Entrust empowers 3Key Company to deliver eIDAS-compliant remote signing solution

Challenge

Many enterprises and financial institutions in the European Union are looking at ways of incorporating remote signing capabilities that are compliant with eIDAS, the EU regulation for electronic identities and signatures. But the implementation of a scalable, compliant signing service in the EU requires extensive knowledge of eIDAS technical standards and purpose-built engines, as well as a degree of adaptation and a forward-looking perspective of remote signature standards.

Solution

As a signing service solution provider, 3Key Company has been working with Entrust to develop a comprehensive and easy-to-implement remote signing solution for organizations in the EU and beyond. The solution provides secure and legally binding digital signatures in the EU without the need for signers to handle any certificate or hardware themselves. It leverages common criteria-certified signature creation devices that includes a high-performance nShield® Hardware Security Module (HSM) and the Entrust Signature Activation Module (SAM) to improve the security of remote signing deployments.

PARTNER PROFILE

3Key Company's dedicated team of information security professionals help customers use data more effectively to streamline remote business, while protecting critical assets from compromise and misuse by unauthorized parties. Specializing in certificate lifecycle and encryption key management, 3Key Company deploys software and hardware technologies from leading providers like Entrust to deliver the right solutions to customers.

Objectives

3Key Company wanted its remote signing service to deliver:

- Fast time-to-market by eliminating the off-line process of obtaining a wet signature from customers and business partners
- eIDAS regulatory compliance, helping to ensure interoperability across the EU and beyond

3KEYCOMPANY

3Key Company Case Study

3Key Company's remote signing solution will allow organizations to provide a high-assurance digital signing service including:

- A signature creation device aligned with existing and anticipated eIDAS requirements
- A direct integration with document and signature management solutions

- Strong user authentication and remote signature authorization
- Signature creation application supporting all advanced electronic signature formats
- Management of cryptographic keys and certificates
- Easy and comprehensive reporting, monitoring, and dashboards
- Automation of signing-related procedures and tasks

The Transformation

eIDAS standards are created by regulatory bodies such as ETSI and CEN, and they are constantly reviewed, updated, or replaced by stronger versions. This is why eIDAS is an evolving regulation and remote signing service solution providers must be prepared to adapt their solution to upcoming changes in technical standards.

To help future-proof remote signing service capabilities, 3Key Company turned to Entrust to incorporate the new Entrust Signature Activation Module (SAM), together with an Entrust nShield Hardware Security Module (HSM) to form an eIDAS-compliant remote Qualified Signature Creation Device (QSCD) for 3Key Company's remote signing implementations. This QSCD deployment is based on the latest standards and is expected to become the new reference in the next eIDAS implementation act or revision of the eIDAS regulation.

> « **Empowered by the powerful combination of the Entrust Signature Activation Module and nShield Hardware Security Module, we have been able to develop a cost-effective Qualified Signature Creation Device for our remote signing service implementations. This solution helps achieve eIDAS compliance today, and it is also developed for the next anticipated version of eIDAS as well and can be deployed rapidly to provide a high-performance, high-assurance solution.** »
>
> Roman Cinkais, CEO, 3Key Company

The Entrust Advantage

In a remote signing deployment, the signatures are generated in a specific QSCD module. The latest version of QSCDs consists of one or more HSMs bundled with one or more Signature Activation Modules (SAMs). The SAM is a security endpoint that receives the signer's authentication data, the signer's signing key, and the data to sign. Once it has verified and authorized all elements, the SAM "activates" the signature of the data with the HSM. The design of the Entrust SAM is based on the Trustworthy Systems Supporting Server Signing (TW4S) architecture described in the CEN EN 419 241 standards. The cryptographic module used with the Entrust SAM module is an Entrust nShield HSM, which is Common Criteria certified for FIPS 140-2 Level 3.

As such, Entrust brings:

- Deep expertise in PKI, digital signing, and HSM solutions

- A one-stop-shop for certified QSCDs, with or without SAM

- Global 24/7 multi-language customer support

- A global presence in 150+ countries, with 2,500+ employees focused on enabling trusted identities, payments, and data protection

Learn more about our HSMs at entrust.com/HSM

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