

SOLUTION BRIEF

Entrust empowers OmniTrust to deliver eIDAS-compliant remote signing solution



Challenge

Many enterprises and financial institutions in the European Union are looking to add remote signing capabilities that are compliant with eIDAS, the EU framework for electronic identity and trust services – now significantly expanded by eIDAS 2 and the European Digital Identity Framework. But implementing a scalable, compliant signing service requires deep knowledge of eIDAS technical standards, purpose-built signing engines, and a forward-looking view of how remote signature requirements will develop.

Solution

As a remote signing service solution provider, OmniTrust 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 include 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

OmniTrust'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, OmniTrust deploys software and hardware technologies from leading providers like Entrust to deliver the right solutions to customers.

Objectives

OmniTrust wanted its remote signing service to deliver:

- Fast time-to-market by eliminating the offline process of obtaining a wet signature from customers and business partners
- eIDAS regulatory compliance, helping to ensure interoperability across the EU and beyond
- A ready-made technology solution that supports the certification of qualified electronic signatures
- High assurance in the security of the signing process
- Remote and instant identity verification of all document signers
- High levels of integration with existing systems
- An open signing solution that can be integrated with components from established technology providers

Technology

- Entrust Signature Activation Module
- Qualified Signature Creation Devices (QSCDs):
 - Entrust nShield 5s and nShield 5c HSMs



OmniTrust'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 is an evolving framework. Its technical standards are set by bodies such as ETSI and CEN and are regularly reviewed and updated, so remote signing providers must be able to adapt as requirements move. That shift is now underway: Regulation (EU) 2024/1183 – widely known as eIDAS 2 – entered into force in May 2024 and establishes the European Digital Identity Framework, including the EUDI Wallet, which Member States are making available to citizens and businesses.

Critically for signing service providers, eIDAS 2 reinforces remote qualified electronic signatures, in which signer's key is held and used within a secure device operated by the trust service provider and activated through strong authentication – removing the need for the smart card and reader that have long limited QES adoption.

To meet this shift, OmniTrust turned to Entrust, combining the Entrust Signature Activation Module (SAM) with an Entrust nShield Hardware Security Module (HSM) to form a remote Qualified Signature Creation Device (QSCD) for OmniTrust's signing implementations. Built on the CEN EN 419 241 and EN 419 221-5 standards that underpin the eIDAS framework, the deployment supports OmniTrust's compliance position today and gives it a foundation that can evolve as implementing acts and technical standards continue to develop.





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 is designed to support evolving eIDAS requirements and can be deployed rapidly to provide a high-performance, high-assurance solution.

ROMAN CINKAIS, SVP ENTERPRISE PRODUCTS, OMNITRUST

The Entrust Advantage

In a remote signing deployment, the signatures are generated in a specific QSCD module. Remote QSCDs typically consist of one or more HSMs used 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 is an Entrust nShield HSM, which is FIPS 140-3 Level 3 validated and Common Criteria EAL4+ (EN 419 221-5) certified.

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

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.