NFQES
powered by BRAIN:IT

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

NFQES Archive

Long-term archiving of electronic signatures / seals

NFQES Enterprise Archive is a software component designed for the secure long-term preservation of electronic signatures and electronic seals in compliance with the requirements of the eIDAS Regulation. The product is intended for deployment directly within your on-premise infrastructure, ensuring full control over stored data and archival processes.

NFQES Enterprise Archive represents a reliable and secure solution for organizations requiring the highest level of data protection and compliance with legislative standards for electronic identification and trust services.

Key features:

- **eIDAS compliance** – ensures compliance with European standards and legislation for the long-term preservation of electronic signatures and seals.
- **Flexible deployment** – deployment directly within your infrastructure for full control over data.
- **Integration with the NFQES platform:**
  - **SaaS mode** – the ability to use NFQES SaaS API services for long-term archiving via the NFQES cloud platform.
  - **On-Premise mode** – use of the NFQES PKI API together with the customer's internal certification authority, with all operations performed exclusively within the customer's infrastructure.

Key benefits of the solution

- **Long-term verifiability of electronic documents** – support for documents signed with a qualified electronic signature, with or without a trusted timestamp.
- **Easy integration with DMS** – seamless integration with document management systems via a REST interface.
- **Scalability and flexibility** – easy adaptation of the solution to the size and needs of the organization.
- **Reduced costs and complexity** – thanks to integration into existing PKI infrastructures.

Basic Principle of Operation

The long-term validity of electronically signed documents is ensured through:

- cryptographic hashing of documents,
- periodic re-signing,
- time-based signature chaining.

Each archived document is re-signed at regular intervals (typically once per year), creating a cryptographic chain of signatures that:

- protects the integrity of the document,
- ensures the immutability of its content,
- enables retrospective verification of the signature's validity at any point in time.

Archiving Levels

Non-qualified archiving

- Documents or their cryptographic hashes are re-signed annually using the customer's certificate.
- The customer manages their own certificates and cryptographic keys.
- Suitable for internal archiving processes and systems without the requirement for a qualified trust service.

Qualified archiving

- Archiving is performed through integration with the NFQES HashArchive API.
- Documents are re-signed using the NFQES technical certificate.
- The resulting archives represent a trusted archive suitable for regulatory, legal, and audit purposes.
- The solution is designed in compliance with the requirements of the eIDAS Regulation.

Archiving Model

NFQES Enterprise Archive supports two basic archiving scenarios:

- ***Archiving of document hashes*** – storage of cryptographic hashes of documents without the document content itself
- ***Archiving of hashes together with documents*** – complete storage of the document including its cryptographic proof

This approach makes it possible to optimize:

- archive size,
- security requirements,
- legislative and operational demands.

NFQES Hash Archive API

NFQES Hash Archive API is a REST API service designed to ensure the long-term archiving of electronically signed documents through the archiving of cryptographic hashes or hashes together with documents. The service provides mechanisms for the long-term preservation, renewal, and validation of evidence proving the validity of electronic signatures.

API Functional Scope

- archiving of a document hash,
- archiving of a hash together with the document,
- validation of an archived hash or document,
- retrieval of a list of archived documents,
- archive management, including the ability to delete records.

NFQES Hash Archive API serves as a key component for qualified archiving within the NFQES Enterprise Archive solution.

Authentication and Security

Access to the NFQES Hash Archive API is protected by multiple authentication mechanisms:

- authentication using an authentication certificate,
- authentication via Basic OAuth (username and password).

Characteristics

- **Wide support for document formats** – signing and validating of PDF, DOCX, ODT, XML, and other formats.

  Security in compliance with eIDAS and Slovak legislation – the application meets the requirements of Regulation (EU) No. 910/2014 (eIDAS).

Supported cryptographic standards

- X.509 Public Key Certificates, CMS Advanced Electronic Signatures, XML Advanced Electronic Signatures, PDF Advanced Electronic Signatures, JSON Advanced Electronic Signatures
- Support for trusted timestamps and the EU Trusted List (EUTL)

Supported cryptographic algorithms

- RSA, DSA, ECDSA
- MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- RIPEMD128, RIPEMD160, RIPEMD256

Operational and system requirements

- **Compatibility** – RHEL, Oracle Linux, Ubuntu Linux, Windows.
- **Relational database support** – MySQL, MariaDB, PostgreSQL, Oracle or built-in databases.