NFQES
powered by BRAIN:IT

ISO 20000 | ISO 9001 | ISO 27001 | ISO 22301 | ISO 14001 | ISO 45001

NFQES Web Signer

An enterprise e-signature solution designed for deployment directly within the customer's infrastructure

It enables full integration of electronic signatures into existing business processes, internal systems, and workflows.

Use Cases

- Digitalization of internal business processes
- Electronic communication with external partners
- Signing documents intended for public authorities
- Automated signing within information systems

Supported documents and formats

- .pdf
- .docx, .doc
- .xlsx, .xlsm
- .jpeg, .png

Other formats can be supported based on customer requirements.

Modular architecture

Signer

A backend component **designed for the actual signing of documents, supporting all levels of electronic signatures**.

It enables signing using:

- digital signatures,
- certificates stored on QSCD devices / ID cards,
- remote certificates via the NFQES Virtual HSM API,
- the customer's own HSM (on-premise).

Validator

A backend validation module that **verifies the status and integrity of documents**.

It verifies:

- whether the document **is signed**,
- **the level** of the signature,
- **the validity** of the signature,
- **the integrity** of the document (whether it has been altered).

Viewer

A frontend module **used to operate the Signer and Validator**.

- User interface for signing and validating documents.
- Ability to create a graphical signature that is visually embedded into the document.
- Intuitive operation for end users.
- Customizable design aligned with the customer's visual identity.

The solution can be extended with signature tablets for use in customer service centers.

Signature tablets

Signature tablets provide a fast and easy way to sign applications, forms, and contracts without the need for paper and printing at branches.

- Suitable for tablets – **Android, iOS**, and dedicated devices (e.g. **Wacom**).
- **Legal certainty** of electronic signatures with easy deployment across branches.
- **Elimination of costs** related to printing, paper, and archiving.
- **Improved user experience** for signatories.
- **Optimization of processes** related to contracts, forms, etc..
- **Easy integration** into the customer's infrastructure and via APIs (contracts, web forms, etc.).
- **2FA option** via SMS or email.

Characteristics

- **Support for Qualified Electronic Signatures** (QES)
- **Access to functionalities via standardized APIs** (REST/SOAP)
- **Compatibility with QSCD and certified HSM devices**
- **Wide support for document formats** – signing and verification of PDF, DOCX, ODT, XML, and others
- **Security in compliance with eIDAS and Slovak legislation** – the application meets the requirements of Regulation (EU) No. 910/2014 (eIDAS)
- **OCSP protocol support** – real-time certificate validation according to RFC 6960
- **Robust integration** – the solution can operate with any certification authority
- **Multi-instance support** – high availability and reliability through a scalable architecture.

Supported Qualified Electronic Signature Formats

- CAdES: CAdES-B, CAdES-T, CAdES-LT, CAdES-LTA
- XAdES: XAdES-B, XAdES-T, XAdES-LT, XAdES-LTA
- PAdES: PAdES-B, PAdES-T, PAdES-LT, PAdES-LTA
- JAdES: JAdES-B, JAdES-T, JAdES-LT, JAdES-LTA

Supported Cryptographic Standards

- CMS Advanced Electronic Signatures
- XML Advanced Electronic Signatures
- PDF Advanced Electronic Signatures
- JSON Advanced Electronic Signatures
- Support for time stamps and Trusted Lists (EUTL)
- RFC 5280 – X.509 Public Key Infrastructure – Certificates and Certificate Revocation Lists (CRL)
- RFC 6960 – Online Certificate Status Protocol (OCSP)

Supported Cryptographic Algorithms

- RSA, DSA, EC, ECDSA
- MD2, MD4, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- RIPEMD128, RIPEMD (128, 160, 256, 320)

Benefits

- Fast integration into existing systems (IS, ERP, DMS)
- Reduced operating and maintenance costs through automation.