Building Trust into eInvoicing:
Key Requirements and Strategies

WHITE PAPER

Executive Summary

eInvoicing presents a host of advantages for organizations looking to move away from paper-based invoicing processes—but these benefits can only be realized if businesses can ensure the integrity, accuracy, and security
of these digitalized files.
This paper looks at the key requirements for building a secure eInvoicing infrastructure, and it describes how businesses can both boost security and optimize the business benefits of their eInvoicing investments.

Introduction

For years, the digitalization of assets has been underway, completely transforming entire industries, from healthcare to music. In the same way, the move to digitalization has also brought fundamental change to the way businesses manage invoices. By moving to electronic invoicing, known as eInvoicing, organizations in a host of industries can realize a range of benefits

- **Reduced costs.** By eliminating the purchase of paper for invoice printing, reducing the time and expense of physical invoice handling, reducing the space and expense of paper-based file storage, and eliminating postage, organizations can realize direct, upfront cost savings.
- **Boost operational efficiency.** eInvoicing fosters streamlined processes for the creation, management, and distribution of invoices, and it enables integration with backend applications to enable streamlined controls.
- **Speed invoice processing.** By eliminating manual processes and physical mail, organizations can significantly reduce billing and approval cycles.
- **Improved accuracy.** By eliminating a host of manual, error-prone tasks, eInvoicing fosters increased accuracy in invoice creation.
- **Reduce carbon footprint.** Electronic invoices reduce paper and printing usage and the fossil fuel usage associated with physical shipments.

Beyond the benefits above, many organizations have been compelled to adopt eInvoicing approaches in order to comply with regulatory mandates. Examples of these mandates include the following:

- **European Directive on Invoicing.** This measure was adopted in order to provide European Union member states with a single, simplified set of rules on invoicing, rather than contending with different rules across each state. To comply with this regulation, an eInvoice's authenticity and integrity must be guaranteed through the use of electronic signatures or electronic data interchange (EDI).

To effectively implement secure eInvoicing, organizations need to establish trust throughout the process. To do so, they need capabilities to do the following:

- Ensure integrity of invoice
- Provide non-repudiation of receipt and origin
- Secure electronic tracking and storage.
- Scale to accommodate high volumes of invoices.

- **Brazil Nota Fiscal (NF-e).** This is the Brazilian Government's rule regarding the use of electronic bill-of-lading files that document the movement of goods and services provided between parties. A legally valid NF-e document is associated with the issuer's digital signature and guarantees receipt by tax authorities before the actual shipment of goods or delivery of services.

Without Trust eInvoicing is not a Solution

For all the benefits outlined earlier however, eInvoicing simply isn't feasible without the ability to ensure trust throughout the process. How can organizations ensure authorized personnel have approved invoices, without a paper trail? How can organizations ensure digital files aren't modified after they're generated and distributed? How can the business receiving an invoice be sure it came from the business that claims to have sent it?

To effectively implement secure eInvoicing, organizations need to establish trust throughout the process. To do so, they need capabilities to do the following:

- **Ensure integrity of invoice.** All parties involved need to be certain that all invoice information, including amounts, billing addresses, payment information, and more, are accurate and haven't been modified since original generation.
- **Provide non-repudiation of receipt and origin.** Organizations need to be sure that, when eInvoices are generated and approved, these processes are verifiable, and can't later be refuted or disavowed.
- **Secure electronic tracking and storage.** Organizations need to have visibility into who has accessed an eInvoice, and ensure the storage and archival of eInvoices is secure.
- **Scale to accommodate high volumes of invoices.** Organizations need to ensure that the processing of eInvoices can scale to meet immediate and long-term demands.

The Role of HSMs in eInvoicing

As outlined above, trust is a critical requirement for the feasibility of eInvoicing. Digital signatures, powered by encryption and public key infrastructure (PKI), represent the means for establishing trust in eInvoicing. Digital signatures give all parties the confidence required to trust that invoices come from known entities, and that they have not been altered in transit. In turn, these digital signatures need to have foolproof, comprehensive security mechanisms to protect them: If digital signatures are in any way compromised, the entire eInvoicing infrastructure will be compromised. This is where hardware security modules (HSMs) come into play.

Cryptographic keys are used to lock and unlock access to digitalized information. Even if the strongest encryption algorithm is used, security is still weak if cryptographic keys are not adequately secured. HSMs are dedicated systems that physically and logically secure the cryptographic keys and cryptographic processing that are at the heart of digital signatures.

HSMs support the following functions:

- Life-cycle management, including key generation, distribution, rotation, storage, termination, and archival.
- Cryptographic processing, which produces the dual benefits of isolating and offloading cryptographic processing from application servers.

eInvoices are digitally signed with a secure private signing key, which requires an HSM capable of performing certificate authority management tasks. The HSM stores the keys within the secure confines of the appliance throughout the key life cycle. The HSM enables the organization to secure digitally certified invoices and to cryptographically bind the identity of the certifying party to the invoice. By storing cryptographic keys in a centralized, hardened device, HSMs can eliminate the risks associated with having these assets housed on disparate, poorly secured platforms. In addition, this centralization can significantly streamline security administration.

The Advantages of HSMs

Compared to the process of storing cryptographic keys in software residing on general purpose application servers, HSMs deliver several advantages:

Completeness

HSMs are fully contained solutions for cryptographic processing, key generation, and key storage. As purpose-built appliances, they automatically include the required hardware and firmware (i.e., software) in an integrated package. Physical and logical protection of the appliance is supported by a tamper resistant/evident shell; and protection from logical threats, depending on the vendor's products, is supported by integrated firewall and intrusion prevention defenses. Some HSM vendors also include integrated support for two-factor authentication. Security certification is typically pursued by HSM vendors and positioned as a product feature.

Software for these same functions is not a complete out-of-the-box solution. Server hardware is a separate purchase, unless unused servers are present, as is firewall, intrusion prevention, and two-factor authentication. Being tamper resistant is not a trait typically associated with general-purpose servers. Security certification encompassing the combination of hardware platform and software would be the responsibility of the user organization and can be a lengthy and very costly activity, especially if involvement with certification bodies is not standard operating practice for the organization using the software.

Performance

Cryptography is a resource intensive process that will introduce latency to any application that depends on it. Depending on the application involved and organization, the objective could be to minimize the latency introduced by cryptography. HSMs have an advantage over software as they are designed to optimize the efficiency of cryptographic processing. Compared to software running on general purpose servers, HSMs will accelerate processing; an outcome of being purpose-built.

Compliant and Secure

Frequently, cryptography is used to meet compliance mandates. Cryptography use, however, does not guarantee that information is secure. Further, there are no security guarantees (i.e., promises of no security instances ever) with any security solution so the objective becomes one of managing risk by reducing the number of vulnerabilities and the likelihood of vulnerabilities being exploited. The aforementioned completeness attributes of HSMs allow organizations that deploy HSMs to take efficient and simultaneous steps toward compliance and security.

Centralization of Key Management

An attribute of software is its portability; software can be installed on several servers. Consequently, cryptographic keys have greater likelihood to reside in several locations/software hosts. This multi-location characteristic will add to administrative complexity and potential lapses in the life-cycle management of cryptographic keys (e.g., rotation and revocation). In addition, if consistency in the protective layer of the software host (e.g., firewall, intrusion prevention, and access control) cannot be ensured, the risk of keys being compromised increases. With HSMs, the tendency is to store keys in a single unit. Not only does this streamline administration and reduce the potential for management lapses but it also supports a consistent layer of key protection.

The Benefits of eInvoicing with SafeNet

SafeNet offers a broad set of HSMs that are ideally suited to the demands of eInvoicing infrastructures. By employing SafeNet HSMs, organizations can realize a range of benefits:

Enhance Security and Ensure Compliance

SafeNet HSMs deliver sophisticated security capabilities that enable businesses to enjoy maximum security in their eInvoicing implementations, ensuring optimal trust in the entire invoicing lifecycle. SafeNet HSMs address the following critical requirements:

- **Certification.** Many SafeNet HSMs meet the demanding requirements of FIPS and Common Criteria certification.
- **Compliance.** SafeNet HSMs offer the robust security capabilities that ensure compliance with the European Directive on Invoicing, Brazil Notal Fiscal (NF-e), and other regulations.
- **Multiple signatures.** With SafeNet HSMs managing digital signatures, organizations can manage multiple signatures per invoice.

"According to the European Association of Corporate Treasurers' (CAST) Project, an average cost savings of 80% can be achieved by using electronic invoicing."
~ European Electronic Invoicing Final Report

Optimize Operational Performance

By leveraging SafeNet's secure HSMs in a secure eInvoicing deployment, organizations can realize significant gains in operational performance:

- **Efficient retrieval, processing.** By working with electronic files, business can more quickly generate, locate, retrieve, and process invoices.
- **Elimination of time consuming, inefficient paper-based processes.** Secure eInvoicing systems enable businesses to eliminate a host of manual, error-prone processes associated with the handling and distribution of paper invoices.
- **Improve vendor relations.** By ensuring trust and optimizing speed and efficiency throughout the invoicing process, businesses can improve relationships with vendors.

Reduced errors, reconciliation times. With eInvoicing, businesses can improve accuracy in invoice generation and approval processes, and, in the event of questions or disputes with a given invoice, businesses can much more quickly reconcile those issues and speed payment cycles.

- **Efficiency through back office integration.** With a secure eInvoicing system in place, organizations are well equipped to integrate digital invoicing process with other backend applications, such as procurement and enterprise resource planning, which can lead to further efficiency and accuracy gains.

Reduce Cost

With SafeNet powering eInvoicing systems, businesses can realize an array of cost saving benefits. For example, by centralizing cryptographic keys and policy management on SafeNet HSMs, businesses can significantly reduce the administration associated with managing digital signatures in a distributed, disparate fashion. Also, by eliminating the need to do filing of paper invoices, business can reduce the overhead and expense of paper invoice storage costs. Finally, the digitization of invoices leads to significant reductions in the time and staffing costs associated with paper based invoicing processing.

SafeNet's Breadth of HSM Offerings

SafeNet HSMs provide reliable protection for applications, transactions, and information assets by safeguarding the cryptographic keys that are at the heart of any encryption-based security solution. SafeNet HSMs are the fastest, most secure, and easiest to integrate application security solution for enterprise and government organizations to ensure regulatory compliance, reduce the risk of legal liability, and improve profitability.

HSM Advantages:

- Completeness
- Performance
- Compliant and Secure
- Centralization of Key Management

SafeNet offers these HSM products:

General Purpose HSMs, Network Attached

- **Luna SA.** Luna SA offers award-winning application protection through powerful cryptographic processing and hardware key management. Luna PCI for Luna SA 4.1has received Common Criteria EAL4+ certification.
- **Luna SP.** The SafeNet Luna SP allows developers to securely deploy Web applications, Web services, and other Java applications in a protected, hardened security appliance.
- **Luna XML.** SafeNet Luna XML is designed to secure next-generation XML Web services and service-oriented architectures (SOAs). Other HSMs take months to integrate with new applications due to complex security APIs. Luna XML has zero footprint on the host application server, providing for rapid, independent, flexible, and highly scalable deployments.
- **ProtectServer External.** The SafeNet ProtectServer External is a networkattached HSM that connects via TCP/IP to a single machine or complete network (LAN) to function as a central cryptographic subsystem that delivers symmetric and asymmetric cryptographic services. All operations that would otherwise be performed on insecure servers are securely processed within the HSM, ensuring that sensitive keys are always protected from compromise.
- **Luna SX.** The SafeNet Luna SX is a central management console for rapid HSM setup and easy remote administration for the SafeNet Luna SA and Luna SP. Using a simple GUI, SafeNet HSMs can be managed remotely and securely.

General Purpose HSMs, Embedded

- **Luna CA4 HSM.** The SafeNet Luna CA4 offers a complete hardware security solution for the protection of sensitive root keys belonging to certificate authorities used in public key infrastructures (PKI).
- **Luna PCI.** SafeNet Luna PCI is designed to protect cryptographic keys and accelerate sensitive cryptographic operations across a wide range of security applications.
- **Luna PCM.** SafeNet Luna PCM is a low-cost family of compact HSMs, offering hardware-based key management and hardware-accelerated cryptographic performance within a compact PCMCIA card.
- **ProtectServer HSMs.** For server systems and support applications that require high performance symmetric and asymmetric cryptographic operations, ProtectServer Gold and ProtectServer Internal-Express provide tamper-protected hardware security.

Customer Profile: Antwerp Port Authority

Challenge

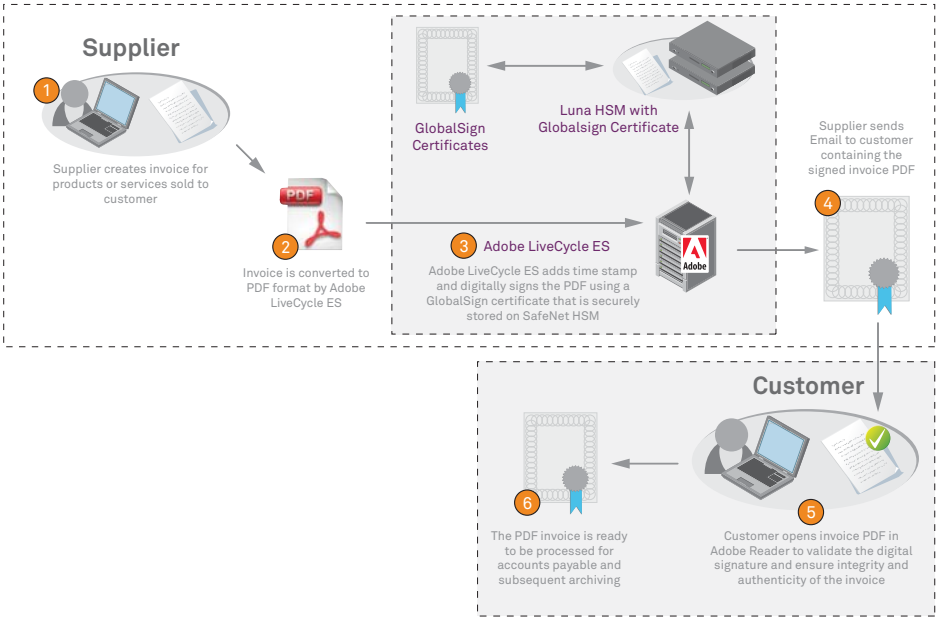
The European Directive on Invoicing (EC/115/2001) requires member states, including Belgium, to implement electronic invoicing into their local value-added tax (VAT) legislation to improve and streamline cross-border invoicing. The VAT rules require suppliers to guarantee the authenticity of origin and the integrity of the content for the invoices they create.

Solution

In order to comply with the VAT law, Antwerp Port Authority implemented an advanced e-invoice solution based on digital signatures. Antwerp Port Authority leveraged its multi-partner investment in Adobe's LiveCycle Enterprise Suite (ES) and GlobalSign's DocumentSign digital certificates by selecting SafeNet's hardware security modules (HSMs) for storage of digital signatures and protection of cryptographic keys.

Benefits

The SafeNet, Adobe, and GlobalSign joint solution allows the Antwerp Port Authority to leverage their IT investments and apply a compliant security solution that guarantees the authenticity and integrity of electronic invoices. By applying digital signatures and encryption technologies within a PKI network environment, Antwerp Port Authority quickly brought digital invoicing processes online, thereby streamlining workflow, lowering costs, and meeting mandatory European directives for compliance.



When an eInvoice deployment integrates leading solutions like Addobe LiveCycle ES, GlobalSign certificates, and SafeNet HSMs, organizations can enjoy optimal efficiency, and security, in their invoice processing.

Conclusion

eInvoicing presents organizations with a host of benefits when compared to paper-based invoicing processes—including cost savings, improved efficiency and accuracy, and reduced environmental impact. However, unless businesses can establish and ensure trust throughout the process, any eInvoice initiative is doomed to fail. It is only by harnessing HSMs to fully secure digital signatures and cryptographic keys that organizations can optimize the security of their eInvoicing infrastructure. Today, SafeNet offers a broad range of HSMs, solutions that accommodate the needs of a range of deployments, and ensure organizations enjoy maximum return from their eInvoicing investments.

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies and in over 100 countries trust their information security needs to SafeNet.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected