NFQES PKI API

API interface for QES services

NFQES PKI API is a modern, powerful and flexible REST/SOAP application interface without a separate graphical interface designed for integrating advanced cryptographic services into applications and enterprise architectures. It is an integration component for integrating hardware and virtual cryptographic material repositories.

Solution description

NFQES PKI API serves as a supporting product within the NFQES portfolio, which ensures the management of key pairs and digital certificates required for secure digital processes.

It enables key generation, creation of CSR (Certificate Signing Request) and subsequent obtaining of a certificate from a certification authority. The product functions as an integration layer between applications and PKI infrastructure.

It is suitable as a basic building block together with solutions:

- NFQES Certificate Provider
- NFQES Certificate Hub
- NFQES Virtual HSM

NFQES PKI API

API interface for QES services

Advantages

- Quick integration into existing systems
- Automate certificate and key management
- Reduction of operation and maintenance costs
- Deployment flexibility (cloud / on-premise)
- Support for a wide range of devices and scenarios
- Scalability for small and large organizations

Key functionalities

- Generating key pairs (locally and on devices)
- Creating a CSR and storing the certificate via the NFQES SaaS API CertificateProvider or another SaaS/On-Premise component.
- Integration with Certificate Authorities (CAs)
- Support for both qualified and unqualified devices
- Direct integration with QSCD and HSM devices
- Use of certified signature algorithms
- Connection to a central PKI infrastructure (e.g. NFQES Enterprise CA)

NFQES

Who is the solution intended for?

- Small, medium and large businesses
- Organizations using electronic signature
- Companies building their own PKI infrastructure
- Integrators and developers who need to work with certificates

Characteristics

Qualified Electronic Signature (QES) support

Access to functionalities via standardized API (REST/SOAP)

Compatibility with QSCD and certified HSM devices

Supported standards and algorithms:

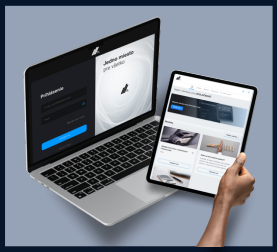
- Algorithms:
  - RSA
  - EC
  - MD2, MD4, MD5, RIPEMD (128, 160, 256, 320)
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

System requirements:

- Operating system: GNU/Linux (Ubuntu, Red Hat), Windows
- Supported keystores: HSM, PEM, JKS
- Supported databases: MySQL, MariaDB, PostgreSQL, SQLite

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