Entrust helps businesses maintain trust in multi-party invoicing scenarios

Entrust hardware security modules (HSMs) help to secure electronic invoicing

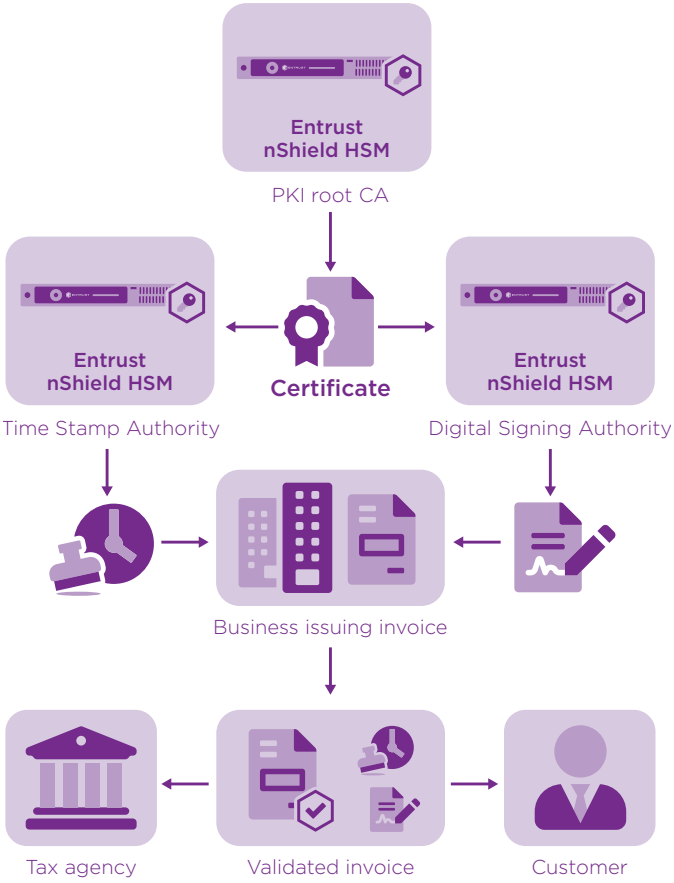
HIGHLIGHTS

- Automates trust and verification among electronic business systems
- Leverages Public Key Infrastructure with high assurance private key protection at the root and issuing certificate authority levels
- Provides trusted document authenticity and non-repudiation
- Extends security controls to documents as they leave the organization
- Safeguards critical signing keys in a FIPS 140-2 Level 3 certified module

The problem: authenticity and integrity

Preparing, sending, and paying invoices is a critical process for any business. electronic invoicing, or e-invoicing, provides efficiency and is widely used in day-to-day transactions. Globally it is used to register purchases, as required to enforce the collection of value added taxes.

Electronically communicating the sensitive information inherent to invoices necessitates automated protection. And submitting invoices to taxation authorities requires the utmost trust in the chain of custody.



LEARN MORE AT ENTRUST.COM/HSM

Entrust helps businesses maintain trust in multi-party invoicing scenarios

To securely implement e-invoicing, you need to ensure that the documents you send reach their destination with no tampering along the way. As an example, a successful man-in-the-middle attack could result in your bank's information being replaced by someone else's. Further, government authorities may require proof that you're sending them the record at the same time that you're submitting the invoice to your vendors—you need absolute confidence in delivering this proof.

The solution: digital signatures and time stamping

The accepted standard for trust among electronic systems is digital signatures backed by a public key infrastructure (PKI). The PKI serves as a root of trust that vouches for the identities of the systems involved by issuing certificates on their behalf.

Digital signatures are used to authenticate transactions, prove that the senders sent them and that they weren't tampered with, and to prove non-repudiation—the receiving system cannot deny it received the transaction.

Signed time stamps provide proof in cases where, for instance, invoices must be submitted to the tax authority at the same time they are sent to the recipient.

When certificates provide identity and digital signatures convey authenticity, the trust in the underlying signature mechanism rests on the protection of the private cryptographic keys. Protection and control of these keys becomes the cornerstone of the trust model.

Why use nShield® HSMs and time stamp servers to protect signing keys?

Entrust nShield hardware security modules (HSMs) generate the signing keys and enforce how they are used, so that the key owners have ultimate control over which documents and certificates get signed.

Entrust time stamp service attests the origin and time of electronic records, providing a digital trail.

Entrust helps businesses maintain trust in multi-party invoicing scenarios

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.

Entrust time stamp service

Entrust time stamp service protects time stamping keys and provides highly accurate time. Available via an option pack on nShield HSMs, the time stamp service performs the following functions:

- Maintains time stamps auditable to Universal Coordinated Time (UTC)
- Supports traceability to national atomic clocks
- Prevents insiders from being able to manipulate time

Certified cryptographic solutions

Entrust nShield HSMs and time stamp service utilising the Time Stamp Option Pack are certified to Federal Information Processing Standard (FIPS) 140-2 Level 3, the most widely adopted security benchmark for cryptographic solutions in government and commercial enterprises. The certification facilitates integration with leading PKI software vendors and ensures compliance with regulatory requirements.

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