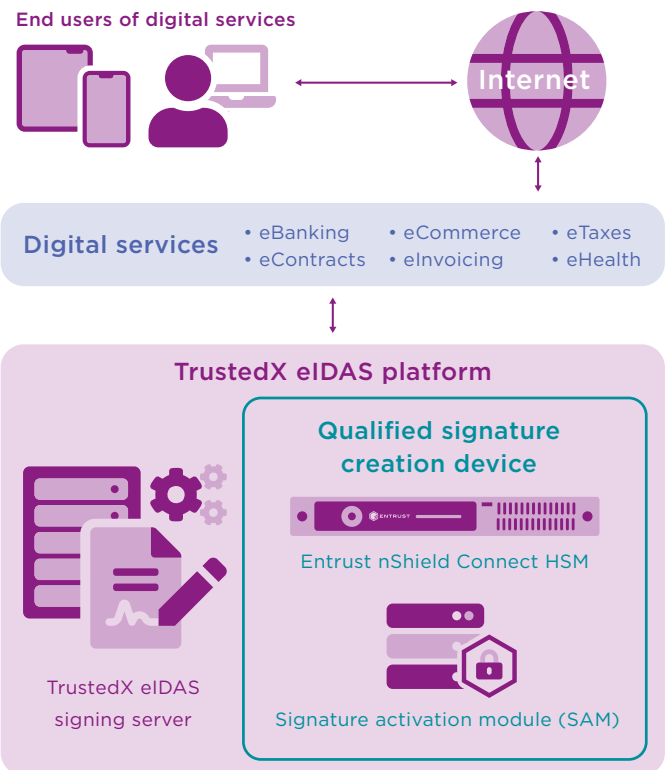# Enabling eIDAS compliant remote signing services

Scalable user-centric digital signing

HIGHLIGHTS

- Document signatures are approved remotely by users from their device

- Based on ETSI and CEN standards

- FIPS 140-2 Level 3, Common Criteria EAL 4+ and CEN EN 419 221-5 root of trust

- Alignment with EU eIDAS Regulation

The problem: eIDAS compliance for digital signature services require a high level of expertise and a very specific implementation

The significant increase in remote business and the development of regulations such as eIDAS are paving the way for digital signatures in lieu of wet-ink signatures: no more face-to-face required, no more "print, sign, scan and email", shorter execution times and reduced operational costs. However, the implementation of a scalable and compliant signing service requires specific expertise and purpose-built engines.

End users of digital services

Internet

Digital services
- eBanking
- eCommerce
- eTaxes
- eContracts
- eInvoicing
- eHealth

TrustedX eIDAS platform

Qualified signature creation device

Entrust nShield Connect HSM

Signature activation module (SAM)

TrustedX eIDAS signing server

Entrust nShield Connect HSMs integrate with the Entrust TrustedX eIDAS platform to protect the PKI key attributes

Enabling eIDAS compliant remote signing services

The challenge: implementing a user-centric, compliant signing service that can be easily integrated to service providers and identity providers

An eIDAS-compliant remote signing service must be set up in accordance with very specific standards and cover a large number of end-users with a wide variety of devices. It also requires strong integration capabilities to identity providers and PKI services, while maintaining a fully-transparent user experience.

The solution: a platform providing a legally-compliant, cloud-based signing service that can be used through a web API, with signing keys centrally protected within an HSM

TrustedX eIDAS is a platform providing a legally-compliant cloud-based signing service that can be used through a Web API. Signing keys are centrally protected within a hardware security module (HSM), and document signatures are approved remotely by users from their device, without the need for a hardware or software token.

The platform provides advanced and qualified signatures as defined by eIDAS. It is based on ETSI and CEN standards, which guarantee a very high level of trust and a broad interoperability with the industry products that require digital signatures. The user onboarding and signing process is transparent, does not require specific knowledge and can be done from any device.

Entrust solutions cover both current and future eIDAS compliance needs:

- As per the current eIDAS regulation, Entrust nShield® Connect+ HSM is certified as a qualified signature creation device (QSCD) under Common Criteria EAL4+

- As per the upcoming eIDAS amendment, the combination of the Entrust nShield XC HSM (Common Criteria CEN EN 419 221-5) and the Entrust Signature Activation Module (CEN EN 419 241-2) provide a fully-compliant QSCD

Why use Entrust nShield HSMs with the Entrust TrustedX eIDAS platform?

Cryptographic keys handled outside the protected boundary of a certified HSM are vulnerable to attacks, which can lead to security breaches. HSMs offer a proven and auditable way to secure valuable cryptographic material. Entrust nShield HSMs integrate with the TrustedX eIDAS platform to provide comprehensive logical and physical protection of the PKI key attributes. The combined solution delivers an auditable method for enforcing security policies which:

- Enable customers and service providers to meet EU cross-border standards

- Generate and manage sensitive cryptographic keys in a certified, tamper-resistant hardware environment

- Deliver a root of trust for all derived digital services

Enabling eIDAS compliant remote signing services

Providing a mechanism to enforce security policies, and a secure tamper resistant environment, Entrust nShield HSMs enables customers to:

- Secure keys within a carefully designed cryptographic boundary that uses a robust access control mechanism, so keys are only used for their authorized purpose

- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed

- Deliver superior performance to support the most demanding applications

Entrust TrustedX eIDAS platform

The purpose built TrustedX eIDAS platform provides:

- eIDAS compliant advanced and qualified signature solutions

- Single platform for digital signature across end user devices

- Increased user security and convenience with Mobile ID, a mobile application (also available in SDK) for user authentication and signature approval

- Easy integration with other Entrust solutions: PKI, authentication, timestamping services, etc.

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.

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.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