Cryptomathic Delivers Qualified Electronic Signatures Using Entrust nShield HSMs

Secure your customers' online journey with a centralized solution for qualified electronic signatures
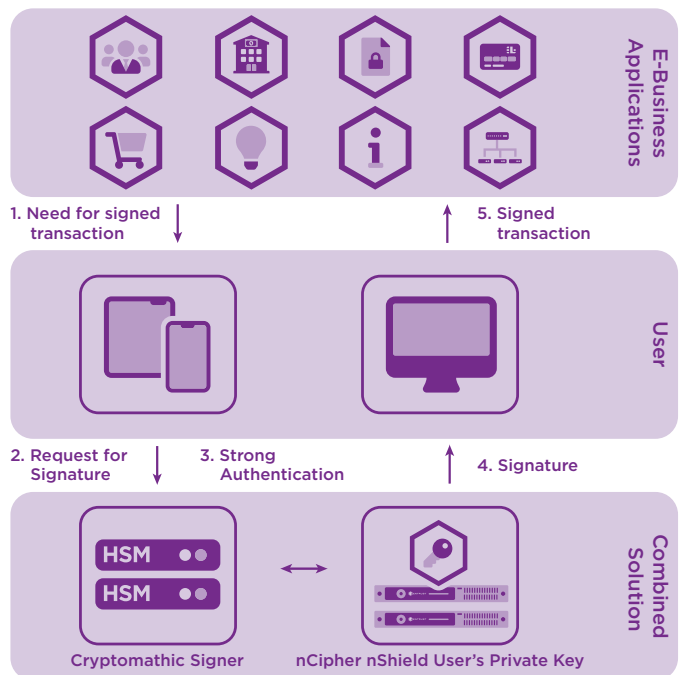
HIGHLIGHTS

- Sign transactions and documents, anytime, anywhere
- Enable a pan-European compliant secured solution
- Support non-repudiation with "what you see is what you sign"
- Reduce operational costs of managing physical documents
- Provide remote Qualified Electronic Signatures

The Problem:

Online banking services that require users to physically sign legally binding transactions and documents only deliver an incomplete digital solution

As you strive to deliver a complete digital journey to your online customers, being able to provide trust and convenience is critical. While most transactional aspects of online banking have now been digitized, the last step of this journey — the one where end — users provide their legally binding consent to what is presented on their connected device, has been missing from available offerings.

E-Business Applications

1. Need for signed transaction

5. Signed transaction

User

2. Request for Signature

3. Strong Authentication

4. Signature

HSM
HSM

Cryptomathic Signer   nCipher nShield User's Private Key

Combined Solution

Entrust nShield® Connect HSMs safeguard and manage the private key used by Cryptomathic Signer to deliver Qualified Electronic Signatures to online banking customers. nShield HSMs can be deployed on-premises or as a service.

LEARN MORE ABOUT HSM AT ENTRUST.COM

The Challenge:
Delivering a trusted digital signing experience that completes your customer digital journey

Your online customers demand solutions that allow them to do everything from any device without breaking the browser experience. Enabling them to digitally sign legally binding transactions and documents from anywhere at any time, while providing non-repudiation requires high assurance digital signature technology. In Europe, the regulation on electronic identification and trust services for electronic transactions (eIDAS) is becoming a strong enabler for business' digital transformation strategies.

The Solution:
Qualified electronic signatures for high assurance, and zero footprint signing for ease of use from anywhere

Digital signatures are the next step to providing the full digital customer journey that moves remaining offline operations and transactions completely online. To drive this technological innovation, eIDAS has provided specific requirements to which businesses must adhere in order for electronic signatures to be considered legally binding in the EU. Cryptomathic patented technology enables your business to deliver an electronic signature solution to your end-users in a centrally managed, secure, and user-friendly manner. And with zero footprint, it does not require download of an application onto the end-user's device.

Cryptomathic Signer is a remote signing solution, incorporating Cryptomathic's eIDAS certified qualified signature creation device (QSCD), which helps banks and trust centers provide large scale, legally binding digital signature services to clients and end-users. Used by banks and government departments processing millions of transactions each month across Europe, the solution combines strong security with user convenience by using "what you see is what you sign" (WYSIWYS) technology that builds and enhances consumer trust.

Cryptomathic Signer integrates with Entrust nShield® Connect hardware security modules (HSMs) to protect users' private keys. Leveraging both companies' expertise in supporting evolving payments and digital ecosystem for e-banking and e-government, Cryptomathic Signer integrates smoothly with existing web banking services and does not require software install, plug in, or additional components on the client side. It can be used anywhere at any time from any device with browsing capacity. It is also virtually impossible for users to lose their signing key or for the key to be compromised, as it is securely stored and protected within the secure FIPS 140-2 Level 3 and Common Criterial EAL4+ certified security boundary of the nShield Connect HSM that can be deployed on-premises or as a service.

Why use Entrust nShield Connect with Cryptomathic Signer?

Cryptographic keys handled outside the boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise. HSMs are the only proven and auditable way to secure valuable cryptographic material. In order to offer mobility, the user's signing key is stored

centrally in the tamper-resistant environment of the trust center. Cryptomathic Signer enables a direct secure connection from the user's browser to the nShield Connect HSM, where users' keys are safely stored and which can be deployed on-premises or as a service.

Users authenticate themselves using existing two-factor authentication in order to access and use their signing key.

Entrust nShield Connect is a high-performance network-attached HSM that delivers secure cryptographic services as a shared resource for distributed application instances and virtual machines. The solution enables appropriate levels of physical and logical controls to be enforced over server-based applications where software-based cryptography fails to meet risk management targets. nShield Connect HSMs deliver high levels of cryptographic performance, scalability, and resilience. Latest cryptographic algorithms and key management schemes makes it a future-proof solution as standards emerge especially for mobile applications. Its capability to enable development of custom code to run inside the HSM provides an indispensable tool to meet specialized customer requirements.

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.

Cryptomathic

Cryptomathic Signer delivers a central digital signing experience to online customers across all channels, including web browsers, desktop, and mobile. The purpose-built solution:

- Delivers eIDAS complaint Qualified Electronic Signatures

- Leverages and enhances the security of existing two-factor authentication deployments

- Applies non-repudiation for legal enforcement

cryptomathic.com

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

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

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