced Topics

5.3.3.1. Usage of Account Manager and Permission

To use each method of AccountManager class, it's necessary to declare to use the appropriate Permission respectively, in application's AndroidManifest.xml. In Android 5.1 (API Level 22) and earlier versions, privileges such as AUTHENTICATE_ACCOUNTS, GET_ACCOUNTS, or MANAGE_ACCOUNTS are required; the privileges corresponding to various methods are shown in Table 5.3-1.

Table 5.3-1 Function of Account Manager and Permission

	Functions that Account Manager provides	
Permission	Method	Explanation
AUTHENTICATE_ACCOUNTS (Only Packages which are signed by the same key of Authenticator, can use.)	getPassword()	To get password
	getUserData()	To get user information
	addAccountExplicitly()	To add accounts to DB
	peekAuthToken()	To get cached token
	setAuthToken()	To register authentication token
	setPassword()	To change password
	setUserData()	To set user information
	renameAccount()	To rename account
GET_ACCOUNTS	getAccounts()	To get a list of all accounts
	getAccountsByType()	To get a list of accounts which account types are same
	getAccountsByTypeAndFeatures()	To get a list of accounts which have the specified function
	addOnAccountsUpdatedListener()	To register event listener
	hasFeatures()	Whether it has the specified function or not
MANAGE_ACCOUNTS	getAuthTokenByFeatures()	To get authentication token of the accounts which have the specified function
	addAccount()	To request a user to add accounts
	removeAccount()	To remove an account
	clearPassword()	Initialize password
	updateCredentials()	Request a user to change password
	editProperties()	Change Authenticator setting
	confirmCredentials()	Request a user to input password again

USE_CREDENTIALS	getAuthToken()	To get authentication token
	blockingGetAuthToken()	To get authentication token
MANAGE_ACCOUNTS or USE_CREDENTIALS	invalidateAuthToken()	To delete cached token

In case using methods group which AUTHENTICATE_ACCOUNTS Permission is necessary, there is a restriction related to package signature key along with Permission. Specifically, the key for signature of package that provides Authenticator and the key for signature of package in the application that uses methods, should be the same. So, when distributing an application which uses method group which AUTHENTICATE_ACCOUNTS Permission is necessary other than Authenticator, signature should be signed by the key which is the same as Authenticator.

In Android 6.0 (API Level 23) and later versions, Permissions other than GET_ACCOUNTS are not used, and there is no difference between what may be done whether or not it is declared. For methods that request AUTHENTICATE_ACCOUNTS on Android 5.1 (API Level 22) and earlier versions, note that—even if you wish to request a Permission—the call can only be made if signatures match (if the signatures do not match then a SecurityException is generated).

In addition, access controls for API routines that require GET_ACCOUNTS changed in Android 8.0 (API Level 26). In this and later versions, if the targetSdkVersion of the app on the side using the account information is 26 or higher, account information can generally not be obtained if the signature does not match that of the Authenticator app, even if GET_ACCOUNTS has been granted. However, if the Authenticator app calls the setAccountVisibility method to specify a package name, account information can be provided even to apps with non-matching signatures.

In a development phase by Android Studio, since a fixed debug keystore might be shared by some Android Studio projects, developers might implement and test Account Manager by considering only permissions and no signature. It's necessary for especially developers who use the different signature keys per applications, to be very careful when selecting which key to use for applications, considering this restriction. In addition, since the data which is obtained by AccountManager includes the sensitive information, so need to handle with care in order to decrease the risk like leakage or unauthorized use.

5.3.3.2. Exception Occurs When Signature Keys of User Application and Authenticator Application Are Different, in Android 4.0.x

When authentication token acquisition function, is required by the user application which is signed by the developer key which is different from the signature key of Authenticator application that includes Authenticator, AccountManager verifies users whether to grant the usage of authentication token or not, by displaying the authentication token license screen (GrantCredentialsPermissionActivity.) However, there's a bug in Android Framework of Android 4.0.x, as soon as this screen in opened by AccountManager, exception occurs, and application is force

closed. (Figure 5.3-3:). See https://code.google.com/p/android/issues/detail?id=23421 for the details of the bug. This bug cannot be found in Android 4.1.x. and later.

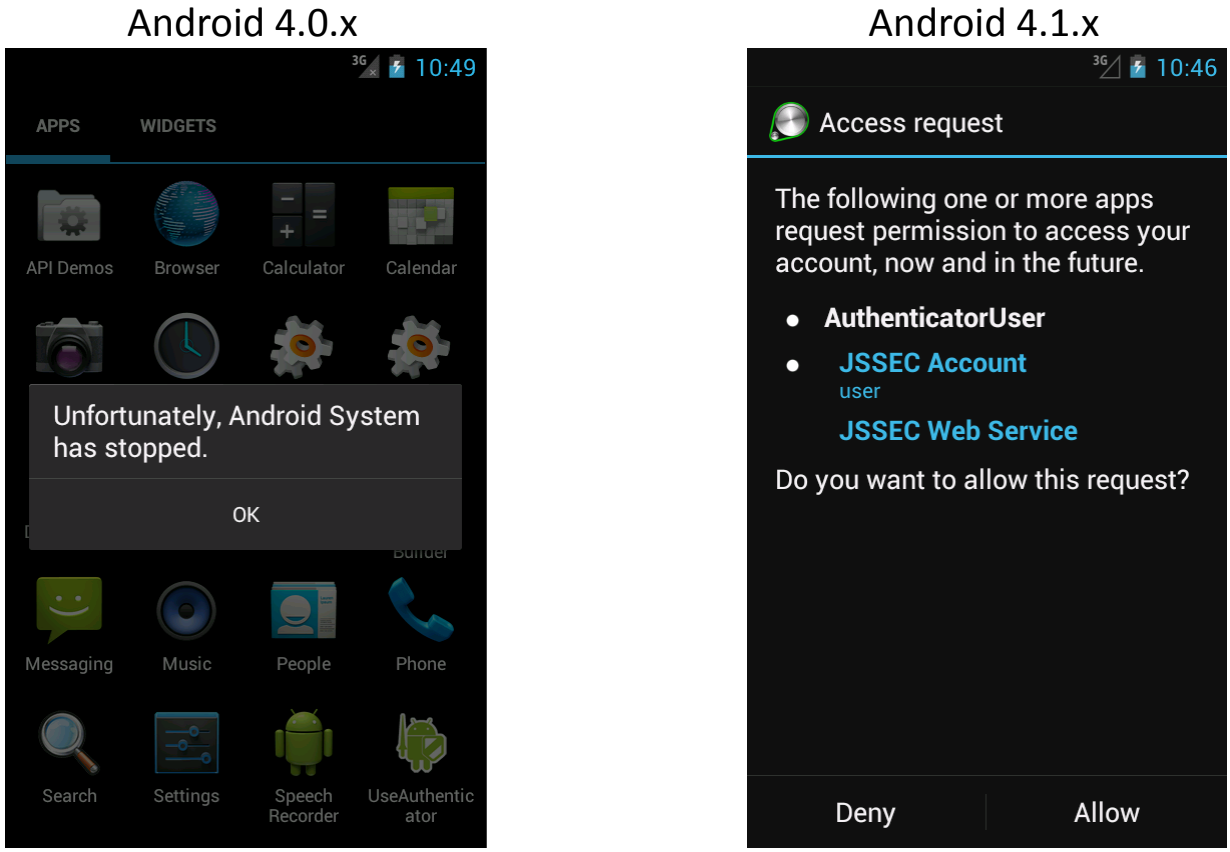


Figure 5.3-3: When displaying Android standard authentication token license screen.

5.3.3.3. Cases in which Authenticator accounts with non-matching signatures may be read in Android 8.0 (API Level 26) or later

In Android 8.0 (API Level 26) and later versions, account-information-fetching methods that required GET_ACCOUNTS Permission in Android 7.1 (API Level 25) and earlier versions may now be called without that permission. Instead, account information may now be obtained only in cases where the signature matches or in which the setAccountVisibility method has been used on the Authenticator app side to specify an app to which account information may be provided However, note carefully that there are a number of exceptions to this rule, implemented by the framework. In what follows we discuss these exceptions.

First, when the targetSdkVersion of the app using the account information is 25 (Android 7.1) or below, the above rule does not apply; in this case apps with the GET_ACCOUNTS permission may obtain account information within the terminal regardless of its signature. However, below we discuss how this behavior may be changed depending on the Authenticator-side implementation.

Next, account information for Authenticators that declare the use of WRITE_CONTACTS Permission may be read by other apps with READ_CONTACTS Permission, regardless of signature. This is not a bug, but

is rather the way the framework is designed.[30] Note again that this behavior may differ depending on the Authenticator-side implementation.

Thus we see that there are some exceptional cases in which account information may be read even for apps with non-matching signatures and for which the setAccountVisibility method has not been called to specify a destination to which account information is to be provided. However, these behaviors may be modified by calling the setAccountVisibility method on the Authenticator side, as in the following snippet.

Do not provide account information to third-party apps

```
accountManager.setAccountVisibility(account, // account for which to change visibility
        AccountManager.PACKAGE_NAME_KEY_LEGACY_VISIBLE,
        AccountManager.VISIBILITY_USER_MANAGED_NOT_VISIBLE);
```

By proceeding this way, we can avoid the framework's default behavior regarding account information for Authenticators that have called the setAccountVisibility method; the above modification ensures that account information is not provided even in cases where targetSdkVersion <= 25 or READ_CONTACTS permission is present.

[30] It is assumed that Authenticators that declare the use of WRITE_CONTACTS Permission will write account information to ContactsProvider, and that apps with READ_CONTACTS Permission will be granted permission to obtain account information.

5.4. Communicating via HTTPS

Most of smartphone applications communicate with Web servers on the Internet. As methods of communications, here we focus on the 2 methods of HTTP and HTTPS. From the security point of view, HTTPS communication is preferable. Lately, major Web services like Google or Facebook have been coming to use HTTPS as default. However, among HTTPS connection methods, those that use SSLv3 are known to be susceptible to a vulnerability (commonly known as POODLE), and we strongly recommend against the use of such methods.[31]

Since 2012, many defects in implementation of HTTPS communication have been pointed out in Android applications. These defects might have been implemented for accessing testing Web servers operated by server certificates that are not issued by trusted third party certificate authorities, but issued privately (hereinafter, called private certificates).

In this section, communication methods of HTTP and HTTPS are explained and the method to access safely with HTTPS to a Web server operated by a private certificate is also described.

5.4.1. Sample Code

You can find out which type of HTTP/HTTPS communication you are supposed to implement through the following chart (Figure 5.4-1) shown below.

[31] In Android 8.0 (API Level 26) and later versions, connections using SSLv3 are unsupported at the platform level.

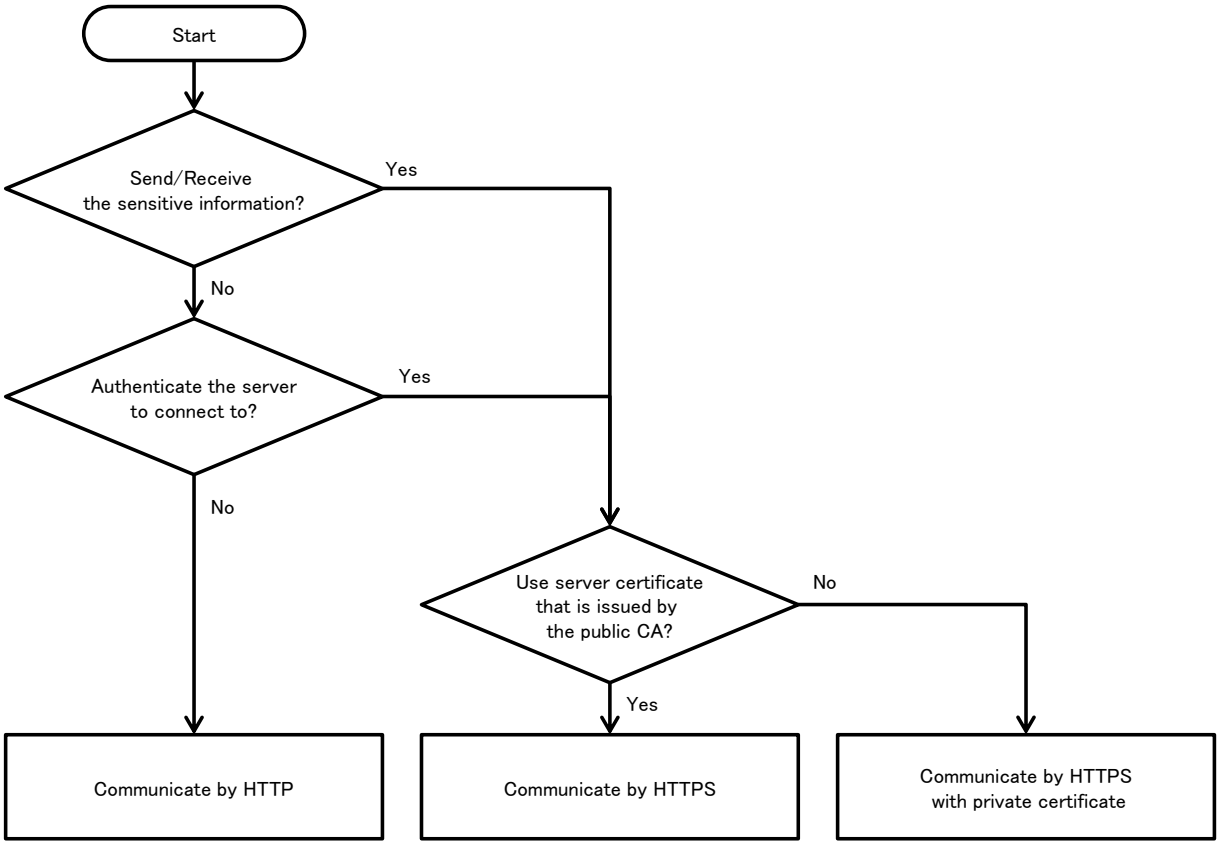


Figure 5.4-1 Flow Figure to select sample code of HTTP/HTTPS

When sensitive information is sent or received, HTTPS communication is to be used because its communication channel is encrypted with SSL/TLS. HTTPS communication is required for the following sensitive information.

- Login ID/Password for Web services.
- Information for keeping authentication state (session ID, token, Cookie etc.)
- Important/confidential information depending on Web services (personal information, credit card information etc.)

A smartphone application with network communication is a part of "system" as well as a Web server. And you have to select HTTP or HTTPS for each communication based on secure design and coding considering the whole "system". Table 5.4-1 is for a comparison between HTTP and HTTPS. And Table 5.4-2 is for the differences in sample codes.

Table 5.4-1 Comparison between HTTP communication method and HTTPS communication method

		HTTP	HTTPS
Characteristics	URL	Starting with http://	Starting with https://
	Encrypting contents	Not available	Available
	Tampering detection of contents	Impossible	Possible
	Authenticating a server	Impossible	Possible
Damage Risk	Reading contents by attackers	High	Low
	Modifying contents by attackers	High	Low

	Application's access to a fake server	High	Low

Table 5.4-2 Explanation of HTTP/HTTPS communication Sample code

Sample code	Communi-cation	Sending/Receiving sensitive information	Server certificate
Communicating via HTTP	HTTP	Not applicable	-
Communicating via HTTPS	HTTPS	OK	Server certificates issued by trusted third party's certificate authorities like Cybertrust and VeriSign etc.
Communicating via HTTPS with private certificate	HTTPS	OK	Private certificate * Operation mode which can be often seen in intra server or in test server.

Android supports java.net.HttpURLConnection/javax.net.ssl.HttpsURLConnection as HTTP/HTTPS communication APIs. Support for the Apache HttpClient, which is another HTTP client library, is removed at the release of the Android 6.0(API Level 23).

5.4.1.1. Communicating via HTTP

It is based on two premises that all contents sent/received through HTTP communications may be sniffed and tampered by attackers and your destination server may be replaced with fake servers prepared by attackers. HTTP communication can be used only if no damage is caused or the damage is within the permissible extent even under the premises. If an application cannot accept the premises, please refer to "5.4.1.2 Communicating via HTTPS" and "5.4.1.3 Communicating via HTTPS with private certificate."

The following sample code shows an application which performs an image search on a Web server, gets the result image and shows it. HTTP communication with the server is performed twice a search. The first communication is for searching image data and the second is for getting it. The worker thread for communication process using AsyncTask is created to avoid the communications performing on the UI thread. Contents sent/received in the communications with the server are not considered as sensitive (e.g. the character string for searching, the URL of the image, or the image data) here. So, the received data such as the URL of the image and the image data may be provided by attackers. To show the sample code simply, any countermeasures are not taken in the sample code by considering the received attacking data as tolerable. Also, the handlings for possible exceptions during JSON purse or showing image data are omitted. It is necessary to handle the exceptions properly depending on the application specs. [32]

Points:

1. Sensitive information must not be contained in send data.
2. Suppose that received data may be sent from attackers.

HttpImageSearch.java

```
package org.jssec.android.https.imagesearch;

import android.os.AsyncTask;

import org.json.JSONException;
import org.json.JSONObject;

import java.io.BufferedInputStream;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.net.HttpURLConnection;
import java.net.URL;

public abstract class HttpImageSearch extends AsyncTask<String, Void, Object> {

    @Override
    protected Object doInBackground(String... params) {
        byte[] responseArray;
```

[32] The Google Image Search API used as an image-search API in this sample code officially ceased to provide service on February 15, 2016. Thus, to execute the sample code as is requires switching to an equivalent service.

```
        // ---------------------------------------------------------
        // Communication 1st time: Execute image search
        // ---------------------------------------------------------

        // *** POINT 1 *** Sensitive information must not be contained in send data.
        // Send image search character string
        StringBuilder s = new StringBuilder();
        for (String param : params){
            s.append(param);
            s.append('+');
        }
        s.deleteCharAt(s.length() - 1);

        String search_url = "http://ajax.googleapis.com/ajax/services/search/images?v=1.0&q=" +
                s.toString();

        responseArray = getByteArray(search_url);
        if (responseArray == null) {
            return null;
        }

        // *** POINT 2 *** Suppose that received data may be sent from attackers.
        // This is sample, so omit the process in case of the searching result is the data from an attack
er.
        // This is sample, so omit the exception process in case of JSON purse.
        String image_url;
        try {
            String json = new String(responseArray);
            image_url = new JSONObject(json).getJSONObject("responseData")
                    .getJSONArray("results").getJSONObject(0).getString("url");
        } catch(JSONException e) {
            return e;
        }

        // ---------------------------------------------------------
        // Communication 2nd time: Get images
        // ---------------------------------------------------------
        // *** POINT 1 *** Sensitive information must not be contained in send data.
        if (image_url != null ) {
            responseArray = getByteArray(image_url);
            if (responseArray == null) {
                return null;
            }
        }

        // *** POINT 2 *** Suppose that received data may be sent from attackers.
        return responseArray;
    }

    private byte[] getByteArray(String strUrl) {
        byte[] buff = new byte[1024];
        byte[] result = null;
        HttpURLConnection response;
        BufferedInputStream inputStream = null;
        ByteArrayOutputStream responseArray = null;
        int length;

        try {
            URL url = new URL(strUrl);
            response = (HttpURLConnection) url.openConnection();
```



```
            response.setRequestMethod("GET");
            response.connect();
            checkResponse(response);

            inputStream = new BufferedInputStream(response.getInputStream());
            responseArray = new ByteArrayOutputStream();

            while ((length = inputStream.read(buff)) != -1) {
                if (length > 0) {
                    responseArray.write(buff, 0, length);
                }
            }
            result = responseArray.toByteArray();
        } catch (IOException e) {
            e.printStackTrace();
        } finally {
            if (inputStream != null) {
                try {
                    inputStream.close();
                } catch (IOException e) {
                    // This is sample, so omit the exception process
                }
            }
            if (responseArray != null) {
                try {
                    responseArray.close();
                } catch (IOException e) {
                    // This is sample, so omit the exception process
                }
            }
        }
        return result;
    }

    private void checkResponse(HttpURLConnection response) throws IOException {
        int statusCode = response.getResponseCode();
        if (HttpURLConnection.HTTP_OK != statusCode) {
            throw new IOException("HttpStatus: " + statusCode);
        }
    }
}
```

ImageSearchActivity.java

```
package org.jssec.android.https.imagesearch;

import android.app.Activity;
import android.graphics.Bitmap;
import android.graphics.BitmapFactory;
import android.os.AsyncTask;
import android.os.Bundle;
import android.view.View;
import android.widget.EditText;
import android.widget.ImageView;
import android.widget.TextView;

public class ImageSearchActivity extends Activity {

    private EditText mQueryBox;
```

```
    private TextView mMsgBox;
    private ImageView mImgBox;
    private AsyncTask<String, Void, Object> mAsyncTask ;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        mQueryBox = (EditText)findViewById(R.id.querybox);
        mMsgBox = (TextView)findViewById(R.id.msgbox);
        mImgBox = (ImageView)findViewById(R.id.imageview);
    }

    @Override
    protected void onPause() {
        // After this, Activity may be deleted, so cancel the asynchronization process in advance.
        if (mAsyncTask != null) mAsyncTask.cancel(true);
        super.onPause();
    }

    public void onHttpSearchClick(View view) {
        String query = mQueryBox.getText().toString();
        mMsgBox.setText("HTTP:" + query);
        mImgBox.setImageBitmap(null);

        // Cancel, since the last asynchronous process might not have been finished yet.
        if (mAsyncTask != null) mAsyncTask.cancel(true);

        // Since cannot communicate by UI thread, communicate by worker thread by AsynchTask.
        mAsyncTask = new HttpImageSearch() {
            @Override
            protected void onPostExecute(Object result) {
                // Process the communication result by UI thread.
                if (result == null) {
                    mMsgBox.append("¥nException occurs¥n");
                } else if (result instanceof Exception) {
                    Exception e = (Exception)result;
                    mMsgBox.append("¥nException occurs¥n" + e.toString());
                } else {
                    // Exception process when image display is omitted here, since it's sample.
                    byte[] data = (byte[])result;
                    Bitmap bmp = BitmapFactory.decodeByteArray(data, 0, data.length);
                    mImgBox.setImageBitmap(bmp);
                }
            }
                }.execute(query);   // pass search character string and start asynchronous process
    }

    public void onHttpsSearchClick(View view) {
        String query = mQueryBox.getText().toString();
        mMsgBox.setText("HTTPS:" + query);
        mImgBox.setImageBitmap(null);

        // Cancel, since the last asynchronous process might not have been finished yet.
        if (mAsyncTask != null) mAsyncTask.cancel(true);

        // Since cannot communicate by UI thread, communicate by worker thread by AsynchTask.
        mAsyncTask = new HttpsImageSearch() {
            @Override
```



```
            protected void onPostExecute(Object result) {
                // Process the communication result by UI thread.
                if (result instanceof Exception) {
                    Exception e = (Exception)result;
                    mMsgBox.append("¥nException occurs¥n" + e.toString());
                } else {
                    byte[] data = (byte[])result;
                    Bitmap bmp = BitmapFactory.decodeByteArray(data, 0, data.length);
                    mImgBox.setImageBitmap(bmp);
                }
            }
        }.execute(query);    // pass search character string and start asynchronous process
    }
}
```

AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.https.imagesearch"
    android:versionCode="1"
    android:versionName="1.0">

    <uses-permission android:name="android.permission.INTERNET"/>

    <application
        android:icon="@drawable/ic_launcher"
        android:allowBackup="false"
        android:label="@string/app_name" >
        <activity
            android:name=".ImageSearchActivity"
            android:label="@string/app_name"
            android:theme="@android:style/Theme.Light"
            android:exported="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

5.4.1.2. Communicating via HTTPS

In HTTPS communication, a server is checked whether it is trusted or not as well as data transferred is encrypted. To authenticate the server, Android HTTPS library verifies "server certificate" which is transmitted from the server in the handshake phase of HTTPS transaction with following points:

- The server certificate is signed by a trusted third party certificate authority
- The period and other properties of the server certificate are valid
- The server's host name matches the CN (Common Name) or SAN (Subject Alternative Names) in the Subject field of the server certificate

SSLException (server certificate verification exception) is raised if the above verification is failed. This possibly means man-in-the-middle attack or just server certificate defects. Your application has to handle the exception with an appropriate sequence based on the application specifications.

The next a sample code is for HTTPS communication which connects to a Web server with a server certificate issued by a trusted third party certificate authority. For HTTPS communication with a server certificate issued privately, please refer to "5.4.1.3 Communicating via HTTPS with private certificate."

The following sample code shows an application which performs an image search on a Web server, gets the result image and shows it. HTTPS communication with the server is performed twice a search. The first communication is for searching image data and the second is for getting it. The worker thread for communication process using AsyncTask is created to avoid the communications performing on the UI thread. All contents sent/received in the communications with the server are considered as sensitive (e.g. the character string for searching, the URL of the image, or the image data) here. To show the sample code simply, no special handling for SSLException is performed. It is necessary to handle the exceptions properly depending on the application specifications. [33] Also, the sample code below allows communication using SSLv3. [34] In general we recommend configuring settings on remote servers to disable SSLv3 in order to avoid attacks targeting a vulnerability in SSLv3 (known as POODLE).

Points:

1. URI starts with https://.
2. Sensitive information may be contained in send data.
3. Handle the received data carefully and securely, even though the data was sent from the server

[33] The Google Image Search API used as an image-search API in this sample code officially ceased to provide service on February 15, 2016. Thus, to execute the sample code as is requires switching to an equivalent service.

[34] Connections via SSLv3 will not arise, as these are prohibited at the platform level in Android 8.0 (API Level 26) and later versions; however, we recommend that steps to disable SSLv3 be taken on the server side.

connected by HTTPS.

4. SSLException should be handled with an appropriate sequence in an application.

HttpsImageSearch.java

```
package org.jssec.android.https.imagesearch;

import org.json.JSONException;
import org.json.JSONObject;

import android.os.AsyncTask;

import java.io.BufferedInputStream;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.net.HttpURLConnection;
import java.net.URL;

public abstract class HttpsImageSearch extends AsyncTask<String, Void, Object> {

    @Override
    protected Object doInBackground(String... params) {
        byte[] responseArray;
        // ---------------------------------------------------------
        // Communication 1st time : Execute image search
        // ---------------------------------------------------------

        // *** POINT 1 *** URI starts with https://.
        // *** POINT 2 *** Sensitive information may be contained in send data.
        StringBuilder s = new StringBuilder();
        for (String param : params){
            s.append(param);
            s.append('+');
        }
        s.deleteCharAt(s.length() - 1);

        String search_url = "https://ajax.googleapis.com/ajax/services/search/images?v=1.0&q=" +
                s.toString();

        responseArray = getByteArray(search_url);
        if (responseArray == null) {
            return null;
        }

        // *** POINT 3 *** Handle the received data carefully and securely,
        // even though the data was sent from the server connected by HTTPS.
        // Omitted, since this is a sample. Please refer to "3.2 Handling Input Data Carefully and Secure
ly."
        String image_url;
        try {
            String json = new String(responseArray);
            image_url = new JSONObject(json).getJSONObject("responseData")
                    .getJSONArray("results").getJSONObject(0).getString("url");
        } catch(JSONException e) {
            return e;
        }

        // ---------------------------------------------------------
        // Communication 2nd time : Get image
        // ---------------------------------------------------------
```

```
        // *** POINT 1 *** URI starts with https://.
        // *** POINT 2 *** Sensitive information may be contained in send data.
        if (image_url != null ) {
            responseArray = getByteArray(image_url);
            if (responseArray == null) {
                return null;
            }
        }

        return responseArray;
    }

    private byte[] getByteArray(String strUrl) {
        byte[] buff = new byte[1024];
        byte[] result = null;
        HttpURLConnection response;
        BufferedInputStream inputStream = null;
        ByteArrayOutputStream responseArray = null;
        int length;

        try {
            URL url = new URL(strUrl);
            response = (HttpURLConnection) url.openConnection();
            response.setRequestMethod("GET");
            response.connect();
            checkResponse(response);

            inputStream = new BufferedInputStream(response.getInputStream());
            responseArray = new ByteArrayOutputStream();

            while ((length = inputStream.read(buff)) != -1) {
                if (length > 0) {
                    responseArray.write(buff, 0, length);
                }
            }
            result = responseArray.toByteArray();
        } catch (IOException e) {
            e.printStackTrace();
        } finally {
            if (inputStream != null) {
                try {
                    inputStream.close();
                } catch (IOException e) {
                    // This is sample, so omit the exception process
                }
            }
            if (responseArray != null) {
                try {
                    responseArray.close();
                } catch (IOException e) {
                    // This is sample, so omit the exception process
                }
            }
        }
        return result;
    }

    private void checkResponse(HttpURLConnection response) throws IOException {
        int statusCode = response.getResponseCode();
```



```
        if (HttpURLConnection.HTTP_OK != statusCode) {
            throw new IOException("HttpStatus: " + statusCode);
        }
    }
}
```

Other sample code files are the same as "5.4.1.1 Communicating via HTTP," so please refer to "5.4.1.1 Communicating via HTTP."

5.4.1.3. Communicating via HTTPS with private certificate

This section shows a sample code of HTTPS communication with a server certificate issued privately (private certificate), but not with that issued by a trusted third party authority. Please refer to "5.4.3.1 How to Create Private Certificate and Configure Server Settings" for creating a root certificate of a private certificate authority and private certificates and setting HTTPS settings in a Web server. The sample program has a cacert.crt file in assets. It is a root certificate file of private certificate authority.

The following sample code shows an application which gets an image on a Web server and shows it. HTTPS is used for the communication with the server. The worker thread for communication process using AsyncTask is created to avoid the communications performing on the UI thread. All contents (the URL of the image and the image data) sent/received in the communications with the server are considered as sensitive here. To show the sample code simply, no special handling for SSLException is performed. It is necessary to handle the exceptions properly depending on the application specifications.

Points:

1. Verify a server certificate with the root certificate of a private certificate authority.
2. URI starts with https://.
3. Sensitive information may be contained in send data.
4. Received data can be trusted as same as the server.
5. SSLException should be handled with an appropriate sequence in an application.

PrivateCertificathettpsGet.java

```
package org.jssec.android.https.privatecertificate;

import java.io.BufferedInputStream;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.net.HttpURLConnection;
import java.net.URL;
import java.security.KeyStore;
import java.security.SecureRandom;

import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLException;
import javax.net.ssl.SSLSession;
```

```
import javax.net.ssl.TrustManagerFactory;

import android.content.Context;
import android.os.AsyncTask;

public abstract class PrivateCertificateHttpsGet extends AsyncTask<String, Void, Object> {

    private Context mContext;

    public PrivateCertificateHttpsGet(Context context) {
        mContext = context;
    }

    @Override
    protected Object doInBackground(String... params) {
        TrustManagerFactory trustManager;
        BufferedInputStream inputStream = null;
        ByteArrayOutputStream responseArray = null;
        byte[] buff = new byte[1024];
        int length;

        try {
            URL url = new URL(params[0]);
            // *** POINT 1 *** Verify a server certificate with the root certificate of a private certifi
cate authority.
            // Set keystore which includes only private certificate that is stored in assets, to client.
            KeyStore ks = KeyStoreUtil.getEmptyKeyStore();
            KeyStoreUtil.loadX509Certificate(ks,
                    mContext.getResources().getAssets().open("cacert.crt"));

            // *** POINT 2 *** URI starts with https://.
            // *** POINT 3 *** Sensitive information may be contained in send data.
            trustManager = TrustManagerFactory.getInstance(TrustManagerFactory.getDefaultAlgorithm());
            trustManager.init(ks);
            SSLContext sslCon = SSLContext.getInstance("TLS");
            sslCon.init(null, trustManager.getTrustManagers(), new SecureRandom());

            HttpURLConnection con = (HttpURLConnection)url.openConnection();
            HttpsURLConnection response = (HttpsURLConnection)con;
            response.setDefaultSSLSocketFactory(sslCon.getSocketFactory());

            response.setSSLSocketFactory(sslCon.getSocketFactory());
            checkResponse(response);

            // *** POINT 4 *** Received data can be trusted as same as the server.
            inputStream = new BufferedInputStream(response.getInputStream());
            responseArray = new ByteArrayOutputStream();
            while ((length = inputStream.read(buff)) != -1) {
                if (length > 0) {
                    responseArray.write(buff, 0, length);
                }
            }
            return responseArray.toByteArray();
        } catch(SSLException e) {
            // *** POINT 5 *** SSLException should be handled with an appropriate sequence in an applicat
ion.
            // Exception process is omitted here since it's sample.
            return e;
        } catch(Exception e) {
            return e;
```



```
        } finally {
            if (inputStream != null) {
                try {
                    inputStream.close();
                } catch (Exception e) {
                    // This is sample, so omit the exception process
                }
            }
            if (responseArray != null) {
                try {
                    responseArray.close();
                } catch (Exception e) {
                    // This is sample, so omit the exception process
                }
            }
        }
    }

    private void checkResponse(HttpURLConnection response) throws IOException {
        int statusCode = response.getResponseCode();
        if (HttpURLConnection.HTTP_OK != statusCode) {
            throw new IOException("HttpStatus: " + statusCode);
        }
    }
}
```

KeyStoreUtil.java

```
package org.jssec.android.https.privatecertificate;

import java.io.IOException;
import java.io.InputStream;
import java.security.KeyStore;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.cert.Certificate;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import java.util.Enumeration;

public class KeyStoreUtil {
    public static KeyStore getEmptyKeyStore() throws KeyStoreException,
            NoSuchAlgorithmException, CertificateException, IOException {
        KeyStore ks = KeyStore.getInstance("BKS");
        ks.load(null);
        return ks;
    }

    public static void loadAndroidCAStore(KeyStore ks)
            throws KeyStoreException, NoSuchAlgorithmException,
            CertificateException, IOException {
        KeyStore aks = KeyStore.getInstance("AndroidCAStore");
        aks.load(null);
        Enumeration<String> aliases = aks.aliases();
        while (aliases.hasMoreElements()) {
            String alias = aliases.nextElement();
            Certificate cert = aks.getCertificate(alias);
            ks.setCertificateEntry(alias, cert);
```

```
        }
    }

    public static void loadX509Certificate(KeyStore ks, InputStream is)
            throws CertificateException, KeyStoreException {
        try {
            CertificateFactory factory = CertificateFactory.getInstance("X509");
            X509Certificate x509 = (X509Certificate)factory.generateCertificate(is);
            String alias = x509.getSubjectDN().getName();
            ks.setCertificateEntry(alias, x509);
        } finally {
            try { is.close(); } catch (IOException e) { /* This is sample, so omit the exception process
*/ }
        }
    }
}
```

PrivateCertificateHttpsActivity.java

```
package org.jssec.android.https.privatecertificate;

import android.app.Activity;
import android.graphics.Bitmap;
import android.graphics.BitmapFactory;
import android.os.AsyncTask;
import android.os.Bundle;
import android.view.View;
import android.widget.EditText;
import android.widget.ImageView;
import android.widget.TextView;

public class PrivateCertificateHttpsActivity extends Activity {

    private EditText mUrlBox;
    private TextView mMsgBox;
    private ImageView mImgBox;
    private AsyncTask<String, Void, Object> mAsyncTask ;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        mUrlBox = (EditText)findViewById(R.id.urlbox);
        mMsgBox = (TextView)findViewById(R.id.msgbox);
        mImgBox = (ImageView)findViewById(R.id.imageview);
    }

    @Override
    protected void onPause() {
        // After this, Activity may be discarded, so cancel asynchronous process in advance.
        if (mAsyncTask != null) mAsyncTask.cancel(true);
        super.onPause();
    }

    public void onClick(View view) {
        String url = mUrlBox.getText().toString();
        mMsgBox.setText(url);
        mImgBox.setImageBitmap(null);
```



```
        // Cancel, since the last asynchronous process might have not been finished yet.
        if (mAsyncTask != null) mAsyncTask.cancel(true);

        // Since cannot communicate through UI thread, communicate by worker thread by AsynchTask.
        mAsyncTask = new PrivateCertificateHttpsGet(this) {
            @Override
            protected void onPostExecute(Object result) {
                // Process the communication result through UI thread.
                if (result instanceof Exception) {
                    Exception e = (Exception)result;
                    mMsgBox.append("¥nException occurs¥n" + e.toString());
                } else {
                    byte[] data = (byte[])result;
                    Bitmap bmp = BitmapFactory.decodeByteArray(data, 0, data.length);
                    mImgBox.setImageBitmap(bmp);
                }
            }
        }.execute(url); // Pass URL and start asynchronization process
    }
}
```

5.4.2. Rule Book

Follow the rules below to communicate with HTTP/HTTPS.

1.	Sensitive Information Must Be Sent/Received over HTTPS Communication	(Required)
2.	Received Data over HTTP Must be Handled Carefully and Securely	(Required)
3.	SSLException Must Be Handled Appropriately like Notification to User	(Required)
4.	Custom TrustManager Must Not Be Created	(Required)
5.	Custom HostnameVerifier Must Not Be Created	(Required)

5.4.2.1. Sensitive Information Must Be Sent/Received over HTTPS Communication (Required)

In HTTP transaction, sent and received information might be sniffed or tampered and the connected server might be masqueraded. Sensitive information must be sent/ received by HTTPS communication.

5.4.2.2. Received Data over HTTP Must be Handled Carefully and Securely (Required)

Received data in HTTP communications might be generated by attackers for exploiting vulnerability of an application. So you have to suppose that the application receives any values and formats of data and then carefully implement data handlings for processing received data so as not to put any vulnerabilities in. Furthermore you should not blindly trust the data from HTTPS server too. Because the HTTPS server may be made by the attacker or the received data may be made in other place from the HTTPS server. Please refer to "3.2 Handling Input Data Carefully and Securely"

5.4.2.3. SSLException Must Be Handled Appropriately like Notification to User (Required)

In HTTPS communication, SSLException occurs as a verification error when a server certificate is not valid or the communication is under the man-in-the-middle attack. So you have to implement an appropriate exception handling for SSLException. Notifying the user of the communication failure, logging the failure and so on can be considered as typical implementations of exception handling. On the other hand, no special notice to the user might be required in some case. Like this, because how to handle SSLException depends on the application specs and characteristics you need to determine it after first considering thoroughly.

As mentioned above, the application may be attacked by man-in-the-middle attack when SSLException occurs, so it must not be implemented like trying to send/receive sensitive information again via non secure protocol such as HTTP.

5.4.2.4. Custom TrustManager Must Not Be Created (Required)

Just Changing KeyStore which is used for verifying server certificates is enough to communicate via HTTPS with a private certificate like self-signed certificate. However, as explained in "5.4.3.3 Risky Code that Disables Certificate Verification," there are so many dangerous TrustManager

implementations as sample codes for such purpose on the Internet. An Application implemented by referring to these sample codes may have the vulnerability.

When you need to communicate via HTTPS with a private certificate, refer to the secure sample code in "5.4.1.3 Communicating via HTTPS with private certificate."

Of course, custom TrustManager can be implemented securely, but enough knowledge for encryption processing and encryption communication is required so as not to implement vulnerable codes. So this rule dare be (Required).

5.4.2.5. Custom HostnameVerifier Must Not Be Created (Required)

Just Changing KeyStore which is used for verifying server certificates is enough to communicate via HTTPS with a private certificate like self-signed certificate. However, as explained in "5.4.3.3 Risky Code that Disables Certificate Verification," there are so many dangerous HostnameVerifier implementations as sample codes for such purpose on the Internet. An Application implemented by referring to these sample codes may have the vulnerability.

When you need to communicate via HTTPS with a private certificate, refer to the secure sample code in "5.4.1.3 Communicating via HTTPS with private certificate."

Of course, custom HostnameVerifier can be implemented securely, but enough knowledge for encryption processing and encryption communication is required so as not to implement vulnerable codes. So this rule dare be (Required).

5.4.3. Advanced Topics

5.4.3.1. How to Create Private Certificate and Configure Server Settings

In this section, how to create a private certificate and configure server settings in Linux such as Ubuntu and CentOS is described. Private certificate means a server certificate which is issued privately and is told from server certificates issued by trusted third party certificate authorities like Cybertrust and VeriSign.

Create private certificate authority

First of all, you need to create a private certificate authority to issue a private certificate. Private certificate authority means a certificate authority which is created privately as well as private certificate. You can issue plural private certificates by using the single private certificate authority. PC in which the private certificate authority is stored should be limited strictly to be accessed just by trusted persons.

To create a private certificate authority, you have to create two files such as the following shell script newca.sh and the setting file openssl.cnf and then execute them. In the shell script, CASTART and CAEND stand for the valid period of certificate authority and CASUBJ stands for the name of certificate authority. So these values need to be changed according to a certificate authority you create. While executing the shell script, the password for accessing the certificate authority is asked for 3 times in total, so you need to input it every time.

newca.sh – Shell Script to create certificate authority

```
#!/bin/bash

umask 0077

CONFIG=openssl.cnf
CATOP=./CA
CAKEY=cakey.pem
CAREQ=careq.pem
CACERT=cacert.pem
CAX509=cacert.crt
CASTART=130101000000Z   # 2013/01/01 00:00:00 GMT
CAEND=230101000000Z     # 2023/01/01 00:00:00 GMT
CASUBJ="/CN=JSSEC Private CA/O=JSSEC/ST=Tokyo/C=JP"

mkdir -p ${CATOP}
mkdir -p ${CATOP}/certs
mkdir -p ${CATOP}/crl
mkdir -p ${CATOP}/newcerts
mkdir -p ${CATOP}/private
touch ${CATOP}/index.txt

export HOSTNAME=””

openssl req -new -newkey rsa:2048 -sha256 -subj "${CASUBJ}" ¥
       -keyout ${CATOP}/private/${CAKEY} -out ${CATOP}/${CAREQ}
openssl ca -selfsign -md sha256 -create_serial -batch ¥
```



```
        -keyfile ${CATOP}/private/${CAKEY} ¥
        -startdate ${CASTART} -enddate ${CAEND} -extensions v3_ca ¥
        -in ${CATOP}/${CAREQ} -out ${CATOP}/${CACERT} ¥
        -config ${CONFIG}
openssl x509 -in ${CATOP}/${CACERT} -outform DER -out ${CATOP}/${CAX509}
```

openssl.cnf – Setting file of openssl command which 2 shell scripts refers in common.

```
[ ca ]
default_ca      = CA_default           # The default ca section

[ CA_default ]
dir            = ./CA                # Where everything is kept
certs          = $dir/certs           # Where the issued certs are kept
crl_dir        = $dir/crl             # Where the issued crl are kept
database       = $dir/index.txt       # database index file.
#Proprietary-defined  _subject = no                  # Set to 'no' to allow creation of
                                    # several ctificates with same subject.
new_certs_dir   = $dir/newcerts        # default place for new certs.
certificate     = $dir/cacert.pem      # The CA certificate
serial         = $dir/serial          # The current serial number
crlnumber      = $dir/crlnumber       # the current crl number
                                    # must be commented out to leave a V1 CRL
crl            = $dir/crl.pem         # The current CRL
private_key     = $dir/private/cakey.pem# The private key
RANDFILE       = $dir/private/.rand    # private random number file
x509_extensions = usr_cert             # The extentions to add the cert
name_opt       = ca_default           # Subject Name options
cert_opt       = ca_default           # Certificate field options
policy         = policy_match

[ policy_match ]
countryName            = match
stateOrProvinceName     = match
organizationName       = supplied
organizationalUnitName  = optional
commonName             = supplied
emailAddress           = optional

[ usr_cert ]
basicConstraints=CA:FALSE
nsComment                      = "OpenSSL Generated Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
subjectAltName=@alt_names

[ v3_ca ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
basicConstraints = CA:true

[ alt_names ]
DNS.1=${ENV::HOSTNAME}
DNS.2=*.${ENV::HOSTNAME}
```

After executing the above shall script, a directory named CA is created just under the work directory. This CA directory is just a private certificate authority. CA/cacert.crt file is the root

certificate of the private certificate authority. And it's stored in assets directory of an application as described in "5.4.1.3 Communicating via HTTPS with private certificate," or it's installed in Android device as described in "5.4.3.2 Install Root Certificate of Private Certificate Authority to Android OS's Certification Store."

Create private certificate

To create a private certificate, you have to create a shell script like the following newca.sh and execute it. In the shell script, SVSTART and SVEND stand for the valid period of private certificate, and SVSUBJ stands for the name of Web server, so these values need to be changed according to the target Web server. Especially, you need to make sure not to set a wrong host name to /CN of SVSUBJ with which the host name of Web server is to be specified. While executing the shell script, the password for accessing the certificate authority is asked, so you need to input the password which you have set when creating the private certificate authority. After that, y/n is asked 2 times in total and you need to input y every time.

newsv.sh – Shell script which issues private certificate

```
#!/bin/bash

umask 0077

CONFIG=openssl.cnf
CATOP=./CA
CAKEY=cakey.pem
CACERT=cacert.pem
SVKEY=svkey.pem
SVREQ=svreq.pem
SVCERT=svcert.pem
SVX509=svcert.crt
SVSTART=130101000000Z   # 2013/01/01 00:00:00 GMT
SVEND=230101000000Z     # 2023/01/01 00:00:00 GMT
HOSTNAME=selfsigned.jssec.org
SVSUBJ="/CN="${HOSTNAME}"/O=JSSEC Secure Coding Group/ST=Tokyo/C=JP"

export HOSTNAME=${HOSTNAME}

openssl genrsa -out ${SVKEY} 2048
openssl req -new -key ${SVKEY} -subj "${SVSUBJ}" -out ${SVREQ}
openssl ca -md sha256 ¥
       -keyfile ${CATOP}/private/${CAKEY} -cert ${CATOP}/${CACERT} ¥
       -startdate ${SVSTART} -enddate ${SVEND} ¥
       -in ${SVREQ} -out ${SVCERT} -config ${CONFIG}
openssl x509 -in ${SVCERT} -outform DER -out ${SVX509}
```

After executing the above shell script, both svkey.pem (private key file) and svcert.pem (private certificate file) for Web server are generated just under work directory.

When Web server is Apache, you will specify prikey.pem and cert.pem in the configuration file as follows.

```
SSLCertificateFile    "/path/to/svcert.pem"
```



```
SSLCertificateKeyFile "/path/to/svkey.pem"
```

5.4.3.2. Install Root Certificate of Private Certificate Authority to Android OS's Certification Store

In the sample code of "5.4.1.3 Communicating via HTTPS with private certificate," the method to establish HTTPS sessions to a Web server from one application using a private certificate by installing the root certificate into the application is introduced. In this section, the method to establish HTTPS sessions to Web servers from all applications using private certificates by installing the root certificate into Android OS is to be introduced. Note that all you install should be certificates issued by trusted certificate authorities including your own certificate authorities.

First of all, you need to copy the root certificate file "cacert.crt" to the internal storage of an Android device. You can also get the root certificate file used in the sample code from https://selfsigned.jssec.org/cacert.crt.

And then, you will open Security page from Android Settings and you can install the root certificate in an Android device by doing as follows.

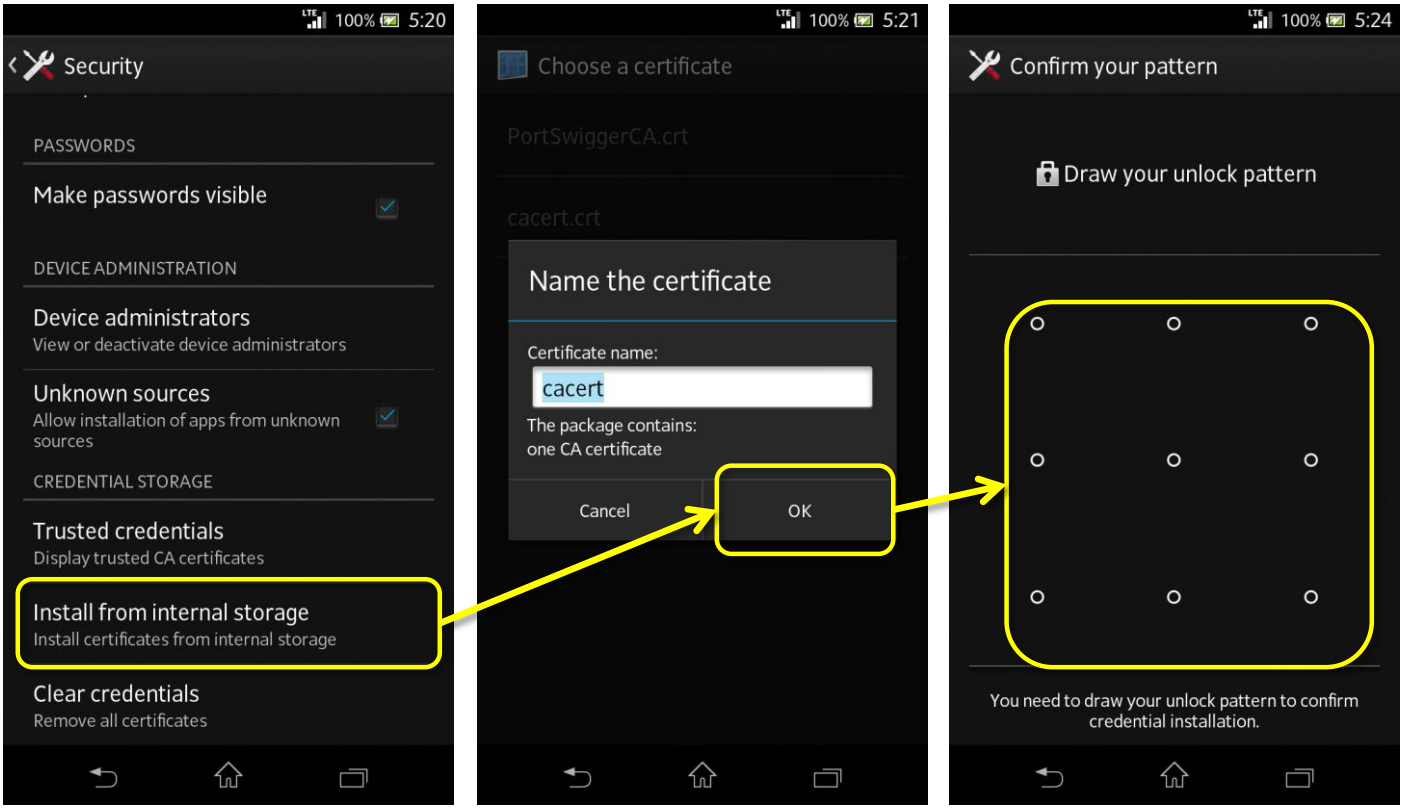


Figure 5.4-2 Steps to install root certificate of private certificate authority

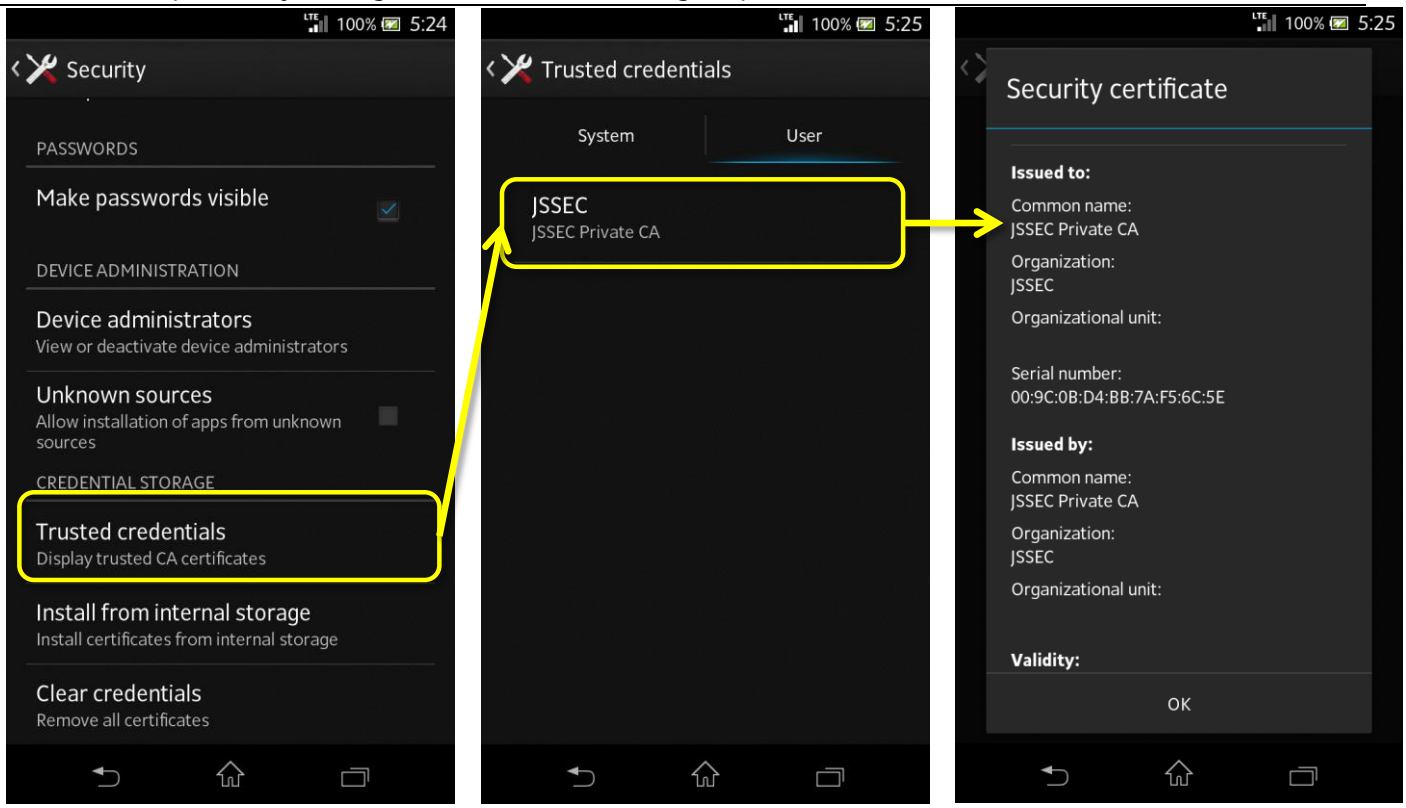


Figure 5.4-3 Checking if root certificate is installed or not

Once the root certificate is installed in Android OS, all applications can correctly verify every private certificate issued by the certificate authority. The following figure shows an example when displaying https://selfsigned.jssec.org/droid_knight.png in Chrome browser.

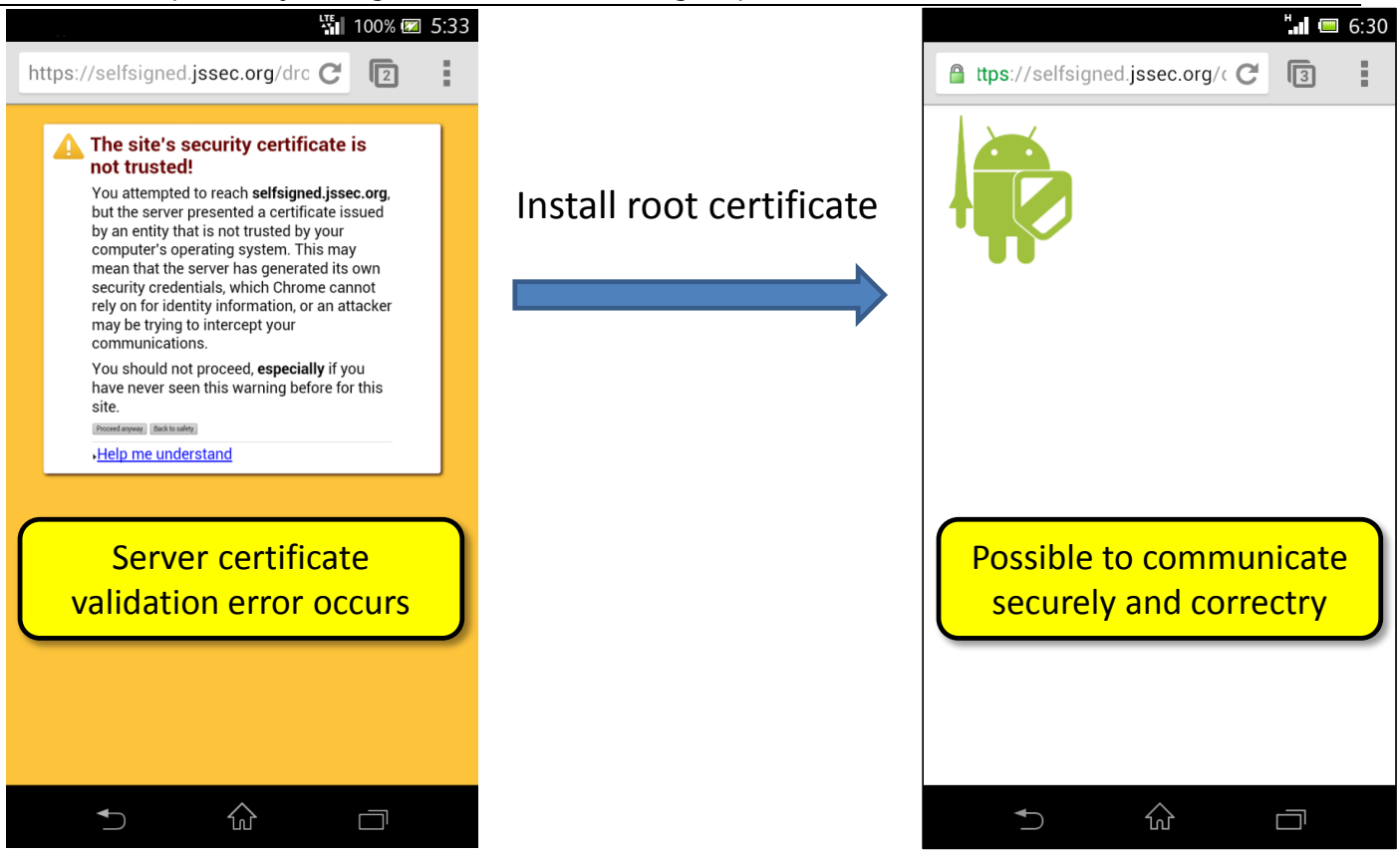


Figure 5.4-4 Once root certificate installed, private certificates can be verified correctly.

By installing the root certificate this way, even applications using the sample code "5.4.1.2 Communicating via HTTPS" can correctly connect via HTTPS to a Web server which is operated with a private certificate.

5.4.3.3. Risky Code that Disables Certificate Verification

A lot of incorrect samples (code snippets), which allow applications to continue to communicate via HTTPS with Web servers even after certificate verification errors occur, are found on the Internet. Since they are introduced as the way to communicate via HTTPS with a Web server using a private certificate, there have been so many applications created by developers who have used those sample codes by copy and paste. Unfortunately, most of them are vulnerable to man-in-the-middle attack. As mentioned in the top of this article, "In 2012, many defects in implementation of HTTPS communication were pointed out in Android applications", many Android applications which would have implemented such vulnerable codes have been reported.

Several code snippets to cause vulnerable HTTPS communication are shown below. When you find this type of code snippets, it's highly recommended to replace the sample code of "5.4.1.3 Communicating via HTTPS with private certificate."

Risk:Case which creates empty TrustManager

```
TrustManager tm = new X509TrustManager() {

    @Override
    public void checkClientTrusted(X509Certificate[] chain,
            String authType) throws CertificateException {
        // Do nothing -> accept any certificates
    }

    @Override
    public void checkServerTrusted(X509Certificate[] chain,
            String authType) throws CertificateException {
        // Do nothing -> accept any certificates
    }

    @Override
    public X509Certificate[] getAcceptedIssuers() {
        return null;
    }
};
```

Risk:Case which creates empty HostnameVerifier

```
HostnameVerifier hv = new HostnameVerifier() {
    @Override
    public boolean verify(String hostname, SSLSession session) {
        // Always return true -> Accespt any host names
        return true;
    }
};
```

Risk:Case that ALLOW_ALL_HOSTNAME_VERIFIER is used.

```
SSLSocketFactory sf;
[...]
sf.setHostnameVerifier(SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER);
```

5.4.3.4. A note regarding the configuration of HTTP request headers

If you wish to specify your own individual HTTP request header for HTTP or HTTPS communication, use the setRequestProperty() or addRequestProperty() methods in the URLConnection class. If you will be using input data received from external sources as parameters for these methods, you must implement HTTP header-injection protections. The first step in attacks based on HTTP header injection is to include carriage-return codes—which are used as separators in HTTP headers—in input data. For this reason, all carriage-return codes must be eliminated from input data.

Configure HTTP request header

```
public byte[] openConnection(String strUrl, String strLanguage, String strCookie) {
       // HttpURLConnection is a class derived from URLConnection
       HttpURLConnection connection;

       try {
           URL url = new URL(strUrl);
           connection = (HttpURLConnection) url.openConnection();
           connection.setRequestMethod("GET");

           // *** POINT *** When using input values in HTTP request headers,
           // check the input data in accordance with the application's requirements
           // (see Section 3.2: Handling Input Data Carefully and Securely)
           if (strLanguage.matches("^[a-zA-Z ,-]+$")) {
               connection.addRequestProperty("Accept-Language", strLanguage);
           } else {
               throw new IllegalArgumentException("Invalid Language : " + strLanguage);
           }
           // *** POINT *** Or URL-encode the input data (as appropriate for the purposes of the app in
queestion)
           connection.setRequestProperty("Cookie", URLEncoder.encode(strCookie, "UTF-8"));

           connection.connect();

           [...]
```

5.4.3.5. Notes and sample implementations for pinning

When an app uses HTTPS communication, one step in the handshake procedure carried out at the start of the communication is to check whether or not the certificate sent from the remote server is signed by a third-party certificate authority. However, attackers may acquire improper certificates from third-party authentication agents, or may acquire signed keys from a certificate authority to construct improper certificates. In such cases, apps will be unable to detect the attack during the handshake process—even in the event of a lure to an improper server established by the attacker, or of an man-in-the-middle attack —and, as a result, there is a possibility that damage may be done.

The technique of *pinning* is an effective strategy for preventing man-in-the-middle attacks using these types of certificates from improper third-party certificate authorities. In this method, certificates and public keys for remote servers are stored in advance within an app, and this information is used for handshake processing and re-testing after handshake processing has completed.

Pinning may be used to restore the security of communications in cases where the credibility of a third-party certificate authority—the foundation of public-key infrastructure—has been tarnished. App developers should assess the asset level handled by their own apps and decide whether or not to implement these tests.

Use certificates and public keys stored within an app during the handshake procedure

To use information contained in remote-server certificates or public keys stored within an app during the handshake procedure, an app must create its own KeyStore containing this information and use it when communicating. This will allow the app to detect improprieties during the handshake procedure even in the event of a man-in-the-middle attack using a certificate from an improper third-party certificate authority, as described above. Consult the sample code presented in the section titled "5.4.1.3 Communicating via HTTPS with private certificate" for detailed methods of establishing your app's own KeyStore to conduct HTTPS communication.

Use certificates and public-key information stored within an app for re-testing after the handshake procedure is complete

To re-test the remote server after the handshake procedure has completed, an app first obtains the certificate chain that was tested and trusted by the system during the handshake, then compares this certificate chain against the information stored in advance within the app. If the result of this comparison indicates agreement with the information stored within the app, the communication may be permitted to proceed; otherwise, the communication procedure should be aborted.

However, if an app uses the methods listed below in an attempt to obtain the certificate chain that the system trusted during the handshake, the app may not obtain the expected certificate chain, posing a risk that the pinning may not function properly[35].

- javax.net.ssl.SSLSession.getPeerCertificates()
- javax.net.ssl.SSLSession.getPeerCertificateChain()

What these methods return is not the certificate chain that was trusted by the system during the handshake, but rather the very certificate chain that the app received from the communication partner itself. For this reason, even if an man-in-the-middle attack has resulted in a certificate from an improper certificate authority being appended to the certificate chain, the above methods will not return the certificate that was trusted by the system during the handshake; instead, the certificate of the server to which the app was originally attempting to connect will also be returned at the same time. This certificate—the certificate of the server to which the app was originally attempting to connect—will, because of pinning, be equivalent to the certificate pre-stored within the app; thus

[35] The following article explains this risk in detail:
https://www.cigital.com/blog/ineffective-certificate-pinning-implementations/

re-testing it will not detect any improprieties. For this and other similar reasons, it is best to avoid using the above methods when implementing re-testing after the handshake.

On Android versions 4.2 (API Level 17) and later, using the checkServerTrusted() method within net.http.X509TrustManagerExtensions will allow the app to obtain only the certificate chain that was trusted by the system during the handshake.

An example illustrating pinning using X509TrustManagerExtensions

```
// Store the SHA-256 hash value of the public key included in the correct certificate for the remote ser
ver (pinning)
private static final Set<String> PINS = new HashSet<>(Arrays.asList(
       new String[] {
              "d9b1a68fceaa460ac492fb8452ce13bd8c78c6013f989b76f186b1cbba1315c1",
              "cd13bb83c426551c67fabcff38d4496e094d50a20c7c15e886c151deb8531cdc"
       }
));

// Communicate using AsyncTask work threads
protected Object doInBackground(String... strings) {

    [...]

   // Obtain the certificate chain that was trusted by the system by testing during the handshake
   X509Certificate[] chain = (X509Certificate[]) connection.getServerCertificates();
   X509TrustManagerExtensions trustManagerExt = new X509TrustManagerExtensions((X509TrustManager) (trus
tManagerFactory.getTrustManagers()[0]));
   List<X509Certificate> trustedChain = trustManagerExt.checkServerTrusted(chain, "RSA", url.getHost())
;

   // Use public-key pinning to test
   boolean isValidChain = false;
   for (X509Certificate cert : trustedChain) {
       PublicKey key = cert.getPublicKey();
       MessageDigest md = MessageDigest.getInstance("SHA-256");
       String keyHash = bytesToHex(md.digest(key.getEncoded()));

       // Compare to the hash value stored by pinning
       if(PINS.contains(keyHash)) isValidChain = true;
   }
   if (isValidChain) {
       // Proceed with operation
   } else {
       // Do not proceed with operation
   }

    [...]
}

private String bytesToHex(byte[] bytes) {
    StringBuilder sb = new StringBuilder();
    for (byte b : bytes) {
        String s = String.format("%02x", b);
        sb.append(s);
    }
    return sb.toString();
}
```


5.4.3.6. Strategies for addressing OpenSSL vulnerabilities using Google Play Services

Google Play Services (version 5.0 and later) provides a framework known as Provider Installer. This may be used to address vulnerabilities in Security Provider, an implementation of OpenSSL and other encryption-related technologies. For details, see Section "5.6.3.5 Addressing Vulnerabilities with Security Provider from Google Play Services".

5.4.3.7. Network Security Configuration

Android 7.0 (API Level 24) introduced a framework known as Network Security Configuration that allows individual apps to configure their own security settings for network communication. Using this framework makes it easy for apps to incorporate a variety of techniques for improving app security, including not only HTTPS communication with private certificates and public key pinning but also prevention of unencrypted (HTTP) communication and the use of private certificates enabled only during debugging.[36]

The various types of functionality offered by Network Security Configuration may be accessed simply by configuring settings in xml files, which may be applied to the entirety of an app's HTTP and HTTPS communications. This eliminates the need for modifying an app's code or carrying out any additional processing, simplifying implementation and providing an effective protection against Incorporating bugs or vulnerabilities.

Communicating via HTTPS with private certificates

Section “5.4.1.3 Communicating via HTTPS with private certificate” presents sample code that performs HTTPS communication with private certificates (e.g. self-signed certificates or intra-company certificates). However, by using Network Security Configuration, developers may use private certificates without implementation presented in the sample code of Section “5.4.1.2 Communicating via HTTPS”.

Use private certificates to communicate with specific domains

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config>
        <domain includeSubdomains="true">jssec.org</domain>
        <trust-anchors>
            <certificates src="@raw/private_ca" />
        </trust-anchors>
    </domain-config>
</network-security-config>
```

In the example above, the private certificates (`private_ca`) used for communication may be stored as resources within the app, with the conditions for their use and their range of applicability described

[36] For more information on Network Security Configuration, see https://developer.android.com/training/articles/security-config.html

in .xml files. By using the <domain-config> tag, it is possible to apply private certificates to specific domains only. To use private certificates for all HTTPS communications performed by the app, use the <base-config> tag, as shown below.

Use private certificates for all HTTPS communications performed by the app

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config>
        <trust-anchors>
            <certificates src="@raw/private_ca" />
        </trust-anchors>
    </base-config>
</network-security-config>
```

Pinning

We mentioned public key pinning in Section "5.4.3.5 Notes and sample implementations for pinning" By using Network Security Configuration to configure settings as in the example below, you eliminate the need to implement the authentication process in your code; instead, the specifications in the xml file suffice to ensure proper authentication.

Use public key pinning for HTTPS communication

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config>
        <domain includeSubdomains="true">jssec.org</domain>
        <pin-set expiration="2018-12-31">
            <pin digest="SHA-256">e30Lky+iWK21yHSls5DJoRzNikOdvQUOGXvurPidc2E=</pin>
            <!-- バックアップ用 -->
            <pin digest="SHA-256">fwza0LRMXouZHRC8Ei+4PyuldPDcf3UKgO/04cDM1oE=</pin>
        </pin-set>
    </domain-config>
</network-security-config>
```

The quantity described by the <pin> tag above is the base64-encoded hash value of the public key used for pinning. The only supported hash function is SHA-256.

Prevent unencrypted (HTTP) communication

Using Network Security Configuration allows you to prevent HTTP communication (unencrypted communication) from apps.

Prevent unencrypted (HTTP) communication

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config cleartextTrafficPermitted="false">
        <domain includeSubdomains="true">jssec.org</domain>
    </domain-config>
</network-security-config>
```

In the example above we specified the attribute cleartextTrafficPermitted="false" in the

<domain-config> tag. This prevents HTTP communication with the specified domain, forcing the use of HTTPS communication. Including this attribute setting in the <base-config> tag will prevent HTTP communication to all domains.[37] Also, in Android 8.0 (API Level 26) and later these settings may also be applied to WebView; however, note with caution that these settings may *not* be applied to WebView in Android 7.0 (API Level 25) or earlier versions.

Private certificates exclusively for debugging purposes

For purposes of debugging during app development, developers may wish to use private certificates to communicate with certain HTTPS servers that exist for app-development purposes. In this case, developers must be careful to ensure that no dangerous implementations—including code that disables certificate authentication—are incorporated into the app; this is discussed in Section "5.4.3.3 Risky Code that Disables Certificate Verification". In Network Security Configuration, settings may be configured as in the example below to specify a set of certificates to be used only when debugging (only if android:debuggable is set to "true" in the file AndroidManifest.xml). This eliminates the risk that dangerous code may inadvertently be retained in the release version of an app, thus constituting a useful means of preventing vulnerabilities.

Use private certificates only when debugging

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <debug-overrides>
        <trust-anchors>
            <certificates src="@raw/private_cas" />
        </trust-anchors>
    </debug-overrides>
</network-security-config>
```

5.4.3.8. (Column): Transitioning to TLS1.2 for secure connections

The U.S. National Institute of Standards and Technology (NIST)[38] has reported security issues in SSL and TLS 1.0, and these protocols have been deprecated for use in servers. In particular, several vulnerabilities were announced in 2014 and 2015, including Heartbleed[39] (April 2014), POODLE[40] (October 2014), and FREAK[41] (March 2015); of these, the Heartbleed vulnerability, discovered in

---

[37] See the following API reference about how the Network Security Configuration works for non-HTTP connections.
https://developer.android.com/reference/android/security/NetworkSecurityPolicy.html#isCleartextTrafficPermitted()

[38] US National Institute of Standards and Technology (NIST) (https://www.nist.gov/)

[39] Heartbleed(CVE-2014-0160), IPA (https://www.ipa.go.jp/security/ciadr/vul/20140408-openssl.html)

[40] POODLE(CVE-2014-3566), IPA (https://www.ipa.go.jp/security/announce/20141017-ssl.html)

[41] FREAK(CVE-2015-0204), NIST (https://nvd.nist.gov/vuln/detail/CVE-2015-0204)

OpenSSL (a software library for encryption), was used to target Japanese companies, yielding improper accesses that led to leakage of customer data and other harmful consequences.[42]

Because of this history, the use of these technologies is prohibited for U.S. government procurement; however, the breadth of their influence in commercial settings ensures that the techniques widely used today as Internet encryption methods (with security patches applied to TLS 1.0 in particular). However, given the rash of security incidents in recent years and the availability of new TLS versions, an increasing number of sites and services are discontinuing support for "old versions of SSL or TLS," and the transition to TLS 1.2 is well underway.[43]

For example, one manifestation of this transition is a new security standard known as the Payment Card Industry Data Security Standard (PCI DSS), established by the Payment Card Industry Security Standards Council (PCI SSC).[44]

Smartphones and tablets are also widely used for E-commerce today, with credit cards typically used for payment. Indeed, we expect that many users of this document (Android Application Secure Design / Secure Coding Guide) will offer services that send credit-card information and other data to the server side; when using credit cards in networked environments, it is essential to ensure the security of the data pathway, and PCI DSS is a standard that governs the handling of member data in services of this type, designed with the objective of preventing improper card use, information leaks, and other harmful consequences. Among these security standards, the use of TLS 1.0 is deprecated for credit-card handling on the Internet; instead, apps should support standards such as TLS 1.2 [which allows the use of stronger encryption algorithms, including SHA-2 hash functions (SHA-256 or SHA-384) and support for encryption suites that offer usage modes with authenticated encryption].

In communication between smartphones and servers, the need to ensure the security of data pathways is not restricted to handling of credit-card information, but is also an extremely important aspect of operations involving the handling of private data or other sensitive information. Thus, the need to transition to secure connections using TLS 1.2 on the service-provision (server) side may now be said to be an urgent requirement.

On the other hand, in Android—which runs on the client side—WebView functionality supporting TLS

---

42 TLS/SSL Known vulnerabilities, Wiki
(https://ja.wikipedia.org/wiki/Transport_Layer_Security#TLS/SSL%E3%81%AE%E6%97%A2%E7%9F%A5%E3%81%AE%E8%84%86%E5%BC%B1%E6%80%A7)

43 SSL/TLS Encryption Design Guidelines, IPA (https://www.ipa.go.jp/files/000045645.pdf)

44 Payment Card Industry Data Security Standard (PCI DSS), PCI SSC,
(https://ja.pcisecuritystandards.org/minisite/env2/)

1.1 and later versions has been available since Android 4.3 (late Jelly Bean), and for direct HTTP communication since Android 4.1 (early Jelly Bean), although some additional implementation is needed in this case.

Among service developers, the adoption of TLS 1.2 means cutting off access to users of Android 4.3 and earlier versions, so it might seem that such a step would have significant repercussions. However, as shown in the figure below, the most recent data[45] (current as of January 2018) show that Android versions 4.3 and later account for the overwhelming majority—94.3%—of all Android systems currently in use. In view of this fact, and considering the importance of guaranteeing the security of assets handled by apps, we recommend that serious consideration be paid to transitioning to TLS 1.2.

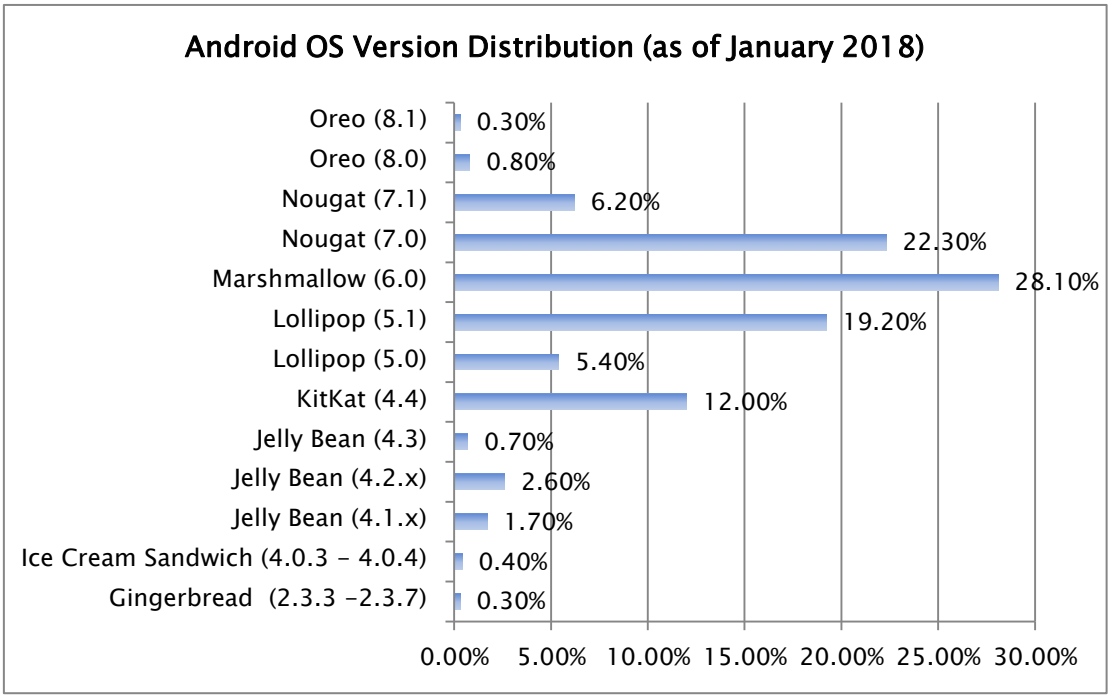


Figure 5.4-5 Distribution of OS versions among Android systems in current use (Source: Android Developers site)

[45] Android OS platform versions, Android Developers dashboard
(https://developer.android.com/about/dashboards/index.html)

In recent years, "Privacy-by-Design" concept has been proposed as a global trend to protect the privacy data. And based on the concept, governments are promoting legislation for privacy protection.

Applications that make use of user data in smartphones must take steps to ensure that users may use the application safely and securely without fears regarding privacy and personal data. These steps include handling user data appropriately and asking users to choose whether or not an application may use certain data. To this end, each application must prepare and display an application privacy policy indicating which information the application will use and how it will use that information; moreover, when fetching and using certain information, the application must first ask the user's permission. Note that application privacy policies differ from other documents that may have been present in the past—such as "Personal Data Protection Policies" or "Terms of Use"—and must be created separately from any such documents.

For details on the creation and execution of privacy policies, see the document "Smartphone Privacy Initiative" and "Smartphone Privacy Initiative II" (JMIC's SPI) released by Japan's Ministry of Internal Affairs and Communications (MIC).

The terminology used in this section is defined in the text and in Section "5.5.3.2Glossary of Terms".

5.5.1. Sample Code

When preparing application privacy policy, you may use the "Tools to Assist in Creating Application Privacy Policies [46]". These tools output two files—a summary version and a detailed version of the application privacy policy —both in HTML format and XML format. The HTML and XML content of these files comports with the recommendations of MIC's SPI including features such as search tags. In the sample code below, we will demonstrate the use of this tool to present application privacy policy using the HTML files prepared by this tool.

[46] http://www.kddilabs.jp/tech/public-tech/appgen.html

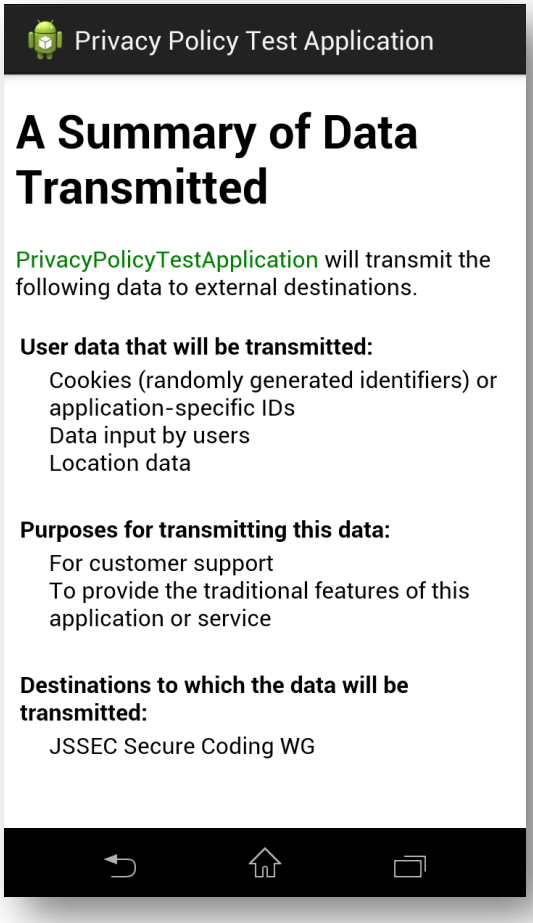


Figure 5.5-1 Sample of Abstract Application Privacy Policy

More specifically, you may use the following flowchart to determine which sample code to use.

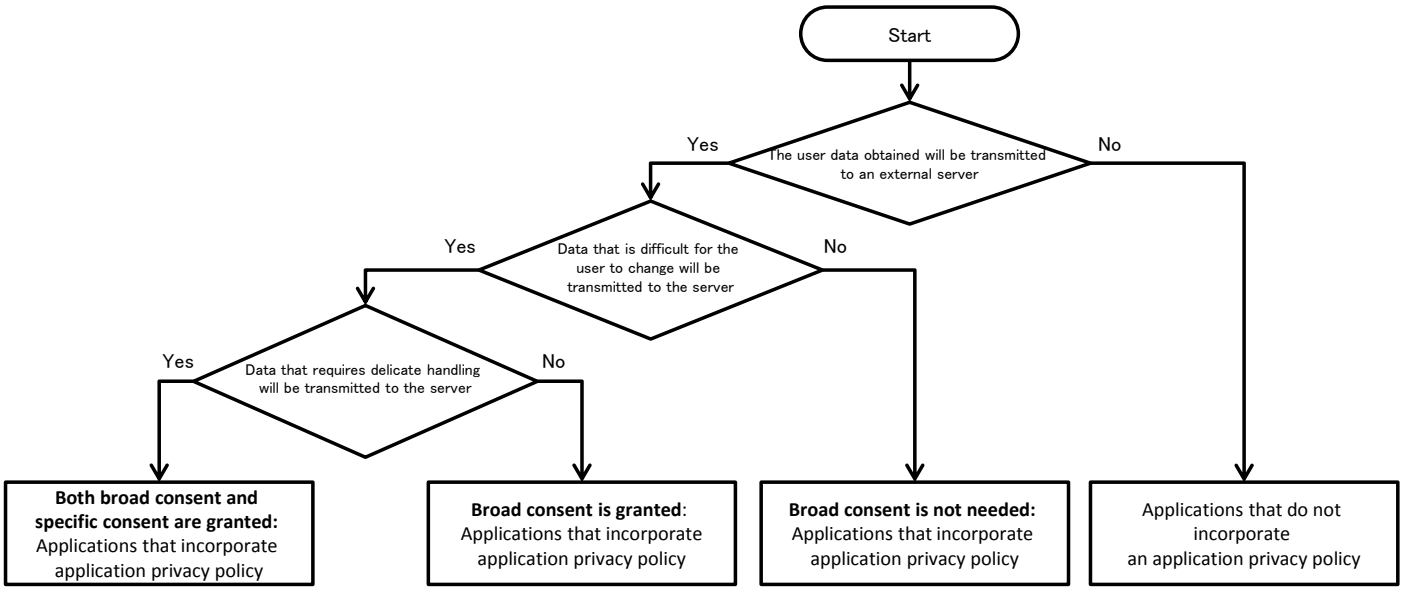


Figure 5.5-2 Flow Figure to select sample code of handling privacy data

Here the phrase “broad consent” refers to a broad permission, granted by the user to the application

upon the first launch of the application through display and review of the application privacy policy, for the application to transmit user data to servers.
In contrast, the phrase “specific consent” refers to pre consent obtained immediately prior to the transmission of specific user data.

5.5.1.1. Both broad consent and specific consent are granted: Applications that incorporate application privacy policy

Points: (Both broad consent and specific consent are granted: Applications that incorporate application privacy policy)

1. On first launch (or application update), obtain broad consent to transmit user data that will be handled by the application.
2. If the user does not grant broad consent, do not transmit user data.
3. Obtain specific consent before transmitting user data that requires particularly delicate handling.
4. If the user does not grant specific consent, do not transmit the corresponding data.
5. Provide methods by which the user can review the application privacy policy.
6. Provide methods by which transmitted data can be deleted by user operations.
7. Provide methods by which transmitting data can be stopped by user operations.
8. Use UUIDs or cookies to keep track of user data.
9. Place a summary version of the application privacy policy in the assets folder.

MainActivity.java

```
package org.jssec.android.privacypolicy;

import java.io.IOException;
import org.json.JSONException;
import org.json.JSONObject;
import org.jssec.android.privacypolicy.ConfirmFragment.DialogListener;

import com.google.android.gms.common.ConnectionResult;
import com.google.android.gms.common.GooglePlayServicesClient;
import com.google.android.gms.common.GooglePlayServicesUtil;
import com.google.android.gms.location.LocationClient;

import android.location.Location;
import android.os.AsyncTask;
import android.os.Bundle;
import android.content.Intent;
import android.content.IntentSender;
import android.content.SharedPreferences;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.support.v4.app.FragmentActivity;
import android.support.v4.app.FragmentManager;
import android.text.Editable;
import android.text.TextWatcher;
import android.view.Menu;
import android.view.MenuItem;
import android.view.View;
import android.widget.TextView;
import android.widget.Toast;
```



```
public class MainActivity extends FragmentActivity implements GooglePlayServicesClient.ConnectionCallba
cks, GooglePlayServicesClient.OnConnectionFailedListener, DialogListener {
    private static final String BASE_URL = "https://www.example.com/pp";
    private static final String GET_ID_URI = BASE_URL + "/get_id.php";
    private static final String SEND_DATA_URI = BASE_URL + "/send_data.php";
    private static final String DEL_ID_URI = BASE_URL + "/del_id.php";

    private static final String ID_KEY = "id";
    private static final String LOCATION_KEY = "location";
    private static final String NICK_NAME_KEY = "nickname";

    private static final String PRIVACY_POLICY_COMPREHENSIVE_AGREED_KEY = "privacyPolicyComprehensiveAg
reed";
    private static final String PRIVACY_POLICY_DISCRETE_TYPE1_AGREED_KEY = "privacyPolicyDiscreteType1A
greed";

    private static final String PRIVACY_POLICY_PREF_NAME = "privacypolicy_preference";
    private static final int CONNECTION_FAILURE_RESOLUTION_REQUEST = 257;

    private String UserId = "";
    private LocationClient mLocationClient = null;

    private final int DIALOG_TYPE_COMPREHENSIVE_AGREEMENT = 1;
    private final int DIALOG_TYPE_PRE_CONFIRMATION = 2;

    private static final int VERSION_TO_SHOW_COMPREHENSIVE_AGREEMENT_ANEW = 1;

    private TextWatcher watchHandler = new TextWatcher() {

        @Override
        public void beforeTextChanged(CharSequence s, int start, int count, int after) {
        }

        @Override
        public void onTextChanged(CharSequence s, int start, int before, int count) {
            boolean buttonEnable = (s.length() > 0);

            MainActivity.this.findViewById(R.id.buttonStart).setEnabled(buttonEnable);
        }

        @Override
        public void afterTextChanged(Editable s) {
        }
    };

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        // Fetch user ID from serverFetch user ID from server
        new GetDataAsyncTask().execute();

        findViewById(R.id.buttonStart).setEnabled(false);
        ((TextView) findViewById(R.id.editTextNickname)).addTextChangedListener(watchHandler);

        int resultCode = GooglePlayServicesUtil.isGooglePlayServicesAvailable(this);
        if (resultCode == ConnectionResult.SUCCESS) {
            mLocationClient = new LocationClient(this, this, this);
```

```
        }
    }

    @Override
    protected void onStart() {
        super.onStart();

        SharedPreferences pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE);
        int privacyPolicyAgreed = pref.getInt(PRIVACY_POLICY_COMPREHENSIVE_AGREED_KEY, -1);

        if (privacyPolicyAgreed <= VERSION_TO_SHOW_COMPREHENSIVE_AGREEMENT_ANEW) {
            // *** POINT 1 *** On first launch (or application update), obtain broad consent to transmit
user data that will be handled by the application.
            // When the application is updated, it is only necessary to renew the user's grant of broad c
onsent if the updated application will handle new types of user data.
            ConfirmFragment dialog = ConfirmFragment.newInstance(R.string.privacyPolicy, R.string.agreeP
rivacyPolicy, DIALOG_TYPE_COMPREHENSIVE_AGREEMENT);
            dialog.setDialogListener(this);
            FragmentManager fragmentManager = getSupportFragmentManager();
            dialog.show(fragmentManager, "dialog");
        }

        // Used to obtain location data
        if (mLocationClient != null) {
            mLocationClient.connect();
        }
    }

    @Override
    protected void onStop() {
        if (mLocationClient != null) {
            mLocationClient.disconnect();
        }
        super.onStop();
    }

    public void onSendToServer(View view) {
        // Check the status of user consent.
        // Actually, it is necessary to obtain consent for each user data type.
        SharedPreferences pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE);
        int privacyPolicyAgreed = pref.getInt(PRIVACY_POLICY_DISCRETE_TYPE1_AGREED_KEY, -1);
        if (privacyPolicyAgreed <= VERSION_TO_SHOW_COMPREHENSIVE_AGREEMENT_ANEW) {
            // *** POINT 3 *** Obtain specific consent before transmitting user data that requires partic
ularly delicate handling.
            ConfirmFragment dialog = ConfirmFragment.newInstance(R.string.sendLocation, R.string.cofirmS
endLocation, DIALOG_TYPE_PRE_CONFIRMATION);
            dialog.setDialogListener(this);
            FragmentManager fragmentManager = getSupportFragmentManager();
            dialog.show(fragmentManager, "dialog");
        } else {
            // Start transmission, since it has the user consent.
            onPositiveButtonClick(DIALOG_TYPE_PRE_CONFIRMATION);
        }
    }

    public void onPositiveButtonClick(int type) {
        if (type == DIALOG_TYPE_COMPREHENSIVE_AGREEMENT) {
            // *** POINT 1 *** On first launch (or application update), obtain broad consent to transmit
user data that will be handled by the application.
            SharedPreferences.Editor pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE)
```



```
.edit();
            pref.putInt(PRIVACY_POLICY_COMPREHENSIVE_AGREED_KEY, getVersionCode());
            pref.apply();
        } else if (type == DIALOG_TYPE_PRE_CONFIRMATION) {
            // *** POINT 3 *** Obtain specific consent before transmitting user data that requires partic
ularly delicate handling.
            if (mLocationClient != null && mLocationClient.isConnected()) {
                Location currentLocation = mLocationClient.getLastLocation();
                if (currentLocation != null) {
                    String locationData = "Latitude:" + currentLocation.getLatitude() + ", Longitude:" +
currentLocation.getLongitude();
                    String nickname = ((TextView) findViewById(R.id.editTextNickname)).getText().toString
();

                    Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + "¥n - nickname :
" + nickname + "¥n - location : " + locationData, Toast.LENGTH_SHORT).show();

                    new SendDataAsyncTack().execute(SEND_DATA_URI, UserId, locationData, nickname);
                }
            }
            // Store the status of user consent.
            // Actually, it is necessary to obtain consent for each user data type.
            SharedPreferences.Editor pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE)
.edit();
            pref.putInt(PRIVACY_POLICY_DISCRETE_TYPE1_AGREED_KEY, getVersionCode());
            pref.apply();
        }
    }

    public void onNegativeButtonClick(int type) {
        if (type == DIALOG_TYPE_COMPREHENSIVE_AGREEMENT) {
            // *** POINT 2 *** If the user does not grant general consent, do not transmit user data.
            // In this sample application we terminate the application in this case.
            finish();
        } else if (type == DIALOG_TYPE_PRE_CONFIRMATION) {
            // *** POINT 4 *** If the user does not grant specific consent, do not transmit the correspon
ding data.
            // The user did not grant consent, so we do nothing.
        }
    }

    private int getVersionCode() {
        int versionCode = -1;
        PackageManager packageManager = this.getPackageManager();
        try {
            PackageInfo packageInfo = packageManager.getPackageInfo(this.getPackageName(), PackageManage
r.GET_ACTIVITIES);
            versionCode = packageInfo.versionCode;
        } catch (NameNotFoundException e) {
            // This is sample, so omit the exception process
        }

        return versionCode;
    }

    @Override
    public boolean onCreateOptionsMenu(Menu menu) {
        getMenuInflater().inflate(R.menu.main, menu);
        return true;
    }
```

```
    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
        switch (item.getItemId()) {
            case R.id.action_show_pp:
                // *** POINT 5 *** Provide methods by which the user can review the application privacy p
olicy.
                Intent intent = new Intent();
                intent.setClass(this, WebViewAssetsActivity.class);
                startActivity(intent);
                return true;
            case R.id.action_del_id:
                // *** POINT 6 *** Provide methods by which transmitted data can be deleted by user opera
tions.
                new SendDataAsyncTack().execute(DEL_ID_URI, UserId);
                return true;
            case R.id.action_donot_send_id:
                // *** POINT 7 *** Provide methods by which transmitting data can be stopped by user oper
ations.

                // If the user stop sending data, user consent is deemed to have been revoked.
                SharedPreferences.Editor pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIV
ATE).edit();
                pref.putInt(PRIVACY_POLICY_COMPREHENSIVE_AGREED_KEY, 0);
                pref.apply();

                // In this sample application if the user data cannot be sent by user operations,
                // finish the application because we do nothing.
                String message  = getString(R.string.stopSendUserData);
                Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + message, Toas
t.LENGTH_SHORT).show();
                finish();

                return true;
        }

        return false;
    }

    @Override
    public void onConnected(Bundle connectionHint) {
        if (mLocationClient != null && mLocationClient.isConnected()) {
            Location currentLocation = mLocationClient.getLastLocation();
            if (currentLocation != null) {
                String locationData = "Latitude ¥t: " + currentLocation.getLatitude() + "¥n¥tLongitude ¥t
: " + currentLocation.getLongitude();

                String text = "¥n" + getString(R.string.your_location_title) + "¥n¥t" + locationData;

                TextView appText = (TextView) findViewById(R.id.appText);
                appText.setText(text);
            }
        }
    }

    @Override
    public void onConnectionFailed(ConnectionResult result) {
        if (result.hasResolution()) {
            try {
                result.startResolutionForResult(this, CONNECTION_FAILURE_RESOLUTION_REQUEST);
```



```
            } catch (IntentSender.SendIntentException e) {
                e.printStackTrace();
            }
        }
    }

    @Override
    public void onDisconnected() {
        mLocationClient = null;
    }

    private class GetDataAsyncTask extends AsyncTask<String, Void, String> {
        private String extMessage = "";

        @Override
        protected String doInBackground(String... params) {
            // *** POINT 8 *** Use UUIDs or cookies to keep track of user data
            // In this sample we use an ID generated on the server side
            SharedPreferences sp = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE);
            UserId = sp.getString(ID_KEY, null);
            if (UserId == null) {
                // No token in SharedPreferences; fetch ID from server
                try {
                    UserId = NetworkUtil.getCookie(GET_ID_URI, "", "id");
                } catch (IOException e) {
                    // Catch exceptions such as certification errors
                    extMessage = e.toString();
                }

                // Store the fetched ID in SharedPreferences
                sp.edit().putString(ID_KEY, UserId).commit();
            }
            return UserId;
        }

        @Override
        protected void onPostExecute(final String data) {
            String status = (data != null) ? "success" : "error";
            Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + status + " : " +
extMessage, Toast.LENGTH_SHORT).show();
        }
    }

    private class SendDataAsyncTack extends AsyncTask<String, Void, Boolean> {
        private String extMessage = "";

        @Override
        protected Boolean doInBackground(String... params) {
            String url = params[0];
            String id = params[1];
            String location = params.length > 2 ? params[2] : null;
            String nickname = params.length > 3 ? params[3] : null;

            Boolean result = false;
            try {
                JSONObject jsonData = new JSONObject();
                jsonData.put(ID_KEY, id);
                if (location != null)
                    jsonData.put(LOCATION_KEY, location);
```

```
                if (nickname != null)
                    jsonData.put(NICK_NAME_KEY, nickname);

                NetworkUtil.sendJSON(url, "", jsonData.toString());

                result = true;
            } catch (IOException e) {
                // Catch exceptions such as certification errors
                extMessage = e.toString();
            } catch (JSONException e) {
                extMessage = e.toString();
            }
            return result;
        }

        @Override
        protected void onPostExecute(Boolean result) {
            String status = result ? "Success" : "Error";
            Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + status + " : " +
extMessage, Toast.LENGTH_SHORT).show();
        }
    }
}
```

ConfirmFragment.java

```
package org.jssec.android.privacypolicy;

import android.app.Activity;
import android.app.AlertDialog;
import android.app.Dialog;
import android.content.Context;
import android.content.DialogInterface;
import android.content.Intent;
import android.os.Bundle;
import android.support.v4.app.DialogFragment;
import android.view.LayoutInflater;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.TextView;

public class ConfirmFragment extends DialogFragment {

    private DialogListener mListener = null;

    public static interface DialogListener {
        public void onPositiveButtonClick(int type);

        public void onNegativeButtonClick(int type);
    }

    public static ConfirmFragment newInstance(int title, int sentence, int type) {
        ConfirmFragment fragment = new ConfirmFragment();
        Bundle args = new Bundle();
        args.putInt("title", title);
        args.putInt("sentence", sentence);
        args.putInt("type", type);
        fragment.setArguments(args);
        return fragment;
```



```
    }

    @Override
    public Dialog onCreateDialog(Bundle args) {
        // *** POINT 1 *** On first launch (or application update), obtain broad consent to transmit user
 data that will be handled by the application.
        // *** POINT 3 *** Obtain specific consent before transmitting user data that requires particula
rly delicate handling.
        final int title = getArguments().getInt("title");
        final int sentence = getArguments().getInt("sentence");
        final int type = getArguments().getInt("type");

        LayoutInflater inflater = (LayoutInflater) getActivity().getSystemService(Context.LAYOUT_INFLAT
ER_SERVICE);
        View content = inflater.inflate(R.layout.fragment_comfirm, null);
        TextView linkPP = (TextView) content.findViewById(R.id.tx_link_pp);
        linkPP.setOnClickListener(new OnClickListener() {
            @Override
            public void onClick(View v) {
                // *** POINT 5 *** Provide methods by which the user can review the application privacy p
olicy.
                Intent intent = new Intent();
                intent.setClass(getActivity(), WebViewAssetsActivity.class);
                startActivity(intent);
            }
        });

        AlertDialog.Builder builder = new AlertDialog.Builder(getActivity());
        builder.setIcon(R.drawable.ic_launcher);
        builder.setTitle(title);
        builder.setMessage(sentence);
        builder.setView(content);

        builder.setPositiveButton(R.string.buttonConsent, new DialogInterface.OnClickListener() {
            public void onClick(DialogInterface dialog, int whichButton) {
                if (mListener != null) {
                    mListener.onPositiveButtonClick(type);
                }
            }
        });
        builder.setNegativeButton(R.string.buttonDonotConsent, new DialogInterface.OnClickListener() {
            public void onClick(DialogInterface dialog, int whichButton) {
                if (mListener != null) {
                    mListener.onNegativeButtonClick(type);
                }
            }
        });

        Dialog dialog = builder.create();
        dialog.setCanceledOnTouchOutside(false);

        return dialog;
    }

    @Override
    public void onAttach(Activity activity) {
        super.onAttach(activity);
        if (!(activity instanceof DialogListener)) {
            throw new ClassCastException(activity.toString() + " must implement DialogListener.");
        }
```

```
        mListener = (DialogListener) activity;
    }

    public void setDialogListener(DialogListener listener) {
        mListener = listener;
    }
}
```

WebViewAssetsActivity.java

```
package org.jssec.android.privacypolicy;

import android.app.Activity;
import android.os.Bundle;
import android.webkit.WebSettings;
import android.webkit.WebView;

public class WebViewAssetsActivity extends Activity {
    // *** POINT 9 *** Place a summary version of the application privacy policy in the assets folder
    private static final String ABST_PP_URL = "file:///android_asset/PrivacyPolicy/app-policy-abst-priv
acypolicy-1.0.html";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_webview);

        WebView webView = (WebView) findViewById(R.id.webView);
        WebSettings webSettings = webView.getSettings();

        webSettings.setAllowFileAccess(false);

        webView.loadUrl(ABST_PP_URL);
    }
}
```

5.5.1.2. Broad consent is granted: Applications that incorporate application privacy policy

Points: (Broad consent is granted: Applications that incorporate application privacy policy)

1. On first launch (or application update), obtain broad consent to transmit user data that will be handled by the application.
1. If the user does not grant broad consent, do not transmit user data.
2. Provide methods by which the user can review the application privacy policy.
3. Provide methods by which transmitted data can be deleted by user operations.
4. Provide methods by which transmitting data can be stopped by user operations.
5. Use UUIDs or cookies to keep track of user data.
6. Place a summary version of the application privacy policy in the assets folder.

MainActivity.java

```
package org.jssec.android.privacypolicynopreconfirm;

import java.io.IOException;
```



```
import org.json.JSONException;
import org.json.JSONObject;
import org.jssec.android.privacypolicynopreconfirm.MainActivity;
import org.jssec.android.privacypolicynopreconfirm.R;
import org.jssec.android.privacypolicynopreconfirm.ConfirmFragment.DialogListener;


import android.os.AsyncTask;
import android.os.Bundle;
import android.content.Intent;
import android.content.SharedPreferences;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.pm.PackageManager.NameNotFoundException;
import android.support.v4.app.FragmentActivity;
import android.support.v4.app.FragmentManager;
import android.telephony.TelephonyManager;
import android.text.Editable;
import android.text.TextWatcher;
import android.view.Menu;
import android.view.MenuItem;
import android.view.View;
import android.widget.TextView;
import android.widget.Toast;

public class MainActivity extends FragmentActivity implements DialogListener {
    private final String BASE_URL = "https://www.example.com/pp";
    private final String GET_ID_URI = BASE_URL + "/get_id.php";
    private final String SEND_DATA_URI = BASE_URL + "/send_data.php";
    private final String DEL_ID_URI = BASE_URL + "/del_id.php";

    private final String ID_KEY = "id";
    private final String NICK_NAME_KEY = "nickname";
    private final String IMEI_KEY = "imei";

    private final String PRIVACY_POLICY_AGREED_KEY = "privacyPolicyAgreed";

    private final String PRIVACY_POLICY_PREF_NAME = "privacypolicy_preference";

    private String UserId = "";

    private final int DIALOG_TYPE_COMPREHENSIVE_AGREEMENT = 1;

    private final int VERSION_TO_SHOW_COMPREHENSIVE_AGREEMENT_ANEW = 1;

    private TextWatcher watchHandler = new TextWatcher() {

        @Override
        public void beforeTextChanged(CharSequence s, int start, int count, int after) {
        }

        @Override
        public void onTextChanged(CharSequence s, int start, int before, int count) {
            boolean buttonEnable = (s.length() > 0);

            MainActivity.this.findViewById(R.id.buttonStart).setEnabled(buttonEnable);
        }

        @Override
        public void afterTextChanged(Editable s) {
```

```
        }
    };

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        // Fetch user ID from serverFetch user ID from server
        new GetDataAsyncTask().execute();

        findViewById(R.id.buttonStart).setEnabled(false);
        ((TextView) findViewById(R.id.editTextNickname)).addTextChangedListener(watchHandler);
    }

    @Override
    protected void onStart() {
        super.onStart();

        SharedPreferences pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE);
        int privacyPolicyAgreed = pref.getInt(PRIVACY_POLICY_AGREED_KEY, -1);

        if (privacyPolicyAgreed <= VERSION_TO_SHOW_COMPREHENSIVE_AGREEMENT_ANEW) {
            // *** POINT 1 *** On first launch (or application update), obtain broad consent to transmit
user data that will be handled by the application.
            // When the application is updated, it is only necessary to renew the user's grant of broad c
onsent if the updated application will handle new types of user data.
            ConfirmFragment dialog = ConfirmFragment.newInstance(R.string.privacyPolicy, R.string.agreeP
rivacyPolicy, DIALOG_TYPE_COMPREHENSIVE_AGREEMENT);
            dialog.setDialogListener(this);
            FragmentManager fragmentManager = getSupportFragmentManager();
            dialog.show(fragmentManager, "dialog");
        }
    }

    public void onSendToServer(View view) {
        String nickname = ((TextView) findViewById(R.id.editTextNickname)).getText().toString();
        TelephonyManager tm = (TelephonyManager) getSystemService(TELEPHONY_SERVICE);
        String imei = tm.getDeviceId();
        Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + "¥n - nickname : " + nicknam
e + ", imei = " + imei, Toast.LENGTH_SHORT).show();
        new SendDataAsyncTack().execute(SEND_DATA_URI, UserId, nickname, imei);
    }

    public void onPositiveButtonClick(int type) {
        if (type == DIALOG_TYPE_COMPREHENSIVE_AGREEMENT) {
            // *** POINT 1 *** On first launch (or application update), obtain broad consent to transmit
user data that will be handled by the application.
            SharedPreferences.Editor pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE)
.edit();
            pref.putInt(PRIVACY_POLICY_AGREED_KEY, getVersionCode());
            pref.apply();
        }
    }

    public void onNegativeButtonClick(int type) {
        if (type == DIALOG_TYPE_COMPREHENSIVE_AGREEMENT) {
            // *** POINT 2 *** If the user does not grant general consent, do not transmit user data.
            // In this sample application we terminate the application in this case.
            finish();
```



```
        }
    }

    private int getVersionCode() {
        int versionCode = -1;
        PackageManager packageManager = this.getPackageManager();
        try {
            PackageInfo packageInfo = packageManager.getPackageInfo(this.getPackageName(), PackageManage
r.GET_ACTIVITIES);
            versionCode = packageInfo.versionCode;
        } catch (NameNotFoundException e) {
            // This is sample, so omit the exception process
        }

        return versionCode;
    }

    @Override
    public boolean onCreateOptionsMenu(Menu menu) {
        getMenuInflater().inflate(R.menu.main, menu);
        return true;
    }

    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
        switch (item.getItemId()) {
        case R.id.action_show_pp:
            // *** POINT 3 *** Provide methods by which the user can review the application privacy polic
y.
            Intent intent = new Intent();
            intent.setClass(this, WebViewAssetsActivity.class);
            startActivity(intent);
            return true;
        case R.id.action_del_id:
            // *** POINT 4 *** Provide methods by which transmitted data can be deleted by user operation
s.
            new SendDataAsyncTack().execute(DEL_ID_URI, UserId);
            return true;
        case R.id.action_donot_send_id:
            // *** POINT 5 *** Provide methods by which transmitting data can be stopped by user operatio
ns.

            // If the user stop sending data, user consent is deemed to have been revoked.
            SharedPreferences.Editor pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE)
.edit();
            pref.putInt(PRIVACY_POLICY_AGREED_KEY, 0);
            pref.apply();

            // In this sample application if the user data cannot be sent by user operations,
            // finish the application because we do nothing.
            String message  = getString(R.string.stopSendUserData);
            Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + message, Toast.L
ENGTH_SHORT).show();
            finish();

            return true;       }
        return false;
    }

    private class GetDataAsyncTask extends AsyncTask<String, Void, String> {
```

```
        private String extMessage = "";

        @Override
        protected String doInBackground(String... params) {
            // *** POINT 6 *** Use UUIDs or cookies to keep track of user data
            // In this sample we use an ID generated on the server side
            SharedPreferences sp = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE);
            UserId = sp.getString(ID_KEY, null);
            if (UserId == null) {
                // No token in SharedPreferences; fetch ID from server
                try {
                    UserId = NetworkUtil.getCookie(GET_ID_URI, "", "id");
                } catch (IOException e) {
                    // Catch exceptions such as certification errors
                    extMessage = e.toString();
                }

                // Store the fetched ID in SharedPreferences
                sp.edit().putString(ID_KEY, UserId).commit();
            }
            return UserId;
        }

        @Override
        protected void onPostExecute(final String data) {
            String status = (data != null) ? "success" : "error";
            Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + status + " : " +
extMessage, Toast.LENGTH_SHORT).show();
        }
    }

    private class SendDataAsyncTack extends AsyncTask<String, Void, Boolean> {
        private String extMessage = "";

        @Override
        protected Boolean doInBackground(String... params) {
            String url = params[0];
            String id = params[1];
            String nickname = params.length > 2 ? params[2] : null;
            String imei = params.length > 3 ? params[3] : null;

            Boolean result = false;
            try {
                JSONObject jsonData = new JSONObject();
                jsonData.put(ID_KEY, id);

                if (nickname != null)
                    jsonData.put(NICK_NAME_KEY, nickname);

                if (imei != null)
                    jsonData.put(IMEI_KEY, imei);

                NetworkUtil.sendJSON(url, "", jsonData.toString());

                result = true;
            } catch (IOException e) {
                // Catch exceptions such as certification errors
                extMessage = e.toString();
            } catch (JSONException e) {
                extMessage = e.toString();
```



```
            }
            return result;
        }

        @Override
        protected void onPostExecute(Boolean result) {
            String status = result ? "Success" : "Error";
            Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + status + " : " +
extMessage, Toast.LENGTH_SHORT).show();
        }
    }
}
```

ConfirmFragment.java

```
package org.jssec.android.privacypolicynopreconfirm;

import android.app.Activity;
import android.app.AlertDialog;
import android.app.Dialog;
import android.content.Context;
import android.content.DialogInterface;
import android.content.Intent;
import android.os.Bundle;
import android.support.v4.app.DialogFragment;
import android.view.LayoutInflater;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.TextView;

public class ConfirmFragment extends DialogFragment {

    private DialogListener mListener = null;

    public static interface DialogListener {
        public void onPositiveButtonClick(int type);

        public void onNegativeButtonClick(int type);
    }

    public static ConfirmFragment newInstance(int title, int sentence, int type) {
        ConfirmFragment fragment = new ConfirmFragment();
        Bundle args = new Bundle();
        args.putInt("title", title);
        args.putInt("sentence", sentence);
        args.putInt("type", type);
        fragment.setArguments(args);
        return fragment;
    }

    @Override
    public Dialog onCreateDialog(Bundle args) {
        // *** POINT 1 *** On first launch (or application update), obtain broad consent to transmit user
 data that will be handled by the application.
        final int title = getArguments().getInt("title");
        final int sentence = getArguments().getInt("sentence");
        final int type = getArguments().getInt("type");

        LayoutInflater inflater = (LayoutInflater) getActivity().getSystemService(Context.LAYOUT_INFLAT
```

```
ER_SERVICE);
        View content = inflater.inflate(R.layout.fragment_comfirm, null);
        TextView linkPP = (TextView) content.findViewById(R.id.tx_link_pp);
        linkPP.setOnClickListener(new OnClickListener() {
            @Override
            public void onClick(View v) {
                // *** POINT 3 *** Provide methods by which the user can review the application privacy p
olicy.
                Intent intent = new Intent();
                intent.setClass(getActivity(), WebViewAssetsActivity.class);
                startActivity(intent);
            }
        });

        AlertDialog.Builder builder = new AlertDialog.Builder(getActivity());
        builder.setIcon(R.drawable.ic_launcher);
        builder.setTitle(title);
        builder.setMessage(sentence);
        builder.setView(content);

        builder.setPositiveButton(R.string.buttonConsent, new DialogInterface.OnClickListener() {
            public void onClick(DialogInterface dialog, int whichButton) {
                if (mListener != null) {
                    mListener.onPositiveButtonClick(type);
                }
            }
        });
        builder.setNegativeButton(R.string.buttonDonotConsent, new DialogInterface.OnClickListener() {
            public void onClick(DialogInterface dialog, int whichButton) {
                if (mListener != null) {
                    mListener.onNegativeButtonClick(type);
                }
            }
        });

        Dialog dialog = builder.create();
        dialog.setCanceledOnTouchOutside(false);

        return dialog;
    }

    @Override
    public void onAttach(Activity activity) {
        super.onAttach(activity);
        if (!(activity instanceof DialogListener)) {
            throw new ClassCastException(activity.toString() + " must implement DialogListener.");
        }
        mListener = (DialogListener) activity;
    }

    public void setDialogListener(DialogListener listener) {
        mListener = listener;
    }
}
```


WebViewAssetsActivity.java

```
package org.jssec.android.privacypolicynopreconfirm;

import org.jssec.android.privacypolicynopreconfirm.R;

import android.app.Activity;
import android.os.Bundle;
import android.webkit.WebSettings;
import android.webkit.WebView;

public class WebViewAssetsActivity extends Activity {
    // *** POINT 7 *** Place a summary version of the application privacy policy in the assets folder
    private final String ABST_PP_URL = "file:///android_asset/PrivacyPolicy/app-policy-abst-privacypoli
cy-1.0.html";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_webview);

        WebView webView = (WebView) findViewById(R.id.webView);
        WebSettings webSettings = webView.getSettings();

        webSettings.setAllowFileAccess(false);

        webView.loadUrl(ABST_PP_URL);
    }
}
```

5.5.1.3. Broad consent is not needed: Applications that incorporate application privacy policy

Points: (Broad consent is not needed: Applications that incorporate application privacy policy)

1. Provide methods by which the user can review the application privacy policy.
2. Provide methods by which transmitted data can be deleted by user operations.
3. Provide methods by which transmitting data can be stopped by user operations
4. Use UUIDs or cookies to keep track of user data.
5. Place a summary version of the application privacy policy in the assets folder.

MainActivity.java

```
package org.jssec.android.privacypolicynocomprehensive;

import java.io.IOException;
import org.json.JSONException;
import org.json.JSONObject;

import android.os.AsyncTask;
import android.os.Bundle;
import android.content.Intent;
import android.content.SharedPreferences;
import android.support.v4.app.FragmentActivity;
import android.text.Editable;
import android.text.TextWatcher;
import android.view.Menu;
import android.view.MenuItem;
import android.view.View;
import android.widget.TextView;
import android.widget.Toast;

public class MainActivity extends FragmentActivity {
    private static final String BASE_URL = "https://www.example.com/pp";
    private static final String GET_ID_URI = BASE_URL + "/get_id.php";
    private static final String SEND_DATA_URI = BASE_URL + "/send_data.php";
    private static final String DEL_ID_URI = BASE_URL + "/del_id.php";

    private static final String ID_KEY = "id";
    private static final String NICK_NAME_KEY = "nickname";

    private static final String PRIVACY_POLICY_PREF_NAME = "privacypolicy_preference";

    private String UserId = "";

    private TextWatcher watchHandler = new TextWatcher() {

        @Override
        public void beforeTextChanged(CharSequence s, int start, int count, int after) {
        }

        @Override
        public void onTextChanged(CharSequence s, int start, int before, int count) {
            boolean buttonEnable = (s.length() > 0);

            MainActivity.this.findViewById(R.id.buttonStart).setEnabled(buttonEnable);
        }

        @Override
```



```
        public void afterTextChanged(Editable s) {
        }
    };

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        // Fetch user ID from serverFetch user ID from server
        new GetDataAsyncTask().execute();

        findViewById(R.id.buttonStart).setEnabled(false);
        ((TextView) findViewById(R.id.editTextNickname)).addTextChangedListener(watchHandler);
    }

    public void onSendToServer(View view) {
        String nickname = ((TextView) findViewById(R.id.editTextNickname)).getText().toString();
        Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + "¥n - nickname : " + nickname, Toast.LENGTH_SHORT).show();
        new sendDataAsyncTack().execute(SEND_DATA_URI, UserId, nickname);
    }

    @Override
    public boolean onCreateOptionsMenu(Menu menu) {
        getMenuInflater().inflate(R.menu.main, menu);
        return true;
    }

    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
        switch (item.getItemId()) {
        case R.id.action_show_pp:
            // *** POINT 1 *** Provide methods by which the user can review the application privacy policy.
            Intent intent = new Intent();
            intent.setClass(this, WebViewAssetsActivity.class);
            startActivity(intent);
            return true;
        case R.id.action_del_id:
            // *** POINT 2 *** Provide methods by which transmitted data can be deleted by user operations.
            new sendDataAsyncTack().execute(DEL_ID_URI, UserId);
            return true;
        case R.id.action_donot_send_id:
            // *** POINT 3 *** Provide methods by which transmitting data can be stopped by user operations.

            // In this sample application if the user data cannot be sent by user operations,
            // finish the application because we do nothing.
            String message  = getString(R.string.stopSendUserData);
            Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + message, Toast.LENGTH_SHORT).show();
            finish();

            return true;
        }
        return false;
    }
```

```
    private class GetDataAsyncTask extends AsyncTask<String, Void, String> {
        private String extMessage = "";

        @Override
        protected String doInBackground(String... params) {
            // *** POINT 4 *** Use UUIDs or cookies to keep track of user data
            // In this sample we use an ID generated on the server side
            SharedPreferences sp = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE);
            UserId = sp.getString(ID_KEY, null);
            if (UserId == null) {
                // No token in SharedPreferences; fetch ID from server
                try {
                    UserId = NetworkUtil.getCookie(GET_ID_URI, "", "id");
                } catch (IOException e) {
                    // Catch exceptions such as certification errors
                    extMessage = e.toString();
                }

                // Store the fetched ID in SharedPreferences
                sp.edit().putString(ID_KEY, UserId).commit();
            }
            return UserId;
        }

        @Override
        protected void onPostExecute(final String data) {
            String status = (data != null) ? "success" : "error";
            Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + status + " : " +
extMessage, Toast.LENGTH_SHORT).show();
        }
    }

    private class sendDataAsyncTack extends AsyncTask<String, Void, Boolean> {
        private String extMessage = "";

        @Override
        protected Boolean doInBackground(String... params) {
            String url = params[0];
            String id = params[1];
            String nickname = params.length > 2 ? params[2] : null;

            Boolean result = false;
            try {
                JSONObject jsonData = new JSONObject();
                jsonData.put(ID_KEY, id);

                if (nickname != null)
                    jsonData.put(NICK_NAME_KEY, nickname);

                NetworkUtil.sendJSON(url, "", jsonData.toString());

                result = true;
            } catch (IOException e) {
                // Catch exceptions such as certification errors
                extMessage = e.toString();
            } catch (JSONException e) {
                extMessage = e.toString();
            }
            return result;
        }
```



```
        @Override
        protected void onPostExecute(Boolean result) {
            String status = result ? "Success" : "Error";
            Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + " - " + status + " : " +
extMessage, Toast.LENGTH_SHORT).show();
        }
    }
}
```

WebViewAssetsActivity.java

```
package org.jssec.android.privacypolicynocomprehensive;

import org.jssec.android.privacypolicynocomprehensive.R;

import android.app.Activity;
import android.os.Bundle;
import android.webkit.WebSettings;
import android.webkit.WebView;

public class WebViewAssetsActivity extends Activity {
    // *** POINT 5 *** Place a summary version of the application privacy policy in the assets folder
    private static final String ABST_PP_URL = "file:///android_asset/PrivacyPolicy/app-policy-abst-priv
acypolicy-1.0.html";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_webview);

        WebView webView = (WebView) findViewById(R.id.webView);
        WebSettings webSettings = webView.getSettings();

        webSettings.setAllowFileAccess(false);

        webView.loadUrl(ABST_PP_URL);
    }
}
```

5.5.1.4. Applications that do not incorporate an application privacy policy

Points: (Applications that do not incorporate an application privacy policy)

1. You do not need to display an application privacy policy if your application will only use the information it obtains within the device.
2. In the documentation for marketplace applications or similar applications, note that the application does not transmit the information it obtains to the outside world

MainActivity.java

```
package org.jssec.android.privacypolicynoinfosent;

import com.google.android.gms.common.ConnectionResult;
import com.google.android.gms.common.GooglePlayServicesClient;
import com.google.android.gms.location.LocationClient;
```

```
import android.location.Location;
import android.net.Uri;
import android.os.Bundle;
import android.content.Intent;
import android.content.IntentSender;
import android.support.v4.app.FragmentActivity;
import android.view.Menu;
import android.view.View;
import android.widget.TextView;
import android.widget.Toast;

public class MainActivity extends FragmentActivity implements GooglePlayServicesClient.ConnectionCallba
cks, GooglePlayServicesClient.OnConnectionFailedListener {
    private LocationClient mLocationClient = null;

    private final int CONNECTION_FAILURE_RESOLUTION_REQUEST = 257;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        mLocationClient = new LocationClient(this, this, this);
    }

    @Override
    protected void onStart() {
        super.onStart();

        // Used to obtain location data
        if (mLocationClient != null) {
            mLocationClient.connect();
        }
    }

    @Override
    protected void onStop() {
        if (mLocationClient != null) {
            mLocationClient.disconnect();
        }
        super.onStop();
    }

    @Override
    public boolean onCreateOptionsMenu(Menu menu) {
        getMenuInflater().inflate(R.menu.main, menu);
        return true;
    }

    public void onStartMap(View view) {
        // *** POINT 1 *** You do not need to display an application privacy policy if your application w
ill only use the information it obtains within the device.
        if (mLocationClient != null && mLocationClient.isConnected()) {
            Location currentLocation = mLocationClient.getLastLocation();
            if (currentLocation != null) {
                Intent intent = new Intent(Intent.ACTION_VIEW, Uri.parse("geo:" + currentLocation.getLat
itude() + "," + currentLocation.getLongitude()));
                startActivity(intent);
            }
        }
```



```
    }

    @Override
    public void onConnected(Bundle connectionHint) {
        if (mLocationClient != null && mLocationClient.isConnected()) {
            Location currentLocation = mLocationClient.getLastLocation();
            if (currentLocation != null) {
                String locationData = "Latitude ¥t: " + currentLocation.getLatitude() + "¥n¥tLongitude ¥t
: " + currentLocation.getLongitude();

                String text = "¥n" + getString(R.string.your_location_title) + "¥n¥t" + locationData;

                Toast.makeText(MainActivity.this, this.getClass().getSimpleName() + text, Toast.LENGTH_S
HORT).show();

                TextView appText = (TextView) findViewById(R.id.appText);
                appText.setText(text);
            }
        }
    }

    @Override
    public void onConnectionFailed(ConnectionResult result) {
        if (result.hasResolution()) {
            try {
                result.startResolutionForResult(this, CONNECTION_FAILURE_RESOLUTION_REQUEST);
            } catch (IntentSender.SendIntentException e) {
                e.printStackTrace();
            }
        }
    }

    @Override
    public void onDisconnected() {
        mLocationClient = null;
        Toast.makeText(this, "Disconnected. Please re-connect.", Toast.LENGTH_SHORT).show();
    }
}
```

Sample description on the marketplace is below.

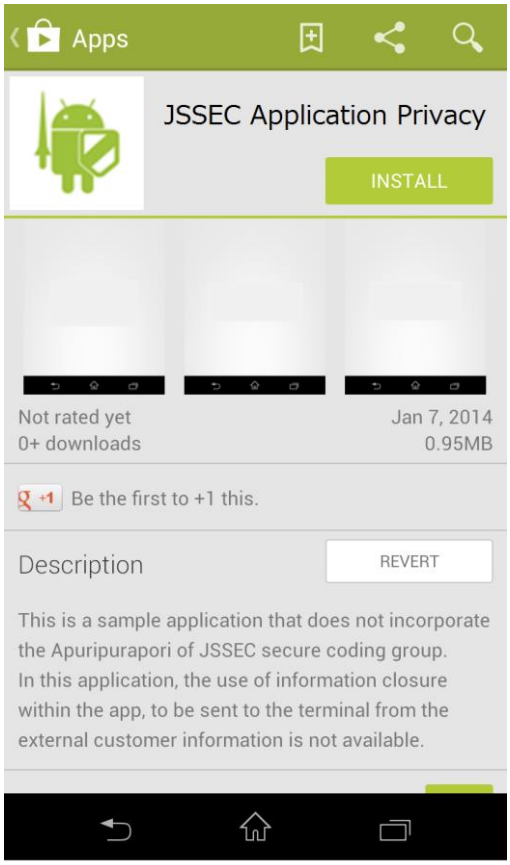


Figure 5.5-3 Description on the marketplace

5.5.2. Rule Book

When working with private date, obey the following rules.

1.	Restrict transmissions of user data to the minimum necessary (Required)
2.	On first launch (or application update), obtain broad consent to transmit user data that requires particularly delicate handling or that may be difficult for users to change (Required)
3.	Obtain specific consent before transmitting user data that requires particularly delicate handling (Required)
4.	Provide methods by which the user can review the application privacy policy (Required)
5.	Place a summary version of the application privacy policy in the assets folder(Recommended)
6.	Provide methods by which transmitted data can be deleted and transmitting data can be stopped by user operations (Recommended)
7.	Separate device-specific IDs from UUIDs and cookies (Recommended)
8.	If you will only be using user data within the device, notify the user that data will not be transmitted externally. (Recommended)

5.5.2.1. Restrict transmissions of user data to the minimum necessary (Required)

When transmitting usage data to external servers or other destinations, restrict transmissions to the bare minimum necessary to provide service. In particular, you should design that applications have access to only user data of which purpose of use the user can imagine on the basis of the application description.

For example, an application that the user can imagine it is an alarm application, must not have access location data. On the other hand, if an alarm application can sound the alarm depending on the location of user and its feature is written on the description of the application, the application may have access to location data.

In cases where information need only be accessed within an application, avoid transmitting it externally and take other steps to minimize the possibility of inadvertent leakage of user data.

5.5.2.2. On first launch (or application update), obtain broad consent to transmit user data that requires particularly delicate handling or that may be difficult for users to change (Required)

If an application will transmit to external servers any user data that may be difficult for users to change, or any user data that requires particularly delicate handling, the application must obtain advance consent (opt-in) from the user—before the user begins using the application—informing the user of what types of information will be sent, for what purposes, to servers, and whether or not any third-party providers will be involved. More specifically, on first launch the application should display its application privacy policy and confirm that the user has reviewed it and consented. Also, whenever an application is updated in such a way that it now transmits new types of user data to external servers, it must again confirm that the user has reviewed and consented to these changes. If the user does not consent, the application should terminate or otherwise take steps to ensure that all

functions requiring the transmission of data are disabled.

These steps serve to guarantee that users understand how their data will be handled when they use an application, providing users with a sense of security and enhancing their trust in the application.

MainActivity.java

```
protected void onStart() {
        super.onStart();

        (some portions omitted)
        if (privacyPolicyAgreed <= VERSION_TO_SHOW_COMPREHENSIVE_AGREEMENT_ANEW) {
                // *** POINT *** On first launch (or application update), obtain broad consent to
 transmit user data that will be handled by the application.
                // When the application is updated, it is only necessary to renew the user's gran
t of broad consent if the updated application will handle new types of user data.

                ConfirmFragment dialog = ConfirmFragment.newInstance(
                        R.string.privacyPolicy, R.string.agreePrivacyPolicy,
                        DIALOG_TYPE_COMPREHENSIVE_AGREEMENT);
                dialog.setDialogListener(this);
                FragmentManager fragmentManager = getSupportFragmentManager();
                dialog.show(fragmentManager, "dialog");
        }
```

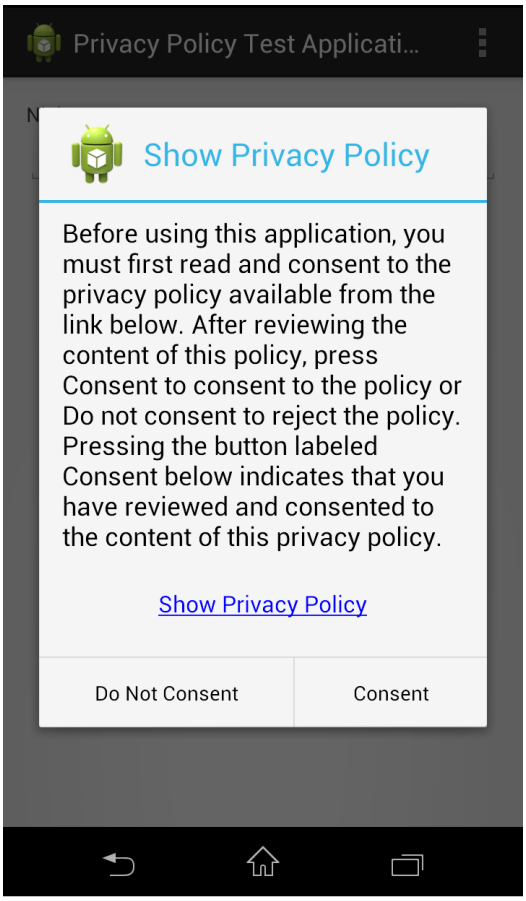


Figure 5.5-4 Example of broad consent

5.5.2.3. Obtain specific consent before transmitting user data that requires particularly delicate handling (Required)

When transmitting to external servers any user data that requires particularly delicate handling, an application must obtain advance consent (opt-in) from users for each such type of user data (or for each feature that involves the transmission of user data); this is in addition to the need to obtain general consent. If the user does not grant consent, the application must not send the corresponding data to the external server.

This ensures that users can obtain a more thorough understanding of the relationship between an application's features (and the services it provides) and the transmission of user data for which the user granted general consent; at the same time, application providers can expect to obtain user consent on the basis of more precise decision-making.

MainActivity.java

```
    public void onSendToServer(View view) {
            // *** POINT *** Obtain specific consent before transmitting user data that requires part
icularly delicate handling.
            ConfirmFragment dialog = ConfirmFragment.newInstance(R.string.sendLocation, R.string.cofi
rmSendLocation, DIALOG_TYPE_PRE_CONFIRMATION);
            dialog.setDialogListener(this);
            FragmentManager fragmentManager = getSupportFragmentManager();
            dialog.show(fragmentManager, "dialog");
    }
```

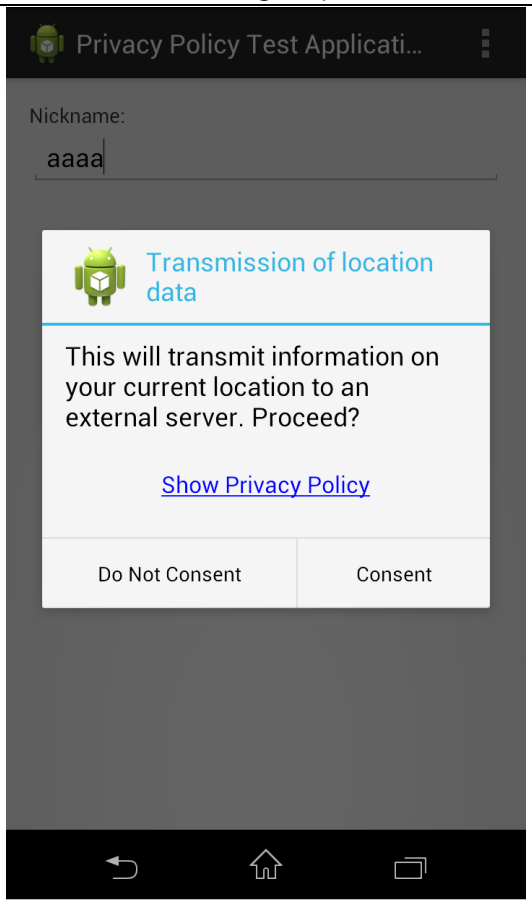


Figure 5.5-5 Example of specific consent

5.5.2.4. Provide methods by which the user can review the application privacy policy (Required)

In general, the Android application marketplace will provide links to application privacy policies for users to review before choosing to install the corresponding application. In addition to supporting this feature, it is important for applications to provide methods by which users can review application privacy policies after installing applications on their devices. It is particularly important to provide methods by which users can easily review application privacy policies in cases involving consent to transmit user data to external servers to assist users in making appropriate decisions.

MainActivity.java

```
    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
            switch (item.getItemId()) {
            case R.id.action_show_pp:
                    // *** POINT *** Provide methods by which the user can review the application pri
vacy policy.
                    Intent intent = new Intent();
                    intent.setClass(this, WebViewAssetsActivity.class);
                    startActivity(intent);
                    return true;
```

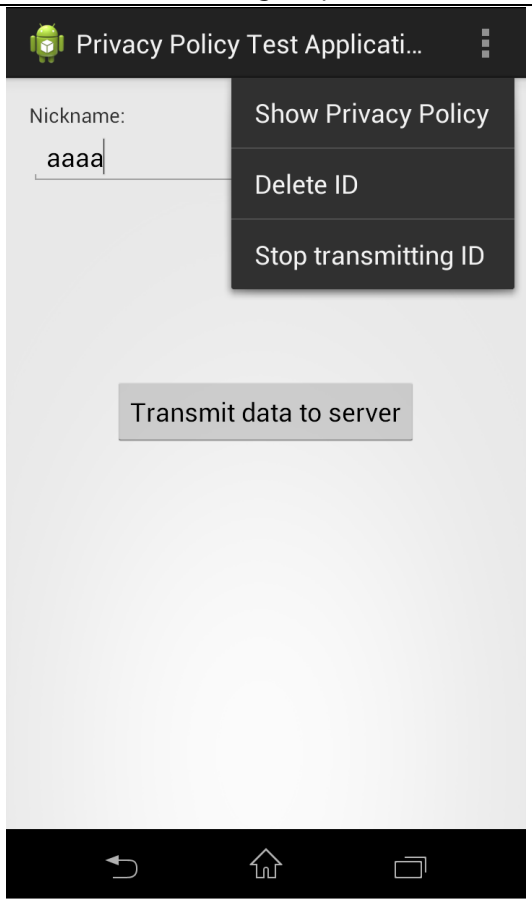



Figure 5.5-6 Context menu to show privacy policy

5.5.2.5. Place a summary version of the application privacy policy in the assets folder (Recommended)

It is a good idea to place a summary version of the application privacy policy in the assets folder to ensure that users may review it as necessary. Ensuring that the application privacy policy is present in the assets folder not only allows users to access it easily at any time, but also avoids the risk that users may see a counterfeit or corrupted version of the application privacy policy prepared by a malicious third party.

5.5.2.6. Provide methods by which transmitted data can be deleted and transmitting data can be stopped by user operations (Recommended)

It is a good idea to provide methods by which user data that has been transmitted to external servers can be deleted at the user's request. Similarly, in cases in which the application itself has stored user data (or a copy thereof) within the device, it is a good idea to provide users with methods for deleting this data. And, it is a good idea to provide methods by which transmitting user data can be stopped at the user's request.

This rule (recommendation) is codified by the "right to be forgotten" promoted in the EU; more generally, in the future it seems clear that various proposals will call for further strengthening the rights of users to have their data protected, and for this reason in these guidelines we recommend the provision of methods for the deletion of user data unless there is some specific reason to do

otherwise. And, regarding stop transmitting data, it is the one that is defined by the point of view "Do Not Track (deny track)" of the correspondence by the browser is progressing mainly.

MainActivity.java

```
    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
            switch (item.getItemId()) {
            (some portions omitted)
            case R.id.action_del_id:
                    // *** POINT *** Provide methods by which transmitted data can be deleted by user
operations.
                    new SendDataAsyncTack().execute(DEL_ID_URI, UserId);
                    return true;
            }
```

5.5.2.7. Separate device-specific IDs from UUIDs and cookies (Recommended)

IMEIs and other device-specific IDs should not be transmitted in ways that are tied to user data. Indeed, if a device -specific ID and a piece of user data are bundled together and released or leaked to public—even just once—it will be impossible subsequently to change that device -specific ID, whereupon it will be impossible (or at least difficult) to sever ties between the ID and the user data. In such cases, it is better to use UUIDs or cookies—that is, variable IDs that are regenerated each time based on random numbers—in place of device -specific IDs when transmitting together with user data. This allows an implementation of the notion, discussed above, of the “right to be forgotten.”

MainActivity.java

```
            @Override
            protected String doInBackground(String... params) {
                    // *** POINT *** Use UUIDs or cookies to keep track of user data
                    // In this sample we use an ID generated on the server side
                    SharedPreferences sp = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVA
TE);
                    UserId = sp.getString(ID_KEY, null);
                    if (UserId == null) {
                            // No token in SharedPreferences; fetch ID from server
                            try {
                                    UserId = NetworkUtil.getCookie(GET_ID_URI, "", "id");
                            } catch (IOException e) {
                                    // Catch exceptions such as certification errors
                                    extMessage = e.toString();
                            }

                            // Store the fetched ID in SharedPreferences
                            sp.edit().putString(ID_KEY, UserId).commit();
                    }
                    return UserId;
            }
```


5.5.2.8. If you will only be using user data within the device, notify the user that data will not be transmitted externally. (Recommended)

Even in cases in which user data will only be accessed temporarily within the user's device, it is a good idea to communicate this fact to the user to ensure that the user's understanding of the application's behavior remains full and transparent. More specifically, users should be informed that the user data accessed by an application will only be used within the device for a certain specific purpose and will not be stored or sent. Possible methods for communicating this content to users include specifying it within the description of the application on the application marketplace. Information that is only used temporarily within a device need not be discussed in the application privacy policy.

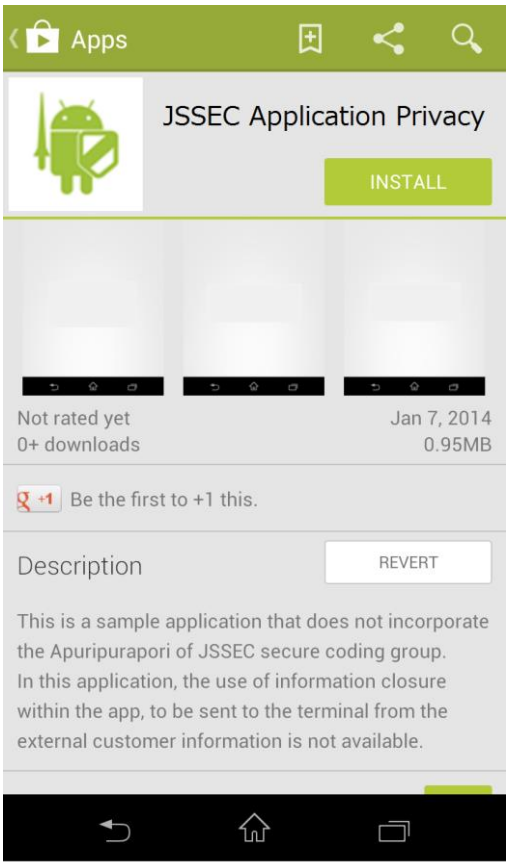


Figure 5.5-7 Description on the marketplace

5.5.3. Advanced Topics

5.5.3.1. Some background and context regarding privacy policies

For cases in which a smartphone application will obtain user data and transmit this data externally, it is necessary to prepare and display an application privacy policy to inform users of details such as the types of data will be collected and the ways in which the data will be handled. The content that should be included in an application privacy policy is detailed in the Smartphone Privacy Initiative advocated by JMIC's SPI. The primary objective of the application privacy policy should be to state clearly all types of user data that will be accessed by an application, the purposes for which the data will be used, where the data will be stored, and to what destinations the data will be transmitted.

A second document, separate from and required in addition to the application privacy policy, is the Enterprise Privacy Policy, which details how all user data gathered by a corporation from its various applications will be stored, managed, and disposed of. This Enterprise Privacy Policy corresponds to the privacy policy that would traditionally have been prepared to comply with Japan's Personal Information Protection Law.

A detailed description of proper methods for preparing and displaying privacy policies, together with a discussion of the roles played by the various different types of privacy policies, may be found in the document "A Discussion of the Creation and Presentation of Privacy Policies for JSSEC Smartphone Applications", available at this URL: http://www.jssec.org/event/20140206/03-1_app_policy.pdf (Japanese only).

5.5.3.2. Glossary of Terms

In the table below we define a number of terms that are used in these guidelines; these definitions are taken from the document "A Discussion of the Creation and Presentation of Privacy Policies for JSSEC Smartphone Applications" (http://www.jssec.org/event/20140206/03-1_app_policy.pdf) (Japanese only).

Table 5.5-1

Term	Description
Enterprise Privacy Policy	A privacy policy that defines a corporation's policies for protecting personal data. Created in accordance with Japan's Personal Information Protection Law.
Application Privacy Policy	An application-specific privacy policy. Created in accordance with the guidelines of the Smartphone Privacy Initiative (SPI) of Japan's Ministry of Internal Affairs and Communications (MIC). It is best to provide both summary and detailed versions containing easily understandable explanations.
Summary version of the Application Privacy Policy	A brief document that concisely summarizes what user information an application will use, for what purpose, and whether or not this information will be provided to third parties.
Detailed version of the Application Privacy Policy	A detailed document that complies with the 8 items specified by the Smartphone Privacy Initiative (SPI) and the Smartphone Privacy Initiative II (SPI II) of Japan's Ministry of Internal Affairs and Communications (MIC).

User data that is easy for users to change	Cookies, UUIDs, etc.
User data that is difficulty for users to change	IMEIs, IMSIs, ICCIDs, MAC addresses, OS-generated IDs, etc.
User data requiring particularly delicate handling	Location information, address books, telephone numbers, email addresses, etc.

5.5.3.3. Version-dependent differences in handling of Android IDs

The Android ID (Settings.Secure.ANDROID_ID) is a randomly-generated 64-bit number expressed as a hexadecimal character string that serves as an identifier to identify individual terminals (although duplicate identifiers are possible in extremely rare cases). For this reason, incorrect usage can create serious risks associated with user tracking, and thus special care must be taken when using Android IDs. However, the rules governing aspects such as ID generation and accessible ranges differ for terminals running Android 7.1 (API Level 25) versus terminals running Android 8.0 (API Level 26). In what follows we describe these differences.

Terminals running Android 7.1(API Level 25) or earlier

For terminals running Android 7.1(API Level 25) or earlier, only one Android ID value exists in a given terminal; this value may be accessed by all apps running on that terminal. However, note that, for terminals with multiuser support, separate values are generated for each user. Android IDs are generated upon the first startup of a terminal after shipping from the factory, and are newly regenerated upon each subsequent factory reset.

Terminals running Android 8.0 (API Level 26) or later

For terminals running Android 8.0 (API Level 26) or later, each app (developer) has its own distinct value, which may only be accessed by the app in question. More specifically, whereas the values used in Android 7.1 (API Level 25) and earlier were user-specific and terminal-specific but not app-specific, in Android 8.0 (API Level 26) and later versions the app signature is added to the list of elements used to generate unique values, so that apps with different signatures now have different Android ID values. (Apps with identical signatures have identical Android ID values.)

The occasions on which Android ID values are generated or modified remain essentially unchanged, but there are a few points to note, as discussed below.

- On package uninstallation / reinstallation:
  As long as the signature of the app remains unchanged, its Android ID will be unchanged after uninstalling and reinstalling. On the other hand, note that, if the key used as the signature is modified, the Android ID will be different after re-installation, even if the package name is unchanged.

- On updates to terminals running Android 8.0 (API Level 26) or later:
  If an app was already installed on a terminal running Android 7.1 (API Level 25) or earlier, the

Android ID value that may be obtained by the app remains unchanged after the terminal is updated to Android 8.0 (API Level 26) or later. However, this excludes cases in which apps are uninstalled and reinstalled after the update.

Note that all Android IDs are classified as *User information that is difficult for users to exchange* (as described in Section 5.5.3.2, *Glossary of Terms*), and thus—as noted at the beginning of this discussion—we recommend that similar levels of caution be employed when using Android IDs.

In the security world, the terms "confidentiality", "integrity", and "availability" are used in analyzing responses to threats. These three terms refer, respectively, to measures to prevent the third parties from viewing private data, protections to ensure that the data referenced by users has not been modified (or techniques for detecting when it has been falsified) and the ability of users to access services and data at all times. All three of these elements are important to consider when designing security protections. In particular, encryption techniques are frequently used to ensure confidentiality and integrity, and Android is equipped with a variety of cryptographic features to allow applications to realize confidentiality and integrity.

In this section we will use sample code to illustrate methods by which Android applications can securely implement encryption and decryption (to ensure confidentiality) and message authentication codes (MAC) or digital signatures (to ensure integrity).

5.6.1. Sample Code

A variety of cryptographic methods have been developed for specific purposes and conditions, including use cases such as encrypting and decrypting data (to ensure confidentiality) and detecting falsification of data (to ensure integrity). Here is sample code that is categorized into three broad groups of cryptography techniques on the basis of the purpose of each technology. The features of the cryptographic technology in each case should make it possible to choose an appropriate encryption method and key type. For cases in which more detailed considerations are necessary, see Section “5.6.3.1 Choosing encryption methods“.

Before designing an implementation that uses encryption technology, be sure to read Section “5.6.3.3 Measures to Protect against Vulnerabilities in Random-Number Generators“.

- Protecting data from third-party eavesdropping

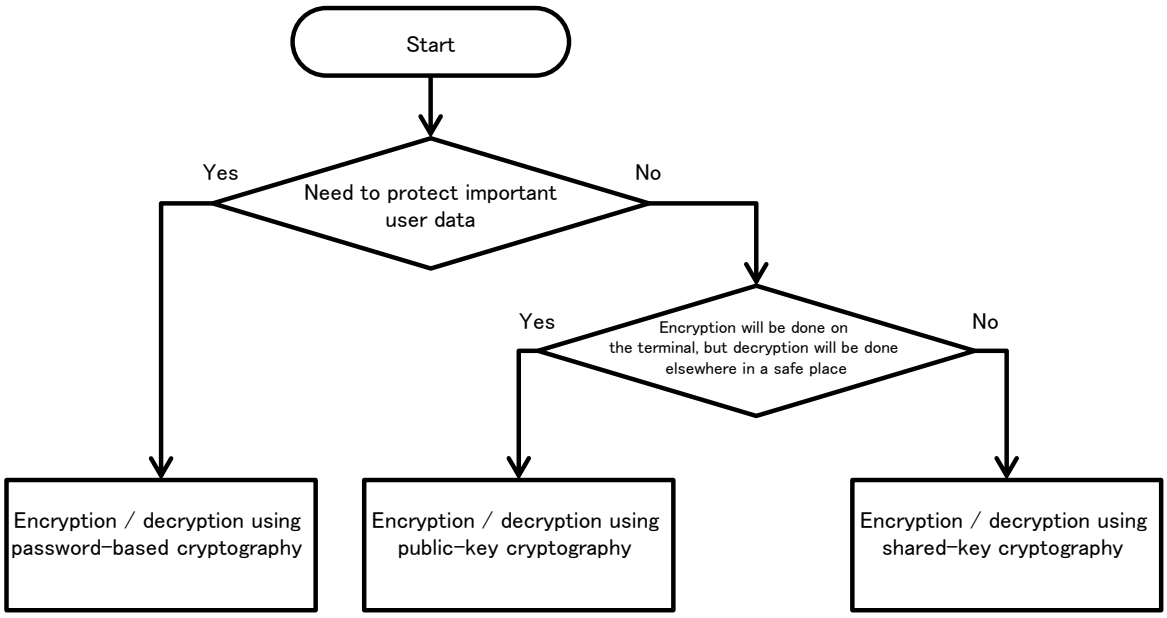


Figure 5.6-1

- Detecting falsification of data made by a third party

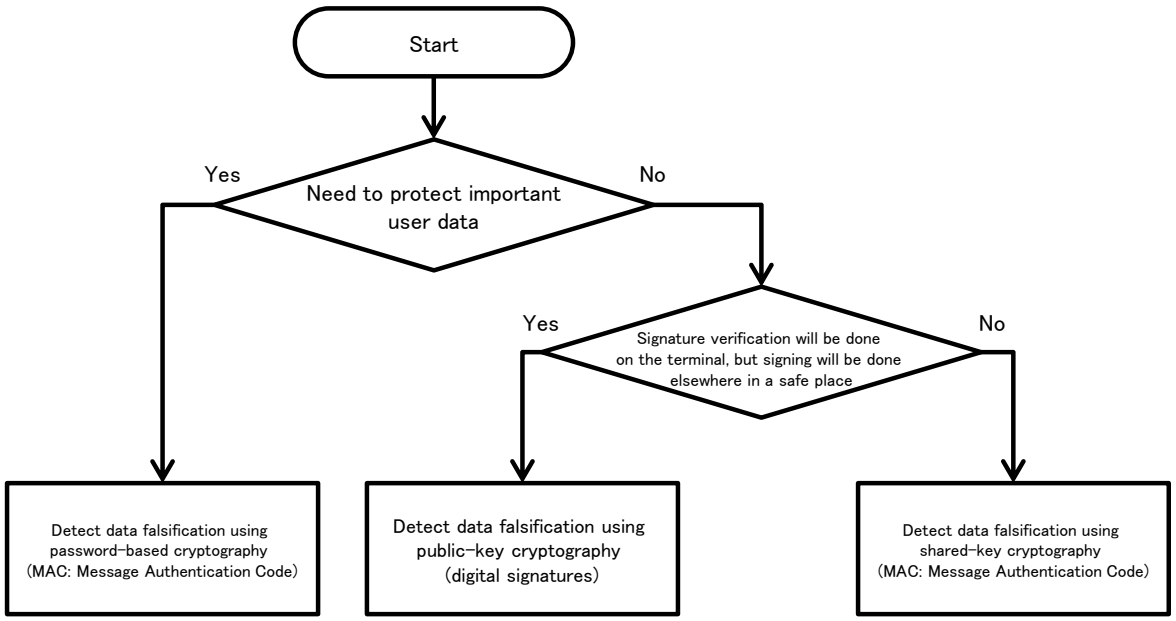


Figure 5.6-2

5.6.1.1. Encrypting and Decrypting With Password-based Keys

You may use password-based key encryption for the purpose of protecting a user's confidential data assets.

Points:

1. Explicitly specify the encryption mode and the padding.
2. Use strong encryption technologies (specifically, technologies that meet the relevant criteria), including algorithms, block cipher modes, and padding modes.
3. When generating a key from password, use Salt.
4. When generating a key from password, specify an appropriate hash iteration count.
5. Use a key of length sufficient to guarantee the strength of encryption.

AesCryptoPBEKey.java

```
package org.jssec.android.cryptsymmetricpasswordbasedkey;

import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;
import java.security.spec.InvalidKeySpecException;
import java.util.Arrays;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.PBEKeySpec;

public final class AesCryptoPBEKey {

    // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
    // *** POINT 2 *** Use strong encryption technologies (specifically, technologies that meet the rele
vant criteria), including algorithms, block cipher modes, and padding modes.
    // Parameters passed to the getInstance method of the Cipher class: Encryption algorithm, block encr
yption mode, padding rule
    // In this sample, we choose the following parameter values: encryption algorithm=AES, block encrypt
ion mode=CBC, padding rule=PKCS7Padding
    private static final String TRANSFORMATION = "AES/CBC/PKCS7Padding";

    //  A string used to fetch an instance of the class that generates the key
    private static final String KEY_GENERATOR_MODE = "PBEWITHSHA256AND128BITAES-CBC-BC";

    // *** POINT 3 *** When generating a key from a password, use Salt.
    // Salt length in bytes
    public static final int SALT_LENGTH_BYTES = 20;

    // *** POINT 4 *** When generating a key from a password, specify an appropriate hash iteration coun
t.
    // Set the number of mixing repetitions used when generating keys via PBE
    private static final int KEY_GEN_ITERATION_COUNT = 1024;

    // *** POINT 5 *** Use a key of length sufficient to guarantee the strength of encryption.
    // Key length in bits
    private static final int KEY_LENGTH_BITS = 128;

    private byte[] mIV = null;
    private byte[] mSalt = null;
```

```
    public byte[] getIV() {
        return mIV;
    }

    public byte[] getSalt() {
        return mSalt;
    }

    AesCryptoPBEKey(final byte[] iv, final byte[] salt) {
        mIV = iv;
        mSalt = salt;
    }

    AesCryptoPBEKey() {
        mIV = null;
        initSalt();
    }

    private void initSalt() {
        mSalt = new byte[SALT_LENGTH_BYTES];
        SecureRandom sr = new SecureRandom();
        sr.nextBytes(mSalt);
    }

    public final byte[] encrypt(final byte[] plain, final char[] password) {
        byte[] encrypted = null;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption technologies (specifically, technologies that meet t
he relevant criteria), including algorithms, modes, and padding.
            Cipher cipher = Cipher.getInstance(TRANSFORMATION);

            // *** POINT 3 *** When generating keys from passwords, use Salt.
            SecretKey secretKey = generateKey(password, mSalt);
            cipher.init(Cipher.ENCRYPT_MODE, secretKey);
            mIV = cipher.getIV();

            encrypted = cipher.doFinal(plain);
        } catch (NoSuchAlgorithmException e) {
        } catch (NoSuchPaddingException e) {
        } catch (InvalidKeyException e) {
        } catch (IllegalBlockSizeException e) {
        } catch (BadPaddingException e) {
        } finally {
        }

        return encrypted;
    }

    public final byte[] decrypt(final byte[] encrypted, final char[] password) {
        byte[] plain = null;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption technologies (specifically, technologies that meet t
he relevant criteria), including algorithms, block cipher modes, and padding modes.
            Cipher cipher = Cipher.getInstance(TRANSFORMATION);

            // *** POINT 3 *** When generating a key from a password, use Salt.
```



```
            SecretKey secretKey = generateKey(password, mSalt);
            IvParameterSpec ivParameterSpec = new IvParameterSpec(mIV);
            cipher.init(Cipher.DECRYPT_MODE, secretKey, ivParameterSpec);

            plain = cipher.doFinal(encrypted);
        } catch (NoSuchAlgorithmException e) {
        } catch (NoSuchPaddingException e) {
        } catch (InvalidKeyException e) {
        } catch (InvalidAlgorithmParameterException e) {
        } catch (IllegalBlockSizeException e) {
        } catch (BadPaddingException e) {
        } finally {
        }

        return plain;
    }

    private static final SecretKey generateKey(final char[] password, final byte[] salt) {
        SecretKey secretKey = null;
        PBEKeySpec keySpec = null;

        try {
            // *** POINT 2 *** Use strong encryption technologies (specifically, technologies that meet t
he relevant criteria), including algorithms, block cipher modes, and padding modes.
            // Fetch an instance of the class that generates the key
            // In this example, we use a KeyFactory that uses SHA256 to generate AES-CBC 128-bit keys.
            SecretKeyFactory secretKeyFactory = SecretKeyFactory.getInstance(KEY_GENERATOR_MODE);

            // *** POINT 3 *** When generating a key from a password, use Salt.
            // *** POINT 4 *** When generating a key from a password, specify an appropriate hash iterati
on count.
            // *** POINT 5 *** Use a key of length sufficient to guarantee the strength of encryption.
            keySpec = new PBEKeySpec(password, salt, KEY_GEN_ITERATION_COUNT, KEY_LENGTH_BITS);
            // Clear password
            Arrays.fill(password, '?');
            // Generate the key
            secretKey = secretKeyFactory.generateSecret(keySpec);
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeySpecException e) {
        } finally {
            keySpec.clearPassword();
        }

        return secretKey;
    }
}
```

5.6.1.2. Encrypting and Decrypting With Public Keys

In some cases, only data encryption will be performed –using a stored public key– on the application side, while decryption is performed in a separate safe location (such as a server) under a private key. In cases such as this, it is possible to use public-key (asymmetric-key) encryption.

Points:

1. Explicitly specify the encryption mode and the padding
2. Use strong encryption methods (specifically, technologies that meet the relevant criteria), including algorithms, block cipher modes, and padding modes.
3. Use a key of length sufficient to guarantee the strength of encryption.

RsaCryptoAsymmetricKey.java

```
package org.jssec.android.cryptasymmetrickey;

import java.security.InvalidKeyException;
import java.security.KeyFactory;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.interfaces.RSAPublicKey;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.PKCS8EncodedKeySpec;
import java.security.spec.X509EncodedKeySpec;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;

public final class RsaCryptoAsymmetricKey {

    // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
    // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the relevant
criteria), including algorithms, block cipher modes, and padding modes..
    // Parameters passed to getInstance method of the Cipher class: Encryption algorithm, block encrypti
on mode, padding rule
    // In this sample, we choose the following parameter values: encryption algorithm=RSA, block encrypt
ion mode=NONE, padding rule=OAEPPADDING.
    private static final String TRANSFORMATION = "RSA/NONE/OAEPPADDING";

    // encryption algorithm
    private static final String KEY_ALGORITHM = "RSA";

    // *** POINT 3 *** Use a key of length sufficient to guarantee the strength of encryption.
    // Check the length of the key
    private static final int MIN_KEY_LENGTH = 2000;

    RsaCryptoAsymmetricKey() {
    }

    public final byte[] encrypt(final byte[] plain, final byte[] keyData) {
        byte[] encrypted = null;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes..
            Cipher cipher = Cipher.getInstance(TRANSFORMATION);

            PublicKey publicKey = generatePubKey(keyData);
            if (publicKey != null) {
                cipher.init(Cipher.ENCRYPT_MODE, publicKey);
                encrypted = cipher.doFinal(plain);
```



```
            }
        } catch (NoSuchAlgorithmException e) {
        } catch (NoSuchPaddingException e) {
        } catch (InvalidKeyException e) {
        } catch (IllegalBlockSizeException e) {
        } catch (BadPaddingException e) {
        } finally {
        }

        return encrypted;
    }

    public final byte[] decrypt(final byte[] encrypted, final byte[] keyData) {
        // In general, decryption procedures should be implemented on the server side;
        // however, in this sample code we have implemented decryption processing within the application
 to ensure confirmation of proper execution.
        // When using this sample code in real-world applications, be careful not to retain any private k
eys within the application.

        byte[] plain = null;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes..
            Cipher cipher = Cipher.getInstance(TRANSFORMATION);

            PrivateKey privateKey = generatePriKey(keyData);
            cipher.init(Cipher.DECRYPT_MODE, privateKey);

            plain = cipher.doFinal(encrypted);
        } catch (NoSuchAlgorithmException e) {
        } catch (NoSuchPaddingException e) {
        } catch (InvalidKeyException e) {
        } catch (IllegalBlockSizeException e) {
        } catch (BadPaddingException e) {
        } finally {
        }

        return plain;
    }

    private static final PublicKey generatePubKey(final byte[] keyData) {
        PublicKey publicKey = null;
        KeyFactory keyFactory = null;

        try {
            keyFactory = KeyFactory.getInstance(KEY_ALGORITHM);
            publicKey = keyFactory.generatePublic(new X509EncodedKeySpec(keyData));
        } catch (IllegalArgumentException e) {
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeySpecException e) {
        } finally {
        }

        // *** POINT 3 *** Use a key of length sufficient to guarantee the strength of encryption.
        // Check the length of the key
        if (publicKey instanceof RSAPublicKey) {
            int len = ((RSAPublicKey) publicKey).getModulus().bitLength();
            if (len < MIN_KEY_LENGTH) {
```

```
                publicKey = null;
            }
        }

        return publicKey;
    }

    private static final PrivateKey generatePriKey(final byte[] keyData) {
        PrivateKey privateKey = null;
        KeyFactory keyFactory = null;

        try {
            keyFactory = KeyFactory.getInstance(KEY_ALGORITHM);
            privateKey = keyFactory.generatePrivate(new PKCS8EncodedKeySpec(keyData));
        } catch (IllegalArgumentException e) {
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeySpecException e) {
        } finally {
        }

        return privateKey;
    }
}
```

5.6.1.3. Encrypting and Decrypting Using Pre Shared Keys

Pre shared keys may be used when working with large data sets or to protect the confidentiality of an application's or a user's assets.

Points:

1. Explicitly specify the encryption mode and the padding
2. Use strong encryption methods (specifically, technologies that meet the relevant criteria), including algorithms, block cipher modes, and padding modes.
3. Use a key of length sufficient to guarantee the strength of encryption.

AesCryptoPreSharedKey.java

```
package org.jssec.android.cryptsymmetricpresharedkey;

import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;

public final class AesCryptoPreSharedKey {

    // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
    // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the relevant
```



```
criteria), including algorithms, block cipher modes, and padding modes.
    // Parameters passed to getInstance method of the Cipher class: Encryption algorithm, block encrypti
on mode, padding rule
    // In this sample, we choose the following parameter values: encryption algorithm=AES, block encrypt
ion mode=CBC, padding rule=PKCS7Padding
    private static final String TRANSFORMATION = "AES/CBC/PKCS7Padding";

    // Encryption algorithm
    private static final String KEY_ALGORITHM = "AES";

    // Length of IV in bytes
    public static final int IV_LENGTH_BYTES = 16;

    // *** POINT 3 *** Use a key of length sufficient to guarantee the strength of encryption
    // Check the length of the key
    private static final int MIN_KEY_LENGTH_BYTES = 16;

    private byte[] mIV = null;

    public byte[] getIV() {
        return mIV;
    }

    AesCryptoPreSharedKey(final byte[] iv) {
        mIV = iv;
    }

    AesCryptoPreSharedKey() {
    }

    public final byte[] encrypt(final byte[] keyData, final byte[] plain) {
        byte[] encrypted = null;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes.
            Cipher cipher = Cipher.getInstance(TRANSFORMATION);

            SecretKey secretKey = generateKey(keyData);
            if (secretKey != null) {
                cipher.init(Cipher.ENCRYPT_MODE, secretKey);
                mIV = cipher.getIV();

                encrypted = cipher.doFinal(plain);
            }
        } catch (NoSuchAlgorithmException e) {
        } catch (NoSuchPaddingException e) {
        } catch (InvalidKeyException e) {
        } catch (IllegalBlockSizeException e) {
        } catch (BadPaddingException e) {
        } finally {
        }

        return encrypted;
    }

    public final byte[] decrypt(final byte[] keyData, final byte[] encrypted) {
        byte[] plain = null;
```

```
        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes.
            Cipher cipher = Cipher.getInstance(TRANSFORMATION);

            SecretKey secretKey = generateKey(keyData);
            if (secretKey != null) {
                IvParameterSpec ivParameterSpec = new IvParameterSpec(mIV);
                cipher.init(Cipher.DECRYPT_MODE, secretKey, ivParameterSpec);

                plain = cipher.doFinal(encrypted);
            }
        } catch (NoSuchAlgorithmException e) {
        } catch (NoSuchPaddingException e) {
        } catch (InvalidKeyException e) {
        } catch (InvalidAlgorithmParameterException e) {
        } catch (IllegalBlockSizeException e) {
        } catch (BadPaddingException e) {
        } finally {
        }

        return plain;
    }

    private static final SecretKey generateKey(final byte[] keyData) {
        SecretKey secretKey = null;

        try {
            // *** POINT 3 *** Use a key of length sufficient to guarantee the strength of encryption
            if (keyData.length >= MIN_KEY_LENGTH_BYTES) {
                // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet th
e relevant criteria), including algorithms, block cipher modes, and padding modes.
                secretKey = new SecretKeySpec(keyData, KEY_ALGORITHM);
            }
        } catch (IllegalArgumentException e) {
        } finally {
        }

        return secretKey;
    }
}
```


5.6.1.4. Using Password-based Keys to Detect Data Falsification

You may use password-based (shared-key) encryption to verify the integrity of a user's data.

Points:

1. Explicitly specify the encryption mode and the padding.
2. Use strong encryption methods (specifically, technologies that meet the relevant criteria), including algorithms, block cipher modes, and padding modes.
3. When generating a key from a password, use Salt.
4. When generating a key from a password, specify an appropriate hash iteration count.
5. Use a key of length sufficient to guarantee the MAC strength.

HmacPBEKey.java

```
package org.jssec.android.signsymmetricpasswordbasedkey;

import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;
import java.security.spec.InvalidKeySpecException;
import java.util.Arrays;

import javax.crypto.Mac;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.PBEKeySpec;

public final class HmacPBEKey {

    // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
    // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the relevant
criteria), including algorithms, block cipher modes, and padding modes.
    // Parameters passed to the getInstance method of the Mac class: Authentication mode
    private static final String TRANSFORMATION = "PBEWITHHMACSHA1";

    // A string used to fetch an instance of the class that generates the key
    private static final String KEY_GENERATOR_MODE = "PBEWITHHMACSHA1";

    // *** POINT 3 *** When generating a key from a password, use Salt.
    // Salt length in bytes
    public static final int SALT_LENGTH_BYTES = 20;

    // *** POINT 4 *** When generating a key from a password, specify an appropriate hash iteration coun
t.
    // Set the number of mixing repetitions used when generating keys via PBE
    private static final int KEY_GEN_ITERATION_COUNT = 1024;

    // *** POINT 5 *** Use a key of length sufficient to guarantee the MAC strength.
    // Key length in bits
    private static final int KEY_LENGTH_BITS = 160;

    private byte[] mSalt = null;

    public byte[] getSalt() {
        return mSalt;
    }
```

```
    HmacPBEKey() {
        initSalt();
    }

    HmacPBEKey(final byte[] salt) {
        mSalt = salt;
    }

    private void initSalt() {
        mSalt = new byte[SALT_LENGTH_BYTES];
        SecureRandom sr = new SecureRandom();
        sr.nextBytes(mSalt);
    }

    public final byte[] sign(final byte[] plain, final char[] password) {
        return calculate(plain, password);
    }

    private final byte[] calculate(final byte[] plain, final char[] password) {
        byte[] hmac = null;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes.
            Mac mac = Mac.getInstance(TRANSFORMATION);

            // *** POINT 3 *** When generating a key from a password, use Salt.
            SecretKey secretKey = generateKey(password, mSalt);
            mac.init(secretKey);

            hmac = mac.doFinal(plain);
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeyException e) {
        } finally {
        }

        return hmac;
    }

    public final boolean verify(final byte[] hmac, final byte[] plain, final char[] password) {

        byte[] hmacForPlain = calculate(plain, password);

        if (Arrays.equals(hmac, hmacForPlain)) {
            return true;
        }
        return false;
    }

    private static final SecretKey generateKey(final char[] password, final byte[] salt) {
        SecretKey secretKey = null;
        PBEKeySpec keySpec = null;

        try {
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes.
            // Fetch an instance of the class that generates the key
            // In this example, we use a KeyFactory that uses SHA1 to generate AES-CBC 128-bit keys.
```



```
            SecretKeyFactory secretKeyFactory = SecretKeyFactory.getInstance(KEY_GENERATOR_MODE);

            // *** POINT 3 *** When generating a key from a password, use Salt.
            // *** POINT 4 *** When generating a key from a password, specify an appropriate hash iterati
on count.
            // *** POINT 5 *** Use a key of length sufficient to guarantee the MAC strength.
            keySpec = new PBEKeySpec(password, salt, KEY_GEN_ITERATION_COUNT, KEY_LENGTH_BITS);
            // Clear password
            Arrays.fill(password, '?');
            // Generate the key
            secretKey = secretKeyFactory.generateSecret(keySpec);
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeySpecException e) {
        } finally {
            keySpec.clearPassword();
        }

        return secretKey;
    }

}
```

5.6.1.5. Using Public Keys to Detect Data Falsification

When working with data whose signature is determined using private keys stored in distinct, secure locations (such as servers), you may utilize public-key (asymmetric-key) encryption for applications involving the storage of public keys on the application side solely for the purpose of authenticating data signatures.

Points:

1. Explicitly specify the encryption mode and the padding.
2. Use strong encryption methods (specifically, technologies that meet the relevant criteria), including algorithms, block cipher modes, and padding modes.
3. Use a key of length sufficient to guarantee the signature strength.

RsaSignAsymmetricKey.java

```
package org.jssec.android.signasymmetrickey;

import java.security.InvalidKeyException;
import java.security.KeyFactory;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.Signature;
import java.security.SignatureException;
import java.security.interfaces.RSAPublicKey;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.PKCS8EncodedKeySpec;
import java.security.spec.X509EncodedKeySpec;

public final class RsaSignAsymmetricKey {

    // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
    // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the relevant
```

```
criteria), including algorithms, block cipher modes, and padding modes.
    // Parameters passed to the getInstance method of the Cipher class: Encryption algorithm, block encr
yption mode, padding rule
    // In this sample, we choose the following parameter values: encryption algorithm=RSA, block encrypt
ion mode=NONE, padding rule=OAEPPADDING.
    private static final String TRANSFORMATION = "SHA256withRSA";

    // encryption algorithm
    private static final String KEY_ALGORITHM = "RSA";

    // *** POINT 3 *** Use a key of length sufficient to guarantee the signature strength.
    // Check the length of the key
    private static final int MIN_KEY_LENGTH = 2000;

    RsaSignAsymmetricKey() {
    }

    public final byte[] sign(final byte[] plain, final byte[] keyData) {
        // In general, signature procedures should be implemented on the server side;
        // however, in this sample code we have implemented signature processing within the application
to ensure confirmation of proper execution.
        // When using this sample code in real-world applications, be careful not to retain any private k
eys within the application.

        byte[] sign = null;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes.
            Signature signature = Signature.getInstance(TRANSFORMATION);

            PrivateKey privateKey = generatePriKey(keyData);
            signature.initSign(privateKey);
            signature.update(plain);

            sign = signature.sign();
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeyException e) {
        } catch (SignatureException e) {
        } finally {
        }

        return sign;
    }

    public final boolean verify(final byte[] sign, final byte[] plain, final byte[] keyData) {

        boolean ret = false;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes.
            Signature signature = Signature.getInstance(TRANSFORMATION);

            PublicKey publicKey = generatePubKey(keyData);
            signature.initVerify(publicKey);
            signature.update(plain);
```



```
            ret = signature.verify(sign);

        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeyException e) {
        } catch (SignatureException e) {
        } finally {
        }

        return ret;
    }

    private static final PublicKey generatePubKey(final byte[] keyData) {
        PublicKey publicKey = null;
        KeyFactory keyFactory = null;

        try {
            keyFactory = KeyFactory.getInstance(KEY_ALGORITHM);
            publicKey = keyFactory.generatePublic(new X509EncodedKeySpec(keyData));
        } catch (IllegalArgumentException e) {
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeySpecException e) {
        } finally {
        }

        // *** POINT 3 *** Use a key of length sufficient to guarantee the signature strength.
        // Check the length of the key
        if (publicKey instanceof RSAPublicKey) {
            int len = ((RSAPublicKey) publicKey).getModulus().bitLength();
            if (len < MIN_KEY_LENGTH) {
                publicKey = null;
            }
        }

        return publicKey;
    }

    private static final PrivateKey generatePriKey(final byte[] keyData) {
        PrivateKey privateKey = null;
        KeyFactory keyFactory = null;

        try {
            keyFactory = KeyFactory.getInstance(KEY_ALGORITHM);
            privateKey = keyFactory.generatePrivate(new PKCS8EncodedKeySpec(keyData));
        } catch (IllegalArgumentException e) {
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeySpecException e) {
        } finally {
        }

        return privateKey;
    }
}
```

5.6.1.6. Using Pre Shared Keys to Detect Data Falsification

You may use pre-shared keys to verify the integrity of application assets or user assets.

Points:

1. Explicitly specify the encryption mode and the padding.
2. Use strong encryption methods (specifically, technologies that meet the relevant criteria), including algorithms, block cipher modes, and padding modes.
3. Use a key of length sufficient to guarantee the MAC strength.

HmacPreSharedKey.java

```
package org.jssec.android.signsymmetricpresharedkey;

import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.util.Arrays;

import javax.crypto.Mac;
import javax.crypto.SecretKey;
import javax.crypto.spec.SecretKeySpec;

public final class HmacPreSharedKey {

    // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
    // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the relevant
criteria), including algorithms, block cipher modes, and padding modes.
    // Parameters passed to the getInstance method of the Mac class: Authentication mode
    private static final String TRANSFORMATION = "HmacSHA256";

    // Encryption algorithm
    private static final String KEY_ALGORITHM = "HmacSHA256";

    // *** POINT 3 *** Use a key of length sufficient to guarantee the MAC strength.
    // Check the length of the key
    private static final int MIN_KEY_LENGTH_BYTES = 16;

    HmacPreSharedKey() {
    }

    public final byte[] sign(final byte[] plain, final byte[] keyData) {
        return calculate(plain, keyData);
    }

    public final byte[] calculate(final byte[] plain, final byte[] keyData) {
        byte[] hmac = null;

        try {
            // *** POINT 1 *** Explicitly specify the encryption mode and the padding.
            // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet the re
levant criteria), including algorithms, block cipher modes, and padding modes.
            Mac mac = Mac.getInstance(TRANSFORMATION);

            SecretKey secretKey = generateKey(keyData);
            if (secretKey != null) {
                mac.init(secretKey);

                hmac = mac.doFinal(plain);
            }
        } catch (NoSuchAlgorithmException e) {
        } catch (InvalidKeyException e) {
        } finally {
        }
```



```
        return hmac;
    }

    public final boolean verify(final byte[] hmac, final byte[] plain, final byte[] keyData) {
        byte[] hmacForPlain = calculate(plain, keyData);

        if (hmacForPlain != null && Arrays.equals(hmac, hmacForPlain)) {
            return true;
        }

        return false;
    }

    private static final SecretKey generateKey(final byte[] keyData) {
        SecretKey secretKey = null;

        try {
            // *** POINT 3 *** Use a key of length sufficient to guarantee the MAC strength.
            if (keyData.length >= MIN_KEY_LENGTH_BYTES) {
                // *** POINT 2 *** Use strong encryption methods (specifically, technologies that meet th
e relevant criteria), including algorithms, block cipher modes, and padding modes.
                secretKey = new SecretKeySpec(keyData, KEY_ALGORITHM);
            }
        } catch (IllegalArgumentException e) {
        } finally {
        }

        return secretKey;
    }
}
```

5.6.2. Rule Book

When using encryption technology, it is important to obey the following rules.

1.	When Specifying an Encryption Algorithm, Explicitly Specify the Encryption Mode and the Padding (Required)
2.	Use Strong Algorithms (Specifically, Algorithms that Meet the Relevant Criteria) (Required)
3.	When Using Password-based Encryption, Do Not Store Passwords on Device (Required)
4.	When Generating Keys from Passwords, Use Salt (Required)
5.	When Generating Key from Password, Specify Appropriate Hash Iteration Count (Required)
6.	Take Steps to Increase the Strengths of Passwords (Recommended)

5.6.2.1. When Specifying an Encryption Algorithm, Explicitly Specify the Encryption Mode and the Padding (Required)

When using cryptographic technologies such as encryption and data verification, it is important that the encryption mode and the padding be explicitly specified. When using encryption in Android application development, you will primarily use the Cipher class within java.crypto. To use the Cipher class, you will first create an instance of Cipher class object by specifying the type of encryption to use. This specification is called a Transformation, and there are two formats in which Transformations may be specified:

- “algorithm/mode/padding”
- “algorithm”

In the latter case, the encryption mode and the padding will be implicitly set to the appropriate default values for the encryption service provider that Android may access. These default values are chosen to prioritize convenience and compatibility and in some cases may not be particularly secure choices. For this reason, to ensure proper security protections it is mandatory to use the former of the two formats, in which the encryption mode and padding are explicitly specified.

5.6.2.2. Use Strong Algorithms (Specifically, Algorithms that Meet the Relevant Criteria) (Required)

When using cryptographic technologies it is important to choose strong algorithms which meet certain criteria. In addition, in cases where an algorithm allows multiple key lengths, it is important to consider the application’s full product lifetime and to choose keys of length sufficient to guarantee security. Moreover, for some encryption modes and padding modes there exist known strategies of attack; it is important to make choices that are robust against such threats.

Indeed, choosing weak encryption methods can have disastrous consequences; for example, files which were supposedly encrypted to prevent eavesdropping by a third party may in fact be only ineffectually protected and may allow third-party eavesdropping. Because the continual progress of IT leads to continual improvements in encryption-analysis technologies, it is crucial to consider and select algorithms that can guarantee security throughout the entire period during which you expect

an application to remain in operation.

Standards for actual encryption technologies differ from country to country, as detailed in the tables below.

Table 5.6-1 NIST(USA) NIST SP800-57

Algorithm Lifetime	Symmetric-key encryption	Asymmetric-key encryption	Elliptic-curve encryption	HASH (digital signature, HASH)	HASH (HMA, KD, random-number generation)
～2010	80	1024	160	160	160
～2030	112	2048	224	224	160
2030～	128	3072	256	256	160

Unit: bit

Table 5.6-2 ECRYPT II (EU)

Algorithm lifetime	Symmetric-key encryption	Asymmetric-key encryption	Elliptic-curve encryption	HASH
2009～2012	80	1248	160	160
2009～2020	96	1776	192	192
2009～2030	112	2432	224	224
2009～2040	128	3248	256	256
2009～	256	15424	512	512

Unit: bit

Table 5.6-3 CRYPTREC(Japan) CRYPTREC Ciphers List

Technology family		Name
Public-key cryptography	Signature	DSA,ECDSA,RSA-PSS,RSASSA-PKCS1-V1_5
	Confidentiality	RSA-OAEP
	Key sharing	DH,ECDH
Shared-key cryptography	64 bit block encryption	3-key Triple DES
	128 bit block encryption	AES,Camellia
	Stream encryption	KCipher-2
Hash function		SHA-256,SHA-384,SHA-512
Encryption usage mode	Cipher mode	CBC,CFB,CTR,OFB
	Authenticated cipher modes	CCM,GCM
Message authentication codes		CMAC,HMAC
Entity authentication		ISO/IEC 9798-2,ISO/IEC 9798-3

5.6.2.3. When Using Password-based Encryption, Do Not Store Passwords on Device (Required)

In password-based encryption, when generating an encryption key based on a password input by a user, do not store the password within the device. The advantage of password-based encryption is that it eliminates the need to manage encryption keys; storing the password on the device eliminates this advantage. Needless to say, storing passwords on a device invites the risk of eavesdropping by other applications, and thus storing passwords on devices is also unacceptable for security reasons.

5.6.2.4. When Generating Keys from Passwords, Use Salt (Required)

In password-based encryption, when generating an encryption key based on a password input by a user, always use Salt. In addition, if you are providing features to different users within the same device, use a different Salt for each user. The reason for this is that, if you generate encryption keys using only a simple hash function without using Salt, the passwords may be easily recovered using a technique known as a "rainbow table." When Salt is applied, keys generated from the same password will be distinct (different hash values), preventing the use of a rainbow table to search for keys.

(Sample) When generating keys from passwords, use salt

```
    public final byte[] encrypt(final byte[] plain, final char[] password) {
            byte[] encrypted = null;

            try {
                    // *** POINT *** Explicitly specify the encryption mode and the padding.
                    // *** POINT *** Use strong encryption methods (specifically, technologies that m
eet the relevant criteria), including algorithms, block cipher modes, and padding modes.
                    Cipher cipher = Cipher.getInstance(TRANSFORMATION);

                    // *** POINT *** When generating keys from passwords, use Salt.
                    SecretKey secretKey = generateKey(password, mSalt);
```

5.6.2.5. When Generating Key from Password, Specify Appropriate Hash Iteration Count (Required)

In password-based encryption, when generating an encryption key based on a password input by a user, you will choose a number of times for the hashing procedure to be repeated during the process of key generation ("stretching"); it is important to specify this number large enough to ensure security. In general, the iteration count equal to 1,000 or greater is considered sufficient. If you are using the key to protect even more valuable assets, specify a count equal to 1,000,000 or greater. Because the processing time required for a single computation of the hash function is minuscule, it may be easy for attackers to launch brute-force attacks. Thus, by using the stretching method – in which hash processing is repeated many times – we can purposely ensure that the process consumes significant time and thus that brute-force attacks are more costly. Note that the number of stretching repetitions will also affect your application's processing speed, so take care in choosing an appropriate value.

(Sample) When generating key from password, Set hash iteration counts

```
      private static final SecretKey generateKey(final char[] password, final byte[] salt) {
               SecretKey secretKey = null;
               PBEKeySpec keySpec = null;

                        (Omit)

                        // *** POINT *** When generating a key from password, use Salt.
                        // *** POINT *** When generating a key from password, specify an appropriate hash
 iteration count.
                        // *** POINT *** Use a key of length sufficient to guarantee the strength of encr
yption.                          keySpec = new PBEKeySpec(password, salt, KEY_GEN_ITERATION_COUNT, KEY_LE
NGTH_BITS);
```

5.6.2.6. Take Steps to Increase the Strengths of Passwords (Recommended)

In password-based encryption, when generating an encryption key based on a password input by a user, the strength of the generated key is strongly affected by the strength of the user's password, and thus it is desirable to take steps to strengthen the passwords received from users. For example, you might require that passwords be at least 8 characters long and contain multiple types of characters—perhaps at least one letter, one numeral, and one symbol.

5.6.3. Advanced Topics

5.6.3.1. Choosing encryption methods

In the above sample codes, we showed implementation examples involving three types of cryptographic methods each for encryption and decryption and for detecting data falsification. You may use “Figure 5.6-1“, “Figure 5.6-2“ to make a coarse-grained choice of which cryptographic method to use based on your application. On the other hand, more fine-tuned choices of cryptographic methods require more detailed comparisons of the features of various methods. In what follows we consider some of these comparisons.

- Comparison of cryptographic methods for encryption and decryption

Public-key cryptography has high processing cost and thus is not well suited for large-scale data processing. However, because the keys used for encryption and for decryption are different, it is relatively easy to manage keys in cases where you handle only the public key on the application side (i.e. you only perform encryption) and perform decryption in a separate (secure) location. Shared-key cryptography is an all-purpose encryption scheme with few limitations, but in this case the same key is used for encryption and decryption, and thus it is necessary to store the key securely within the application, making key management difficult. Password-based cryptography (shared-key cryptography based on a password) generates keys from user-specified passwords, obviating the need to store key-related secrets within devices. This method is used for applications protecting only user assets but not application assets. Because the strength of the encryption depends on the strength of the password, it is necessary to choose passwords whose complexity grows in proportion to the value of assets to be protected. Please refer to “5.6.2.6 Take Steps to Increase the Strengths of Passwords (Recommended)“.

Table 5.6-4 Comparison of cryptographic methods for encryption and decryption

Encryption method / Item	Public key	Shared key	Password-based
Processing of large-scale data	NO (processing cost too high)	OK	OK
Protecting application (or service) assets	OK	OK	NO (allows eavesdropping by users)
Protecting user assets	OK	OK	OK
Strength of encryption	Depends on key length	Depends on key length	Depends on strength of password, on Salt, and on the number of hash repetitions
Key storage	Easy (only public keys)	Difficult	Easy
Processing carried out by application	Encryption (decryption is done on servers or	Encryption and decryption	Encryption and decryption

	elsewhere)		

- Comparison of cryptographic methods for detecting data falsification

The comparison here is similar to that discussed above for encryption and decryption, with the exception that that table item corresponding to data size is no longer relevant.

Table 5.6-5 Comparison of cryptographic methods for detecting data falsification

Encryption method / Item	Public key	Shared key	Password-based
Protecting application (or service) assets	OK	OK	NO (allows falsification by users)
Protecting user assets	OK	OK	OK
Strength of encryption	Depends on key length	Depends on key length	Depends on strength of password, on Salt, and on the number of hash repetitions
Key storage	Easy (only public keys)	Difficult Please refer to "5.6.3.4Protecting Key"	Easy
Processing carried out by application	Signature verification (signing is done on servers or elsewhere)	MAC computation; MAC verification	MAC computation; MAC verification

MAC: Message authentication code

Note that these guidelines are primarily concerned with the protection of assets deemed low-level or medium-level assets according to the classification discussed in Section "3.1.3 Asset Classification and Protective Countermeasures". Because the use of encryption involves the consideration of a greater number of issues—such as the problem of key storage—than other preventative measures (such as access controls), encryption should only be considered for cases in which assets cannot be adequately protected within the Android OS security mode.

5.6.3.2. Generation of random numbers

When using cryptographic technologies, it is extremely important to choose strong encryption algorithms and encryption modes and sufficiently long keys in order to ensure the security of the data handled by applications and services. However, even if all of these choices are made appropriately, the strength of the security guaranteed by the algorithms in use plummets immediately to zero when the keys that form the linchpin of the security protocol are leaked or guessed.

Even for the initial vector (IV) used for shared-key encryption under AES and similar protocols, or the Salt used for password-based encryption, large biases can make it easy for third parties to launch attacks, heightening the risk of exposure to data leakage or corruption. To prevent such situations, it is necessary to generate keys and IVs in such a way as to make it difficult for third parties to guess their values, and random numbers play an immensely important role in ensuring the realization of this imperative. A device that generates random numbers is called a random-number generator. Whereas hardware random-number generators (RNGs) may use sensors or other devices to produce random numbers by measuring natural phenomena that cannot be predicted or reproduced, it is more common to encounter software-implemented random-number generators, known as pseudorandom-number generators (PRNGS).

In Android applications, random numbers of sufficient security for use in encryption may be generated via the SecureRandom class. The functionality of the SecureRandom class is provided by an implementation known as Provider. It is possible for multiple Providers (implementations) to exist internally, and if no Provider is clearly specified than the default Provider will be selected. For this reason, it is also possible to use SecureRandom in implementation without being aware of the existence of Providers. In what follows we offer examples to demonstrate the use of SecureRandom.

Note that SecureRandom may exhibit a number of weaknesses depending on the Android version, requiring preventative measures to be put in place in implementations. Please refer to "5.6.3.3 Measures to Protect against Vulnerabilities in Random-Number Generators".

Using SecureRandom (using the default implementation)

```
import java.security.SecureRandom;
[...]
      SecureRandom random = new SecureRandom();
      byte[] randomBuf = new byte [128];

      random.nextBytes(randomBuf);
[...]
```

Using SecureRandom (with explicit specification of the algorithm)

```
import java.security.SecureRandom;
[...]
      SecureRandom random = SecureRandom.getInstance("SHA1PRNG");
      byte[] randomBuf = new byte [128];

      random.nextBytes(randomBuf);
[...]
```

Using SecureRandom (with explicit specification of the implementation (Provider))

```
import java.security.SecureRandom;
[...]
      SecureRandom random = SecureRandom.getInstance("SHA1PRNG", "Crypto");
      byte[] randomBuf = new byte [128];

      random.nextBytes(randomBuf);
[...]
```

The pseudorandom-number generators found in programs like SecureRandom typically operate on

the basis of a process like that illustrated in "Figure 5.6-3 Inner process of pseudorandom number generator". A random number seed is entered to initialize the internal state; thereafter, the internal state is updated each time a random number is generated, allowing the generation of a sequence of random numbers.

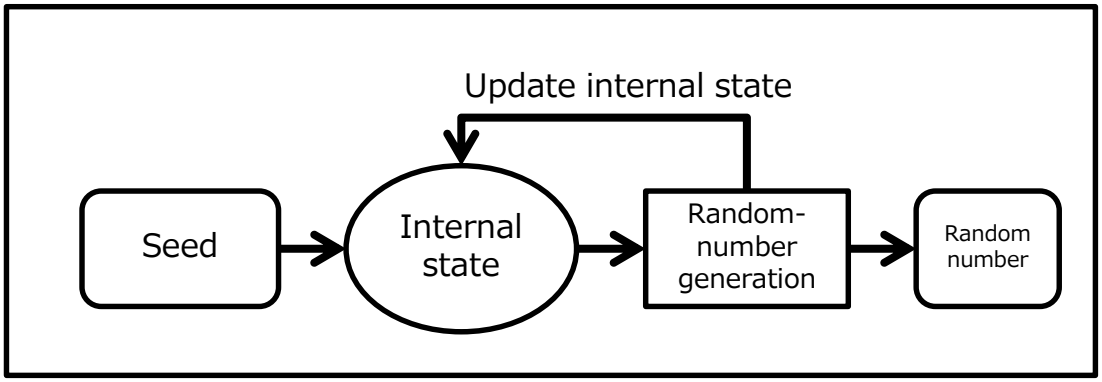


Figure 5.6-3 Inner process of pseudorandom number generator

Random number seeds

The seed plays an extremely important role in a pseudorandom number generator (PRNG).

As noted above, PRNGs must be initialized by specifying a seed. Thereafter, the process used to generate random numbers is a deterministic algorithm, so if you specify the same seed you will get the same sequence of random numbers. This means that if a third party gains access to (that is, eavesdrops upon) or guesses the seed of a PRNG, he can produce the same sequence of random numbers, thus destroying the properties of confidentiality and integrity that the random numbers provide.

For this reason, the seed of a random number generator is itself a highly confidential piece of information—and one which must be chosen in such a way as to be impossible to predict or guess. For example, time information or device-specific data (such as a MAC address, IMEI, or Android ID) should not be used to construct RNG seeds. On many Android devices, /dev/urandom or /dev/random is available, and the default implementation of SecureRandom provided by Android uses these device files to determine seeds for random number generators. As far as confidentiality is concerned, as long as the RNG seed exists only in memory, there is little risk of discovery by third parties with the exception of malware tools that acquire root privileges. If you need to implement security measures that remain effective even on rooted devices, consult an expert in secure design and implementation.

The internal state of a pseudorandom number generator

The internal state of a pseudorandom number generator is initialized by the seed, then updated each time a random number is generated. Just as for the case of PRNGs initialized by the same seed, two PRNGs with the same internal state will subsequently produce precisely the same sequence of random numbers. Consequently, it is also important to protect the internal state against eavesdropping by third parties. However, because the internal state exists in memory, there is little

risk of discovery by third parties except in cases involving malware tools that acquire root access. If you need to implement security measures that remain effective even on rooted devices, consult an expert in secure design and implementation.

5.6.3.3. Measures to Protect against Vulnerabilities in Random-Number Generators

The "Crypto" Provider implementation of SecureRandom, found in Android versions 4.3.x and earlier, suffered from the defect of insufficient entropy (randomness) of the internal state. In particular, in Android versions 4.1.x and earlier, the "Crypto" Provider was the only available implementation of SecureRandom, and thus most applications that use SecureRandom either directly or indirectly were affected by this vulnerability. Similarly, the "AndroidOpenSSL" Provider offered as the default implementation of SecureRandom in Android versions 4.2 and later exhibited the defect that the majority of the data items used by OpenSSL as random-number seeds were shared between applications (Android versions 4.2.x—4.3.x), creating a vulnerability in which any one application can easily predict the random numbers generated by other applications. The table below details the impact of the vulnerabilities present in various versions of Android OS.

Table 5.6-6 Android OS version and feature influenced by each vulnerabilities

Vulnerability / Android OS	Insufficient entropy in the "Crypto" Provider implementation of SecureRandom	Can guess the random number seeds used by OpenSSL in other applications
Android 4.1.x and before	-Default implementation of SecureRandom -Explicit use of Crypto Provider -Encryption functionality provided by the Cipher class -HTTPS communication functionality, etc.	No impact
Android 4.2 - 4.3.x	-Use a clearly identified Crypto Provider	-Default implementation of SecureRandom -Explicit use of AndroidOpenSSL Provider -Direct use of random-number generation functionality provided by OpenSSL -Encryption functionality provided by the Cipher class -HTTPS communication functionality, etc.
Android 4.4 and later	No impact	No impact

Since August 2013, patches that remove these Android OS vulnerabilities have been distributed by Google to its partners (device makers, etc.)
However, these vulnerabilities associated with SecureRandom affected a wide range of

applications—including encryption functionality and HTTPS communication functionality—and presumably many devices remain unpatched. For this reason, when designing applications targeted at Android 4.3.x and earlier, we recommend that you incorporate the countermeasures (implementations) discussed in the following site.

http://android-developers.blogspot.jp/2013/08/some-securerandom-thoughts.html

5.6.3.4. Protecting Key

When using encryption techniques to ensure the security (confidentiality and integrity) of sensitive data, even the most robust encryption algorithm and key lengths will not protect data from third-party attacks if the data content of the keys themselves are readily available. For this reason, the proper handling of keys is among the most important items to consider when using encryption. Of course, depending on the level of the assets you are attempting to protect, the proper handling of keys may require extremely sophisticated design and implementation techniques which exceed the scope of these guidelines. Here we can only offer some basic ideas regarding the secure handling of keys for various applications and key storage locations; our discussion does not extend to specific implementation methods, and as necessary we recommend that you consult an expert in secure design and implementation for Android.

To begin, "Figure 5.6-4 Places of encrypt keys and strategies for protecting them." illustrates the various places in which keys used for encryption and related purposes in Android smartphones and tablets may exist, and outlines strategies for protecting them.

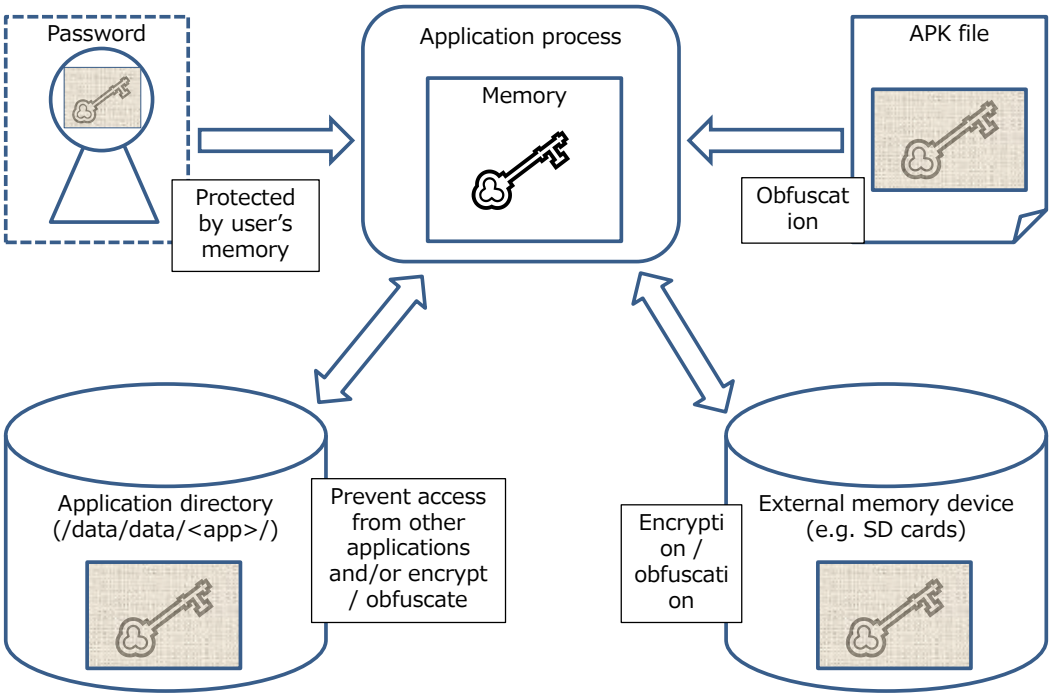


Figure 5.6-4 Places of encrypt keys and strategies for protecting them.

The table below summarizes the asset classes of the assets protected by keys, as well as the protection policies appropriate for various asset owners. For more information on asset classes,

please refer to "3.1.3 Asset Classification and Protective Countermeasures".

Table 5.6-7 Asset classification and protective countermeasures

Asset owner	Device User		Application / Service Provider	
Asset level	High	Medium / Low	High	Medium / Low
Key storage location	Protection policy			
User's memory	Improve password strength		Disallow the use of user passwords	
Application directory (non-public storage)	Encryption or obfuscation of key data	Forbid read/write operations from outside the application	Encryption or obfuscation of key data	Forbid read/write operations from outside the application
APK file	Obfuscation of key data **Note:** Be aware that most Java obfuscation tools, such as Proguard, do not obfuscate data (character) strings.			
SD card or elsewhere (public storage)	Encryption or obfuscation of key data			

In what follows, we will augment the discussion of protective measures appropriate for the various places in which keys may be stored.

Keys stored in a user's memory

Here we are considering password-based encryption. When keys are generated from passwords, the key storage location is the user's memory, so there is no danger of leakage due to malware. However, depending on the strength of the password, it may be easy to reproduce keys. For this reason, it is necessary to take steps—similar to those taken when asking users to specify service login passwords—to ensure the strength of passwords; for example, passwords may be restricted by the UI, or warning messages may be used. Please refer to "5.6.2.6 Take Steps to Increase the Strengths of Passwords (Recommended)". Of course, when passwords are stored in a user's memory one must keep in mind the possibility that the password will be forgotten. To ensure that data may be recovered in the event of a forgotten password, it is necessary to store backup data in a secure location other than the device (for example, on a server).

Keys stored in application directories

When keys are stored in Private mode in application directories, the key data cannot be read by other applications. In addition, if the application has disabled backup functionality, users will also be unable to access the data. Thus, when storing keys used to protect application assets in application directories, you should disable backups.
However, if you also need to protect keys from applications or users with root privileges, you must

encrypt or obfuscate the keys. For keys used to protect user assets, you may use password-based encryption. For keys used to encrypt application assets that you wish to keep private from users as well, you must store the key used for key encryption in an APK file, and the key data must be obfuscated.

Keys stored in APK Files

Because data in APK files may be accessed, in general this is not an appropriate place to store confidential data such as keys. When storing keys in APK files, you must obfuscate the key data and take steps to ensure that the data may not be easily read from the APK file.

Keys stored in public storage locations (such as SD cards)

Because public storage can be accessed by all applications, in general it is not an appropriate place to store confidential data such as passwords. When storing keys in public locations, it is necessary to encrypt or obfuscate the key data to ensure that the data cannot be easily accessed. See also the protections suggested above under “Keys stored in application directories” for cases in which keys must also be protected from applications or users with root privileges.

Handling of keys within process memory

When using the cryptographic technologies available in Android, key data that have been encrypted or obfuscated somewhere other than the application process shown in the figure above must be decrypted (or, for password-based keys, generated) in advance of the encryption procedure; in this case, key data will reside in process memory in unencrypted form. On the other hand, the memory of an application process may not generally be read by other applications, so if the asset class falls within the range covered by these guidelines there is no particular need to take specific steps to ensure security. In cases where—due to the specific objective in question or to the level of the assets handled by an application—it is unacceptable for key data to appear in unencrypted form (even though they are present that way in process memory), it may be necessary to resort to obfuscation or other techniques for key data and encryption logic. However, these methods are difficult to realize at the Java level; instead, you will use obfuscation tools at the JNI level. Such measures fall outside the scope of these guidelines; consult an expert in secure design and implementation.

5.6.3.5. Addressing Vulnerabilities with Security Provider from Google Play Services

Google Play Services (Version 5.0 and later) provides a framework known as *Provider Installer* that may be used to address vulnerabilities in Security Provider.

First, Security Provider provides implementations of various encryption-related algorithms based on Java Cryptography Architecture (JCA). These Security Provider algorithms may be used via classes such as Cipher, Signature, and Mac to make use of encryption technology in Android apps. In general, rapid response is required whenever vulnerabilities are discovered in encryption-technology-related implementations. Indeed, the exploitation of such vulnerabilities for malicious purposes could result in major damage. Because encryption technologies are also relevant for Security Provider, it is desirable that revisions designed to address vulnerabilities be reflected as quickly as possible.

The most common method of reflecting Security Provider revisions is to use device updates. The process of reflecting revisions via device updates begins with the device manufacturer preparing an update, after which users apply this update to their devices. Thus, the question of whether or not an app has access to an up-to-date version of Security Provider—including the most recent revisions—depends in practice on compliance from both manufacturers and users. In contrast, using Provider Installer from Google Play Services ensures that apps have access to automatically-updated versions of Security Provider.

With Provider Installer from Google Play Services, calling Provider Installer from an app allows access to Security Provider as provided by Google Play Services. Google Play Services is automatically updated via the Google Play Store, and thus the Security Provider provided by Provider Installer will be automatically updated to the latest version, with no dependence on compliance from manufacturers or users.

Sample code that calls Provider Installer is shown below.

Call Provider Installer

```
import com.google.android.gms.common.GooglePlayServicesUtil;
import com.google.android.gms.security.ProviderInstaller;

public class MainActivity extends Activity
        implements ProviderInstaller.ProviderInstallListener {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);

        ProviderInstaller.installIfNeededAsync(this, this);
        setContentView(R.layout.activity_main);
    }

    @Override
    public void onProviderInstalled() {
        // Called when Security Provider is the latest version, or when installation completes
    }

    @Override
```



```
    public void onProviderInstallFailed(int errorCode, Intent recoveryIntent) {
        GoogleApiAvailability.getInstance().showErrorNotification(this, errorCode);

    }
}
```

5.7. Using fingerprint authentication features

A variety of methods for biological authentication are currently under research and development, with methods using facial information and vocal signatures particularly prominent. Among these methods, methods for using fingerprint authentication to identify individuals have been used since ancient times, and are used today for purposes such as signatures (by thumbprint) and crime investigation. Applications of fingerprinting have also advanced in several areas of the computer world, and in recent years these methods have begun to enjoy wide recognition as highly convenient techniques (offering advantages such as ease of input) for use in areas such as identifying the owner of a smartphone (primarily for unlocking screens).

Capitalizing on these trends, Android 6.0(API Level 23) incorporates a framework for fingerprint authentication on terminals, which allows apps to make use of fingerprint authentication features to identify individuals. In what follows we discuss some security precautions to keep in mind when using fingerprint authentication.

5.7.1. Sample Code

Below we present sample code to allow an app to use Android's fingerprint authentication features.

Points:

1. Declare the use of the USE_FINGERPRINT permission
2. Obtain an instance from the "AndroidKeyStore" Provider
3. Notify users that fingerprint registration will be required to create a key
4. When creating (registering) keys, use an encryption algorithm that is not vulnerable (meets standards)
5. When creating (registering) keys, enable requests for user (fingerprint) authentication (do not specify the duration over which authentication is enabled)
6. Design your app on the assumption that the status of fingerprint registration will change between when keys are created and when keys are used
7. Restrict encrypted data to items that can be restored (replaced) by methods other than fingerprint authentication

MainActivity.java

```
package authentication.fingerprint.android.jssec.org.fingerprintauthentication;

import android.app.AlertDialog;
import android.hardware.fingerprint.FingerprintManager;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.util.Base64;
import android.view.View;
import android.widget.Button;
import android.widget.TextView;

import java.text.SimpleDateFormat;
```



```
import java.util.Date;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;

public class MainActivity extends AppCompatActivity {

    private FingerprintAuthentication mFingerprintAuthentication;
    private static final String SENSITIVE_DATA = "sensitive data";

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        mFingerprintAuthentication = new FingerprintAuthentication(this);

        Button button_fingerprint_auth = (Button) findViewById(R.id.button_fingerprint_auth);
        button_fingerprint_auth.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                if (!mFingerprintAuthentication.isAuthenticating()) {
                    if (authenticateByFingerprint()) {
                        showEncryptedData(null);
                        setAuthenticationState(true);
                    }
                } else {
                    mFingerprintAuthentication.cancel();
                }
            }
        });
    }

    private boolean authenticateByFingerprint() {

        if (!mFingerprintAuthentication.isFingerprintHardwareDetected()) {
            // Terminal is not equipped with a fingerprint sensor
            return false;
        }

        if (!mFingerprintAuthentication.isFingerprintAuthAvailable()) {
            // *** POINT 3 *** Notify users that fingerprint registration will be required to create a ke
y
            new AlertDialog.Builder(this)
                    .setTitle(R.string.app_name)
                    .setMessage("No fingerprint information has been registered.¥n" +
                            "Click ¥"Security¥" on the Settings menu to register fingerprints. ¥n" +
                            "Registering fingerprints allows easy authentication.")
                    .setPositiveButton("OK", null)
                    .show();
            return false;
        }

        // Callback that receives the results of fingerprint authentication
        FingerprintManager.AuthenticationCallback callback = new FingerprintManager.AuthenticationCallb
ack() {
            @Override
            public void onAuthenticationError(int errorCode, CharSequence errString) {
                showMessage(errString, R.color.colorError);
```

```
                reset();
            }

            @Override
            public void onAuthenticationHelp(int helpCode, CharSequence helpString) {
                showMessage(helpString, R.color.colorHelp);
            }

            @Override
            public void onAuthenticationSucceeded(FingerprintManager.AuthenticationResult result) {

                Cipher cipher = result.getCryptoObject().getCipher();
                try {
                    // *** POINT 7*** Restrict encrypted data to items that can be restored (replaced) by
methods other than fingerprint authentication
                    byte[] encrypted = cipher.doFinal(SENSITIVE_DATA.getBytes());
                    showEncryptedData(encrypted);
                } catch (IllegalBlockSizeException | BadPaddingException e) {
                }

                showMessage(getString(R.string.fingerprint_auth_succeeded), R.color.colorAuthenticated);
                reset();
            }

            @Override
            public void onAuthenticationFailed() {
                showMessage(getString(R.string.fingerprint_auth_failed), R.color.colorError);
            }
        };

        if (mFingerprintAuthentication.startAuthentication(callback)) {
            showMessage(getString(R.string.fingerprint_processing), R.color.colorNormal);
            return true;
        }

        return false;
    }


    private void setAuthenticationState(boolean authenticating) {
        Button button = (Button) findViewById(R.id.button_fingerprint_auth);
        button.setText(authenticating ? R.string.cancel : R.string.authenticate);
    }

    private void showEncryptedData(byte[] encrypted) {
        TextView textView = (TextView) findViewById(R.id.encryptedData);
        if (encrypted != null) {
            textView.setText(Base64.encodeToString(encrypted, 0));
        } else {
            textView.setText("");
        }
    }

    private String getCurrentTimeString() {
        long currentTimeMillis = System.currentTimeMillis();
        Date date = new Date(currentTimeMillis);
        SimpleDateFormat simpleDateFormat = new SimpleDateFormat("HH:mm:ss.SSS");

        return simpleDateFormat.format(date);
    }
```



```
    private void showMessage(CharSequence msg, int colorId) {
        TextView textView = (TextView) findViewById(R.id.textView);
        textView.setText(getCurrentTimeString() + " :¥n" + msg);
        textView.setTextColor(getResources().getColor(colorId, null));
    }

    private void reset() {
        setAuthenticationState(false);
    }
}
```

FingerprintAuthentication.java

```
package authentication.fingerprint.android.jssec.org.fingerprintauthentication;

import android.app.KeyguardManager;
import android.content.Context;
import android.hardware.fingerprint.FingerprintManager;
import android.os.CancellationSignal;
import android.security.keystore.KeyGenParameterSpec;
import android.security.keystore.KeyInfo;
import android.security.keystore.KeyPermanentlyInvalidatedException;
import android.security.keystore.KeyProperties;

import java.io.IOException;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.KeyStore;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.UnrecoverableKeyException;
import java.security.cert.CertificateException;
import java.security.spec.InvalidKeySpecException;

import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;

public class FingerprintAuthentication {
    private static final String KEY_NAME = "KeyForFingerprintAuthentication";
    private static final String PROVIDER_NAME = "AndroidKeyStore";

    private KeyguardManager mKeyguardManager;
    private FingerprintManager mFingerprintManager;
    private CancellationSignal mCancellationSignal;
    private KeyStore mKeyStore;
    private KeyGenerator mKeyGenerator;
    private Cipher mCipher;

    public FingerprintAuthentication(Context context) {
        mKeyguardManager = (KeyguardManager) context.getSystemService(Context.KEYGUARD_SERVICE);
        mFingerprintManager = (FingerprintManager) context.getSystemService(Context.FINGERPRINT_SERVICE
);
        reset();
    }
```

```
    public boolean startAuthentication(final FingerprintManager.AuthenticationCallback callback) {
        if (!generateAndStoreKey())
            return false;

        if (!initializeCipherObject())
            return false;

        FingerprintManager.CryptoObject cryptoObject = new FingerprintManager.CryptoObject(mCipher);

        mCancellationSignal = new CancellationSignal();

        // Callback to receive the results of fingerprint authentication
        FingerprintManager.AuthenticationCallback hook = new FingerprintManager.AuthenticationCallback(
) {
            @Override
            public void onAuthenticationError(int errorCode, CharSequence errString) {
                if (callback != null) callback.onAuthenticationError(errorCode, errString);
                reset();
            }

            @Override
            public void onAuthenticationHelp(int helpCode, CharSequence helpString) {
                if (callback != null) callback.onAuthenticationHelp(helpCode, helpString);
            }

            @Override
            public void onAuthenticationSucceeded(FingerprintManager.AuthenticationResult result) {
                if (callback != null) callback.onAuthenticationSucceeded(result);
                reset();
            }

            @Override
            public void onAuthenticationFailed() {
                if (callback != null) callback.onAuthenticationFailed();
            }
        };

        // Execute fingerprint authentication
        mFingerprintManager.authenticate(cryptoObject, mCancellationSignal, 0, hook, null);

        return true;
    }

    public boolean isAuthenticating() {
        return mCancellationSignal != null && !mCancellationSignal.isCanceled();
    }

    public void cancel() {
        if (mCancellationSignal != null) {
            if (!mCancellationSignal.isCanceled())
                mCancellationSignal.cancel();
        }
    }

    private void reset() {
        try {
            // *** POINT 2 ***  Obtain an instance from the "AndroidKeyStore" Provider
            mKeyStore = KeyStore.getInstance(PROVIDER_NAME);
            mKeyGenerator = KeyGenerator.getInstance(KeyProperties.KEY_ALGORITHM_AES, PROVIDER_NAME);
```



```
            mCipher = Cipher.getInstance(KeyProperties.KEY_ALGORITHM_AES
                    + "/" + KeyProperties.BLOCK_MODE_CBC
                    + "/" + KeyProperties.ENCRYPTION_PADDING_PKCS7);
        } catch (KeyStoreException | NoSuchPaddingException
                | NoSuchAlgorithmException | NoSuchProviderException e) {
            throw new RuntimeException("failed to get cipher instances", e);
        }
        mCancellationSignal = null;
    }

    public boolean isFingerprintAuthAvailable() {
        return (mKeyguardManager.isKeyguardSecure()
                && mFingerprintManager.hasEnrolledFingerprints()) ? true : false;
    }

    public boolean isFingerprintHardwareDetected() {
        return mFingerprintManager.isHardwareDetected();
    }

    private boolean generateAndStoreKey() {
        try {
            mKeyStore.load(null);
            if (mKeyStore.containsAlias(KEY_NAME))
                mKeyStore.deleteEntry(KEY_NAME);
            mKeyGenerator.init(
                    // *** POINT 4 *** When creating (registering) keys, use an encryption algorithm that
 is not vulnerable (meets standards)
                    new KeyGenParameterSpec.Builder(KEY_NAME, KeyProperties.PURPOSE_ENCRYPT)
                            .setBlockModes(KeyProperties.BLOCK_MODE_CBC)
                            .setEncryptionPaddings(KeyProperties.ENCRYPTION_PADDING_PKCS7)
                            // *** POINT 5 *** When creating (registering) keys, enable requests for user
(fingerprint) authentication (do not specify the duration over which authentication is enabled)
                            .setUserAuthenticationRequired(true)
                            .build());
            // Generate a key and store it in Keystore(AndroidKeyStore)
            mKeyGenerator.generateKey();
            return true;
        } catch (IllegalStateException e) {
            return false;
        } catch (NoSuchAlgorithmException | InvalidAlgorithmParameterException
                | CertificateException | KeyStoreException | IOException e) {
            throw new RuntimeException("failed to generate a key", e);
        }
    }

    private boolean initializeCipherObject() {
        try {
            mKeyStore.load(null);
            SecretKey key = (SecretKey) mKeyStore.getKey(KEY_NAME, null);
            SecretKeyFactory factory = SecretKeyFactory.getInstance(KeyProperties.KEY_ALGORITHM_AES, PRO
VIDER_NAME);
            KeyInfo info = (KeyInfo) factory.getKeySpec(key, KeyInfo.class);

            mCipher.init(Cipher.ENCRYPT_MODE, key);
            return true;
        } catch (KeyPermanentlyInvalidatedException e) {
            // *** POINT 6 *** Design your app on the assumption that the status of fingerprint registrat
ion will change between when keys are created and when keys are used
            return false;
        } catch (KeyStoreException | CertificateException | UnrecoverableKeyException | IOException
```

```
                | NoSuchAlgorithmException | InvalidKeySpecException | NoSuchProviderException | Invalid
KeyException e) {
            throw new RuntimeException("failed to init Cipher", e);
        }
    }

}
```

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="authentication.fingerprint.android.jssec.org.fingerprintauthentication" >

    <!-- +++ POINT 1 *** Declare the use of the USE_FINGERPRINT permission -->
    <uses-permission android:name="android.permission.USE_FINGERPRINT" />

    <application
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:supportsRtl="true"
        android:theme="@style/AppTheme" >
        <activity
            android:name=".MainActivity"
            android:screenOrientation="portrait" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>
```


5.7.2. Rule Book

Observe the following rules when using fingerprint authentication.

1.	When creating (registering) keys, use an encryption algorithm that is not vulnerable (meets standards). (Required)
2.	Restrict encrypted data to items that can be restored (replaced) by methods other than fingerprint authentication (Required)
3.	Notify users that fingerprint registration will be required to create a key (Recommended)

5.7.2.1. When creating (registering) keys, use an encryption algorithm that is not vulnerable (meets standards). (Required)

Like the password keys and public keys discussed in Section “5.6 Using Cryptography”, when using fingerprint authentication features to create keys it is necessary to use encryption algorithms that are not vulnerable---that is, algorithms that meet certain standards adequate to prevent eavesdropping by third parties. Indeed, safe and non-vulnerable choices must be made not only for encryption algorithms but also for encryption modes and padding.

For more information on selecting algorithms, see Section ”5.6.2.2 Use Strong Algorithms (Specifically, Algorithms that Meet the Relevant Criteria) (Required)”.

5.7.2.2. Restrict encrypted data to items that can be restored (replaced) by methods other than fingerprint authentication (Required)

When an app uses fingerprint authentication features for the encryption of data within the app, the app must be designed in such a way as to allow the data to be recovered (replaced) by methods other than fingerprint authentication.

In general, the use of biological information entails various problems---including secrecy, the difficulty of making modifications, and erroneous identifications---and it is thus best to avoid relying solely on biological information for authentication.

For example, suppose that data internal to an app is encrypted with a key generated using fingerprint authentication features, but that the fingerprint data stored within the terminal is subsequently deleted by the user. Then the key used to encrypt the data is not available for use, nor is it possible to copy the data. If the data cannot be recovered by some means other than fingerprint-authentication functionality, there is substantial risk that the data will be made useless.

Moreover, the deletion of fingerprint information is not the only scenario in which keys created using fingerprint authentication functions can become unusable. In Nexus5X, if fingerprint authentication

features are used to create a key and this key is then newly registered as an addition to the fingerprint information, keys created earlier have been observed to become unusable.[47] In addition, one cannot exclude the possibility that a key which would ordinarily allow correct use may become unusable due to erroneous identification by a fingerprint sensor.

5.7.2.3. Notify users that fingerprint registration will be required to create a key (Recommended)

In order to create a key using fingerprint authentication, it is necessary that a user's fingerprints be registered on the terminal. When designing apps to guide users to the Settings menu to encourage fingerprint registration, developers must keep in mind that fingerprints represent important personal data, and it is desirable to explain to users why it is necessary or convenient for the app to use fingerprint information.

Notify users the fingerprint registration will be required

```
if (!mFingerprintAuthentication.isFingerprintAuthAvailable()) {
    // **Point** Notify users that fingerprint registration will be required to create a key
    new AlertDialog.Builder(this)
            .setTitle(R.string.app_name)
            .setMessage("No fingerprint information has been registered.¥n" +
                    " Click ¥"Security¥" on the Settings menu to register fingerprints.¥n" +
                    " Registering fingerprints allows easy authentication.")
            .setPositiveButton("OK", null)
            .show();
    return false;
}
```

[47] Information current as of the September 1, 2016 version. This may be revised in the future.

5.7.3. Advanced Topics

5.7.3.1. Preconditions for the use of fingerprint authentication features by Android apps

The following two conditions must be satisfied in order for an app to use fingerprint authentication.

- User fingerprints must be registered within the terminal.
- An (application-specific) key must be associated with registered fingerprints.

Registering user fingerprints

User fingerprint information can only be registered via the "Security" option in the Settings menu; ordinary applications may not perform the fingerprint registration procedure. For this reason, if no fingerprints have been registered when an app attempts to use fingerprint authentication features, the app must guide the user to the Settings menu and encourage the user to register fingerprints. At this time, it is desirable for the app to offer the user some explanation of why it is necessary and convenient to use fingerprint information.

In addition, as a necessary precondition for fingerprint registration to be possible, the terminal must be configured with an alternative screen-locking mechanism. If the screen lock is disabled in a state in which fingerprints have been registered in the terminal, the registered fingerprint information will be deleted.

Creating and registering keys

To associate a key with fingerprints registered in a terminal, use a KeyStore instance provided by an "AndroidKeyStore" Provider to create and register a new key or to register an existing key.

To create a key associated with fingerprint information, configure the parameter settings when creating a KeyGenerator to enable requests for user authentication.

Creating and registering a key associated with fingerprint information

```
    try {
        // Obtain an instance from the "AndroidKeyStore" Provider
        KeyGenerator keyGenerator = KeyGenerator.getInstance(KeyProperties.KEY_ALGORITHM_AES, "AndroidK
eyStore");
        keyGenerator.init(
            new KeyGenParameterSpec.Builder(KEY_NAME, KeyProperties.PURPOSE_ENCRYPT)
            .setBlockModes(KeyProperties.BLOCK_MODE_CBC)
            .setEncryptionPaddings(KeyProperties.ENCRYPTION_PADDING_PKCS7)
            .setUserAuthenticationRequired(true)  // Enable requests for user (fingerprint) authenticati
on
            .build());
        keyGenerator.generateKey();
    } catch (IllegalStateException e) {
        // no fingerprints have been registered in this terminal
        throw new RuntimeException("No fingerprint registered", e);
    } catch (NoSuchAlgorithmException | InvalidAlgorithmParameterException
```

```
                | CertificateException | KeyStoreException | IOException e) {
        // failed to generate a key
        throw new RuntimeException("Failed to generate a key", e);
    }
```

To associate fingerprint information with an existing key, register the key with a KeyStore entry to which has been added a setting to enable user authentication requests.

Associating fingerprint information with an existing key

```
    SecretKey key = …;  // existing key

    KeyStore keyStore = KeyStore.getInstance(“AndroidKeyStore”);
    keyStore.load(null);
    keyStore.setEntry(
        "alias_for_the_key",
        new KeyStore.SecretKeyEntry(key),
        new KeyProtection.Builder(KeyProperties.PURPOSE_ENCRYPT)
                .setUserAuthenticationRequired(true)  // Enable requests for user (fingerprint) authentic
ation
                .build());
```


6. Difficult Problems

In Android, there are some problems that it is difficult to assure a security by application implementation due to a specification of Android OS or a function which Android OS provides. By being abused by the malicious third party or used by users carelessly, these functions are always holding risks that may lead to security problems like information leakage. In this chapter, by indicating risk mitigation plans that developers can take against these functions, some topics that needs calling attentions, are picked up as articles.

6.1. Risk of Information Leakage from Clipboard

Copy & paste are the functions which users often use in a casual manner. For example, not a few users use these functions to store curious information or important information to remember in a mail or a web page into a notepad, or to copy and to paste a password from a notepad in which passwords are stored in order not to forget in advance. These are very casual actions at a glance, but actually there's a hidden risk that user handling information may be stolen.

The risk is related to mechanism of copy & paste in Android system. The information which was copied by user or application, is once stored in the buffer called Clipboard. The information stored in Clipboard is distributed to other applications when it is pasted by a user or an application. So there is a risk which leads to information leakage in this Clipboard function. It is because the entity of Clipboard is single in a system and any application can obtain the information stored in Clipboard at any time by using ClipboardManager. It means that all the information which user copied/cut, is leaked out to the malicious application.

Hence, application developers need to take measures to minimize the possibility of information leakage, considering the Android OS specifications.

6.1.1. Sample Code

Roughly speaking, there are two outlooks of counter-measures to mitigate the risk of information leakage form Clipboard.

1. Counter-measure when copying from other applications to your application.
2. Counter-measure when copying from your application to other applications.

Firstly, let us discuss the countermeasure 1 above. Supposing that a user copies character strings from other applications like note pad, Web browser or mailer application, and then paste it to EditText in your application. As it turns out, there's no basic counter-measure to prevent from sensitive information leakage due to copy & paste, in this scenario. Since there's no function in Android to control copy operations by the third party application.

So, regarding the countermeasure 1, there's no method other than explaining users the risk of copying & pasting sensitive information, and just continuing to enlighten users to decrease the

actions themselves continuously.

Next discussion is the countermeasure 2 above, supposing that the scenario that a user copies sensitive information displayed in your application. In this case, the sound counter-measure for leakage is to prohibit copying/cutting operations from View (TextView, EditText etc.). If there are no copy/cut functions in View where the sensitive information (like personal information) is input/output, information leakage will never happen from your application via Clipboard.

There are several methods to prohibit copying/cutting. This section herein describes the easy and effective methods: One method is to disable long press View and another method is to delete copy/cut items from menu when selecting character string.

Necessary of counter-measure can be determined as per the flow of Figure 6.1-1. In Figure 6.1-1, "Input type is fixed to Password attribute" means, the input type is necessarily either of the followings three when application is running. In this case, no counter-measures are required since copy/cut are prohibited as default.

- InputType.TYPE_CLASS_TEXT | InputType.TYPE_TEXT_VARIATION_PASSWORD
- InputType.TYPE_CLASS_TEXT | InputType.TYPE_TEXT_VARIATION_WEB_PASSWORD
- InputType.TYPE_CLASS_NUMBER | InputType.TYPE_NUMBER_VARIATION_PASSWORD

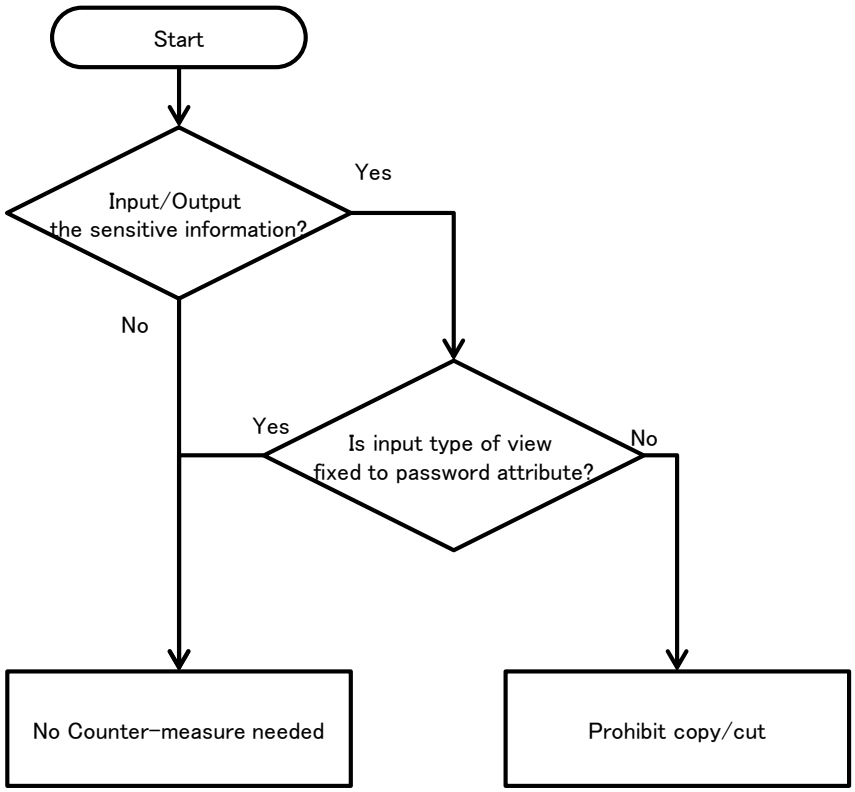


Figure 6.1-1 Decision flow of counter-measure is required or not.

The following subsections detail each countermeasure with sample codes.

6.1.1.1. Delete copy/cut from the menu when character string selection

By TextView.setCustomSelectionActionMODECallback() method, menu when character string selection, can be customized. By using this, if copy/cut item can be deleted from menu when character string selection, user cannot copy/cut character strings any more.

Sample code to delete copy/cut item from menu of character string selection in EditText, is shown as per below.

Points:

1. Delete android.R.id.copy from the menu of character string selection.
2. Delete android.R.id.cut from the menu of character string selection.

UncopyableActivity.java

```
package org.jssec.android.clipboard.leakage;

import android.app.Activity;
import android.os.Bundle;
import android.support.v4.app.NavUtils;
import android.view.ActionMode;
import android.view.Menu;
import android.view.MenuItem;
import android.widget.EditText;

public class UncopyableActivity extends Activity {
    private EditText copyableEdit;
    private EditText uncopyableEdit;

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.uncopyable);

        copyableEdit = (EditText) findViewById(R.id.copyable_edit);
        uncopyableEdit = (EditText) findViewById(R.id.uncopyable_edit);
        // By setCustomSelectionActionMODECallback method,
        // Possible to customize menu of character string selection.
        uncopyableEdit.setCustomSelectionActionModeCallback(actionModeCallback);
    }

    private ActionMode.Callback actionModeCallback = new ActionMode.Callback() {
        public boolean onPrepareActionMode(ActionMode mode, Menu menu) {
            return false;
        }

        public void onDestroyActionMode(ActionMode mode) {
        }

        public boolean onCreateActionMode(ActionMode mode, Menu menu) {
            // *** POINT 1 *** Delete android.R.id.copy from the menu of character string selection.
            MenuItem itemCopy = menu.findItem(android.R.id.copy);
            if (itemCopy != null) {
                menu.removeItem(android.R.id.copy);
            }
            // *** POINT 2 *** Delete android.R.id.cut from the menu of character string selection.
```

```
            MenuItem itemCut = menu.findItem(android.R.id.cut);
            if (itemCut != null) {
                menu.removeItem(android.R.id.cut);
            }
            return true;
        }

        public boolean onActionItemClicked(ActionMode mode, MenuItem item) {
            return false;
        }
    };

    @Override
    public boolean onCreateOptionsMenu(Menu menu) {
        getMenuInflater().inflate(R.menu.uncopyable, menu);
        return true;
    }


    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
        switch (item.getItemId()) {
            case android.R.id.home:
                NavUtils.navigateUpFromSameTask(this);
                return true;
        }
        return super.onOptionsItemSelected(item);
    }

}
```

6.1.1.2. Disable Long Click View

Prohibiting copying/cutting can also be realized by disabling Long Click View. Disabling Long Click View can be specified in layout xml file.

Point:

1. Set false to android:longClickable in View to prohibit copy/cut.

unlongclickable.xml

```
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:orientation="vertical">

    <TextView
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
        android:text="@string/unlongclickable_description" />

    <!-- EditText to prohibit copy/cut EditText -->
    <!-- *** POINT 1 *** Set false to android:longClickable in View to prohibit copy/cut. -->
    <EditText
        android:layout_width="match_parent"
```



```
        android:layout_height="wrap_content"
        android:longClickable="false"
        android:hint="@string/unlongclickable_hint" />
</LinearLayout>
```

6.1.2. Rule Book

Follow the rule below when copying sensitive information from your application to other applications.

1. Disabling Copy/Cut Character Strings that Are Displayed in View (Required)

6.1.2.1. Disabling Copy/Cut Character Strings that Are Displayed in View (Required)

If there's a View which displays sensitive information in an application and besides the information is allowed to be copied/cut like EditText in the View, the information may be leaked via Clipboard. Therefore, copy/cut must be disabled in View where sensitive information is displayed.

There are two methods to disable copy/cut. One method is to delete items of copy/cut from menu of character string selection, and another method is to disable Long Click View.

Please refer to "6.1.3.1 Precautions When Applying Rules."

6.1.3. Advanced Topics

6.1.3.1. Precautions When Applying Rules

In TextView, selecting character string is impossible as default, so normally no counter-measure is required, but in some cases copying is possible depends on application's specifications. The possibility of selecting/copying character strings can be dynamically determined by using TextView.setTextIsSelectable() method. When setting copying possible in TextView, investigate the possibility that any sensitive information is displayed in TextView, and if there are any possibilities, it should not be set as possible to copy.

In addition, described in the decision flow of "6.1.1Sample Code" regarding EditText which is input type (InputType.TYPE_CLASS_TEXT | InputType.TYPE_TEXT_VARIATION_PASSWORD etc.), supposing password input, normally any counter-measures are not required since copying character strings are prohibited as default. However, as described in "5.1.2.2 Provide the Option to Display Password in a Plain Text (Required)," when the option to [display password in a plain text] is prepared, in case of displaying password in a plain text, input type will change and copy/cut is enabled. So the same counter-measure should be required.

Note that, developers should also take usability of application into consideration when applying rules. For example, in the case of View which user can input text freely, if copy/cut is disabled because there is the slight possibility that sensitive information is input, users may feel inconvenience. Of course, the rule should unconditionally be applied to View which treats highly important information or independent sensitive information, but in the case of View other than those, the following questions will help developers to understand how properly to treat View.

- Prepare some other component for the exclusive use of sensitive information
- Send information with alternative methods when the pasted-to application is obvious
- Call users for cautions about inputting/outputting information
- Reconsider the necessity of View

The root cause of the information leakage risk is that the specifications of Clipboard and ClipboardManager in Android OS leave the security risk out of consideration. Application developers need to create higher quality applications in terms of user integrity, usability, functions, and so forth.

6.1.3.2. Operating Information Stored in Clipboard

As mentioned in "6.1 Risk of Information Leakage from Clipboard," an application can manipulate information stored in Clipboard by using ClipboardManager. In addition, there is no need to set particular Permission for using ClipboardManager and thus the application can use ClipboardManager without being recognized by user.

Information, called ClipData, stored in Clipboard can be obtained with ClipboardManager.getPrimaryClip() method. If a listener is registered to ClipboardManager by

ClipboardManager.addPrimaryClipChangedListener() method implementing OnPrimaryClipChangedListener, the listener is called every time copy/cut operations occurred by user. Therefore ClipData can be got without overlooking the timing. Listener call is executed when copy/cut operations occur in any application regardless.

The following shows the source code of Service, which gets ClipData whenever copy/cut is executed in a device and displays it through Toast. You can realize that information stored in Clipboard is leaked out doe to simple codes as follows. It's necessary to pay attention that the sensitive information is not taken at least by the following source code.

ClipboardListeningService.java

```
package org.jssec.android.clipboard;

import android.app.Service;
import android.content.ClipData;
import android.content.ClipboardManager;
import android.content.ClipboardManager.OnPrimaryClipChangedListener;
import android.content.Context;
import android.content.Intent;
import android.os.IBinder;
import android.util.Log;
import android.widget.Toast;

public class ClipboardListeningService extends Service {
    private static final String TAG = "ClipboardListeningService";
    private ClipboardManager mClipboardManager;

    @Override
    public IBinder onBind(Intent arg0) {
        return null;
    }

    @Override
    public void onCreate() {
        super.onCreate();
        mClipboardManager = (ClipboardManager) getSystemService(Context.CLIPBOARD_SERVICE);
        if (mClipboardManager != null) {
            mClipboardManager.addPrimaryClipChangedListener(clipListener);
        } else {
            Log.e(TAG, "Failed to get ClipboardService . Service is closed.");
            this.stopSelf();
        }
    }

    @Override
    public void onDestroy() {
        super.onDestroy();
        if (mClipboardManager != null) {
            mClipboardManager.removePrimaryClipChangedListener(clipListener);
        }
    }

    private OnPrimaryClipChangedListener clipListener = new OnPrimaryClipChangedListener() {
        public void onPrimaryClipChanged() {
            if (mClipboardManager != null && mClipboardManager.hasPrimaryClip()) {
                ClipData data = mClipboardManager.getPrimaryClip();
```



```
                ClipData.Item item = data.getItemAt(0);
                Toast
                    .makeText(
                        getApplicationContext(),
                        "Character stirng that is copied or cut:¥n"
                            + item.coerceToText(getApplicationContext()),
                        Toast.LENGTH_SHORT)
                    .show();
            }
        }
    };
}
```

Next, below shows an example code of Activity which uses ClipboardListeningService touched in the above.

ClipboardListeningActivity.java

```
package org.jssec.android.clipboard;

import android.app.Activity;
import android.content.ComponentName;
import android.content.Intent;
import android.os.Bundle;
import android.util.Log;
import android.view.View;

public class ClipboardListeningActivity extends Activity {
    private static final String TAG = "ClipboardListeningActivity";

    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_clipboard_listening);
    }

    public void onClickStartService(View view) {
        if (view.getId() != R.id.start_service_button) {
            Log.w(TAG, "View ID is incorrect.");
        } else {
            ComponentName cn = startService(
                new Intent(ClipboardListeningActivity.this, ClipboardListeningService.class));
            if (cn == null) {
                Log.e(TAG, "Failed to launch the service.");
            }
        }
    }

    public void onClickStopService(View view) {
        if (view.getId() != R.id.stop_service_button) {
            Log.w(TAG, "View ID is incorrect.");
        } else {
            stopService(new Intent(ClipboardListeningActivity.this, ClipboardListeningService.class));
        }
    }
}
```

Thus far we have introduced methods for obtaining data stored on the Clipboard. It is also possible to use the ClipboardManager.setPrimaryClip() method to store new data on the Clipboard.

Note that setPrimaryClip() method will overwrite the information stored in Clipboard, therefore the information stored by user's copy/cut may be lost. When providing custom copy/cut functions with these methods, it's necessary to design/implement in order not that the contents stored in Clipboard are changed to unexpected contents, by displaying a dialogue to notify the contents are to be changed, according the necessity.

