# THALES AND NEXUS DELIVER HIGHLY SECURE DIGITAL SIGNATURE SERVICE

Does your organization need to:

– 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

HIGHLY SECURE DIGITAL SIGNATURES WITH NEXUS GO SIGNING AND THALES eSECURITY:
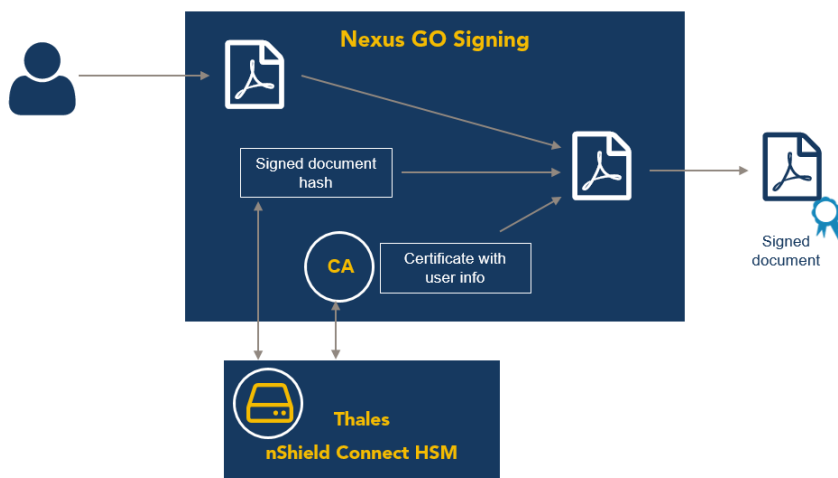
THE PROBLEM: MANUAL PROCESSES INVOLVING DOCUMENT SIGNING ARE ERROR PRONE

Digital documents are a powerful tool, but they can be modified fairly 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.

THE CHALLENGE: IMPLEMENT DIGITAL DOCUMENT SIGNING WITHOUT JEOPARDIZING SECURITY

Document signing needs to ensure that signing credentials are not manipulated and 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.

THALES AND NEXUS DELIVER HIGHLY SECURE DIGITAL SIGNATURE SERVICE

THE SOLUTION: TRUSTED DOCUMENT SIGNING WITH HARDWARE SECURITY MODULES (HSM)

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 sign certificate. Multiple users can sign the same document.

WHY USE THALES HSM WITH NEXUS GO SIGNING?

Thales 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 attack that can compromise critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material.

Thales nShield Connect HSMs enables Nexus' customers for signing solutions 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.

Thales nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With Thales 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, and CNG)

THALES

Thales eSecurity is the leader in advanced data security solutions and services delivering trust wherever information is created, shared, or stored. Security solutions ensure that critical data is both protected and trusted in any deployment – on-premises, in the cloud, in data centers, or in big data environments – without sacrificing business agility. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group.

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.

For more detailed technical specifications, please visit: www.thalesesecurity.com or www.nexusgroup.com