IgniSign Ignites E-signing Workflows with Entrust QSCD solution

Challenge

The world is increasingly digital and more and more of us are conducting business remotely. E-signing is replacing physical paper signatures and playing a critical role in providing traceability, accountability, and audit services. To meet legislative, regulatory, and internal controls, clear originator authentication, signed approvals, and assured data integrity and provenance are required.

When creating an easy-to-implement and reasonably priced e-signature application programming interface (API), IgniSign needs to implement a Qualified Signature Creation Device (QSCD) in order to maintain the highest levels of security while offering a smooth and time-sensitive user experience.

Solution

As a Qualified Trust Service Provider (QTSP), IgniSign will offer a complete, affordable solution that is underpinned by a QSCD from Entrust. Entrust bundles the HSM and the SAM so that the QSCD needed for a qualified signature is readily available off-the-shelf. Additionally, the Entrust solution provides IgniSign with the ability for each HSM's capacity to be upgraded and additional HSM and SAM modules can be added like building blocks. This approach creates a price-flexibility balance that is instrumental in IgniSign's implementation.

> **We needed a complete QSCD and Entrust was one of the few partners who could bundle the required components at a competitive price and deliver it reliably and efficiently. More importantly, since the beginning, we've had both a technical and business discussion with Entrust and that made the difference.**
>
> Julien Jenoudet, CEO, IgniSign

Learn more about our our QSCD for remote signing offering at entrust.com

Entrust and IgniSign Case Study

CUSTOMER PROFILE

Luxembourg-based IgniSign was founded by seasoned executives with extensive experience in growth, tech, and regulatory environments. Since the beginning, IgniSign's goal has been to implement a genuinely innovative approach to digital signatures based on new technologies and cryptography.

Objectives

IgniSign implemented the Entrust QSCD to help:

- Obtain eIDAS certification as a Qualified Trust Service Provider (QTSP)
- Provide qualified e-signatures
- Deliver a low operating cost
- Provide the easiest integration possible for developers implementing its API

Technology

- Entrust nShield HSM Connect + ECC + remote admin
- Entrust nShield HSM Edge
- Entrust Signature Activation Module (SAM)
- Rapid Deployment

Results

This implementation delivers:

- Low fixed costs and near-zero marginal cost
- The ability to ramp up capacity as demand grows
- A productive third-party relationship with the hosting company

THE TRANSFORMATION

Enabling qualified electronic signatures

Since its inception, Luxembourg-based IgniSign's goal has been to implement a genuinely innovative, "lean and mean" approach based on new technologies and cryptography to address the e-signature market. IgniSign accomplishes this by offering electronic signature capabilities as an API for customers across EMEA and North America.

Following a thorough review of five potential suppliers, IgniSign selected Entrust to provide the QSCD, which is a combination of the Entrust Signature Activation Module (SAM), together with an Entrust nShield® Hardware Security Module (HSM) to form an eIDAS-compliant platform. This combination provides the root of trust for IgniSign to both sign certificates linked to the identity of a natural person and perform the signature in their name.

As such, the Entrust HSM is used both as the certificate authority (CA) issuing the certificates as well as a signing system. To ensure system integrity, the HSM is hosted in a Tier IV private cloud environment.

Learn more about our our QSCD for remote signing offering at entrust.com

Entrust and IgniSign Case Study

MEASURES OF SUCCESS

- eIDAS certification
- Low cost
- Future scale-up

The Entrust advantage

In a remote signing deployment, the signatures are generated in a specific module called a Type 2 Qualified Signature Creation Device (QSCD). This version of an Entrust QSCD consists of one or more Entrust nShield HSMs bundled with one or more Entrust 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 that is Common Criteria EAL4+ certified. Additionally, Entrust has passed the Common Criteria EAL4+ evaluation for its SAM.

For more information visit: Entrust QSCD

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223