



NFQES Validator

Overovanie elektronických podpisov/pečatí

Produktový list - NFQES Enterprise Validator

NFQES Enterprise Validator je vysoko výkonné riešenie na overovanie platnosti certifikátov a elektronických podpisov v reálnom čase. Aplikácia implementuje Online Certificate Status Protocol (OCSP) a umožňuje rýchlu a spoľahlivú verifikáciu dôveryhodnosti elektronických podpisov pre organizácie a informačné systémy. Riešenie je určené najmä pre poskytovateľov kvalifikovaných dôveryhodných služieb, prevádzkovateľov elektronických podateľní a iné subjekty, ktoré potrebujú zabezpečiť okamžité overovanie digitálnych podpisov a certifikátov.

Charakteristika

- **Podpora OCSP protokolu** – overovanie certifikátov v reálnom čase podľa štandardu RFC 6960.
- **Zvýšená rýchlosť spracovania** – eliminácia potreby získavať zoznamy zrušených certifikátov (CRL), čím sa skracuje čas overenia podpisu.
- **Robustná integrácia** – riešenie je možné prevádzkovať s ľubovoľnou certifikačnou autoritou a môže fungovať ako centrálna validačná služba.

- **Elektronicky podpísané auditné záznamy** – zabezpečenie integrity a ochrana pred neoprávnenou manipuláciou.
- **Podpora viacerých inštancií** – vysoká dostupnosť a spoľahlivosť cez škálovateľnú architektúru.
- **Kompatibilita s NFQES Enterprise Signer** – možnosť integrácie s riešeniami na vytváranie kvalifikovaných elektronických podpisov a pečatí.

Podporované štandardy a algoritmy

- **Štandardy:**
 - RFC 5280 – X.509 Public Key Infrastructure – Certifikáty a zoznamy zrušených certifikátov (CRL)
 - RFC 6960 – Online Certificate Status Protocol (OCSP)
 - RFC 5019 – OCSP pre vysoko výkonné prostredia
- **Algoritmy:**
 - RSA
 - EC
 - MD2, MD4, MD5, RIPEMD (128, 160, 256, 320)
 - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

Systémové požiadavky

- **Operačný systém:** GNU/Linux (Ubuntu, Red Hat), Windows
- **Podporované úložiská kľúčov:** HSM moduly s podporou OpenSSL engine, PEM súbory s PKCS#8
- **Podporované databázy:** MySQL, MariaDB, PostgreSQL, SQLite
- **Hardvérové požiadavky:**
 - Minimálne: 1-jadrové CPU, 512 MB RAM, 50 GB HDD (bez DB)
 - Odporúčané: 4-jadrové CPU, 4 GB RAM, 50 GB HDD (bez DB)

