Basics of PKI certificates for administrators and developers and post-quantum cryptography

Course code: GOC247

The two-day basic course introduces students to the principles and properties of digital certificates and the requirements for PKI infrastructure in the era of pre- and post-quantum cryptographic algorithms. The selection and compatible choice of algorithms such as RSA, ECDSA, ML-DSA and SHA is essential. The contents of certificates such as their Subject, Subject Alternative Name (SAN), Enhanced Key Usage (EKU), serial numbers, revocation/revocation mechanisms such as CRL and OCSP, etc. are discussed. Threat analysis of CA certification hierarchies and their mitigation using HSM modules and offline CAs are discussed. The course is conducted in examples demonstrated on Windows and Microsoft cloud environments and technologies such as TLS, code-signing, Kerberos, SAML/XML, ADCS, Cloud PKI, using Edge, Chrome or Firefox browsers. Participants will learn about the requirements for qualified certificates and a guaranteed digital signature. However, the goal is only a general understanding of PKI principles and not practical work in any specific computer environment, programming language or system.

Assumed entry knowledge

Awareness and basic knowledge within the scope of the courses listed in the Previous courses and Related courses sections

Course outline

- Certification authorities (CAs) and their hierarchy, root and issuing CAs
- The meaning of the hierarchy based on the assessment of threats and subsequent risks
- Various signature algorithms such as RSA, ECDSA and ML-DSA at different levels of the tree, suitable SHA2 and SHA3 algorithms
- PKI without hierarchy (single root issuing CA) and its (non)risks
- self-signed certificates
- registration authorities (RA)
- content of certificates and their signature such as Subject, SAN, Key Usage, EKU, CRL Distribution Points (CDP), AIA, etc.
- choice of validity of certification authority certificates in end-user certificates
- signature and encryption keys
- combination of key algorithms and their security vs. compatibility even in the post-quantum era
- certificate renewal with new keys vs. with the same key
- cryptographic objects such as S/C (smart card), PIV (personal identity verification), electronic ID cards, HSM (hardware security module) vs. FIDO2, which does not use certificates for passkey authentication
- principles of using certificates to log in to systems, sign documents and executable programs and installers
- principles and options for invalidation/revocation/revocation of CRL and OCSP certificates
- considerations about revocation speed and its meaning in general vs. modern Edge/Chrome/Firefox browsers vs. logging in to systems
- timestamps
- guaranteed qualified signature

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