Highly secure digital signatures with Nexus GO Signing and Entrust

Entrust and Nexus deliver highly secure digital signature service

HIGHLIGHTS

- Protect against manipulation of agreements, contracts, and other important documents
- Guarantee a trusted source of the document
- Establish the trusted identity of

Highly secure digital signatures with Nexus GO Signing and Entrust

The challenge: Implement digital document signing without jeopardizing security

Document signing needs to ensure that signing credentials are not manipulated and are securely tied to the correct individual as signatory. To be applicable in many signing cases, the solution needs to comply with regulations such as eIDAS, ETSI and also national requirements.

The solution: Trusted document signing with hardware security modules (HSMs)

Nexus GO Signing produces advanced digital signatures, according to PAdES/XAdES/eIDAS specifications, on PDF and XML documents. The signature ties the content of the document together with a signed hash and a certificate with the user data, which in turn ties the signatory to the signing credentials.

The user gives consent to the signature procedure with strong two-factor authentication. The result is a document, which is compliant with PAdES/XAdES/eIDAS, locked for updating, and with an inserted signature and signed certificate. Multiple users can sign the same document.

Why use nShield HSMs with Nexus GO Signing?

Entrust nShield Connect HSMs integrate with Nexus GO Signing and the Nexus CA to provide comprehensive logical and physical protection of keys. The combination delivers an auditable method for enforcing security policies.

The HSM is used to maintain integrity of signing credentials: it handles the cryptographic keys that are used for signing, and it is the root of trust in issuing certificates that tie the user to the signing keys.

By handling signing credentials and certificate issuance with an HSM, the solution becomes significantly more resistant to attacks that can compromise critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material.

Entrust nShield Connect HSMs enable Nexus' customers to:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Deliver superior performance to support demanding one-time signing key applications including RSA and ECC algorithms

Entrust nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nShield HSMs, you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, CNG and Web Services API in conjunction with nShield Web Services Option Pack)

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available,