Windows Server - Enterprise PKI Deployment

Course code: GOC173

This instructor led course provides students with advanced teoretical knowledge and practical experience in designing, deploying, operating and troubleshooting PKI on Windows platform. The first part of the taining provides recapitulation of public key cryptography princples and the cryptographic and security properties of various algorithms and technologies, such as RSA, DSA, AES, DH, EC-DH, EC-DSA, 3-DES, SHA-1, SHA2 (SHA-256, SHA-384, SHA-512), MD5 and others - not only from the security point of view, but also in regard to their compatibility over wide range of systems starting with Windows 2000 and going through XP, 2003, 7, 2008 R2 and Windows 10 or Windows 2019. The larger part of the training brings deep practical experience with installing, configuring and operating complex hierarchies of AD CS servers. Students will define certification policies (certificate templates), deploy certificates manually as well as automatically (autoenrollment) and will also troubleshoot the deployment and key and certificate lifecycle, implement key backup and recovery and manage CA lifecycle. The course is taught by trainers who are certified on Microsoft Certified Master Directory Services (MCM: Directory).

At course completion students will be able

Understand detailed differences between various properties of cryptographic algorithms currently in use

Assess differences between hash algorithms MD4, MD5, SHA-1, SHA2 (SHA-256, SHA-384 and SHA-512) and their combinations with public key schemes such as RSA, DSA, ECDSA as well as symmetric algorithms such as AES and 3DES

Know about precise support conditions and compatibility problems among the algorithms (not)available in Windows 2012 and older

Understand SSL/TLS protocol, its versions and available algorithm suites and their compatibility

Plan and install AD CS certification authorities in the most secure yet flexible manner

Manage CA and certificate and private key lifecycle, their protection, backup and restore and decommision

Prerequisities

Knowledge in extent of the courses which are listed in the bellow sections Previous Courses and Related Courses

Good understanding of Active Directory and Group Policy

Good understanding of TCP/IP and DNS technologies

Course outline

Recapitulation of basic cryptographic terms

Public key cryptograprhy, Symmetric algorithms, Hashes and their comparison

MD4, MD5, SHA-1, SHA2 (SHA-256, SHA-384, SHA-512), RSA, DSA, ECDSA, DH, ECDH, AES, 3-DES and DES, Suite-B

Comparable algorithm strength and algorithm compatibility in Windows family of systems

CSP and CNG providers and libraries, application and Windows support in Windows 2012 and older

SSL and TLS protocols and versions, algorithm suites and their compatibility

Digital certifiate and their contents

Subject, Issuer, Serial Number, SAN, EKU, AIA, CDP, thumbprint, alternate signature format

Certification Authorities, certificate chains and their validation and trust

CA versioning, certificate and CA renewal and decommision or revocation

Prerequisities to install AD CS certification authority

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Installing AD CS offline root CA and issuing subordinate CA

AD CS integration with Active Directory and administrative role separation

Certification policies, certificate templates and their versions, CSP and CNG templates

Certificate template parameters and security

Autoenrollment, manual enrollment, renewal and enrollment agents

Certificate requirements for server applications such as SSL/TLS severs, SQL, DC, RDS/TS, LDAPS, System Center, Reporting Services, Exchange, SharePoint, UAG

Certificate requirements for client applications such as smart card Kerberos PKINIT logon, IPSec, SSL/TLS logon, EFS

Digital signatures and encryption for email, files, documents and scripts

Certificate revocation, CRL and OCSP

Certificate and private key lifecycle, private key storage, archival, backup and recovery

Certification authority lifecycle, renewal, revocation and decommisioning

Designing and building complex enterprise CA chains

Preparation for Microsoft certification

Most Microsoft certification exams do not require students to attend an official MOC course in order to pass the exam. This applies to all certifications except for MCM

Official Microsoft MOC courses as well as our own GOC courses are good ways of preparation for Microsoft certifications such as MCP, MTA, MCSA, MCSE or MCM

This does not mean that official MOC courses would serve as the only necessary praparation. The primary goal of an MOC course is to provide for sufficient theoretical knowledge and practical experience to effectively work with the related product

MOC courses usually cover most of the topics required by their respective certification exams, but often do not give every topic the same amount of time and emphassis as may be required to completelly pass the exam

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk