Solution Brief

Qualified Remote Signatures with Luna HSMs and Signature Activation Modules (SAM) from Nextsense and Ascertia

Enhance remote digital signing security with an eIDAS-compliant Qualified Signature Creation Device (QSCD) for qualified signatures and seals

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Introduction:

As business processes and government services become increasingly digital, remote signing has become a secure and efficient way to confirm the authenticity of digital documents, transactions, and identities through the use of digital signatures. Digital signatures have become equivalent to traditional handwritten signatures or stamped seals and are legally valid in many jurisdictions around the globe.

As the adoption and legal recognition of digital signatures expands, particularly with evolving regulations like eIDAS and with the use of electronic IDs (eIDs) in Europe which is becoming more common, it is crucial to ensure their authenticity, integrity, and non-repudiation. This involves safeguarding the entire signing process, from guaranteeing signer's sole control of the signing keys, to incorporated measures against cyber threats, such as data breaches and unauthorized access. In a nutshell, the digital signatures must comply with the stringent legal requirements.

The Challenges of Securing Digital Signatures:

Protecting digital signatures from compromise requires mechanisms to secure the cryptographic keys underpinning the digital signatures. Protecting and securely storing private keys is essential for the security of the asymmetric key cryptography employed in Public Key Infrastructures (PKIs) because these private keys are the foundation of digital identity and authentication processes. In PKIs, a pair of keys is generated: a private key and a public key. The integrity of digital signatures and encrypted communications relies heavily on the security of the private key. If a private key is compromised, an attacker can impersonate the key owner, authorize transactions, leading to security breaches and loss of trust.

Secure management of private keys involves several layers of protection, including using hardware security modules (HSMs) to prevent unauthorized access and ensure that key usage is monitored and audited. The protection of private keys within PKIs is crucial for maintaining the overall security posture of organizations relying on digital signatures and secure communications.

Digital signatures get their official status through signing certificates, which authenticate digital documents, content, and owners. A Certificate Authority (CA) is the core component of a PKI and establishes a hierarchical chain of trust, verifying organizations' compliance with standards. If a CA's root key is compromised, the credibility of financial transactions, business processes, and intricate access control systems is adversely affected. Regardless of the use case or industry an organization operates in, private key security must be utilized for signing certificates to be trusted and valued. Otherwise, anyone who can access a legitimate certificate owner's private key can create software that will appear to be signed by that organization.

What is Remote Signing?

Remote signing is a method of signing documents electronically, where the signing party utilizes a remote server or third-party trusted service provider to sign digital assets such as documents and files. This allows users to create a digital signature without needing to be physically present at the location where the document or file is processed and stored. Another key component of the digital signing process is remote signature activation, which is done via a Signature Activation Module (SAM) and involves generating or activating a digital signature using a cryptographic key that then needs to be securely managed or stored in a remote location. This enables the signing party to create digital signatures without physically holding the private key needed for signing.

In remote signing, the private key for creating a digital signature is held by a remote server or trusted service provider. The signing party, whether an individual or organization, authorizes specific credentials that allow designated entities to remotely use the private key, ensuring that only authorized users can execute digital transactions on their behalf. While this process enhances trust in remote operations, stringent compliance and audit requirements require enhanced security measures to protect signature authorization, identity authentication, and private keys.

HSMs can help address these security challenges by providing strict access control mechanisms to the use of signing keys (which must be present inside the HSM to perform the signature), generating secure audit logs and ensuring that keys and signing material are protected within a secure hardware cryptographic boundary.

SAMs also play a significant role in enhancing security for the remote signature process. Since an authorized signer can initiate the signature operation from various devices and through different authentication protocols, additional security controls need to be implemented to ensure end-to-end security. A SAM performs the necessary verifications before the execution of a signature on an HSM, which ensures that the proof of consent of the signature operation is valid and prevents unauthorized use of signing keys. SAMs help protect the integrity and authenticity of the signature process and reinforce trust in remote electronic transactions.

eIDAS Compliant Qualified Remote Digital Signatures:

eIDAS 2 (EU Regulation 2024/1183), introduced in May 2024, builds on the existing eIDAS framework (EU Regulation 910/2014) and includes a phased implementation for EU Member States. eIDAS 2 aims to increase the use of secure remote signing by enhancing

the requirements for implementation of remote Qualified Electronic Signature Creation Devices (rQSCDs), ensuring users retain sole control over their signing keys (even though the signing process happens remotely) and includes a Signature Activation Module (SAM). The SAM is essential for operating remote signing services securely and integrating with digital identity solutions such as the European Digital Identity Wallet (EUDI Wallet). eIDAS is not merely a directive; it's a regulation, so it's not open to interpretation and represents European Union law.

eIDAS recognizes electronic signatures as legally binding and identifies three main types of electronic signatures, based on the level of assurance they provide:

- **Electronic signatures:** basic signatures in electronic form. With eIDAS, eSignatures are recognized legally and can't be denied legal acceptance because they are digital, but their legal validity can be disputed.
- **Advanced electronic signatures (AdES):** require a higher level of security typically met with certificate-based digital IDs. AdES must be uniquely linked to the signatory, can authenticate the signer and the document, and enable the verification of the integrity of the signed agreement. Still, the legal validity of electronic documents signed with AdES can be challenged.
- **Qualified electronic signatures (QES):** also, must be uniquely linked to the signatory but are further required to be based on qualified certificates. Keys used by qualified certificates can only be issued by a certificate authority (CA) accredited and supervised by authorities designated by EU Member States. Qualified certificates must also be created and used on a qualified signature creation device (QSCD), like an HSM. A Signature Activation Module (SAM) is a component of the QSCD which is required for server signing.

To set up a valid eIDAS compliant signing service for creation of qualified electronic signatures, a Trust Service Provider (TSP) must be granted qualified status (QTSP). For this reason, according to eIDAS 2, QTSPs that provide remote QES are defined as a special type of QTSPs that manages remote QSCDs which is certified against Common Criteria (CC). The two main components of a remote QSCD are responsible for:

1. **Authorization of the signature operation, ensuring that the signer has sole control of their signing keys:** This is carried out by a Signature Activation Module (SAM) which activates the signing key within a Cryptographic Module (an HSM). (PP) EN 419-241-2.
2. **Protecting the key:** qualified signatures and certificates require the use of an HSM to protect the keying material. (PP) EN 419 221-5.

The Solution:

Luna HSMs: Luna HSMs address the security and operational needs required to maintain the integrity and protection of private keys associated with PKI digital signatures. They provide a certified and secure environment for managing, using, and storing cryptographic keys and ensure that keys cannot be extracted when tampered with and give sole control for remote QES. They enforce separation of duties to ensure keys are only used by authorized entities and redundancy features to guarantee keys are always accessible by authorized users when needed. All digital signing and verification operations are performed within Luna HSMs and provide an auditable way to secure valuable cryptographic material.

Luna HSMs are FIPS 140-3 Level 3 validated and are certified in accordance with Common Criteria (CC) at EAL4+ level against the electronic Identification, Authentication and Trust Services (eIDAS) Protection Profile (PP) EN 419 221-5. They have also received eIDAS certification as both a Qualified Signature and Qualified Seal Creation Device (QSCD). These certifications provide the highest levels of assurance and conformity for seamless cross-border electronic identification and trust services.

Luna HSMs with Signature Activation Modules: Remote signing applications utilize a Signature Activation Module (SAM) to authorize the signing operation and authenticate the user's identity and HSMs to protect the private keys associated with the digital signatures and secure cryptographic operations.

Luna HSMs are integrated with SAMs from industry-leading Thales Technology Partners Nextsense and Ascertia to deliver secure solutions that comply with the remote signing requirements outlined in the eIDAS regulation for Qualified Trust Service Providers (QTSP). This integration provides organizations with flexible deployment and integration options and seamless operation.

ascertia
AN INFOCERT COMPANY

nextsense

Ascertia and Nextsense offer a Full Remote Qualified Signature Suite and a SAM that can:

1. function independently with organizations own signing solution
2. be integrated into the out-of-the-box Remote Signing Suite (RSS) from Nextsense and Ascertia

External SAM for Luna HSMs: Thales and Ascertia work together to guarantee essential digital trust products and services that deliver complete digital signature solutions. ADSS SAM Appliance is a Common Criteria Certified Remote Qualified Signature Creation Device (RQSCD) that enables TSP to deliver qualified digital signature services for natural persons, legal representatives, timestamps, and eSeals for any document, web form, or transactions.

The SAM Appliance can be shipped with an EN419221-5 certified Hardware Security Module (HSM) OR used with a suitable external

network connected HSM like the Thales Luna Network HSM to authorize the signing or sealing keys securely.

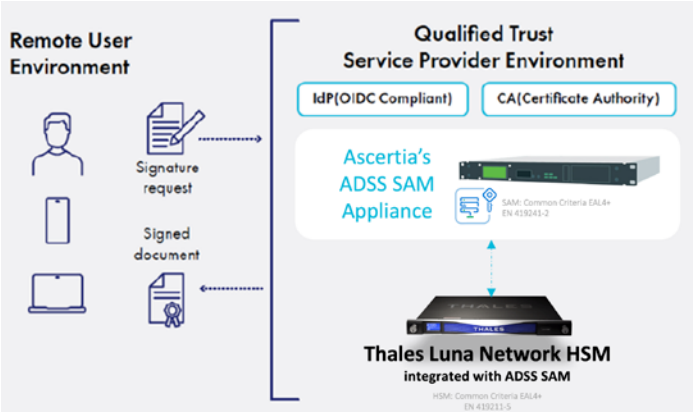

Image caption: Ascertia's Digital Trust Products and Thales Luna HSMs

Embedded SAM for Luna HSMs: Nextsense Signature Activation Module (NSSAM), embedded in Luna Network and PCIe HSMs, provides a highly secure, Common Criteria EAL 4+ AVA_VAN.5 certified, EN 419 241-2, EN 419 221-5 and eIDAS compliant solution, scalable and robust for secure remote digital signing and cryptographic operations. The NSSAM ensures that only the authenticated and authorized user activates the process of creating QES under the user's sole control. These QES cannot be disputed or revoked, supporting legal admissibility. NSSAM together with Luna 7 HSM comprise a QSCD for a signing service that adheres to the remote signing requirements as part of the eIDAS regulation.

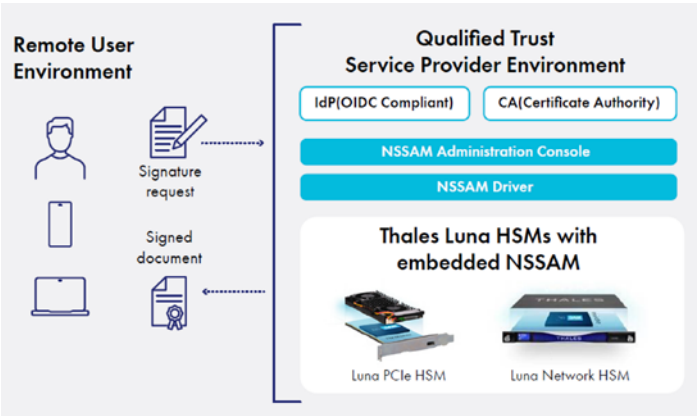

Image caption: Nextsense Signature Activation Module and Thales Luna HSMs

Summary:

Enterprises, governments, and highly regulated industries around the world are moving towards remote digital signing to comply with security standards and regulations, expedite business processes, and reduce operational costs. When adopting digital trust solutions, organizations must implement enhanced security measures to stay protected against cyber threats and ensure compliance with legal standards, regulations, and audit needs. Luna HSMs provide the high-assurance key protections and security requirements needed for eIDAS compliant qualified electronic signatures, seals, and other trust services. Luna HSMs are also integrated with Thales Technology Partner SAMs such as Ascertia ADSS SAM and Nextsense NSSAM, to provide strong authentication and control over the remote signing process and deliver secure digital solutions that meet the signing requirements outlined in the eIDAS regulations for Qualified Trust Service Providers (QTSP). These SAMs integrate with an organization's own signing solution or function as part of the complete digital signing suite from Ascertia and Nextsense, offering flexibility and seamless operation. This trust service is essential, which is why Luna HSMs integrated with SAMs play a vital role in ensuring the compliance, authenticity, and security of digital transactions in today's increasingly digital world.

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us