



NFQES Signer

Aplikácia pre elektronický podpis/pečať

Produktový list - NFQES Enterprise Signer

NFQES Enterprise Signer je serverové riešenie pre kvalifikovaný elektronický podpis a pečať, umožňujúce koncovým používateľom jednoduchým a rýchlym spôsobom vyhotovovať a overovať kvalifikované elektronické podpisy a pečate. Aplikácia interne využíva open-source DSS framework, ktorý zabezpečuje súlad s ETSI štandardmi pre elektronické podpisy ([viac informácií](#)).

Základnú verziu aplikácie možno podľa potreby rozšíriť o ďalšie funkcionality:

- **Hromadné podpisovanie** – umožňuje podpísať viacero dokumentov naraz jedným potvrdením operácie používateľom.
- **Archív** – zabezpečuje dlhodobú overiteľnosť podpisov a pečatí na elektronických dokumentoch.
- **Konverzia PDF** – riešenie umožňuje konverziu PDF minimálne do PDF/A (ISO 19005) s možnosťou rozšírenia na novšie verzie ako A-4 a PDF/UA (ISO 14289).

Moderné používateľské rozhranie poskytuje komfortnú a intuitívnu prácu s kvalifikovaným elektronickým podpisom, vhodnú pre všetky úrovne skúseností.

Charakteristika

- **Podpora eID a QSCD zariadení** – kompatibilita so zariadeniami s dostupným CSP alebo PKCS#11 rozhraním.
- **Široká podpora dokumentových formátov** – podpisovanie a overovanie formátov ako PDF, DOCX, ODT, XML a ďalšie.
- **Zabezpečenie podľa eIDAS a slovenskej legislatívy** – aplikácia spĺňa požiadavky Nariadenia (EÚ) č. 910/2014 (eIDAS).

Podporované formáty kvalifikovaného elektronického podpisu

- **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

Podporované kryptografické štandardy

- X.509 Public Key Certificates, CMS Advanced Electronic Signatures, XML Advanced Electronic Signatures, PDF Advanced Electronic Signatures, JSON Advanced Electronic Signatures
- Podpora časových pečiatok a dôveryhodného zoznamu (EUTL)

Podporované kryptografické algoritmy

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

Systémové požiadavky

- **Kompatibilita** – RHEL, Oracle Linux, Ubuntu Linux, Windows
- **Podpora relačných databáz** – MySQL, MariaDB, PostgreSQL, Oracle alebo built-in databázy