Mastering Public Key Infrastructure

Overview
Public Key Infrastructure (PKI) becomes a critical component of every enterprise IT infrastructure when it comes to confidentiality, data integrity and security in general. Every single organization today is using more or less PKI components – it might be only for Web Servers (HTTPS), data encryption (SQL encryption) or it might be even for user’s authentication (Smart Cards) and encryption (EFS, S/MIME).

PKI is sometimes difficult to understand since it relates to different areas of knowledge – IT infrastructure, security and legal policies, hardware devices (smart cards, hardware security modules).

This three-day instructor-led training provides in-depth training on designing, configuring and troubleshooting Active Directory Certificate Services (PKI) in Windows Server OS (current version is based on Windows Server 2012 R2).

The training is based on Microsoft Official Curriculum and further developed by the security consultants at ITCE including all the experience from real PKI projects. Students will be able to hear best practices, real project challenges and PKI solutions that work in the real life.

Audience
This course is intended for Information Technology (IT) Professionals, Developers and Security Officers interested in Public Key Infrastructure.

Prerequisites
Basic understanding of Microsoft Windows Server and Active Directory Services.

Course Outline
Module 01 – Introduction to Public Key Infrastructure
- Describe Symmetric and Asymmetric Encryption
- Describe PKI and its components
- Describe Microsoft AD Certificate Services in Windows Server 2012

Module 02: Designing a Certification Authority Hierarchy
- Identifying CA Hierarchy Design Requirements
- Common CA Hierarchy Designs
- Documenting Legal Requirements
- Analyzing Design Requirements
- Designing a CA Hierarchy Structure

Lab02 – Design a two-tier PKI solution

Module 03 – Implementing and Managing Certification Authorities
- Options for implementing CA hierarchies
- Deploy a root CA and subordinate CA
- Configure CA properties
- Plan and Configure CRLs
- Planning for High Availability of PKI
- Backup and Restore a CA

Lab03 – Deploy and configure a two-tier PKI solution

Module 04 – Deploying and Configuring Certificates
- Describe certificates and certificate templates
- Configure certificate template settings in Windows Server 2012
- Modify and enable a certificate template
- Key Archival and recovery

Lab04 – Deploy Certificate Templates

Module 05: Configuring Certificate Enrollment
- Introduction to Certificate Enrollment
- Enrolling Certificates Manually
- Creating and managing custom CSRs
- Auto-enrolling Certificates

Lab05 – Enrolling Certificates

Module 06 – Certificates Usage
- Using Certificates for SSL
- Using Certificates in Email Security – S/MIME
- Using Certificates for Digital Signatures
- Using Certificates for Content Encryption
- Using Certificates for Authentication
- Using Certificates for Smart Cards

Lab06 – Practical digital certificate usage

Module 07 – Integration with Hardware Cryptography Service providers
- Using Smart Cards for Authentication
- Using Hardware Security Modules for storing server certificates