DATA SHEET

Entrust Signature Activation Module (SAM)

Security at the heart of your digital signing services

Future-proof your eIDAS-compliant digital signing services

The Entrust Signature Activation Module (SAM) is a security element that can be implemented into signing services that follow the remote signing standards defined by CEN and ETSI as part of the eIDAS regulation.

The Entrust SAM was built for compliance with the CEN EN 419 241-2 standard, and is currently certified against the associated Common Criteria certification.

The Entrust SAM verifies the origin and authenticity of signature requests and authorizes all key-related activities. Adding the Entrust SAM to your signing infrastructure today will not only raise the security posture of your remote signing service, but also ensure its compliance with eIDAS in the longer term.

Benefits

- Provides segregation of roles by acting as security intermediate
- Authorizes the generation, deletion, and assignment of key pairs for the signers
- Verifies the origin and authenticity of signature requests
- Takes care of activating the signing process and sending the signed data back to the signing application
- Guarantees the uniqueness of the signers' keys
- Generates audit records for all security events involved in its operations

Built for Entrust nShield XC and nShield 5 HSMs

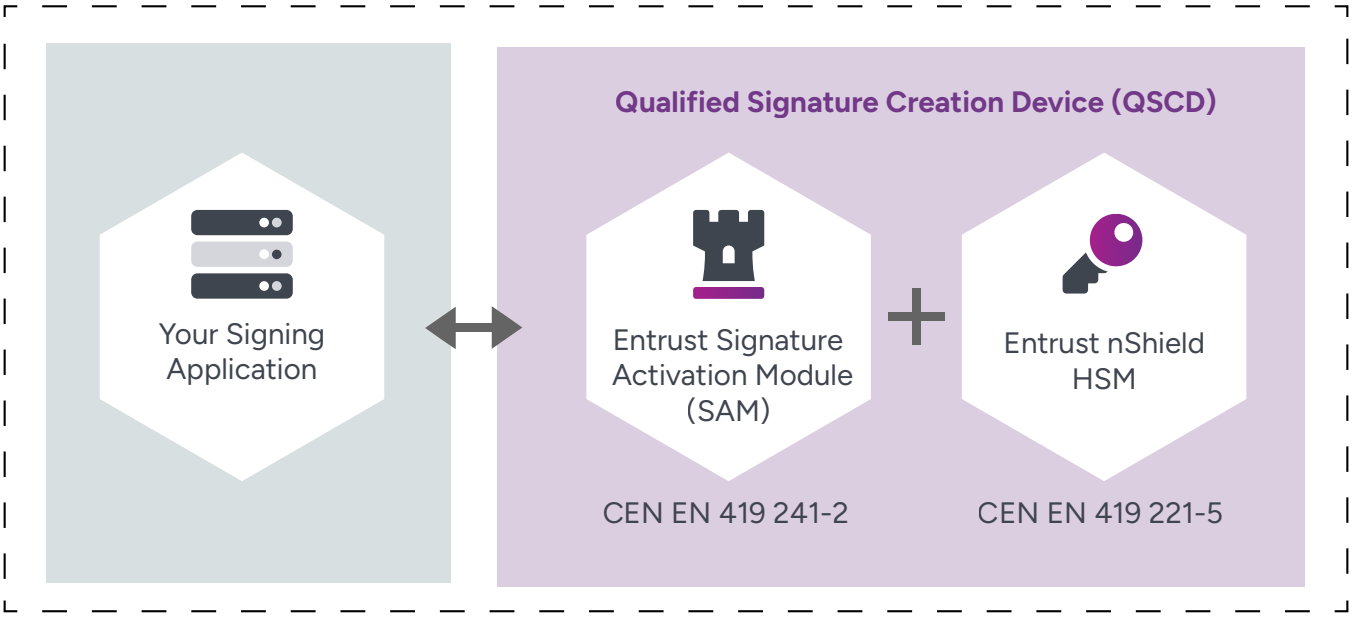
The Entrust nShield Hardware Security Modules (HSMs) from the XC and 5 families are CC EAL4+ (EN 419-221-5 protection profile) certified security appliances that deliver cryptographic services to a variety of applications.

The combined Entrust SAM with Entrust nShield XC or nShield 5 HSMs provide a future-proof Qualified Signature Creation Device (QSCD) for qualified signatures and seals.

ENTRUST

SECURING A WORLD IN MOTION

How It Works



BUILD A FULLY COMPLIANT REMOTE SIGNING SERVICE WITH ENTRUST

Entrust Remote Signing Engine: On-premises solution for deploying a legally compliant, cloud-based signing service easily accessible through a web API

Entrust nShield HSMs: Certified, networked appliances that deliver cryptographic key services to your signing application

Identity Enterprise or Identity as a Service: Integrated IAM platform that supports a full suite of workforce, consumer, and citizen use cases

Entrust Certificate Authority: On-premises PKI solution including certificate authority (CA) and administrative services registration authority; managed by API, command line, or web console-based administration

Entrust Timestamping Authority: On-premises timestamping solution designed to integrate easily and securely with your organization's control systems

Entrust Validation Authority: Multi-CA, on-premises OCSP and CRL solution that reliably verifies the status of digital certificates

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

ENTRUST
SECURING A WORLD IN MOTION