# Windows Server - Enterprise PKI Deployment

Kód kurzu: GOC173

Tento päťdňový kurz zoznámi poslucháčov so všetkými princípmi a technikami plánovania, nasadenia, správy a riešenia problémov s PKI na platforme Windows. V úvode kurzu sa zopakujú princípy kryptografie verejných kľúčov a ďalších algoritmov a technológií, aby účastníci boli schopní plánovať nasadenie algoritmov ako je RSA, SHA-1, SHA2 (SHA-256, SHA-384 a SHA-512), AES, 3-DES, DH, EC-DSA, EC-DH, DSA, MD5 a ďalších – nielen z pohľadu bezpečnosti, ale taktiež s dôrazom na kompatibilitu v širokom rozsahu systémov od Windows Server 2000 cez Windows XP, Windows Server 2003, Windows 7 a Windows Server 2008 R2 až po Windows 10 a Windows Server 2019. Jedným z cieľov je zoznámiť účastníkov s požiadavkami na Suite-B kryptografiu. Počas zvyšku kurzu sa účastníci naučia naplánovať a nasadiť hierarchiu certifikačných autorít pomocou služby AD CS a definovať certifikačné politiky (Certificate Templates) pre rôzne aplikácie od SSL/TLS cez Digital a Code Signing, Secure e-mail a S/MIME až po prihlasovanie klientskymi certifikátmi a čipovými kartami pre Kerberos PKINIT. V priebehu celého kurzu je preberaný životný cyklus certifikátov a ich kľúčov, zálohovanie kľúčov i certifikačných autorít a riešenie problémov pri vydávaní ručným i automatickým spôsobom (Autoenrollment). Všetci lektori kurzu sú certifikovaní na najvyššiu možnú technologickú úroveň v tejto oblasti MCM: Directory.

## Pre koho je kurz určený

Ide o pokročilý kurz pre záujemcov o princípy, plánovanie, nasadenie a správu, sledovanie a dlhodobú údržbu PKI postaveného nad Windows platformou.

Kurz obsahuje kompletnú tematiku AD od verzií Windows 2000 až po Windows Server 2019.

## Čo vás na kurze naučíme

- Zopakujeme si základné princípy kryptografie symetrickej i verejných kľúčov a do detailu preberieme rozdiely medzi jednotlivými algoritmami
- Porovnáme dnešné bežné hešovacie algoritmy ako je MD4, MD5, SHA-1 a SHA2 (SHA-256, SHA-384, SHA-512) a dáme ich do vzťahu s algoritmami šifrovacími
- Budeme porovnávať silu jednotlivých kombinácií algoritmov a kryptografických systémov
- Do detailu si popíšeme (ne)podporu jednotlivých algoritmov v operačných systémoch a aplikáciách od Windows 2000 po Windows 8 a Windows Server 2012
- Porozumiete SSL a TLS protokolom a ich kompatibilite a podpore na Windows operačných systémoch
- Preberieme si všetky polia, ktoré vôbec môžete zbadať vo vnútri digitálnych certifikátov
- Naučíte sa nainštalovať podnikové PKI postavené nad Active Directory a Windows Server 2012
- Budete schopní definovať bezpečné a udržiavateľné certifikačné politiky a uvedomíte si, aké sú možnosti a podmienky životného cyklu certifikátov
- Zvládnete procesy súvisiace so zálohovaním, cestovaním a obnovou privátnych kľúčov
- Pochopíte, ako je potrebné udržiavať a nastaviť životný cyklus certifikačných autorít, zvládnete hladko ich obnovu a predlžovanie i likvidáciu
- Vytvoríte spoľahlivú infraštruktúru pre overenie platnosti a zneplatnenie certifikátov pomocou CRL i OCSP
- Naučíte sa plánovať nasadenie PKI v malých aj rozľahlých podnikových sieťach

## Predpokladané vstupné znalosti

- Znalosti v rozsahu kurzov uvedených v sekcii Predchádzajúce kurzy
- Dobrá znalosť princípov Active Directory a Group Policy
- Dobrá znalosť technológií TCP/IP a DNS

## Osnova kurzu

- Opakovanie kryptografie
- Heše, symetrická kryptografia a kryptografia asymetrická
- Verejné a privátne kľúče, digitálny podpis, časové razítka
- MD4 vs. MD5 vs. SHA-1 vs. SHA-2
- RSA, DSA, ECDSA, DH, ECDH, AES, DES, 3DES, SuiteB

**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

- Porovnanie bezpečnosti na základe dĺžky kľúčov a bitových síl algoritmov
- Comparable Algorithm Strength
- Podpora algoritmov a ich kompatibilita vo Windows
- CSP a CNG poskytovatelia a knižnice, podpora v aplikáciách
- Funkcie SSL a TLS, Algorithm Suites a podpora cez verzie Windows
- Certifikáty, základné a rozšírené polia
- SAN, EKU, Subject, Issuer, Serial Number, Thumbprint, AIA, CDP
- Certifikačné autority, stromy a Certificate Chain, verzie autorít
- Dôveryhodné autority, automatická inštalácia a sťahovanie
- Plánovanie certifikačnej autority, verejné autority vs. súkromné podnikové CA
- Predpoklady pre inštaláciu AD CS certifikačnej autority
- Inštalácia Offline Root CA a Issuing Subordinate CA
- Integrácia AD CS a Active Directory
- Separácia rolí správcov autority a certifikátov
- Certifikačné politiky, Certificate Templates (v1, v2, v3)
- Parametre šablón certifikátov, Issuance Policies a Renewal Policies, Registračné autority (RA)
- Požiadavky na aplikačné certifikáty serverov SSL/TLS, RDS/TS, DC, LDAPS, SQL, System Center, Reporting Services, Exchange Server, SharePoint Server, UAG
- Požiadavky na aplikačné certifikáty klientov a IPSec, prihlasovanie k SSL/TLS, Kerberos PKINIT a čipové karty, EFS
- Šifrovanie a digitálny podpis mailu, súborov, dokumentov a skriptov
- Zneplatnenie certifikátov, CRL a OSCP
- Plánovanie a nasadenie CRL a OCSP distribučných bodov
- Životný cyklus certifikátov a ich privátnych kľúčov, obnova a predĺženie, uloženie kľúčov, zálohovanie kľúčov a ich Roaming
- Životný cyklus certifikačných autorít, ich predĺženie a zneplatnenie
- Plánovanie hierarchie certifikačných autorít
- Zálohovanie, obnova, riešenie problémov, odstránenie, migrácia a upgrade AD CS

## Príprava na certifikačné skúšky

Pri certifikačných skúškach Microsoft platí, že okrem certifikácií MCM, nie je účasť na oficiálnom MOC kurze nutnou podmienkou pre zloženie skúšky.

Oficiálne kurzy MOC spoločnosti Microsoft i naše vlastné kurzy GOC sú vhodnou súčasťou prípravy na certifikačné skúšky Microsoft ako sú MTA, MCP, MCSA, MCSE alebo MCM.

Primárnym cieľom kurzu nie je priamo príprava na certifikačné skúšky, ale zvládnutie teoretických princípov a osvojenie si praktických zručností nutných k efektívnej práci s daným produktom.

MOC kurzy obvykle pokrývajú takmer všetky oblasti požadované pri zodpovedajúcich certifikačných skúškach. Ich prebraniu na kurze ale nebýva daný vždy presne rovnaký čas a dôraz, ako vyžaduje certifikačná skúška.

Ako ďalšiu prípravu k certifikačným skúškam je možné využiť napríklad knihy od MS Press (tzv. Self-paced Training Kit) i elektronický self-test software.

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