NCIPHER

www.ncipher.com

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

- 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

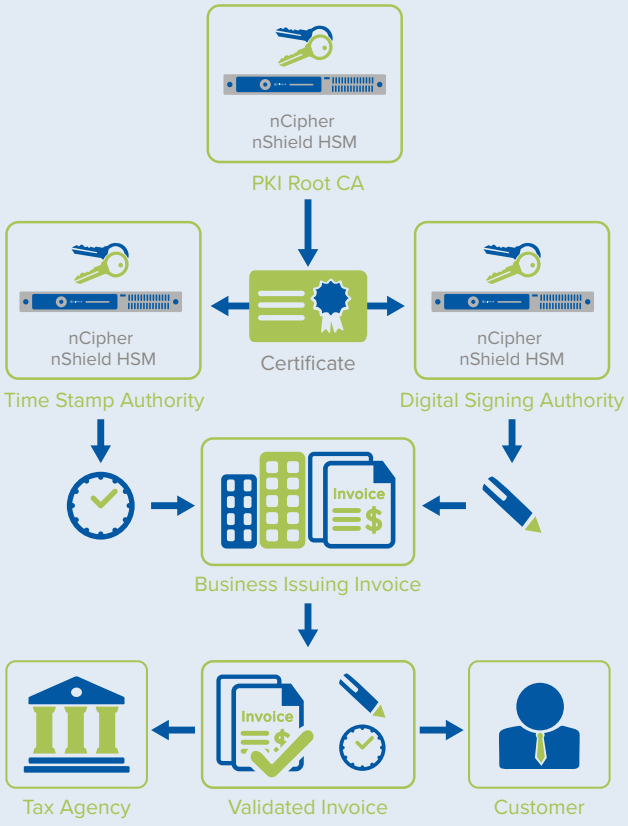
nCipher helps businesses maintain trust in multi-party invoicing scenarios

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.

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.



nCipher helps businesses maintain trust in multi-party invoicing scenarios

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?

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

nCipher Time Stamp Server attests the origin and time of electronic records, providing a digital trail.

NCIPHER NSHIELD HSMS

nCipher nShield HSMs provide high performance cryptographic services for mission-critical applications such as e-Invoicing. Available as network-attached, embedded PCI Express, or USB-connected modules, nShield HSMs perform the following functions:

- **Store encryption and signing keys** in a tightly controlled and tamper-resistant environment
- **Support separation of duties** to protect from insider threats
- **Deliver high performance** elliptic curve cryptography (ECC)

NCIPHER TIME STAMP SERVER

nCipher Time Stamp Server protects time stamping keys and provides highly accurate time. Available as an option on nShield HSMs or as an independent tamper-resistant hardware appliance, Time Stamp Server 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

nCipher nShield HSMs and Time Stamp Servers 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 how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com