# Public key infrastructures («PKI»)

You will learn the theoretical basics of the Public Key Infrastructure (PKI). You will then learn how to set up, correctly configure, manage, secure and troubleshoot all components of a complete PKI environment.

**Duration:** 2 days
**Price:** 1'700.–
**Course documents:** Digicomp course material

## Content

A public key infrastructure (PKI) is an effective tool for protecting systems and services on the internet. Although PKI has been in development for over 20 years, it is only in the last few years that it has become a topic of discussion among security managers. A major market driver are the new possibilities of digital signatures, which require a PKI.

Public-key cryptography is a mature technology that forms the basis for secure protocols. A standard mechanism for the distribution of public keys was not available for a long time. Today, however, progress has been made on both sides. You no longer need to be an expert in public-key cryptography to recognise its advantages. Because today, a wide variety of products are available on the market. This course will help you to choose the right ones for you from the many possibilities and to use them successfully.

**Contents Day 1: Theory day**

Introduction

- Problem definition
- History
- Legal aspects

Cryptographic basics

- Symmetric and asymmetric procedures
- Digital signatures
- Key Management

Authentication

- Password-based
- One-time passwords
- Kerberos
- Public Key Certificates

PKI-based

- Certificates
- Certificate Revocation List
- Policies
- Certification paths

PKI components

- Certification Authority (CA)
- Registration Authority (RA)

- Repository
- Archive
- Certificate holder
- Relying Party

PKI architectures

- Single CA
- Hierarchical infrastructure
- Network structure
- Cross-certification
- Bridges CA

Verification

- Construction and verification of certification paths

Certificate Revocation List (CRL)

- Content
- Creation and distribution of CRLs

Directories

- X.500, LDAP

X.509 certificates

- ASN.1 types
- Basic content
- Extensions
- Use

Trust, procedures, policies

- Certificate Policies (CP)
- Certificate Practice Statement

Applications

- Web: SSL/TLS
- Email: S/MIME
- IPsec

**Contents Day 2: Practical day**

Setting up a two-tier certification authority environment with a stand-alone offline root certification authority

- Setting up an underlying Enterprise (AD-based) Online Sub Certification Authority
- What is configured differently if only a single-tier CA environment (Enterprise Root CA) is used?
- Use of the CaPolicy.inf file
- Complete and correct revocation list configuration (CRL), including configuration of an online responder
- Configuration of certificate templates
- Configuration of automatic certificate request and distribution as well as renewal via GPOs
- Proper configuration and setup of SSL certificates
- Certificate revocation
- Special configurations: archiving private keys, setting up certificate agents, etc.

- Monitoring Certification Authorities
- Backup and restore Certification Authorities
- Using command line tools (e.g. certutil.exe) and PowerShell when configuring and managing Certification Authorities

## Key Learnings

At the end of the theory part you will be able to,

- formulate the architecture and components of a public key infrastructure
- know how to solve problems when setting up a public key infrastructure
- know what to look for when defining certificate content
- know about the most important standard applications

After the public key infrastructure practice day, you will be able to set up, properly configure, manage, secure and troubleshoot all the necessary components of a complete PKI environment

## Methodology & didactics

This seminar is designed for two course days. On the first day, you will learn the theoretical basics of PKI. The second day is a purely practical day, where the basics learned on the first day are put into practice.

## Target audience

Developers and technical architects who want to build a PKI or produce protected applications.

## Further courses

- Administering Microsoft Endpoint Configuration Manager («55348A»)

## Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-security/cyber-security-defense/course-public-key-infrastructures