



NFQES

powered by BRAIN:IT

ISO
20000

ISO
9001

ISO
27001

ISO
22301

ISO
14001

ISO
45001

NFQES Enterprise CA

Component for the basic operation of a certification authority.

Product Sheet – NFQES Enterprise CA

The system provides full lifecycle management of digital certificates, from request intake, through issuance and management, to their expiration.

The solution is designed for both qualified and internal certification authorities and enables operation in compliance with legislative and international certification schemes (including qualified services under eIDAS).

Key Features

- **Certificate issuance**
 - certificate request submission
 - certificate request validation
 - certificate issuance execution

All types and profiles of certificates are supported (based on the customer's certification policies):

- certificates for natural persons (electronic signature)
- certificates for legal entities (electronic seal)
- mandate certificates
- TLS certificates



- other types
- **CRL generation and OCSP server**
- **Certificate lifecycle management**
 - issuance
 - renewal
 - suspension and reactivation
 - revocation
- **PKI hierarchy and certification structure management**

The solution supports:

- management of root certificates
- management of superior and subordinate certification authorities
- support for hierarchical trust structures
- management of certificate profiles and templates
- support for both self-signed and CA-signed root certificates

Publication and Validation Services

- generation and publication of CRL (Certificate Revocation List)
- support for OCSP services for real-time certificate status validation

Deployment

The system can be deployed on-premise at the customer site or as part of an existing security infrastructure.

In an on-premise deployment, it is possible to:

- install the entire system at the customer's site
- integrate a root certificate signed by a superior authority
- establish a trusted certification service
- operate an internal certification authority with a self-signed certificate



Functions

- **Auditability** – generation of electronically signed audit logs
- **Reporting** for supervisory and regulatory authorities
- **Advanced logging**
- **Multi-CA operation** – support for parallel operation of multiple certification authorities
- **Certificate self-renewal – ability** to remotely upload a certificate to a smart card

Users and Roles

The system supports role-based access:

- CA Operator
- CA Administrator
- CA Auditor
- Security Expert
- Other organization-defined roles

Benefits

- Centralized management of the entire PKI infrastructure
- High level of security and auditability
- Support for both regulated and internal certification schemes
- Flexible deployment (on-premise)
- Scalability for large enterprises and public sector institutions
- Compliance with legislative requirements

Characteristics

- **Support for QSCD devices** – compatibility with devices using PKCS#11 interface



- **Support for OCSP protocol** – real-time certificate validation according to RFC 6960
- **Robust integration** – can operate with any certification authority
- **Multi-instance support** – high availability and reliability through scalable architecture
- **eIDAS and Slovak legislative compliance** – meets the requirements of Regulation (EU) No. 910/2014 (eIDAS)

Supported Cryptographic Standards

- **Standards:**
 - RFC 5280 – X.509 Public Key Infrastructure – Certificates and Certificate Revocation Lists (CRL)
 - RFC 6960 – Online Certificate Status Protocol (OCSP)
- **Algorithms:**
 - RSA, EC
 - MD2, MD4, MD5, RIPEMD (128, 160, 256, 320)
 - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

Operational and System Requirements

- **Key stores:** HSM, PEM, JKS
- **Compatibility** – RHEL, Oracle Linux, Ubuntu Linux, Windows
- **Relational database support** – MySQL, MariaDB, PostgreSQL, Oracle, or built-in databases