DATA SHEET

eIDAS-Compliant QSCD With nShield HSM and SAM

A future-proof QSCD for qualified signatures and seals under the eIDAS regulation

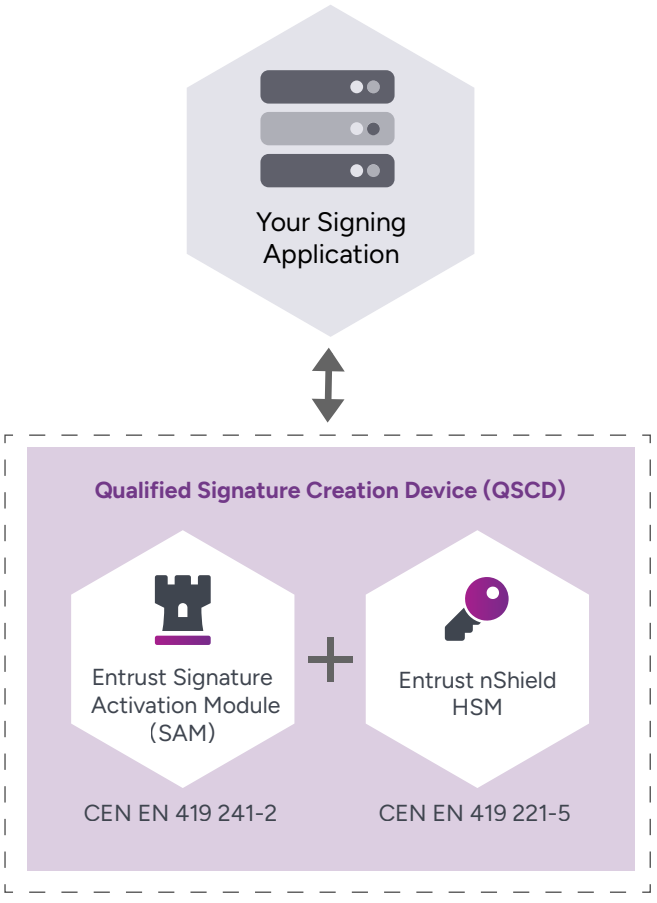
Certifications

- **Entrust nShield® Solo XC, Connect XC, 5s, and 5c certification:** CEN EN 419 221-5 - Common Criteria EAL4+
- **Entrust SAM certification:** CEN EN 419 241-2 - Common Criteria EAL4+

An essential security bundle for qualified signing deployments

Following the directions set by the upcoming Implementation Act of the eIDAS Regulation, Entrust has developed a SAM to improve the security of remote signing deployments. It's installed together with either an nShield XC (Solo or Connect) or an nShield 5 (5c or 5s) HSM to form a fully compliant QSCD.

The Entrust SAM ensures that the signer has sole control of signing operations. All requests go through the SAM for authorization first, which then activates the signing process using the HSM.



The Qualified Signature Creation Device (QSCD) is essential to the deployment of a signing service for eIDAS-qualified signatures and seals.

ENTRUST
SECURING A WORLD IN MOTION

Understanding eIDAS compliance requirements for QSCDs

The QSCD concept is uniquely tied to eIDAS. It is a mandatory element for the generation of "qualified" signatures and seals, which have the highest level of legal recognition in the European Union. Without a QSCD, a qualified trust service provider (QTSP) can only generate "advanced" signatures and seals.

There are currently two CEN Protection Profiles for QSCD requirements:

- **CEN EN 419 241-2:**
  Protection Profile for the SAM
- **CEN EN 419 221-5:**
  Protection Profile for the HSM

Although these two standards were introduced a few years ago, the European Commission has not added them yet to their list of mandatory standards for eIDAS compliance.[1] Since there are currently no standards to refer to, QSCD conformity can be certified by appropriate public or private bodies chosen directly by Member States.

However, once the next Implementing Act of eIDAS is released, the two CEN technical standards above are expected to be added to the eIDAS standards list and become the new norm for QSCD conformity throughout the European Union.

The role of the Entrust nShield HSM in a QSCD

In a "server signing" system for remote signatures and seals, end-users do not have physical access to their signing keys; the signing service generates both keys and signatures on their behalf. It is therefore paramount to provide strong guarantees of the authenticity, integrity, and reliability of the service.

Signing keys used outside of the protected boundary of a certified HSM can be vulnerable to attacks, which can lead to security breaches. HSMs offer a proven and auditable way to secure valuable cryptographic material.

The Entrust nShield XC and nShield 5 HSMs, also referred to as "cryptographic modules" (CMs) in technical descriptions – are Common Criteria (CC) CEN EN 419 241-5 certified. Their function is to generate and encrypt signing keys as well as generate digital signatures upon request.

The nShield Solo XC and the nShield 5s are PCIe cards for embedding in appliances or servers, while the Connect XC and 5c are network-attached appliances.

In a QSCD configuration that incorporates the Entrust SAM (see diagram on next page), the Entrust nShield HSM receives all key operation requests directly from the Entrust SAM.

[1] The eIDAS Regulation itself does not contain any technical guidelines. Rather, it is a list of certifications from other standardization bodies (such as ETSI or CEN) that the European Commission requires all TSPs to obtain in order to become eIDAS-compliant.

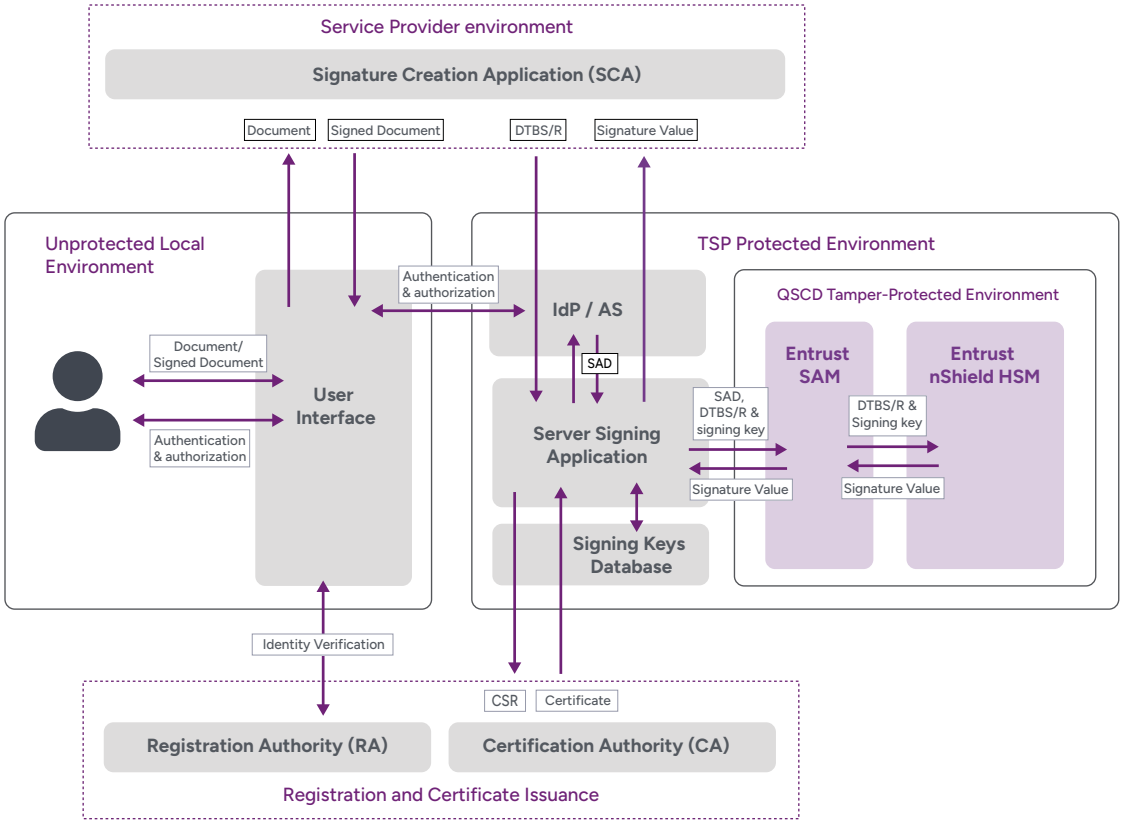
The role of the Entrust Signature Activation Module (SAM) in a QSCD

The Entrust SAM is a security intermediate between your server signing applications and your Entrust nShield HSMs.

The Entrust SAM was built for compliance with CEN EN 419 241-2 standard, and is currently certified against Common Criteria. The Entrust SAM verifies the origin and authenticity of signature requests and authorizes all key-related activities, including key generation, key assignment, key deletion, and signing operations.

In essence, the Entrust SAM guarantees with a high level of confidence that signing keys are used under the signer's sole control.

How It Works



Example of server signing system implementation with a QSCD including the Entrust SAM and the Entrust nShield XC or 5 HSM. The architecture shows a simplified workflow focusing on the QSCD.

Professional Services

In addition to the Entrust SAM and the nShield HSMs, Entrust Professional Services are available to help you deploy your signing solutions, whether you are a TSP or an integrator.

Professional services include:

- Digital signing readiness workshops
- Design and deployment documentation preparation
- Developer support services

The Entrust Professional Services team also offers unmatched expertise in designing and implementing crypto applications for the world's most security-conscious organizations. And they work closely with clients to design and deploy the right solution for their unique environments and to leave their teams with the knowledge to maintain it for years to come.

Why work with Entrust

Entrust has an unrivaled expertise in PKI, HSMs, and digital signing services.

Thanks to our unique product capabilities and expertise, we can cover a very large range of requirements, from individual signing components to a full signing infrastructure.

Our nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION