



Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com

Phone: +420 597 488 811



Windows Server 2019/2016 - Enterprise PKI Deployment

Kód:	DÉLKA:	CENA:
MCS_GOC173	40 Hours (5 DENNÍ)	Kč bez DPH 34,500.00

Description

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 algoritmů 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 kryptografií. 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 certifikováni na nejvyšší možnou technologickou úroveň v této oblasti MCM:Directory a/nebo MCSM:Directory.

Toto školení pořádá společnost GOPAS a.s.

UPOZORNĚNÍ K CENĚ KURZU:

Cena školení pořádaného v Bratislavě je 1050 EUR bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.

Cíle

Zopakujeme základní principy kryptografie symetrické i veřejných klíčů a do detailu probere rozdíl 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 obnovu 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.

Určeno pro

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 tematiku AD od verzí Windows 2000 až po Windows 2019.

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

Program

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 policie a renewal policie, 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 certifikáty 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

Termíny školení

Termíny školení na vyžádání, [kontaktujte nás prosím](#)

Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)