Entrust Certificate Authority Comprehensive (PKI)

Course Description

ENTRUST

About This course

Entrust Certificate Authority Comprehensive is a five-day, hands-on overview of Entrust Authority Security Manager and the components of the Entrust public-key infrastructure (PKI).

The introductory lessons of this course provide you with background information on the organizational requirements related to data security and the cryptographic operations used to satisfy these requirements. The concept of digital ID is introduced which leads into a discussion about digital certificates and the functionality of the Certification Authority (CA).

You will work in a lab with an install Entrust root CA, along with the administration interfaces and client desktop client software already installed. You will assume the different roles in the infrastructure to learn how to manage digital IDs for users and devices, customize policies, create and assign roles and organize the user community.

Advanced customization will be performed through manual editing of the certificate specification file.

Finally, students will have their own opportunity to install Entrust CA by installing a subordinate CA to the instructor's root CA.

Hands-on exercises at the end of each section provide you with the ability to apply the knowledge gained through the lecture segment of each lesson.

Each day's lecture portion of the training will be 3-4 hours long. The remaining time of the class is for lab exercises. There is also a 2–3-hour lab commitment per day for this course.

Lab Exercises

Students will be provided with an AWS lab accessed via RDP for the training duration. Use of the lab will require access to an RDP application and the inclusion of a public IP address in our firewall. The instructor will work with all students to arrange for access to the labs on the first day of class.
Lab assignments are provided at the end of each day of lecture and are to be done prior to the next day's lecture.

Course Objectives

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

- Describe the steps in the encryption and digital signature operations
- Identify the contents of the digital ID and the need for digital certificates
- Identify the components of the public key infrastructure (both required and optional) and describe the role of the Certification Authority
- Install, configure and initialize PKI Enterprise on Windows Server as a subordinate CA
- Assume the roles used in the public-key infrastructure, including Master User, Security Officer, Administrator, Auditor, Directory Administrator, and End User and identify their characteristics
- Use management and client software on Windows Server
- Register and activate digital IDs for administrative users, end users and devices

- Identify the various security stores that can be used to store digital IDs
- Perform typical management operations on users and devices
- Implement the organization's security policy by customizing policies and certificate specifications
- Supplement the built-in certificate types available in PKI Enterprise by creating additional customized types
- Customize the administrative environment using groups, search bases, roles, and templates
- Assess logging information generated by PKI Enterprise
- Recover from disaster scenarios related to digital IDs, the Directory, and PKI

Enterprise Products covered in the course

- Entrust Certificate Authority (PKI) Enterprise
- Certificate Authority (PKI) Enterprise Administration
- Entrust Certificate Agent (Entelligence Security Provider (ESP))
- Certificate Authority (PKI) Enterprise Administration Services UMS, URS and CSRES
- Entrust Cryptographic Security Platform (CSP)

Prerequisites

While prior knowledge of the concepts behind the public-key infrastructure is helpful, participants do not require any previous experience with Entrust products.
Previous experience with the Windows operating system is required as the hands-on exercises are completed on computers running Windows Server

Who should attend this course

This five-day hands-on course is intended for technology professionals who will be responsible for operationally managing and supporting Entrust PKI Certificate Authority and its components. For those with the need to manage a CA with Administration Services it is also recommended to take the 2 day *Managing users in Administration Services* course after this training.

Course Lessons

The PKI Enterprise Comprehensive course includes the following lessons.

LESSON 1 Security concepts

This lesson introduces the cryptographic operations of encryption and digital signatures and the requirements for a digital ID. The key-pair models used in PKI Enterprise are introduced.

LESSON 2 Digital certificates

This lesson details how identities are associated with individuals through the use of digital certificates. The format of the X.509 certificate is described, and the types of certificates available in PKI Enterprise are presented.

LESSON 3 Entrust Certification Authority

This lesson discusses the concept of third-party trust and the responsibilities of the Certification Authority. The different key pairs used by the Certification Authority are reviewed.

LESSON 4 Entrust public-key infrastructure

The lesson describes the components, services, and roles in the Entrust public-key infrastructure.

LESSON 5 The role of the Directory

This lesson describes the role of the Directory, as well as presenting some of the terminology used when discussing Directories in the context of the public-key infrastructure.

LESSON 6 Installing PKI Enterprise

In this lesson, participants will review how to install and initialize PKI Enterprise and take over management of their own pre-installed CA for lab work.

LESSON 7 PKI Enterprise Control Command Shell

This lesson outlines some of the tasks performed by Master Users in PKI Enterprise Command Shell.

LESSON 8 Registering and activating administrative users

This lesson discusses the steps in registering and activating digital IDs for administrative users.

LESSON 9 Managing key pairs

This lesson outlines the creation, storage and automatic rollover of the keys and certificates that make up the digital ID.

LESSON 10 Entrust Certificate Agent (Entelligence Security Provider (ESP))

This lesson introduces Entrust client tool as one form of client software. A customized installation package is created, and the software is installed on the participant's Windows computer. You will register and activate digital IDs using Entrust Certificate Agent, these digital IDs will be used in the lessons that follow.

LESSON 11 Managing users
This lesson describes the day-to-day user management activities performed by administrative users. You will assume the role of an administrative user and will perform typical management operations on members of their user community.

LESSON 12 Distributing revocation information
This lesson discusses the mechanisms for distributing revocation information to client applications.

LESSON 13 General security policy
This lesson describes the general security policy properties and how they are used to customize the behavior of the administrative environment.

LESSON 14 Client policies
This lesson describes the client policy properties and how they are used to customize the behavior of different collections of users.

LESSON 15 Roles and permissions
This lesson defines roles as the mechanism for assigning client policy properties and administrative permissions to users.

LESSON 16 Organizing users
This lesson describes how groups and search bases can simplify the organization of users for administration purposes.

LESSON 17 Bulk operations
This lesson examines bulk operations as a way of automating management tasks.

LESSON 18 Logging and reporting
This lesson describes some of the tasks related to auditing system events and creating reports.

LESSON 19 Certificate definition policies
This lesson describes the certificate definition policy properties and how they are used to customize certificates activated through Entrust *Certificate Agent*.

LESSON 20 Customizing certificate specifications
This lesson describes how the content of a digital certificate can be further customized by modifying certificate specifications.

LESSON 21 Cross-certification
This lesson outlines the reasons for performing cross-certification, the different types of cross-certification and how the operation is performed in PKI Enterprise.

LESSON 22 Hierarchical cross-certification

This lesson examines the specialized hierarchical cross-certification trust model. You will be able to install and initialize a CA as a subordinate in the optional lab.

LESSON 23 CA Key Update

This lesson reviews the procedures and built-in utilities to plan for and perform a CA key update.

LESSON 24 Disaster recovery

This lesson details some possible disaster scenarios that may be encountered when administering PKI Enterprise and provides possible recovery steps.

LESSON 25 PKI Enterprise Administration Services

This appendix introduces the Web-based administration interfaces provided by Administration Services. You will use the User Management Service (UMS) of PKI Enterprise Administration Services to do basic User administration tasks. The differences between the UMS interface and PKI Enterprise Administration will be highlighted. You can also explore URS and CSRES in your lab.

LESSON 26: Entrust Cryptographic Security Platform (CSP).

This lesson introduces the use of full spectrum of cryptographic security implementations, including PKI operations, certificate lifecycle management, automated enrollment protocols, CA Gateway, timestamp services, validation authority and compliance governance—all unified within a single, cohesive platform.