

# Planning & managing Public Key Infrastructure (PKI) - Implementation in Microsoft environment with Active Directory Certificate Services (ADCS)

## COURSE OVERVIEW

This course helps any IT specialists to gain knowledge in managing robust PKI and having better understanding of topics surrounding public key infrastructure. Moreover, the PKI course is a preparation for the increasingly critical technologies which ensures confidentiality, integrity, and authentication in an enterprise. The course provides the knowledge and skills necessary to select, design and deploy PKI, to secure existing and future applications within your organization. It also gives a look into the foundations of cryptography and the working concepts of the algorithms being used.

More specifically, the course focus on PKI implementation in Microsoft Active Directory Certificate Services (ADCS).

It also gives an overview of different Microsoft technologies that use certificates for confidentiality, authentication and integrity.

## INTENDED AUDIENCE

Individuals who needs a working knowledge of PKI or anyone involved in managing or using Public Key Infrastructure in the organization using Microsoft technologies.

## PREREQUISITE

- General knowledge of Windows Server 2008-2012
- General knowledge of networking
- Good understanding of IT administration

## DURATION

4-5 days

## CONTENT

### General PKI Concepts

- Review of symmetric & asymmetric encryption
- Algorithms
- Keys
- Overview of PKI
- Components, CP, CPS
- PKI architectures & design
- RootCA, policy-CA, issuing CA

- Hierarchical model, cross-certification,
- Certificates & Revocation
- Versions, extensions, types of CRL, OCSP
- Enrollment: Manual, automatic
- Using SSL
- PKI and wireless applications
- Using smartcards
- Belgian eID
- Using s/MIME secure mail (signing/encrypting)
- Legal Issues

#### **Overview of Microsoft security &PKI**

- Exploring Identity and Access Solutions
- What's New in AD CS Windows Server 2012

#### **Deploying and Configuring Active Directory Certificate Services (ADCS)**

- Deploying CAs
- Deploying and Managing Certificate Templates
- Implementing Certificate Distribution and Revocation
- Managing Certificate Recovery
- Deploying and Configuring Certificates with ADCS
- Maintaining Windows 2012 ADCS
- OCSP
- Configuring CA policy (CAPolicy.inf)
- Network Device Enrollment Service (NDES)
- Backup of PKI

#### **Planning & designing PKI in Windows Server 2012**

- Planning and Implementing Deployment of a Certification Authority
- Planning and Implementing Certificate Templates
- Planning and Implementing Certificate Distribution and Revocation
- Planning and Implementing Key Archival and Recovery
- 

#### **Microsoft technologies using ADCS**

- EFS, Bit locker (File & volume encryption)
- IIS (Web services)
- FIM
- VPN, IPsec
- Direct Access
- AD RMS Services (Active Directory Rights Management Services)
- AD FS Services (Active Directory Federation Services)
- Exchange: OWA, Outlook Anywhere, EAS, Connector, TLS
- Office signed Documents
- Outlook with s/mime
- Forefront Threat Management Gateway (TMG): VPN, HTTPS Inspection, HTTPS listener

- Microsoft Forefront Identity Manager (FIM)
- Etc.

#### Wariness

- The DOs and DON'Ts of PKI
- Risks of PKI

Conclusions, questions & answers, evaluation.