Highly secure digital signatures with Nexus GO Signing and Entrust

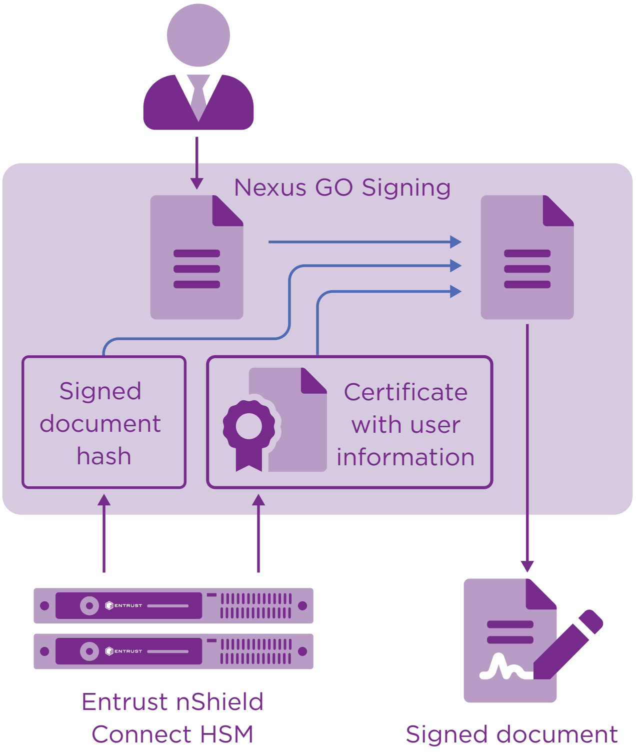
Entrust and Nexus deliver highly secure digital signature service

HIGHLIGHTS

- Protect against manipulation of agreements, contracts, and other important documents
- Guarantee a trusted source of the document
- Establish the trusted identity of the signatory
- Comply with requirements from ETSI, eIDAS, and national standardization bodies
- Digitize and automate manual processes based on paper copies of agreements and other documents

The problem: Manual processes involving document signing are error prone

Digital documents are a powerful tool, but they can be modified easily and it is difficult to establish their source. Many processes for document signing still remain manual due to security reasons, for example processes involving agreements.


Nexus GO Signing
Signed document hash
Certificate with user information
Entrust nShield Connect HSM
Signed document

LEARN MORE AT ENTRUST.COM/HSM

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

Highly secure digital signatures with Nexus GO Signing and Entrust

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, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Nexus Group

Swedish-owned Nexus Group is an innovative and rapidly growing identity and security company. It secures society by enabling trusted identities for people and things in the physical and digital world. Most of its technology is integrated into the Nexus Smart ID solution, which provides standardized and easy-to-use modules that enable organizations to issue and manage physical and digital IDs, manage physical and digital access, enable electronic signatures, and issue and manage public key infrastructure (PKI) certificates. The Smart ID solution is most commonly used for corporate IDs, citizen IDs, and IoT (internet of things) security. Nexus has 300 employees across 17 offices in Europe, India and the US, as well as a global partner network.

Learn More

For more detailed technical specifications, please visit: **entrust.com/HSM** or **www.nexusgroup.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com