Certinia Security Whitepaper

Introduction

Certinia provides enterprise cloud applications including Enterprise Resource Planning suite of services which comprises of Accounting, Revenue Recognition, Billing Central, Order Procurement and Inventory (OPI), Financial Planning and Analysis, and Reporting and Analytics; and Professional Services Organization Services ("PS Cloud") and the Customer Success Organization Services ("CS Cloud") including PSA, Customer Success Operations (CS Ops) Cloud, and Services CPQ (all collectively referred to as Certinia Applications).

Certinia Applications are built on the Salesforce platform, a cloud computing platform provided by Salesforce. Certinia serves its clients (or "user entities") from headquarters in San Jose, California, USA; with EMEA headquarters in Harrogate, UK (also covers the Asia Pacific region). Founded in 2009, Certinia is backed by Salesforce, Technology Crossover Ventures, Unit4 and Advent International.

Customer Base

Our customers are in a wide range of verticals, some with stringent security requirements, including financial services, healthcare, technology, energy and government.

Security Overview

Certinia Applications were designed from the ground up using core information security principles:

- Confidentiality: Prevent the disclosure of information to unauthorized individuals or systems.
- Integrity: Maintain and assure the accuracy and consistency of data over its entire lifecycle.
- Availability: Ensure the information is available when needed.

Certinia is committed to achieving and maintaining these principles and the trust of our

customers. Integral to this is providing a robust security and privacy program that carefully considers security and data protection across our services, including data submitted by customers to our services ("customer data").

Information Security Program

Certinia has a dedicated Security and Trust function that coordinates security policy, program and verification efforts, to ensure that customer and company information assets are adequately protected. Our Information Security Program includes identifying, evaluating and reporting on security risks, compliance with security and privacy regulations and commitments, threat and vulnerability management, and security incident management and response. Certinia has an Information Security Policy and Standards framework aligned with ISO 27002 which describes standards, best-practice guidelines and approaches required to protect customer data and corporate assets (including people, information and infrastructure).

Certinia Security Profiles

Certinia Security has a robust 3rd party risk management program which leverages automation to gain efficiencies. To help you gain a better understanding of Certinia security, we have partnered with Whistic (vendor risk management solution) to provide you with more information about our security including collateral such as SOC reports or cyber insurance or penetration testing report or controls questionnaires such as CSA and VSA, amongst a few others.

To support your security evaluation, you can view our **Public** Security Profile here which contains our SOC 3 Report. We can also share the **Full** Whistic Certinia Security Profile under NDA with you to access and download other confidential reports such as our SOC 1, SOC 2, or the latest Penetration Test. Please contact your account executive to request access to our Full Whistic Profile. All you will need to do to access the Security Profile is create an account with Whistic.

Commitment to Security

At Certinia, we understand that security, availability and application processing integrity are critical for our customers. Certinia is dedicated to providing industry-leading security for our customers' data assets through our Security and Trust program.

People

Everyone at Certinia, from the research and development staff to the executive team, is

committed to security excellence. The company's Head of Information Security coordinates a cross-functional team of experts focused on security-related activities. Certinia also has a Senior Vice President and General Counsel with responsibility for compliance with global privacy laws. All employees receive regular information security awareness training that covers key security threats and risks and employee obligations to protect the security, confidentiality and privacy of customer and company data.

Processes

All key Certinia business processes, including development, support, operations, consulting, and monitoring processes, consider the security of our customer data.

Technology

We leverage industry-leading and proven secure platforms for our products and services. Each component of our technology infrastructure undergoes intensive scrutiny by multiple teams of security professionals.

Customers

We consider our customers, partners, developers and internal users that interact with our systems to be within our security scope. Our security program is designed both to provide them a high degree of security assurance and to protect ourselves from threats they might present.

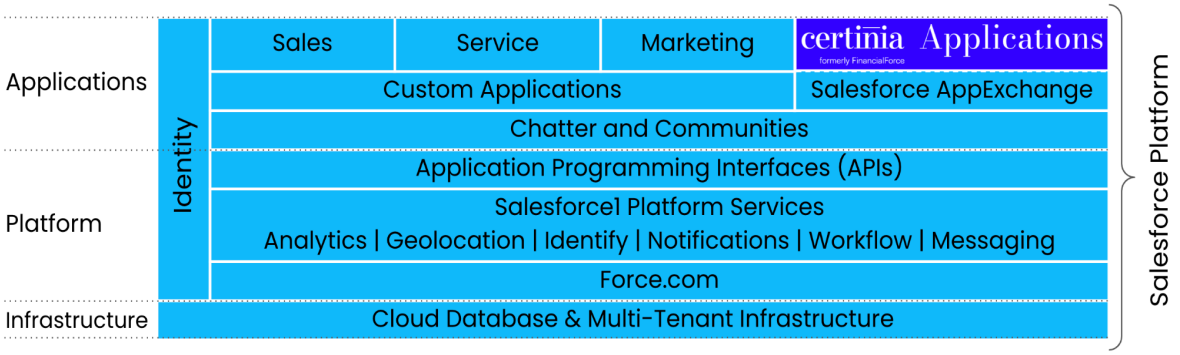
Built on the Salesforce Platform

To support these principles, Certinia Applications were developed on the Salesforce Platform, an industry-leading and mature platform for cloud applications provided by Salesforce. Certinia Applications are listed on AppExchange (Salesforce cloud applications marketplace) and use the Salesforce cloud platform as the underlying technology, which includes tools for development, reporting, workflow authorizations, dashboards, social media (Chatter) and integration. All AppExchange applications go through a qualitative and quantitative review process to ensure applications meet a set of security standards and best practices.

By leveraging an industry-leading cloud platform for business applications, Certinia Applications and our customers' data benefit from a variety of security features and controls in such areas as user management, access control, disaster recovery, backups, physical and network security. As a result, Certinia Applications satisfy our customers'

most stringent data security requirements, and comply with major security, privacy and data protection laws and standards globally.

Certinia Applications and Salesforce Platform Architecture



For more information on the Salesforce Platform, Salesforce compliance certifications and other security guidance please see the Salesforce Security Section below.

Shared Security Responsibility Model

Moving business processes and applications to the cloud creates a shared responsibility model between our customers, Certinia and Salesforce. This shared model maximizes efficiency and flexibility while maintaining a high level of security.

Certinia

Certinia manages and controls its applications and related services. This includes change management, product updates and patch management related to the Certinia Applications. Certinia are fully responsible for the security of the code we produce, which is delivered to our customers in the form of Salesforce ISV packages.

Salesforce

Salesforce offers two distinct platform services where Certinia Applications can reside on. The first is where Salesforce provides its own data centers and physical security, including operating, managing and controlling the components from the API level down to the host operating system and its underlying databases. The second is where the underlying platform is hosted on AWS and is referred to as “Hyperforce” for customers who prefer this option. For more information about Salesforce security, navigate to https://security.salesforce.com.

Amazon Web Services (AWS)

Certinia uses the AWS platform to persist and analyze customer telemetry data that is provided by Salesforce. The telemetry data provided is strictly metadata information on what Certinia products our customers are consuming, and is used by Certinia for measuring product adoption and customer engagement, and for planning purposes. Telemetry data is encrypted-at-rest in AWS. Information about the current version of our products a customer has in production is also persisted in AWS. This information is used by Certinia to facilitate continuous updates (Push Upgrade) of the customer's products.

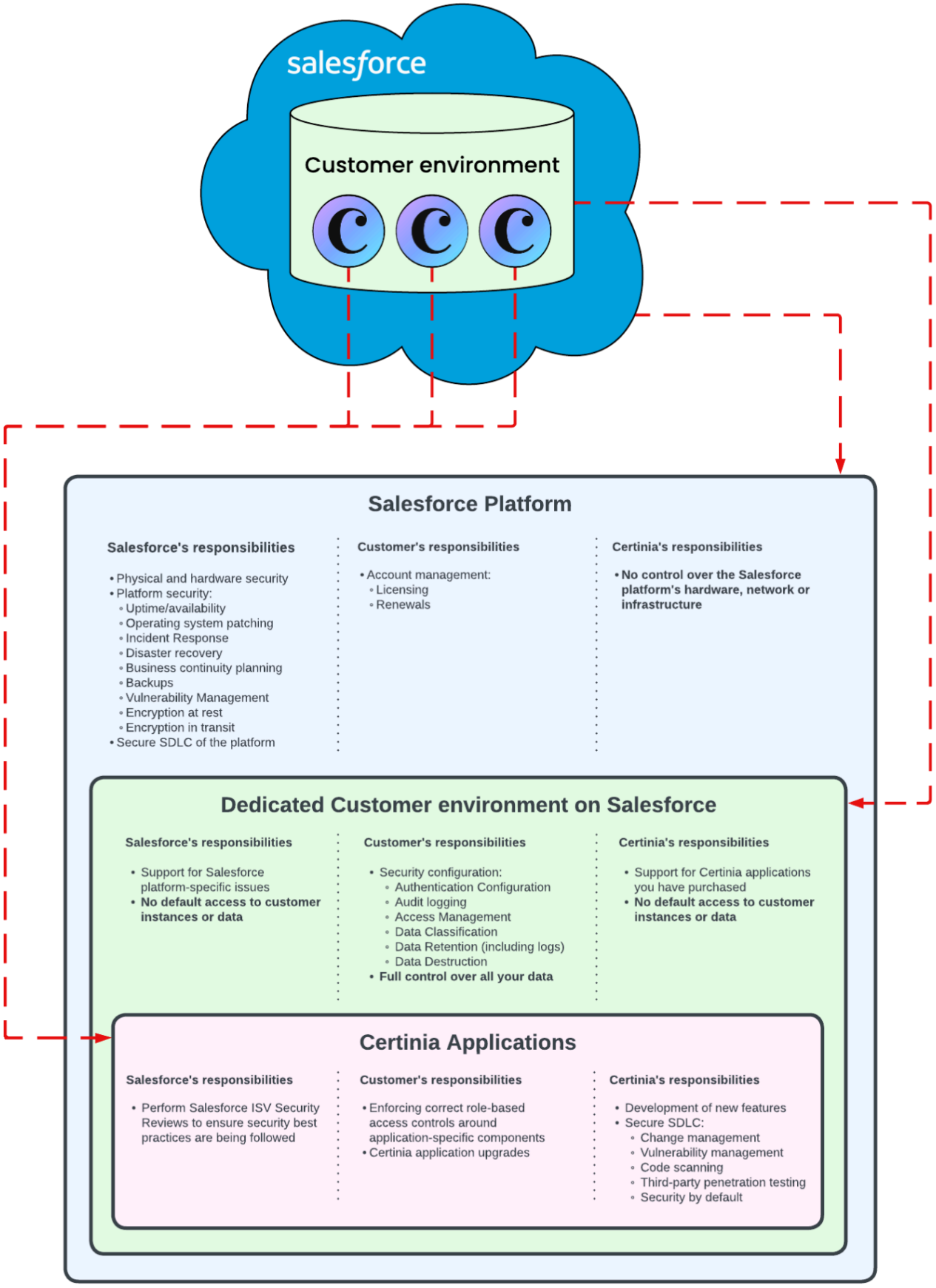
Customers

Customers are responsible for user access and authorization, control and backup of data uploaded to the Certinia Applications, as well as configuration of the underlying Salesforce platform in accordance with their requirements. Customers can also enhance the security of their Certinia implementation and address security and compliance requirements by leveraging security features of the Force.com platform such as data encryption, IP-range restrictions, robust access control, two-factor authentication, single-sign on, strong passwords and/or enforced periodic password changes.

Certinia recognizes that many companies are subject to regulations and standards governing security and handling of information, and therefore maintains a security program that covers policies, practices, people and technology. However, to use Certinia Applications securely, customers must apply sound security practices to their configuration and any customization and integration of Certinia and the underlying Salesforce platform, including customers' design and implementation of related business processes.

Example: Certinia provides applications and views for data entry and reporting, and the Salesforce platform provides authentication technology, but each customer must implement and monitor access and authorization controls (e.g., configuring administrators for managing privileged access, designing roles and processes for access to records, and enabling a field audit trail for monitoring user access to data).

The diagram on the following page helps to visualize the key responsibilities of Salesforce, Customers and Certinia in respect to the different layers comprising a Salesforce/Certinia implementation:



Certifications and Attestations

Certinia Attestations

Cloud Security Alliance

As part of our commitment to Trust, we have published a detailed description of our cloud security controls under the Cloud Security Alliance (CSA) STAR Level 1 - Self-Assessment program. This self-assessment uses the CSA Consensus Assessments Initiative Questionnaire to answer nearly 300 standardized questions that provide transparency into cloud vendor security practices and controls supporting their cloud service delivery and applications. You can access it here:
https://cloudsecurityalliance.org/star/registry/FinancialForce

SSAE 16 SOC Reports

As part of our commitment to trust and security, Certinia has invested in a Service Organization Control (SOC), SOC 1 Type II, SOC 2 Type II, and SOC 3 reports prepared by an independent party - **Coalfire**. The report is prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. The purpose of the report is to provide our customers assurance that the Certinia Description of Services is fairly presented in all material respects, that controls put in place by Certinia are suitably designed to meet their control objectives, and that those controls were tested and operated effectively during the audit period.

Coalfire created an Independent Service Auditors' Report after testing and evaluating Certinia Applications against the following objectives for **SOC 1 Type II**:

Control Area	Description
Control Environment	Foundation for all other components of internal control, providing discipline and structure including control activities, policies and procedures that help make sure that management's directives are carried out.
Risk Assessment	Identification, analysis and management of relevant risks.
Monitoring	Processes to assess the quality of internal control performance.
Information and Communication	Systems that support the identification, capture and exchange of information that enables people to carry out their responsibilities.

IT General Controls	Defined policies, procedures and controls in place for supporting Certinia services.
Change Management	Controls for change initiation, prioritization and release management.
Development and Testing	Development and changes to production application systems are authorized, tested, approved and properly implemented.
Information Security Aspects	Information security policies and procedures for supporting user entities.
Incident Management	Incident monitoring, response, escalation and resolution.
Sub-Service Organizations	Usage of sub-service organizations for infrastructure support and management, physical security, environmental safeguards, and backup and recovery functions to maintain the information systems
Disaster Recovery and Business Continuity.	Disaster recovery and business continuity plan for unplanned, adverse events.

The following trust principles were included for Certinia **SOC 2 Type II** Independent Service Auditors' Report:

Control Area	Description
Security	The system is protected against unauthorized access, both physical and logical.
Confidentiality	Information designated as confidential is protected as committed or agreed.

The SOC reports provide Certinia customers with the additional assurance that our applications are developed and delivered in accordance with transparent standards to ensure high-quality and secure products are deployed to our customers' environments.

Salesforce Certifications

As Certinia Applications are developed and run natively on the Force.com platform, we benefit from various security controls designed and implemented by Salesforce. Salesforce undergoes comprehensive privacy and security assessments by, and has achieved certifications from, multiple auditors and certifying bodies. These include the following security- and privacy-related audits and certifications:

Geographical Recognition

- EU / EEA Binding Corporate Rules for Processors

- EU / EEA and Switzerland Safe Harbor self-certification through the U.S. Department of Commerce
- TRUSTe Certified Privacy Seal

Global Audit Compliance

- ISO 27001
- SSAE 16/ISAE 3402 SOC-1
- SOC 2
- SOC 3
- FedRAMP
- PCI-DSS
- TÜV Rheinland Certified Cloud Service

A current list of security and privacy assessments and certifications of the Salesforce platform can be found at https://trust.salesforce.com/trust/learn/compliance.

Security Controls

Infrastructure Security

Responsible disclosure

Certinia has partnered with BugCrowd with the goal of identifying inherent vulnerabilities within our externally-facing infrastructure. The bug bounty vendor manages the independent researchers and facilitates responsible disclosure of any high risk vulnerabilities identified.

Note to researchers: Please note that we currently only accept responsible disclosure reports via BugCrowd. Visit our program page on BugCrowd for more information about scope, focus areas, eligibility and bounties.

Attack Surface Management

Certinia uses state-of-the-art security technology to protect our digital landscape, including input from industry leading vendors and custom-built Attack Surface Management solutions designed to harden and reduce our attack surface.

Vulnerability Scanning

Certinia uses leading vulnerability scanning solutions to detect potential security weaknesses in our critical infrastructure.

Intrusion Detection

Certinia leverages a real time EDR solution to detect anomalies and potential threats affecting our critical infrastructure. Our solution monitors not only the detailed activity of individual systems by means of an agent, but also security logs on the cloud provider level. Alerts are raised directly to DevOps, IT and Security staff for triage.

Infrastructure as Code

All of Certinia's infrastructure is written in *Terraform*. This enables us to create immutable infrastructure by defining cloud resources declaratively. This allows us to track the current state of our systems in source control, review changes in code reviews, create and reuse secure infrastructure modules, and perform automated static analysis of our infrastructure to identify security weaknesses and harden systems.

Product Security

Product Security Measures

Certinia's secure software development lifecycle incorporates a number of security measures, including:

- Code reviews designed to ensure adherence to Certinia development standards.
- Software security testing and code scanning using SAST and SCA solutions to identify and address security vulnerabilities and open-source software license issues.
- Release reviews and approvals designed to ensure product releases comply with internal process requirements.
- Vulnerability testing and remediation for infrastructure and tools supporting our source code management platform.
- Development and changes to production application systems are authorized, tested, approved and documented.

Application Penetration Testing

Application Penetration testing is conducted annually by a reputable independent 3rd party against our PSA application. As applicable, regression testing is subsequently performed to validate any high risk vulnerabilities identified have been remediated. The PSA Annual Pen Test Report is available for viewing as part of our Full Whistic Security Profile under NDA.

Additionally, Certinia have dedicated security subject-matter experts performing threat modeling and internal penetration testing of key products and developments.

Salesforce AppExchange Security Review

Certinia Applications are submitted to Salesforce as part of the AppExchange Security Review process. Salesforce provides the AppExchange Security Review program to assess the security posture of ISV applications published on the AppExchange against industry best practices for security.

Data Encryption In Transit

Certinia relies on Salesforce platform capabilities for encryption of data in transit. Salesforce uses industry-accepted encryption products to protect customer data and communications during transmissions between a customer's network and the Certinia Applications, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, customer data is encrypted during transmission between data centers for replication purposes.

Data Encryption At Rest

Certinia relies on the Salesforce platform capabilities for encryption of data at rest. By default, Salesforce offers SAN encryption within its first party data centers. Salesforce leverages technologies from both Dell and Hitachi in its first party data centers in order to deliver encryption at-rest at the storage layer (SAN Encryption for Salesforce Core Services). Both the Dell and Hitachi approaches leverage an AES-256 block-based encryption cipher. With this enabled, all data residing on databases and files are encrypted while in storage.

In addition, depending on customer requirements for encryption, as driven by regulatory compliance such as PCI-DSS, customers can choose to purchase the Platform Encryption feature which allows you to encrypt certain standard fields, as well as custom fields, and bears less limitations than Classic Encryption over what custom fields you can encrypt. Platform Encryption uses Advanced Encryption Standard (AES) with 256-bit keys with CBC mode, and a static initialization vector (IV), which is a hash of the entity ID, field ID, and key ID, making it unique to each customer and field per org.

Application Controls

Certinia provides rigorous application controls that ensure your financial transactions have been correctly validated and reviewed prior to posting, have comprehensive audit trails and cannot subsequently be modified via “back door” manipulation of object data.

These application controls include:

- Comprehensive audit trails for transactions, master data modifications and security setup changes.
- Multi-level approval processes for transactions and master file data changes
- Segregation of duties
- Highly granular control of object, record and field level access by means of our patented, admin-friendly and fully customisable RBAC scheme

Disaster Recovery

Because Certinia Applications are 100% Salesforce-native, all data processed by Certinia Applications resides on the Salesforce cloud platform owned, operated and managed by Salesforce. Salesforce provides fully redundant data centers and all customer data resides within the Salesforce data centers. As part of its disaster recovery planning, Certinia, in collaboration with Salesforce, undertakes to ensure that the systems where customer data is stored have a disaster recovery facility that is geographically remote from its primary data center, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data center were to be rendered unavailable.

Change Management

Certinia follows fully documented change management procedures for all aspects of its software lifecycle, including application development, release management, service management and enhancement. The operating effectiveness of the Change Management process and procedure is validated as part of our SOC 2 Type II Report.

Incident Management

Certinia maintains security incident management policies and procedures, which include prompt notification of customers in the event Certinia becomes aware of an actual or reasonably suspected unauthorized use or disclosure of customer data. The operating effectiveness of the Incident Management process and procedure is validated as part of our SOC 2 Type II Report.

Contacts

For security related questions, please email us at security@Certinia.com
For privacy related questions, please email us at privacy@Certinia.com
For business continuity related questions, please email us at

business.continuity@Certinia.com

Additional Resources and Links

Certinia Security and Trust Website
https://www.certinia.com/trust

Certinia Security FAQ
https://certinia.com/wp-content/uploads/2023/06/Certinia-Information-Security-FAQ.pdf

Certinia Whistic Public Security Profile
https://www.certinia.com/trust/security-profile/

Certinia Privacy Data Protection Addendum
https://www.certinia.com/privacy/dpa/

Certinia Privacy Statement
https://www.certinia.com/privacy/privacy-statement/

Overview of Salesforce Security
https://security.salesforce.com/?_ga=2.36262564.525107183.1680039475-781319679.1680039475

Salesforce Security Implementation Guide
https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/