Windows Server - Enterprise PKI Deployment

Kód kurzu: GOC173

Pětidenní kurz seznámí posluchače se všemi principy a technikami plánování, nasazení, správy a řešení potíží s PKI na platformě Windows. V úvodu kurzu se zopakují principy kryptografie veřejných klíčů a dalších algoritmů a technologií, aby účastníci byli schopni plánovat nasazení algortmů jako je RSA, SHA-1, SHA2 (SHA-256, SHA-384 a SHA-512), AES, 3-DES, DH, EC-DSA, EC-DH, DSA, MD5 a dalších - nejen z pohledu bezpečnosti, ale také s důrazem na kompatibilitu v širokém rozsahu systémů od Windows 2000, přes XP, 2003, 7 a 2008 R2 až po Windows 10 a Windows 2019. Jedním z cílů je seznámit účastníky s požadavky na Suite-B kryptografii. Po zbytek kurzu se účastníci naučí naplánovat a nasadit hierarchii certifikačních autorit pomocí služby AD CS a definovat certifikační politiky (certificate templates) pro různé aplikace od SSL/TLS, přes digital a code signing, secure email a S/MIME až po přihlašování klientskými certifikáty a čipovými kartami pro Kerberos PKINIT. V průběhu celého kurzu se probírá životní cyklus certifikátů a jejich klíčů, zálohování klíčů i certifikačních autorit a řešení potíží při vydávání ručním i automatickém (autoenrollment). Všichni lektoři kurzu jsou certifikování na nejvyšší možnou technologickou úroveň v této oblasti MCM:Directory a/nebo MCSM:Directory.

Pro koho je kurz určen

Jedná se o pokročilé školení pro zájemce o principy, plánování, nasazení a správu, sledování a dlouhodobou údržbu PKI postaveného nad Windows platformou.

Kurz obsahuje kompletní tématiku AD od verzí Windows 2000 až po Windows 2019.

Co vás na kurzu naučíme

Zopakujeme základní principy kryptografie symetrické i veřejných klíčů a do detailu probere rozdíly mezi jednotlivými algoritmy

Porovnáme dnešní běžné hešovací algoritmy jako je MD4, MD5, SHA-1 a SHA2 (SHA-256, SHA-384, SHA-512) a dáme je do vztahu s algoritmy šifrovacími

Budeme porovnávat sílu jednotlivých kombinací algoritmů a kryptografických systémů

Do detailu popíšeme (ne)podporu jednotlivých algoritmů v operačních systémech a aplikacích od Windows 2000 po Windows 8 a Windows 2012

Porozumíte SSL a TLS protokolům a jejich kompatibilitě a podpoře na Windows operačních systémech

Probereme všechna pole, která vůbec můžete spatřit uvnitř digitálních certifikátů

Naučíte se nainstalovat podnikové PKI postavení nad Active Directory a Windows 2012

Budete schopni definovat bezpečné a udržovatelné certifikační politiky a uvědomíte si, jaké jsou možnosti a podmínky životního cyklu certifikátů

Zvládnete procesy související se zálohováním, cestováním a obnovou privátních klíčů

Pochopíte, jak je třeba udržovat a nastavit životní cyklus certifikačních autorit, zvládnete hladce jejich obnovy a prodlužování i likvidaci

Vytvoříte spolehlivou infrastrukturu pro ověření platnosti a zneplatnění certifikátů pomocí CRL i OCSP

Naučíte se plánovat nasazení PKI v malých i rozlehlých podnikových sítích

Předpokládané vstupní znalosti

Znalosti v rozsahu kurzů uvedených v sekcích Předchozí kurzy a Související kurzy

Dobrá znalost Active Directory a Group Policy

Dobrá znalost technologií TCP/IP a DNS

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

Windows Server - Enterprise PKI Deployment

Osnova kurzu

Opakování kryptografie

Heše, symetrická kryptografie a kryptografie asymetrická

Veřejné a privátní klíče, digitální podpis, časová razítka

MD4 vs. MD5 vs. SHA-1 vs. SHA-2

RSA, DSA, ECDSA, DH, ECDH, AES, DES, 3DES, SuiteB

Porovnání bezpečnosti na základě délky klíčů a bitových sil algoritmů

Comparable Algorithm Strength

Podpora algoritmů a jejich kompatibilita ve Windows

CSP a CNG poskytovatelé a knihovny, podpora v aplikacích

Funkce SSL a TLS, algorithm suites a podpora přes verze Windows

Certifikáty, základní a rozšířená pole

SAN, EKU, Subject, Issuer, Serial Number, Thumbprint, AIA, CDP

Certifikační autority, stromy a certificate chain, verze autorit

Důvěryhodné autority, automatická instalace a stahování

Plánování certifikační autority, veřejné autority vs. soukromé podnikové CA

Předpoklady pro instalaci AD CS certifikační autority

Instalace offline root CA a issuing subordinate CA

Integrace AD CS a Active Directory

Separace rolí správců autority a certifikátů

Certifikační politiky a jejich životní cyklus, certificate templates (v1, v2, v3)

Parametry šablon certifikátů, issuance policies a renewal policies, registrační autority (RA)

Požadavky na aplikační certifikáty serverů SSL/TLS, RDS/TS, DC, LDAPS, SQL, System Center, Reporting Services, Exchange, SharePoint, UAG

Požadavky na aplikační ceritifkáty klientů a IPSec, přihlašování k SSL/TLS, Kerberos PKINIT a čipové karty, EFS

Šifrování a digitální podpis mailu, souborů, dokumentů a skriptů

Zneplatnění certifikátů, CRL a OSCP

Plánování a nasazení CRL a OCSP distribučních bodů

Životní cyklus certifikátů a jejich privátních klíčů, obnova a prodloužení, uložení klíčů, zálohování klíčů a jejich roaming

Životní cyklus certifikačních autorit, jejich prodloužení a zneplatnění

Plánování hierarchie certifikačních autorit

Zálohování, obnova, řešení potíží, odstranění, migrace a upgrade AD CS

Příprava k certifikačním zkouškám

U certifikačních zkoušek Microsoft platí, že kromě certifikací MCM, není účast na oficiálním MOC kurzu nutnou podmínkou pro složení zkoušky.

Oficiální kurzy MOC společnosti Microsoft i naše vlastní kurzy GOC jsou vhodnou součástí přípravy na certifikační zkoušky firmy Microsoft jako jsou MTA, MCP, MCSA, MCSE nebo MCM.

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

Windows Server - Enterprise PKI Deployment

Primárním cílem kurzu ovšem není přímo příprava na certifikační zkoušky, ale zvládnutí teoretických principů a osvojení si praktických dovedností nutných k efektivní práci s daným produktem.

MOC kurzy obvykle pokrývají téměř všechny oblasti požadované u odpovídajících certifikačních zkoušek. Jejich probrání na kurzu ale nebývá dán vždy přesně stejný čas a důraz, jako vyžaduje certifikační zkouška.

Jako další přípravu k certifikačním zkouškám lze využít například knihy od MS Press (tzv. Self-paced Training Kit) i elektronický self-test software.

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved