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.

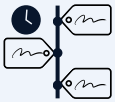
Basic Principle of Operation

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

Cryptographic hashing of document

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 longterm 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)

Selected references

Okte - company that operates in Slovakia as a regulated entity responsible for the operation of the energy market.

- A system covering the complete management of signature processes
- Qualified electronic signature
- Long-term storage of documents in a qualified archive

The delivered solution also included integration with the customer's external DMS and virtual HSM hardware security model.

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.

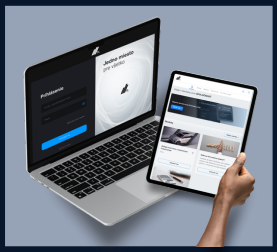
Supported Qualified Electronic Signature Formats	Supported Cryptographic Standards	Supported Cryptographic Algorithms
CAdES: CAdES-B, CAdES-T, CAdES-LT, CAdES-LTA	CMS Advanced Electronic Signatures	RSA, DSA, EC, ECDSA MD2, MD4, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
	XML Advanced Electronic Signatures	
XAdES: XAdES-B, XAdES-T, XAdES-LT, XAdES-LTA	PDF Advanced Electronic Signatures	MD2, MD4, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
	JSON Advanced Electronic Signatures	
PAdES: PAdES-B, PAdES-T, PAdES-LT, PAdES-LTA	Support for time stamps and Trusted Lists (EUTL)	RIPEMD128, RIPEMD (128, 160, 256, 320)
	RFC 5280 – X.509 Public Key Infrastructure	
JAdES: JAdES-B, JAdES-T, JAdES-LT, JAdES-LTA	Support for time stamps and Trusted Lists (EUTL)	

Supported documents and formats						
.PDF	.DOC	.DOCX	.XLSX	.XLSM	.JPEG	.PNG

Other formats can be supported based on customer requirements.

NFQES

Case studies

Tatraleasing	BVS	Medante
		
Reduced workload, lower hardware requirements, time and cost savings, and **high legal certainty.**	**Digitalized communication**, online forms and contracts, electronic **signing via infrastructure or API.**	**Digital signatures** for medical documentation and contracts, **implemented in the existing** MEDANTE **system**.

The NFQES solution can be implemented and customized for a wide range of processes for businesses in various fields.

Contact:

Schedule a consultation with us

+421 918 754 670 sales@nfqes.com nfqes.com

Office Žilina
Veľká Okružná 2215/66
010 01 Žilina

Office Bratislava
Jarošová OC, Jarošova 1
831 01 Bratislava

Clutch TUV ISO 45001 TUV ISO 14001 TUV ISO 22301 TUV ISO 27001 TUV ISO 20000-1 TUV ISO 9001 EU Trusted List