

Course : PKI, implementation

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

Price : 2960 CHF E.T.

★★★★☆ 4,4 / 5

BEST

This course will show you how to carry out a Public Key Infrastructure (PKI) project in the best possible conditions. Practical exercises will teach you how to deploy a certification authority, generate certificates and implement secure messaging and Single Sign-On (SSO) solutions.

Teaching objectives

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

- ✓ Understanding the various symmetrical and asymmetrical encryption algorithms
- ✓ Implementing a hierarchy of certification authorities
- ✓ Implementing secure messaging
- ✓ Implement strong authentication using X509 certificates

Intended audience

Engineers, system and network administrators.

Prerequisites

Good knowledge of systems, networks and IT security.

Course schedule

1 Introduction

- The weaknesses of traditional solutions.
- Why isn't e-mail secure?
- Can we trust password-based authentication?
- Impersonation of the sender of a message.

Hands-on work

Use of protocol gaps.

PARTICIPANTS

Engineers, system and network administrators.

PREREQUISITES

Good knowledge of systems, 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 Cryptography

- Concepts and vocabulary.
- Symmetric and asymmetric encryption algorithms.
- Hash functions: principle and usefulness.
- Key exchange techniques.
- Install and configure an SSH server.
- SSH and Man in the Middle.
- SSH, asymmetric encryption without certificates.

3 Digital certification

- Presentation of the X509 and X509v3 standards.
- Certification authorities.
- Delegation of trust.
- Electronic signature and authentication.
- Personal certificates and private keys.
- Export and import certificates.

Hands-on work

Microsoft certificate stores.

4 PKI architecture

- How to build a certification policy?
- Certification authority. Certificate publication.
- Registration Authority (RA).
- Hierarchical and distributed trust models.
- LDAP v3 protocol overview.
- Implementation of a root certification authority.
- Generate user and server certificates.

Hands-on work

Implementation of a hierarchy of certification authorities.

5 PKI project management: which applications to start with?

- The different components of a PKI project.
- Choice of technologies.
- Legislation.

6 Overview of market offers

- The Microsoft approach.
- Dedicated commercial offers: Betrustrad (ex-Baltimore) and Entrust.
- OpenPKI: the open source community.
- IdealX, between commercial and open source solutions.
- Certplus and Versign outsourced services...

Hands-on work

SSL v3 Web-SSO authentication with application firewall. Strong authentication with X509 certificate. Secure mail server and certificate directory.

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.

REMOTE CLASS

2026 : 2 June, 15 Sep., 15 Dec.