Entrust Cryptographic Security Platform

Course Description

ENTRUST

About this course

This 5-day hands-on course provides comprehensive training on deploying, configuring, and managing the Entrust Cryptographic Security Platform (CSP). It covers the full spectrum of cryptographic security implementations, including PKI operations, certificate lifecycle management, automated certificate enrollment protocols (ACME/WSTEP), CA Gateway as a RESTful interface for managing digital certificates across multiple vendor-neutral CA providers, timestamp services, vault management, and compliance governance—all unified within a single cohesive platform.

Participants will gain practical experience through guided lab exercises that mirror real-world enterprise scenarios. The course begins with CSP fundamentals and lab orientation, progresses through implementing PKI solutions with Certificate Authority and Certificate Manager, explores automated enrollment via ACME and WSTEP, and introduces CA Gateway exercises for vendor-neutral certificate lifecycle management. It then advances to timestamp services and vault management for secrets and key lifecycle operations. The course concludes with the Compliance Manager component, leveraging cryptographic metadata gathered throughout the labs to support governance and audit readiness.

The course emphasizes hands-on learning through scenario-based labs, enabling students to build complete cryptographic infrastructures and gain practical skills to manage certificates, keys, and secrets on a scale. Students implement unified cryptographic solutions that provide enterprise-wide visibility, control, and compliance across the cryptographic estate while preparing for the transition to post-quantum cryptography

Course Objectives

Upon completion of this course, participants will be able to:

PKI and Certificate Management

- Understand the overall structure of CSP and its components, including Certificate Authority, Certificate Manager, Certificate Enrollment Gateway, and CA Gateway
- Build Certificate Authority infrastructure from requirements through deployment in lab environments
- Initialize and configure Certificate Manager for centralized certificate discovery and lifecycle management
- Implement automated certificate enrollment using the ACME protocol for web server certificates
- Configure WSTEP integration for digital identity provisioning in Microsoft enterprise environments
- Deploy and configure CA Gateway as a vendor-neutral interface for managing certificate lifecycle operations across multiple Certification Authorities (CAs)
- Perform certificate issuance, renewal, and revocation through CA Gateway using RESTful APIs
- Integrate CA Gateway with enterprise systems to streamline certificate workflows and reduce operational complexity

- Deploy and configure timestamp services for document integrity and non-repudiation within the PKI ecosystem

Key Management and Cryptographic Operations

- Understand cryptographic fundamentals, including digital signatures and encryption processes within containerized environments
- Implement Entrust Vaults with decentralized vault architecture for secure key storage and management
- Configure Vault for multi-cloud key lifecycle management policies and procedures
- Design cryptographic policies for organizational security requirements using Compliance Manager
- Manage cryptographic assets across distributed enterprise environments using geographically distributed vaults

Compliance Management, Architecture and Administration

- Implement enterprise-wide compliance frameworks using Compliance Manager
- Apply security policies and documentation to reduce cryptographic risk across the organization
- Design ideal CSP architecture implementations with high availability and fault tolerance
- Assess and manage cryptographic risk posture through centralized compliance dashboards
- Configure administrative roles including Platform Administrator, Security Officer, and PKI Administrator using RBAC
- Implement API-driven certificate and key management operations using REST APIs and CLI tools
- Understand high availability and fault tolerance considerations for CSP component architecture
- Configure comprehensive monitoring and logging using integrated observability tools like Grafana

Prerequisites

Previous experience with the following is beneficial:

- Windows/Linux operating systems administration
- Basic networking and security concepts
- Enterprise system administration and integration concepts
- Cloud-native technologies (Kubernetes& docker)
- REST APIs and JSON/YAML configuration formats

Who should attend this course

This five-day hands-on course is intended for technology professionals who will be responsible for planning, implementing, configuring, managing, and supporting Entrust Cryptographic Security Platform services.

Course Lessons

Day 1 Cryptographic Security Platform Course overview

Lesson 1 CRYPTOGRAPHIC SECURITY PLATFORM fundamentals

This lesson will review the overall structure of the Cryptographic Security Platform and the components we will be focusing on in this course. This introduction will also include a demonstration of a working Cryptographic Security Platform environment with the use cases we will learn about already deployed.

Lesson 2 Security fundamentals

Cryptography and PKI fundamental concepts to provide a common language around keys, algorithms and digital processes such as digital signature and data encryption. Security objects are explored, and we explore the policies and documentation introduced in the demonstration.

Lesson 3 Lab orientation

Student access to labs will be provided, and they will have some guided exercises to begin developing their lab. Introduction to the Cryptographic Security Platform, the required components that will be used and the use cases and overall architecture we will be building.

Day 2 Implementing PKI with the Cryptographic Security Platform

Lesson 4 PKI use cases within Cryptographic Security Platform

A deeper look at the structure of the implementation of the Certificate Authority within Cryptographic Security Platform. What are all the services and how do they work together to provide a complete PKI solution, The role of the Entrust Certificate Authority Gateway, the Entrust Certificate Enrollment Gateway will be explained, and the use cases for our labs will be introduced (ACME, WSTEP)

Lesson 5 Implementing PKI with Cryptographic Security Platform

A look at the PKI implemented in the student lab system, understanding the Certificate Authority components and how they were configured.

Lesson 6: Student Lab – Build a Certificate Authority

Students will now be lead through the creation of the Certificate Authority structure based on a set of requirements.

Lesson 7: Entrust Certificate Manager & Initializing

In this lesson, students will initialize and explore the functions of Certificate Manager, gaining a centralized view of certificates and management capabilities.

Lesson 8: Certificate Manger Discovery and Exploring Grafana for Logs

This lesson will focus on the discovery capabilities of Certificate Hub while also introducing students to Grafana for log exploration.

Lesson 9: Entrust Certificate Enrollment Gateway (CEG)

In this lesson, students will learn about the Entrust Certificate Enrollment Gateway and its role in automating certificate enrollment and renewal. The session will cover the overview of CEG, the

installation process, and the protocols it supports.

Day 3 ACME / WSTEP & CA GATEWAY

Lesson 10: ACME use case
A look at how the ACME use case is implemented with Cryptographic Security Platform to leverage the Cryptographic Security Platform PKI to sign webserver certificates. Students will have lab exercises to implement ACME

Lesson 11: WSTEP use case
A look at how WSTEP is integrated with Cryptographic Security Platform to provide digital identities issued by Cryptographic Security Platform PKI to users and devices within a Microsoft enterprise. Demo and walk through of the use of WSTEP and the integration points.

Lesson 12: WSTEP lab
Students will have lab exercises to integrate WSTEP. A look at the WSTEP implementation in the student lab with exercises on policy/management and monitoring

Lesson 13: CA Gateway
In this lesson, you'll learn about the CA Gateway's core functions and its role in integrating with third-party Certification Authorities (CAs) through a flexible Certificate Lifecycle and Policy Management API. The CA Gateway allows applications to efficiently manage digital certificates, renewal, and revocation—across multiple vendor-neutral CA providers.

Day 4: Timestamp, OCSP and Vaults and secrets management

Lesson 14: Timestamp use case
Review of Ideal architecture and where Timestamp fits into architecture. Demo of the Timestamp function and discussion of the components.

Lesson 15: Timestamp Lab
Students will in the lab explore Timestamp integration and use.

Lesson 16: OCSP use case
Review of the OCSP process and components. The lifecycle management of the OCSP certificates and the integration points.

Lesson 17: OCSP Lab
Students will explore the OCSP solution integration in the lab.

Lesson 18: Vaults and Secrets Management
An introduction to vaults and secrets management

Lesson 19: Demo and lab for Vaults
Students will explore common vault use cases.

Day 5: Compliance manager and ideal architecture

Lesson 20: Security objects and compliance manager.

The ideal architecture touchpoints for Cryptographic Security Platform, where the Security Objects are in use cases are and a revisit of the role of the compliance manager.

Lesson 21: Lab and exercises for compliance manager

The students will be provided with guided exercises using the compliance manager on the security objects in their lab environment. They will learn to apply policies and add documentation to reduce risk.

Lesson 22: Architecture considerations

This is about the ideal implementation of the Cryptographic Security Platform and components. High Availability and fault tolerance considerations. More details on initial requirements and installation of the environment in detail.

Further Labs Details

Initial Setup

- LAB-01- Login to CSP with default username and password, change them and create new admin account

Certificate Authority (CA)

- LAB-02 - Initializing the CA
- LAB-03 - Create a root CA
- LAB-04 - Create a sub-CA
- LAB-05 - Connecting to the embedded CA gateway and making some REST API calls to query the database

Certificate Manager (Cert Hub)

- LAB-06 - Initialize the Certificate Manager
- LAB-07 - Connect the CSP CA Gateway to the Certificate Manager
- LAB-08 - Connect the CSP CA to the Certificate Manager
- LAB-09 - Access the CSP CA through Certificate Manager
- LAB-10 - Automate connect the CA Gateway of CSP CA for integrating it to CSP Compliance manager
- LAB-11- Create CSR for CSP Appliance and process it through Certificate Manager
- LAB-12- Connect the CSP PKI to Compliance Manager
- LAB-13 - Discovery scanner

Certificate Enrollment Gateway (CEG)

- LAB-14 - Initialize CEG
- LAB-15 - Enable CEG with ACME and request certificate through ACME client on IIS server

- LAB-16 - Enable WSTEP on CEG
- LAB-17 - Request user certificate through WSTEP
- LAB-18 - Review the configurations on client side (CEP, DC, Group policy, templates)
- LAB-19- How to enable extended logging on CEG

CA Gateway

- LAB-20 - Initialize CA Gateway
- LAB-21 - Configure CA Gateway
- LAB-22 - Enroll MSCS certificate through CA Gateway REST API
- LAB-23 - Integrate dedicated CA Gateway with Certificate Manager
- LAB-24 - Automate connect the CA Gateway of CSP CA for integrating it to CSP CA
- LAB-25 - Review configurations on MS PROXY and MSCA

Timestamping

- LAB-26 - Initialize Timestamping
- LAB-27 - Test Timestamping

Vaults

- LAB-28- Login to CSP Vaults with default username and password, change them and create new admin account
- LAB-29 - Create different vaults
- LAB-30 - Creating a functional BYOK AWS
- LAB-31 - Creating a function Database based vault with MS SQL

CSP Compliance Manager

- LAB-32 - Login to CSP Compliance Manager with default username and password, change them and create new admin account
- LAB-33 - Review security objects
- LAB-34 - Create custom policies and documentation

Administration

- LAB-35 - Backup and recovery
- LAB-36 - High Availability (how to add another node)