PROJECT DESCRIPTION

TLS SERVER CERTIFICATE MANAGEMENT

William Haag, Jr., Tim Polk, Murugiah Souppaya
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

William C. Barker
Dakota Consulting, Inc.

Paul Turner
Venafi

Russ Housley
Vigil Security

November 2017
tls-cert-mgmt-nccoe@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a community of interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

Abstract

This project provides guidance on the governance and management of Transport Layer Security (TLS) server certificates in enterprise environments to reduce outages, improve security, and enable disaster recovery related to certificates. The project will be provided in a freely available NIST Cybersecurity Practice Guide, documenting an example solution that demonstrates how to perform the following actions:

- develop a set of policy attributes
- establish and maintain an inventory of TLS certificates
- assign and track certificate owners
- identify issues and vulnerabilities of the TLS infrastructure
- automate enrollment and installation
- report the status of the TLS certificates
- continuously monitor TLS certificates in the typical enterprise environment

Keywords

transport layer security (TLS); certificate management; private-key security; certification authority (CA); CA compromise; automatic certificate management environment (ACME)*; secure sockets layer (SSL); public key infrastructure (PKI)*

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's NCCoE are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: tls-cert-mgmt-nccoe@nist.gov

Public comment period: October 11, 2017 to October 25, 2017

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Purpose

This document lays out a National Cybersecurity Center of Excellence (NCCoE) project to demonstrate effective certificate management for Transport Layer Security (TLS) servers across an enterprise environment to maximize security and minimize operational risks. In addition to using TLS to encrypt traffic crossing enterprise boundaries, organizations are increasingly encrypting communications between internal systems with TLS. Commercial and government organizations are experiencing challenges with managing the resulting number of TLS server certificates and keys—often numbering in the thousands. Outages due to expired certificates or disaster recovery events (e.g., Certification Authority [CA] compromise) are costing organizations revenue, customers, and reputation. By failing to secure private keys, organizations expose internal and customer data to attackers who are impersonating corporate systems. NIST will collaborate with industry partners to engineer and implement a commercially-supported, standards-based, interoperable, secure, and tested example solution that efficiently and effectively provisions and manages TLS certificates during both normal operations and disaster recovery.

This project will result in a publicly available National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

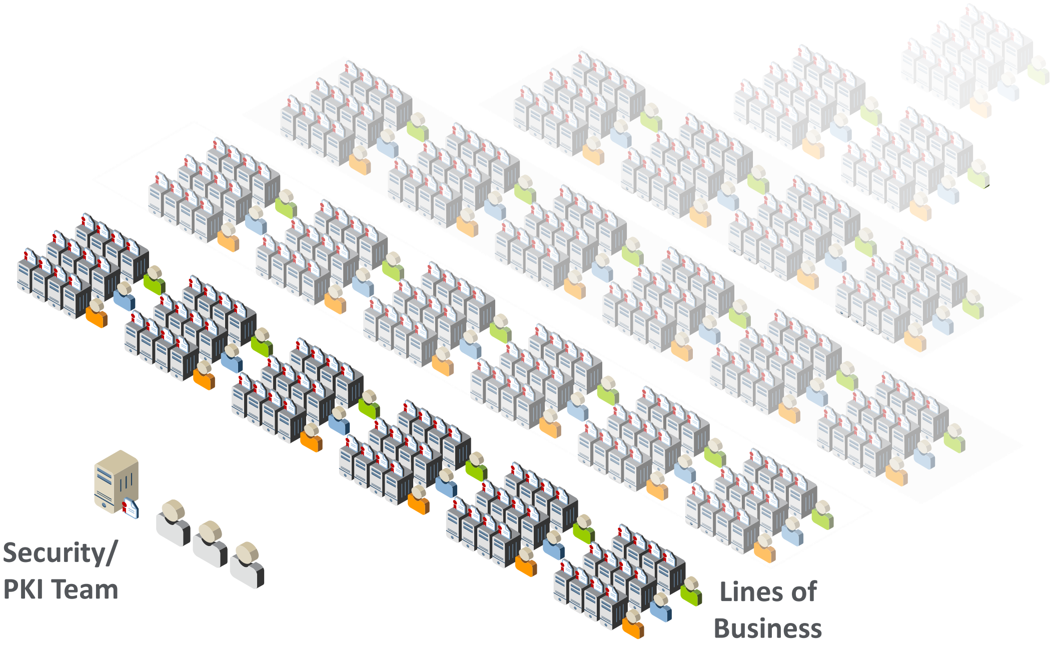
Scope

This project focuses on the management of TLS server certificates in medium and large enterprises that rely on TLS to secure both customer-facing and internal applications. Within the enterprise environment, multiple groups or teams are responsible for different applications and are supported by a central security team to ensure sound certificate/key management policies and practices. This NCCoE project will demonstrate how to establish and maintain an inventory of TLS certificates; assign and track certificate owners (i.e., custodians); identify issues with, and vulnerabilities of, the TLS infrastructure; automate enrollment and installation; report; and continuously monitor TLS certificates in the environment described above.

This project will limit its scope to TLS server certificates. Client certificates may optionally be used in TLS for mutual authentication, but the management of client certificates is outside the scope of this project.

Background

TLS is a broadly used security protocol that facilitates the authentication and encryption of communications between clients and servers. All TLS servers must have a certificate (and the corresponding private key) to authenticate themselves and to establish symmetric keys for encryption. A TLS server certificate and private key is generally installed and managed by the server's system administrator—others usually don't have the access rights required on the system to manage them. To get a certificate, an administrator executes commands on the system to generate a cryptographic key pair (the public key and the private key), and then requests a certificate from a CA. Because most system administrators are not knowledgeable about certificates and cryptography, this process can be confusing and error-prone. Larger organizations often have a central group, often called the Public Key Infrastructure (PKI)[1] team, that is responsible for managing the CAs, which often include external public CAs and internally operated CAs. Due to their expertise in certificates, the PKI team typically supports the system administrators through the key pair generation and certificate request process. Medium and large organizations have many system administrators, but only a handful of people on the PKI team.



Assumptions/Challenges

This distributed management environment for certificates and private keys fosters a variety of risks and challenges:

- **Application Outages:** Nearly every enterprise has experienced significant application outages due to expired TLS server certificates, including examples of outages to online banking, reservations systems, and healthcare services. The drive to encrypt all communications (internal and external) is expanding the reliance on TLS server certificates, making the potential for critical system outages even more likely.
- **Security Risks:** TLS server certificates serve as trusted machine identities. If an attacker can get a fraudulent certificate or compromise a private key, then they can impersonate the server or eavesdrop on communications.
- **Disaster Recovery Risk:** There are several certificate-related incidents that can require an organization to rapidly change large numbers of TLS server certificates, including a CA compromise, algorithm deprecation, or cryptographic library bug. If an organization is

[1] Public key infrastructure (PKI) is the term used for the infrastructure, including certification authorities (CAs), required to support the use of certificates.

not prepared for rapid replacement, then their services could be unavailable for days or weeks.

The goals of this building block are to establish a reference architecture that represents a typical enterprise network and associated TLS infrastructure, to simulate the described risks through a number of usage scenarios, and to address these risks.

2 Scenario

The scenario starts with an organization that has deployed and currently uses TLS certificates across multiple groups and applications. Furthermore, the organization is encountering the problems described earlier in this document. An approach to address these issues with life-cycle management of the certificates can include the following phases:

- **Establish Governance:** The project team defines a set of certificate management policies based on the guidance provided in existing NIST documents to establish consistent governance of TLS certificates.
- **Create and Maintain an Inventory:** The PKI team works with the lines of business and system administrators to establish a complete inventory of all TLS server certificates through automated discovery. The organization leverages configurable rules to automatically organize discovered certificates and associate owners to enable automated notifications.
- **Register for and Install Certificates:** As new certificates are needed or existing certificates must be renewed, certificates are requested and installed. Because enterprise environments are so diverse, with different technical and organizational constraints, there are several possible methods for requesting and installing certificates, including:
    - *Manual:* Security, operational, or technical requirements/constraints mandate that a certificate must be manually requested by the server's system administrator by using command line tools and a certificate management system portal.
    - *Standardized Automated Certificate Installation:* A TLS server is configured to automatically request and install a certificate by using a protocol, such as the Automatic Certificate Management Environment (ACME) protocol developed by the Internet Engineering Task Force (IETF).
    - *Installation Using Proprietary Method:* The certificate management system uses a method that is proprietary to the TLS server to perform the operations needed to install certificates on one or more systems that do not support a standard automated method for requesting and installing certificates.
    - *Development Operations (DevOps)-based Installation:* A DevOps framework that is used to install and configure servers/applications is also used to request and install certificates. This will be done in a cloud environment—where DevOps frameworks are most commonly used.

  The majority of private keys used with certificates are stored in files; however, hardware security modules (HSMs) can be used to increase the security of private keys. One or more of the methods listed above will be performed on a system that uses an HSM for private-key protection.

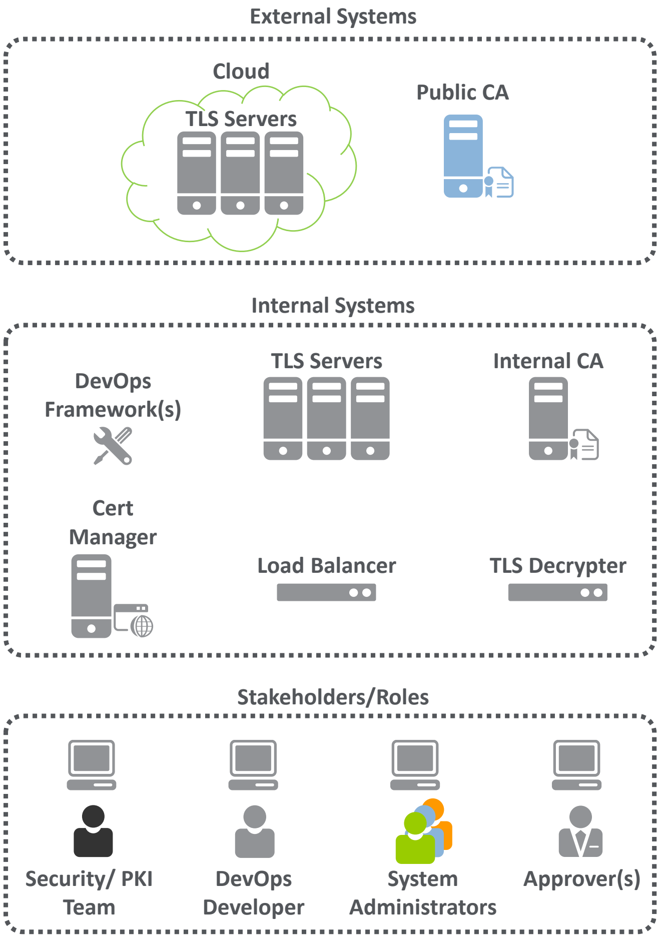
- **Continuously Monitor and Manage:** The inventory of certificates is monitored for expiration, proper operation, and security issues. Notifications and alerts are triggered when anomalies are detected. Management operations are performed to ensure proper operation and security.
- **Detect, Respond, and Recover from Incidents:** An organization encounters a situation, such as a CA compromise or broken algorithm (e.g., cryptographic library bug which created weak keys for certificates), in which a large number of certificates must be rapidly replaced. The certificate management system orchestrates the replacement of all certificates.

3 High-Level Architecture

The scenario for this project encompasses a variety of potential systems and configurations. An important step in this project will be establishing a recommended baseline system configuration that will represent the scenario.

Component List

The high-level architecture will include the following components:



- **External Systems** – The architecture will include the following components that typically reside outside the organizational firewall:
    - **TLS Servers in the Cloud Environment:** The cloud environment will include multiple cloud instances acting as TLS servers. Certificates will be deployed and managed on these systems.
    - **Public CA:** A publicly trusted CA will be used to issue one or more of the certificates used on TLS servers on the internal or external systems.
- **Internal Systems** – The architecture will include several systems that are typically deployed within organizational network environments.
    - **TLS Servers:** Multiple systems will be configured as TLS servers (e.g., webserver, application server, or other service). Certificates will be deployed and managed on these systems.
    - **Load Balancer:** A load balancer will act as a TLS server with a certificate and will facilitate the load balancing of traffic to the other TLS servers.
    - **DevOps Framework(s):** One or more DevOps frameworks (e.g., Docker) will be used to automate the management of cloud instances and the deployment of certificates on those instances.
    - **Internal CA:** An internal CA will be used to issue certificates to some of the TLS servers.
    - **Certificate Manager:** A certificate management system will be used to inventory and manage TLS server certificates deployed in the environment.
    - **Certificate Network Scanning Tool:** A tool, such as a vulnerability scanning or other tool, will be used to facilitate the discovery of TLS server certificates via network scanning.
- **Stakeholders/Roles** – Humans play an important part in the management of TLS server certificates in enterprises; therefore, the following roles will be represented:
    - **Line of Business / Application Owner:** People in leadership positions who are responsible for the line of business or application and who will drive the need for certificates to be deployed
    - **System Administrators:** Responsible for managing TLS servers and ensuring that the load balancer will be represented
    - **DevOps Developer:** Responsible for programming/configuring and managing the DevOps framework
    - **Approver:** One or more stakeholders who will review and approve/reject certificate management operations
    - **PKI Team:** One or more individuals who will manage the certificate management system and public/internal CAs

A more detailed architecture and design that enables the demonstration of all of the uses cases in the lab environment will be developed once the project is approved and the project team has been assembled.

Desired Requirements

An NCCoE build for this project will require the following components:

- TLS servers in the Cloud
- Public CA
- TLS servers, including webservers, application servers, or other services
- TLS load balancers
- DevOps frameworks, including application containers
- Internal CAs
- Certificate management systems
- Certificate network scanning tools, including vulnerability scanning

4 Relevant Standards and Guidance

The following resources and references provide additional information that is used to develop this solution:

- Managing Federal Information as a Strategic Resource, OMB Circular A-130, Executive Office of the President, Office of Management and Budget, July 28, 2016. See https://obamawhitehouse.archives.gov/omb/circulars_a130_a130trans4/
- Minimum Security Requirements for Federal Information and Information Systems, FIPS 200, National Institute of Standards and Technology, March 2006. See http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
- Security Requirements for Cryptographic Modules, FIPS 140-2 (including change notices as of 12-03-2002), National Institute of Standards and Technology, May 2001. See http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, April 2014. See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
- NIST Special Publication 800-57 Part 1, Revision 4. Recommendation for Key Management: Part 1: General, E. Barker, January 2016. See http://doi.org/10.6028/NIST.SP.800-57pt1r4
- NIST SP 800-63-3, Digital Identity Guidelines, June 2017. See https://csrc.nist.gov/publications/detail/sp/800-63/3/final
- NIST SP 800-77, Guide to IPsec VPNs, December, 2005. See http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf
- Cyber Security Framework, National Institute of Standards and Technology, February 2014. See http://www.nist.gov/cyberframework/
- The TLS Protocol Version 1.0, T. Dierks, C. Allen, January 1999. See https://www.ietf.org/rfc/rfc2246.txt
- The Transport Layer Security (TLS) Protocol Version 1.1, T. Dierks, E. Rescorla, April 2006. See https://www.ietf.org/rfc/rfc4346.txt
- The Transport Layer Security (TLS) Protocol Version 1.2, T. Dierks, E. Rescorla, August 2008. See https://www.ietf.org/rfc/rfc5246.txt

- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, May 2008. See https://www.ietf.org/rfc/rfc5280.txt
- draft-ietf-tls-tls13-21 The Transport Layer Security (TLS) Protocol Version 1.3, E. Rescorla, July 3, 2017. See https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/
- draft-ietf-acme-acme-07 Automatic Certificate Management Environment (ACME), R. Barnes, J. Hoffman-Andrews, and J. Kasten, June 21, 2017. See https://datatracker.ietf.org/doc/draft-ietf-acme-acme/

5 Security Control Map

The objective of this building block is to improve the overall security of TLS certificates and private keys. This will be accomplished in the following ways:

- **Governance and Risk Management:** The building block must include clear policies that can be used to educate the lines of business and system administrators to ensure that they understand the security risks and their responsibilities in addressing those risks.
- **Visibility and Awareness:** Most organizations do not have an inventory of their TLS server certificates and private keys, their installed locations, and their responsible individuals/groups. This building block must demonstrate how to achieve the visibility and awareness of all certificates.
- **Reliable and Efficient Certificate Provisioning:** This building block must demonstrate effective processes to ensure the availability of valid certificates and keys for TLS servers, while minimizing overhead and the impact on operations.
- **Certificate Disaster Recovery:** This building block must demonstrate effective processes for organizations to be prepared for, and respond to, large-scale incidents (e.g., CA compromise) that require the rapid replacement of large numbers of certificates and keys.
- **Audit Logging:** Many organizations do not generate, store, and review audit logs for their certificates and associated private keys. This building block must demonstrate how to establish and maintain complete audit trails of certificate and private-key life cycles.
- **Secure Certificate Management Platform:** The certificate management platform in this building block must be deployed on a hardened system and must provide the security attributes required to protect the assets it manages.
- **Private-Key Security:** The building block must demonstrate automated management, which reduces the requirement for direct administrator access to private keys, and HSM-based private key protection, which significantly increases private-key security.

SP 800-53 control classes that apply to the TLS Server Certificate Management project include, at a minimum, Access Control (AC), the configurations settings controls associated with Configuration Management (CM), Systems and Communications Protection (SC), and Systems and Information Integrity (SI). Cybersecurity framework Functions and Categories addressed by the project include the Data Security (DS) category under the Protect Function (PR); the Security Continuous Monitoring (CM) and Detection Processes (DP) category under the Detect Function

(DE); the Information Protection Processes and Procedures (IP), Access Control (AC), and Protective Technology (PT) categories under the Protect Function (PR); the Communications (CO) and Mitigation (MI) categories under the Respond Function (RS); and the Communications (CO) category under the Recover Function (RC).

Appendix A Acronyms and Abbreviations

ACME	Automatic Certificate Management Environment
CA	Certification Authority
CSF	Critical Infrastructure Cybersecurity
DevOps	Development Operations
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
TLS	Transport Layer Security