Základy PKI certifikátů pro správce i vývojáře a post-quantum kryptografie

Kód kurzu: GOC247

Dvoudenní základní kurz seznamuje posluchače s principy a vlastnostmi digitálních certifikátů a požadavky na PKI infrastrukturu v době před i post-quantum kryptografických algoritmů. Podstatný je výběr a kompatibilní volba algoritmů jako jsou RSA, ECDSA, ML-DSA a SHA. Probírají se obsahy certifikátů jako jejich Subject, Subject Alternative Name (SAN), Enhanced Key Usage (EKU), sériová čístla, revokační/odvolací mechanismy jako CRL a OCSP apod. Probírá se analýza hrozeb certifikačních hierarchií CA a jejich zmírnění pomocí HSM modulů a offline CA. Kurz probíhá v příkladech předváděných na Windows a Microsoft cloudovém prostředí a technologiích jako je TLS, code-signing, Kerberos, SAML/XML, ADCS, Cloud PKI, používají se prohlížeče Edge, Chrome nebo Firefox. Účastníci se dozví o požadavcích na kvalifikované certifikáty a zaručený digitální podpis. Cílem je ovšem jen obecné pochopení principů PKI a nikoliv praktická práce v žádném konkrétním počítačovém prostředí, programovacím jazyce ani systému.

Předpokládané vstupní znalosti

Povědomí a základní znalosti v rozsahu kurzů uvedených v sekcích Předchozí kurzy a Související kurzy

Osnova kurzu

- certifikační autority (CA) a jejich hierarchie, kořenové (root CA) a vydávací CA (issuing CA)
- smysl hierarchie založený na hodnocení hrozeb a následných rizik
- různé podpisové algoritmy jako RSA, ECDSA a ML-DSA v různých úrovních stromu, vhodné SHA2 a SHA3 algoritmy
- PKI bez hierarchie (single root issuing CA) a její (ne)rizika, využití Hardware Security Modulů (HSM)
- self-signed certifikáty
- registrační autority (RA)
- obsah certifikátů a jejich podpis jako je Subject, SAN, Key Usage, EKU, CRL Distribution Points (CDP), AIA apod.
- volba platnosti certifikátů certifikačních autorit v certifikátů koncových
- podpisové a šifrovací klíče
- kombinace algoritmů klíčů a jejich bezpečnost vs. kompatibilita i v době post-quantum
- obnova certifikátů s novými klíči vs. se stejným klíčem
- kryptografické předměty jako S/C (smart card), PIV (personal identity verification), elektronické občanské průkazy, HSM (hardware security module) vs. FIDO2, které nepoužívá certifikáty pro passkey autentizaci
- principy použití certifikátů k přihlašování do systémů, podpisu dokumentů a spustitelných programů a instalátorů
- principy a možnosti zneplatnění/odvolání/revokace certifikátů CRL a OCSP
- úvahy o revokační rychlosti a jejím smyslu vůbec vs. moderní prohlížeče Edge/Chrome/Firefox vs. přihlašování do systémů
- časová razítka
- zaručený kvalifikovaný podpis

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