Základy PKI certifikátov pre správcov i vývojárov a post-quantum kryptografia

Kód kurzu: GOC247

Dvojdňový základný kurz zoznamuje poslucháčov s princípmi a vlastnosťami digitálnych certifikátov a požiadavkami na PKI infraštruktúru v čase pred aj post-quantum kryptografických algoritmov. Podstatný je výber a kompatibilná voľba algoritmov ako sú RSA, ECDSA, ML-DSA a SHA. Preberajú sa obsahy certifikátov ako ich Subject, Subject Alternative Name (SAN), Enhanced Key Usage (EKU), sériové čísla, revokačné/odvolacie mechanizmy ako CRL a OCSP a pod. Preberá sa analýza hrozieb certifikačných hierarchií CA a ich zmiernenie pomocou HSM modulov. Kurz prebieha v príkladoch predvádzaných na Windows a Microsoft cloudovom prostredí a technológiách ako je TLS, code-signing, Kerberos, SAML/XML, ADCS, Cloud PKI, používajú sa prehliadače Edge, Chrome alebo Firefox. Účastníci sa dozvedia o požiadavkách na kvalifikované certifikáty a zaručený digitálny podpis. Cieľom je však len všeobecné pochopenie princípov PKI a nie praktická práca v žiadnom konkrétnom počítačovom prostredí, programovacom jazyku ani systéme.

Predpokladané vstupné znalosti

Povedomie a základné znalosti v rozsahu kurzov uvedených v sekciách Predchádzajúce kurzy a Súvisiace kurzy

Osnova kurzu

- certifikačné autority (CA) a ich hierarchie, koreňové (root CA) a vydávacie CA (issuing CA)
- zmysel hierarchie založený na hodnotení hrozieb a následných rizík
- rôzne podpisové algoritmy ako RSA, ECDSA a ML-DSA v rôznych úrovniach stromu, vhodné SHA2 a SHA3 algoritmy
- PKI bez hierarchie (single root issuing CA) a jej (ne)rizika, využitie Hardware Security Modulov (HSM)
- self-signed certifikáty
- registračné autority (RA)
- obsah certifikátov a ich podpis ako je Subject, SAN, Key Usage, EKU, CRL Distribution Points (CDP), AIA a pod.
- voľba platnosti certifikátov certifikačných autorít v certifikátoch koncových
- podpisové a šifrovacie kľúče
- kombinácia algoritmov kľúčov a ich bezpečnosť vs. kompatibilita aj v čase post-quantum
- obnova certifikátov s novými kľúčmi vs. s rovnakým kľúčom
- kryptografické predmety ako S/C (smart card), PIV (personal identity verification), elektronické občianske preukazy, HSM (hardvér security module) vs. FIDO2, ktoré nepoužíva certifikáty pre passkey autentizáciu
- princípy použitia certifikátov na prihlasovanie do systémov, podpisu dokumentov a spustiteľných programov a inštalátorov
- princípy a možnosti zneplatnenia/odvolania/revokácie certifikátov CRL a OCSP
- úvahy o revokačnej rýchlosti a jej zmysle vôbec vs. moderné prehliadače Edge/Chrome/Firefox vs. prihlasovanie do systémov
- časové pečiatky
- 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