

Course : Public Key Infrastructure (PKI) and Windows certificate services

Practical course - 4d - 28h00 - Ref. PKG

Price : 2650 CHF E.T.

NEW

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Master the essentials of encryption
- ✓ Install and configure a Windows certification authority
- ✓ Manage the deployment, renewal and restoration of certificates
- ✓ Use Trusted Platform Module (TPM) and smart cards for certificate storage
- ✓ Implement data encryption, signature and authenticity using certificates
- ✓ Managing certificate revocation

Intended audience

Engineers, system and network administrators.

Prerequisites

Good knowledge of the Windows Server operating system, networks and IT security.

Course schedule

1 The essentials of encryption

- Why PKI?
- Roles and infrastructures.
- The components of an enterprise PKI.
- Symmetrical and asymmetrical encryption.
- Combination of the two encryption methods.

Hands-on work

Understand symmetric encryption protocols and how they can be used in combination with asymmetric encryption.

PARTICIPANTS

Engineers, system and network administrators.

PREREQUISITES

Good knowledge of the Windows Server operating system, networks and IT security.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.

Participants also complete a placement test before and after the course to measure the skills they've developed.

2 Certification authority

- Type of certification authority.
- Implementation of an enterprise root certification authority.
- Setting up and configuring a certification authority.
- Backing up and restoring certification authorities.

Hands-on work

Déploiement manuel et automatisé d'une autorité de certification racine d'entreprise. Gestion des modèles de certificats.

3 Certificate management

- Certificate components.
- Certificate registration.
- Certificate templates.
- Automatic certificate deployment.
- Configure group policies for automatic certificate deployment.
- Certificate templates updated.
- Certificate storage locations.
- Machine and TPM certificates.
- Smart cards and certificate registrars.

Hands-on work

Deploy different Windows certificates manually and automatically. Protect computer certificates using TPM. Smart card management.

4 Data encryption

- An introduction to the concept and benefits of data encryption.
- Implement and troubleshoot EFS (Encrypting File System) encryption.
- Sharing encrypted files.
- Recovery agent implementation.
- Encryption and strong authentication.

Hands-on work

Implement file encryption and recover encrypted files using recovery agents.

5 Data signature

- Data authentication and integrity.
- Concept and techniques for signing with certificates.
- Data integrity validation.

Hands-on work

Configure PowerShell code signing. Automatically deploy "authenticated editors".

6 Website security

- Web server certificate registration.
- Implement a secure web server.
- Handles connection errors.
- Web server certificate revocation.

Hands-on work

Configure authentication and encryption on a secure web server.

TEACHING AIDS AND TECHNICAL RESOURCES

- The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
- At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
- A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

7 Certificate archiving

- Certificate archiving and retrieval concept.
- Creation of recovery agents.
- Enable certificate archiving.
- Retrieve archived certificates.

Hands-on work

Import and export certificates. Archive certificates and retrieve archived certificates.

8 Certificate revocation management

- Certificate revocation process.
- Modification of CDP and AIA certificate lists.
- Publication of revocation lists.
- Publication of revocation in HTTP.

Hands-on work

Modification of CDP (customer data platform) and AIA locations and testing of access to revocation lists.

9 OCSP (Online Certificate Status Protocol) server

- Concept and implementation of an OCSP server.
- OCSP certificate customization.
- Install the OCSP server.
- Modify the certification authority's "extensions".
- Revocation configuration.
- Résolution DNS Interne\Internet du serveur OCSP.
- OCSP revocation for an SSTP VPN server.
- OSCP online answering machine validation.

Hands-on work

Implement, configure and validate a Windows OCSP server.

Dates and locations

REMOTE CLASS

2026: 16 June, 8 Sep., 8 Dec.