SafeNet HSM Reference Guide

HSM Reference Guide

Table of Contents

< Table of contents

Code Signing

INTERNAL REFERENCE GUIDE

SafeNet Value

- Validated security with FIPS 140-2 Level 3 and Common Criteria certification
- Only HSM supply to offer true in hardware key generation and storage
- Extensive backup features for disaster recovery
- Multi-factor authentication for administration and management
- Superior performance: A single Luna SA 5.0 device is capable of up to 6,000 RSA 1024-bit transactions per second and up to 1,200 RSA 2048-bit transactions per second
- Separation of duties with multi-level access control and multi-part splits for all access control keys
- 40,000 RSA keys scale for many code signing certificates

Overview

CodeSigning

Code signing employs PKI technologies, such as keys, certificates, and digital signatures, to ensure the identity and integrity of software. Technology companies share and distribute code through networks with inconsistent and varying security policies, potentially exposing the code to manipulation, corruption, or theft.

Many software providers are now making their product available over the Internet. As such, it is imperative that code published on the Internet be seen as trustworthy by the user who downloads it. While many browsers provide a notice to verify the code's authenticity, noone can determine whether the code has been tampered with prior to delivery. Therefore, a more active approach must be taken to make the Internet a reliable medium for software distribution.

Digital signatures help maintain the electronic integrity and authenticity of code by associating it with a software vendor's unique signature. In this way, distributing software on the Internet is no longer an anonymous activity as digital certificates ensure accountability, just as a manufacturer's brand name does on packaged software.

Digital Certificates

A certificate is a set of data that completely identifies an entity, and is issued by a certification authority (CA). The data set includes the entity's public cryptographic key. When the sender of a message signs it with its private key, the recipient of the message can use the sender's public key (retrieved from the certificate either sent with the message or possibly available elsewhere in the directory service) to verify the sender's identity.

Customer Problem

Preventing software counterfeiting has always been a challenge for publishers. Over time, security measures, such as tamper-proof packaging and unique licensing keys, were developed to minimize bootlegs and unauthorized copies of software distributed on disks. The Internet lacks the subtle security provided by packaging, shelf space, shrink wrap, and the like. Without an assurance of the software's integrity, and without knowing who published the software, it's difficult for end users to know how much to trust software. In addition, Windows, Java, and Apple require code to be compliant with their digital signing requirements. When code is not correlated to a known publisher, a security warning message indicating "Unknown Publisher" is issued requiring the user to authorize the program to run on their machine. For this reason, software publishers are facing increased pressure to sign code.

SafeNet Partners:

- Microsoft Authenticode
- Verisign
- Cybertrust (Verizon)
- GlobalSign
- Entrust
- Code Signing
- Certificates

SafeNet Customers:

- Cisco
- Intel
- Lexmark
- Sony
- Seagate

	Security Threat
▶	Loss of trust in brand
▶	Often disguised as legitimate software, malicious malware can be easily distributed to infect unsuspecting desktops with viruses or to install applications to facilitate fraud.
▶	Code needs protection from viruses to provide confidence of authenticity.

HSM’s Role

To obtain a certificate from a CA, a software publisher must meet the criteria for a commercial publishing certificate. It is recommended that applicants generate and store their private key using a dedicated hardware solution, such as an HSM.

The HSM protects the identity, whether it is a server, virtualization server, or the user. SafeNet HSMs take the security one step further by storing the signing material in a hardware device, thus ensuring the authenticity and integrity of a code file.

Benefits Gained

- Increased Revenue Protection
    - Reduced risk of internal/external compromise preserves brand reputation and eliminates cost to repair infected machines of users
    - Ensures signer authenticity, data integrity, and non-repudiation of documents/code
- Increased Control and Ease of Software Management
    - Simplified key management used to control distribution of the software on the Internet
    - Users are able to sign only if they are part of the system that can be administered remotely
    - Can be accessed from multiple build systems
- Increased Security
    - Separate data from keys
    - Private keys and other necessary signature credentials stored in hardened appliance
- Reduced Cost and Improved Compliance Auditability
    - Simplified compliance – all actions auditable
    - Can be used for enterprise-wide encryption – consolidate and simplify encryption across the enterprise

Targets

Industries:
Independent software vendors
Independent hardware vendors producing drivers
Web developers who create ActiveX controls for internal or public applications
IT administrators who sign third-party drivers and applications for use in a managed network

Many code signing implementations will provide a way to sign the code using private and public key systems, similar to the process employed by SSL or SSH. The developer can either generate this key on his own or obtain one from a trusted certificate authority (CA).

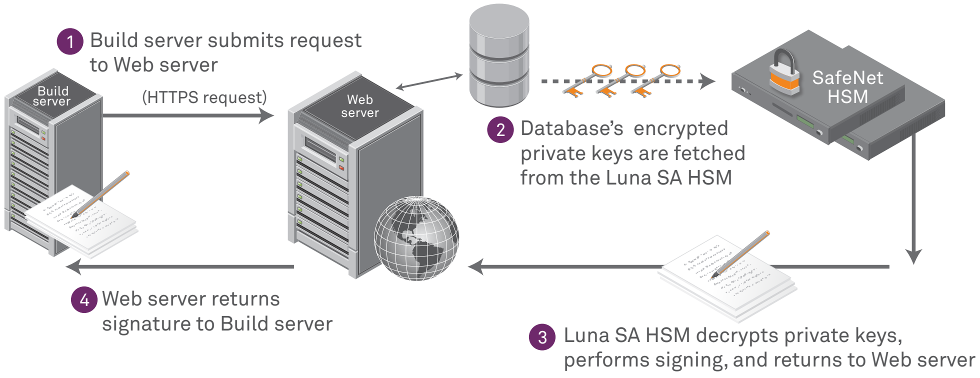
Use Case

A software vendor built their business on providing affordable and user-friendly software over the internet. With the release of Microsoft Windows Vista came the requirement that downloaded code be signed prior to running. If the code was not signed, a warning message would be issued when prospects attempted to install the vendor's software. These messages explained that the download lacked digital code signing certificates to authenticate the source of the software. As a result, many prospects did not trust the authenticity of the downloaded software and sales over the Internet began to slip.

In order to reassure customers that they provide trusted content, the software vendor looked for a solution to sign their code using private and public key systems. The solution was to implement an enterprise PKI featuring VeriSign as the Certificate Authority and a SafeNet HSM for cryptographic key storage. The SafeNet HSM was the right choice because it offered FIPS 140-2 Level 3 and Common Criteria certification in a tamper-proof hardware device.

With the PKI in place, prospects and customers gained the confidence that the content they were downloading was authentic and could be trusted. The software vendor was able to instill user confidence in their brand, eliminate security alerts, and increase Internet sales of their software.

Code Signing


1 Build server submits request to Web server
Build server
(HTTPS request)
Web server
SafeNet HSM
2 Database's encrypted private keys are fetched from the Luna SA HSM
4 Web server returns signature to Build server
3 Luna SA HSM decrypts private keys, performs signing, and returns to Web server

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

< Table of contents

Database Encryption

INTERNAL REFERENCE GUIDE

SafeNet Value

- Master and Encryption keys protected by HSM
- Virtual HSM support for segregated database encryption
- PCI DSS compliance
- Works seamlessly within native database infrastructures

Overview

Database-level encryption allows enterprises to secure data as it is written to and read from a database. This type of deployment is typically done at the column level within a database table and, if coupled with database security and access controls, can prevent theft of critical data.

Advanced security through database encryption is required across many different sectors and increasingly to comply with regulatory mandates. The public sector, for example, uses database encryption to protect citizen privacy and national security. Initiated originally in the United States, many governments now have to meet policies requiring FIPS-validated key storage. For the financial services industry, it is not just a matter of protecting privacy, but also complying with regulations, such as PCI DSS. This creates policies that not only define what data needs to be encrypted and how, but also places some strong requirements on keys and key management.

Customer Problem

Cryptographic operations use up valuable business critical performance engine.

	Security Threat
▶	Unprotected MDF file or backup file can be stolen and all credit card data is compromised, and the corporation fails PCI-DSS compliance

HSM's Role

Enables vendors to integrate with the database, encrypt sensitive data, and store private keys in an external hardware device and have top-level performance together with heightened security.

Benefits Gained

- Alleviation of SQL's cryptographic operations by utilizing an external hardware device
- Execution of all cryptographic operations and storage of virtually an unlimited number of keys, all within the secured SafeNet HSM enclosure
- High performance of bulk cryptographic operations provides the best cost-effective solution for database security
- Support for multiple user sessions (each potentially having multiple keys) with secured authentication and login
- Bulk encryption, decryption, and key management functions in an external hardware device while providing PCI DSS compliance

SafeNet Partners:

- Microsoft
- Protegrity
- Oracle
- RSA
- Vormetric

SafeNet Customers:

- Nautilus
- Telus
- Symantec
- Comidea

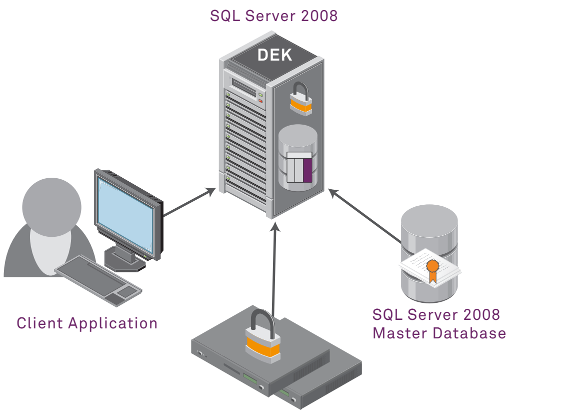
Targets

Industries:	Solution Providers:
• Retail Payment • Healthcare • Financial Services • Government • Manufacturing • TLD providers • Online bank and retail/payment providers • Forgotten password web sites • SaaS providers • Cloud computing providers • DNSSEC key management and zone signing software providers	**DNS ROOT Service Providers** • VeriSign • ICANN (recommending body) • US Gov **TLD Providers:** • VeriSign • Cogent Systems • ISC • Autonomica • RIPE NCC • US DOD

Use Case

Microsoft SQL Server addresses several security issues, including automatic secured updates and encryption of sensitive data. The data encryption exists at a cell level and is accomplished by means of built-in system procedures. SQL Server supports encryption capabilities within the database itself, fully integrated with a key management infrastructure. SQL Server provides an option to put key management in the hands of the end user, making it possible to protect data using secrets that even the administrator does not know. By default, client-server communications are encrypted. However, security problems can occur at many levels. There are some concerns when disaster recovery involves failover to another SQL Server orthere is a need to restore a database containing encrypted data.

Production Deployment



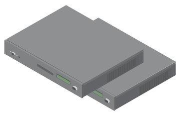
1 TDE uses a Database Encryption Key (DEK) for encrypting the database that is stored in the database boot record

2 DEK is secured by an asymmetric key that resides in the Luna SA/Luna PCI

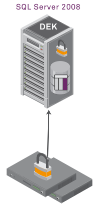
3 Certificate is secured by database master key

Typical HSM Opportunities

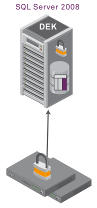
Production Deployment
Two HSMs



Development Deployment
One HSM



User Acceptance Test Deployment
Two HSMs



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

< Table of contents

HSM & Oracle Transparent Database Encryption

SOLUTION BRIEF

SafeNet hardware security modules (HSMs) combine the strongest cryptographic security with the highest performance, reliability, and ease of integration for rapid and affordable application protection using Oracle Advanced Security with Oracle Database 11g.

Overview

Oracle Advanced Security, an option to Oracle Database 11g, helps address privacy and regulatory requirements, including the Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), and numerous breach notification laws. Oracle Advanced Security provides data encryption and strong authentication services to the Oracle database, safeguarding sensitive data against unauthorized access to the network, operating system, or through theft of hardware or backup media. Oracle Advanced Security benefits include:

- No application changes
- Built-in key management
- High performance

The secure storage of master encryption keys is the foundation of any robust security solution. Integration of SafeNet Luna SA hardware security modules (HSMs) with Oracle Advanced Security transparent data encryption (TDE) allows for the Oracle master encryption keys to be stored in the HSM, offering greater database security and centralized key management for Oracle Advanced Security with Oracle Database 11g. The master encryption key never leaves the secure confines of the HSM.

Centralized, Network Storage of Keys with HSMs

Oracle Advanced Security provides built-in key management, eliminating the complex issues associated with traditional encryption solutions. Optionally, storing master encryption keys in a SafeNet Luna SA HSM adds centralized, network-based physical storage of master encryption keys used by Oracle TDE.

The TDE master encryption key is part of a two-tiered key architecture that protects the encryption keys used to encrypt the data. The TDE master key can be stored with minimal security, in software only in an Oracle Wallet (a PKCS#12 formatted file), or in a highly secure and auditable format in the SafeNet Luna SA HSM. This two-tiered key architecture allows for easy re-keying and high performance.

As a centralized, hardened device, HSMs are ideal for securely storing a backup copy of private keys copy. The high-assurance Luna SA HSM also provides a verifiable audit trail, proving that keys have been properly secured throughout their entire lifecycle. The Oracle and SafeNet integration solves the security issue of storing master encryption keys and security cryptographic operations, such as key creation, deletion, encryption, and decryption, for complying with security best practices and industry regulations.

Features and Benefits:

Peace of Mind

- All encryption and decryption, digital signing, and verification operations are performed within the HSM to deliver the highest levels of performance, availability, and security to ensure business processes and systems are running efficiently

Ease of Management & Integration

- Centralized network appliance performs all key management functions in a secure location
- Also offers local and remote key management control for flexibility

High Assurance Protection

- Stored on hardened and FIPS 140-2 Level 3 and Common Criteria EAL 4+ certified cryptographic modules, cryptographic keys never leave the confines of the HSM.
- Prevention of database and key theft, which is easy to do without hardware
- Auditing of cryptographic keys and tracking changes
- Separation of duties between DBA and System Administrator

Cryptographic Offload

- Secure computational storage
- Storage of SSL Cert keys in the HSM
- Eliminate key limit size constraints

Solution offers:

- Eliminates costs associated with:
    - Company brand damage by security breach and information leaking
    - Loss of customer loyalty and confidence
    - Fines by not complying with industry mandates
- Key lifecycle management
- Master encryption key never leaves the HSM
- Restricted access control
- Network-based physical storage of master encryption keys (high assurance)
- Storage of backup private key copy
- Verifiable audit trail
- Compliance with security best practices and industry regulations
- Secures cryptographic operations
- Transparency: No changes to applications required
    - Numbers and text
    - Scanned documents (medical, financial, personnel records)

How the Solution Works

HSMs are dedicated systems that physically and logically secure the cryptographic keys and cryptographic processing that are at the heart of any digital signature and data protection solution. Besides physically securing the master keys used by Oracle Database 11g, HSMs assure restricted access by authorized users.

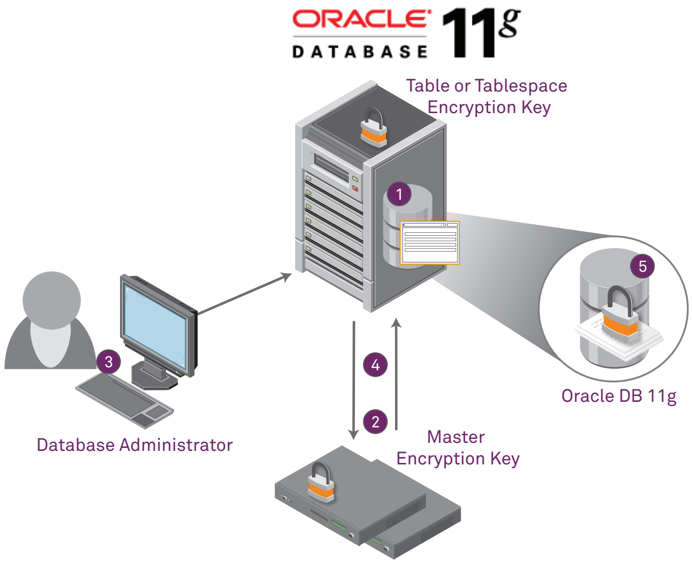
1. Sensitive data is encrypted either with Oracle Advanced Security TDE column or with tablespace encryption (no change to application required). The former encrypts application table columns containing sensitive information like credit card or social security numbers. The latter encrypts entire application tablespaces, eliminating the need to identify sensitive columns. Encrypted data remains encrypted when exported via Oracle Data Pump, or in database backups. (Unstructured data, like scanned financial documents or X-ray images (DICOM), can be stored encrypted in Oracle SecureFiles.)

2. The TDE table keys used for column encryption are stored inside the database. The TDE tablespace keys are stored in the header of the operating system file(s) that contain the tablespaces. Both are encrypted with the Oracle Advanced Security TDE master encryption key that is stored externally, either in the Oracle Wallet or the SafeNet Luna SA HSM.

3. With a single command, the Oracle database security administrator interfaces with the external security module of choice to make the master encryption key available to the database.

4. When using the Oracle Wallet, the TDE master encryption key is loaded into database memory in order to decrypt table or tablespace keys. When using the HSM, table and tablespace keys are sent to the HSM and returned decrypted over a secure connection so they can be used to decrypt or encrypt data in the database.

5. Table and tablespace keys encrypt/decrypt data.



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

< Table of contents

Hardware Security Solutions for Microsoft SQL Server 2008

SOLUTION BRIEF

SafeNet Hardware Security Modules are the first to integrate with Microsoft SQL Server 2008 for robust key management and encryption, delivering unprecedented levels of data security, performance and compliance.

First HSM to work with Microsoft SQL Server 2008

SafeNet is the first HSM vendor to work with Microsoft SQL Server 2008, a relational database management system that provides organizations with a highly secure data platform for storing and managing sensitive data. Unlike its predecessor releases, Microsoft SQL Server 2008 enables the use of third-party HSM devices for storage of keys and cryptographic operations, such as key creation, deletion, encryption, and decryption for complying with security best practices and PCI DSS mandates.

Integration of SafeNet's Luna SA with Microsoft SQL Server 2008 allows storage of the server's master cryptographic keys—the foundation of any robust security solution—within the hardware and not the software, and provides greater application security and performance by offloading select key management functionality. The high-assurance Luna SA provides a verifiable audit trail as evidence that your keys have been properly secured throughout their entire life cycle.

In addition to the Luna SA, the SafeNet Luna PCI, a high-security cryptographic PCI accelerator card, can also be integrated with Microsoft SQL Server 2008. When embedded directly into the database server, the Luna PCI provides added security, as well as accelerated cryptographic performance and CPU offload.

How it Works

SQL Server 2008 introduced Extensible Key Management (EKM) for managing keys outside of SQL Server. Traditionally, all symmetric and asymmetric Keys used by SQL Server reside in the database itself, however EKM allows key creation, storage, encryption and decryption to be done outside the database using an HSM. To use this feature SafeNet (the EKM provider) wrote a module which implements certain interfaces that SQL Server uses for key management and cryptographic operations. Key creation and management DDL supports key creation using EKM providers.

Ease of Integration

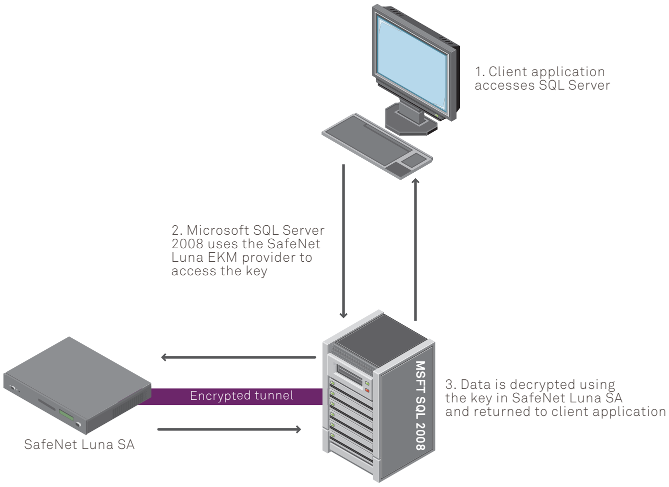
The SafeNet Luna SA and Luna PCI offer users of Microsoft SQL Server 2008 two flexible encryption options for their deployment scenarios. The Luna SA is a network-attached HSM that connects to the server through TCP/IP. It can be leveraged by many servers, offering the ability to securely partition and share the HSM resource, and is a cost-effective way of extending the data platform. The Luna PCI is a PCI-card form factor HSM that connects to the server in the PCI bus and provides seamless deployment to a wide range of security applications. Its full cryptographic application program interface support makes integration quick and easy.

Solution Benefits

- Increased security through separation of cryptographic keys from encrypted data
- Data can be encrypted by using keys that only the database user has access to on the external EKM/HSM
- Simple Windows-based installation of SafeNet Extensible Key Management feature
- Cost-effective extensibility of Microsoft platform
- Designed for HSM Best Practices
- Code Module Signing
- Transparent Data Encryption (TDE) support
- FIPS 140-2 Level 3 validated
- Enables users to meet PCI DSS standards
- PKI root key protection

> "SafeNet's Luna SA provides organizations using SQL Server 2008 additional security features to help meet today's ever-evolving data threats and compliance mandates. Organizations can add a layer of security technology that protects keys to be separate from the data it protects while accelerating complex features such as key rotation."
>
> ~ Mark Jewett
> Director of SQL Server Marketing,
> Microsoft

Integration with Microsoft applications is facilitated via the SafeNet Luna EKM, which is used to set up Extensible Key Management (EKM) for Microsoft SQL Server 2008. Initializing the SafeNet Luna EKM ensures all keys that are generated via SQL Server 2008 or transparent data encryption (TDE) will be stored on the SafeNet HSM. The Luna EKM Configuration Utility allows the flexibility to set parameters required by the EKM module, and thus specify a particular HSM and slot number. Data can be encrypted by using encryption keys that only the database user has access to on the external Luna EKM module.


1. Client application accesses SQL Server
2. Microsoft SQL Server 2008 uses the SafeNet Luna EKM provider to access the key
Encrypted tunnel
MSFT SQL 2008
3. Data is decrypted using the key in SafeNet Luna SA and returned to client application
SafeNet Luna SA

Enterprise Data Protection

SafeNet HSMs are a key component of SafeNet's comprehensive Enterprise Data Protection (EDP) solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet EDP is the only solution that secures data across the connected enterprise, from core to edge, providing protection of data at rest, data in transit, and data in use. Unlike disparate, multi-vendor point solutions that can create limited "islands" of security, SafeNet EDP provides an integrated security platform with centralized policy management and reporting for seamless, cost-efficient management of encrypted data across databases, applications, networks, and endpoint devices. For more information, visit www.safenet-inc.com/EDP.

Related Documents

Product Brief: SafeNet Luna SA

Product Brief: SafeNet Luna PCI

Press Release: SafeNet Offers First Hardware Security Module to Work with Microsoft SQL Server 2008

Solution Brief: SafeNet HSMs for Microsoft Certificate Services

Microsoft® GOLD CERTIFIED Partner

FIPS VALIDATED 140-2 inside

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

< Table of contents

DNSSEC

INTERNAL REFERENCE GUIDE

SafeNet Value

- Native DNSSEC HSM Toolkits
- FIPS 140-2 Level 3 and CC EAL 4+ Compliant
- Virtual HSM supports segregated domains
- High availability mode ensures uptime
- Support for the leading virtual platforms

Overview

DNSSEC, Domain Name Systems Security Extensions, is the process of signing DNS records to ensure that the messages received are the same as those that were sent.

DNS, on its own, has no real security. Cache poisoning, which occurs when a name server has cached data from a non-authoritative DNS server and continues to serve that incorrect/fraudulent data (website redirects), has created a need for security.

To ensure the validity of DNS services, DNSSEC deploys public key cryptography to digitally sign DNS messages. Robust protection of private signing keys is vital to the security of the DNSSEC system because if the keys and their corresponding digital certificates are compromised, the chain of trust in the DNS hierarchy is broken, rendering the security system obsolete.

Major DNS organizations have already implemented DNSSEC, and adoption is accelerating worldwide.

Customer Problem

- Cache poisoning
- DNS signing performance
- Industry compliance/regulations
  - RFCs NSEC (ex. RFC 5011)
  - NSEC3
  - ICANN mandates FIPS 4 for public DNS roots
- Integration of security
- Impersonation of website

	Security Threat
▶	Size of DNSSEC packets and ability for the system to handle large signing volumes. Since DNS updates are very frequent, need to ensure the performance is not slowed down.

HSM’s Role

Next Gen HSMs will have industry-leading ECC performance. This is a fit for smaller ECC-signed data footprints in the DNSSEC packet.

SafeNet Partners:

- VeriSign

Benefits Gained

- Size of signing footprint of ECDSA keys vs. RSA. Sizes for ECDSA keys gets increasingly smaller as a percentage of the equivalent cryptographic protection increases (i.e., ECC signing footprint is one-fifth the size, when comparing equivalent strengths (4096 RSA key, 384 ECC key)).
- Certicom compression would make the signature footprint even smaller
- Protection of the hosting service provider, as well as the incoming requestor or end user

Targets

Industries:	Solution Providers:
• Top level domain providers • Online bank and retail/payment providers • Forgotten password websites • SaaS providers • Cloud computing providers • DNSSEC key management and zone signing software providers • Banking • Retail • Large enterprise • Government • Education	**DNS ROOT Service Providers** • VeriSign • ICANN (recommending body) • U.S. government **Top Level Domain Providers** • VeriSign • Cogent Systems • ISC • Autonomica • RIPE NCC • U.S. DOD **DNSSEC key management and zone signing software providers** • Secure64 DNS Signer

SafeNet Customers:

- VeriSign
- SURFnet

Use Case

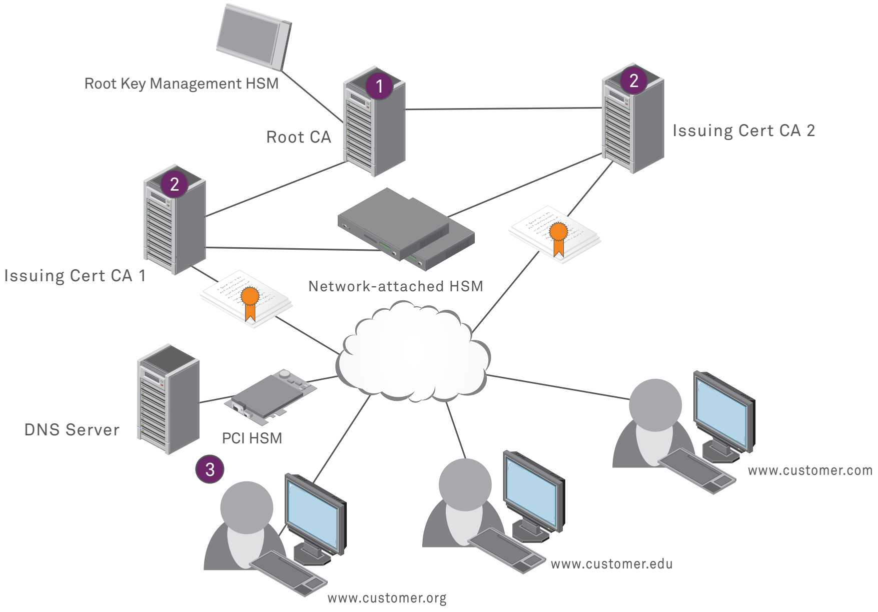
SURFnet, a subsidiary of the SURF organization, allows Dutch universities for applied sciences and research centers to collaborate nationally and internationally on innovative Information and Communication Technologies facilities. The SURFnet network is the national computer network for higher education and research in the Netherlands. SURFnet recognized the need to add a DNSSEC security solution that would allow them to restrict access to the SURFnet network to universities, academic hospitals and teaching hospitals, institutes for higher professional education, research institutes, corporate R & D departments, scientific libraries, and other organizations funded by the Ministry of Education, Culture and Sciences.

After evaluating a number of security vendors' solutions for DNSSEC, SURFnet selected SafeNet's HSMs for its standards-based DNSSEC solution backed by superior customer support. SafeNet HSMs were the right choice because they met PKCS standards and offered FIPS 140-2 Level 3 and Common Criteria EAL 4+ certified security.

Since deploying SafeNet HSMs, SURFnet has revamped its key management capabilities through key generation, distribution, rotation, storage, termination, and archival—keeping the private DNSSEC signing key and DNS server secure at all times. SafeNet HSMs also boosted SURFnet's cryptographic processing capabilities by offloading it from application servers and storing cryptographic keys in a centralized, hardened device, thereby eliminating the risks associated with having these assets housed on poorly secured platforms.

7/1/2010: NIST, ICANN, and Verisign announced plans to deploy DNSSEC at “root” zone

Production Deployment



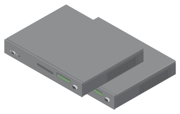
1 The root certificate authority (CA) secures the root key that signs the root certificate for the Domain hierarchy and the certificate for each Domain issuing CA

2 The issuing CA issues the certificates for each name server securely through a PCI HSM, if a single server environment, or a network-attached HSM in a network environment

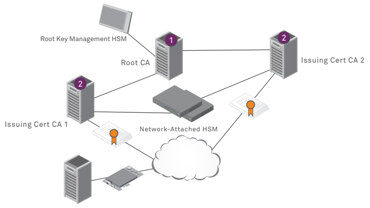
3 The DNS server digitally signs the DNS message with an HSM to ensure authenticity and integrity of all domain name users

Typical HSM Opportunities

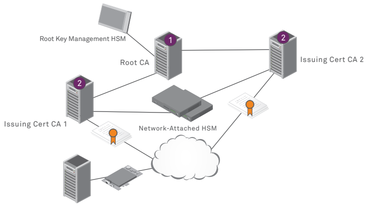
Production Deployment
Two HSMs



Development Deployment
One HSM



User Acceptance Test Deployment
Two HSMs



U.S. federal government mandated that all federal agencies must deploy DNSSEC so that it is operational on all applicable information systems by 12/1/2009

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

SafeNet

SafeNet HSMs for DNSSEC

SOLUTION BRIEF

Features and Benefits

- Two of the three biggest DNS providers trust SafeNet HSMs to protect and accelerate digital signatures for DNSSEC
- Combines strongest cryptographic security with highest performance and availability
- Broadest array of HSMs for any DNSSEC requirement
- Easy to integrate with well documented API's, including PKCS#11, Java, MS CAPI
- Supports DNSSEC and OpenDNSSEC
- World-class support and documentation
- Most worldwide HSM deployments for PKI

For root, top level domain, and enterprise level DNS hierarchies, SafeNet HSMs combine the strongest cryptographic security with the highest performance, reliability, and ease of integration for rapid and affordable DNSSEC implementation.

Security Issues with DNS

At the pinnacle of the Domain Name System (DNS) hierarchy, server clusters carry the DNS root zone data. Web applications, like eCommerce, SaaS, social networking, and even email, rely on DNS. Unfortunately, the DNS contains unsecured and vulnerable cashing name servers that are easy targets for hackers to hijack Web traffic containing sensitive data. With cache poisoning, an attacker inserts a fake address record into a DNS caching server. The caching server stores the fake record, thus "poisoning" the cache unbeknownst to users who think they are dealing with a legitimate site. This vulnerability has spawned an immediate need for security, as security researcher Dan Kaminsky brought to worldwide attention in the summer of 2008.

Why DNSSEC is the Answer

The solution recommended by the DNS developer community is Domain Name System Security Extensions (DNSSEC), which uses digital signatures and public key cryptography to allow Web servers to verify their website domain names and corresponding IP addresses. DNS root zones are in urgent need of being digitally signed as delay is detrimental to the ongoing integrity of the Internet, eCommerce, and Web applications. Signing the zones would, in effect, configure the caching name servers to become security aware. DNSSEC is viewed as the best way to bolster the DNS against vulnerabilities, such as cache poisoning attacks. In fact, security researcher Dan Kaminsky recommends widespread deployment of DNSSEC. The world is paying attention and DNSSEC has been deployed on top-level domains operated by Sweden, Puerto Rico, Bulgaria, Brazil, Portugal, Thailand, Namibia, and the Czech Republic, to name a few.

Key Management for DNSSEC

SafeNet hardware security modules (HSMs) meet the demanding requirements for robust security and availability required to ensure integrity of the domain name space. Like any other security model relying on public key cryptography, it is imperative that private DNSSEC signing keys are kept secure. By definition, the public key can be made widely available; it does not need to be secured. However, if the private key is compromised, a rogue DNS server can masquerade as the real authoritative server for a signed zone. This is where hardware security modules (HSMs) come into play.

HSMs are dedicated systems that physically and logically secure the cryptographic keys and cryptographic processing that are at the heart of digital signatures. HSMs secure the DNS server so the generation of keys, the storing of the private key, and the signing of zones is performed on a DNS server that is physically secure and whose access is restricted to essential personnel only. HSMs also allow the secure storage of a backup private key copy in a centralized, hardened device.

SafeNet HSMs: A Case for Higher Expectations

SafeNet HSMs have been trusted for more than twenty years to protect more digital identities than any other hardware security module in the world. Following are several reasons why banks, retailers, large enterprises, government agencies, and educational institutions are choosing SafeNet:

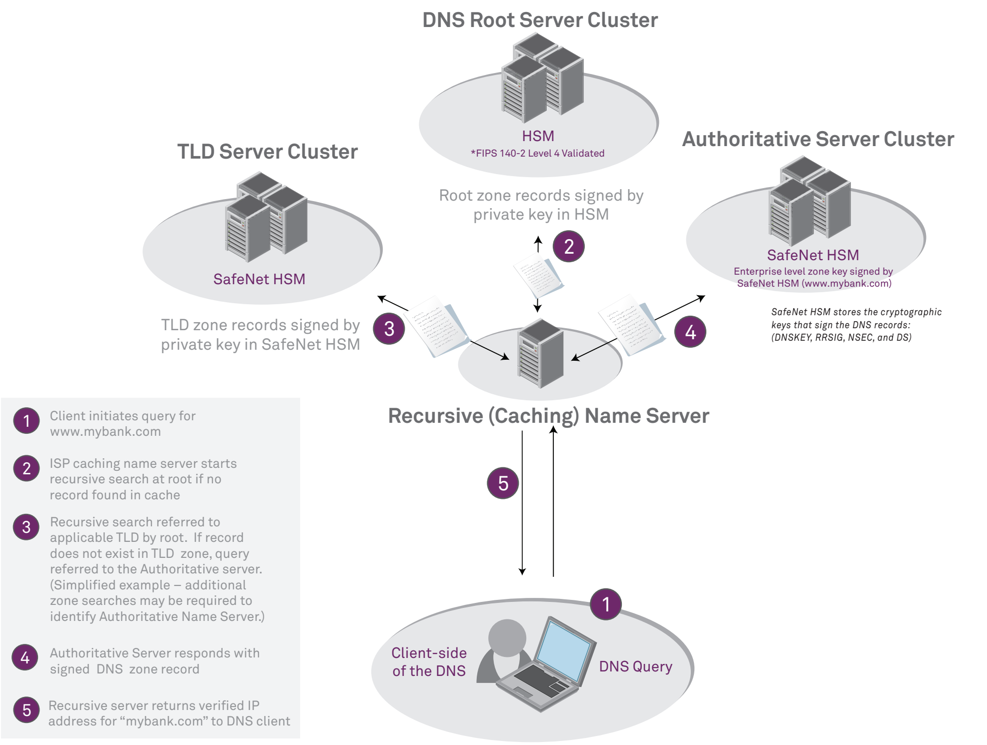
- SafeNet HSMs integrate with the leading DNS platforms, including OpenDNSSEC, BIND, FreeBSD, and Linux
- SafeNet HSMs provide trusted key security used to sign DNS packets and create a secure DNS infrastructure with high-performance solutions, up to 7,000 operations per second, for both Zone Signing Key (ZSK) and Key Signing Key (KSK) scenarios
- SafeNet HSMs feature local and remote key management control for flexibility and ECC key limit size constraints for reduced crypto footprint, allowing for a smaller impact on the DNS packet
- SafeNet HSMs are easy to integrate into any security environment with well-documented APIs, such as PKCS#11, OpenSSL, Java, and MS CAPI, as well as central management consoles for easy and rapid setup
- All digital signing and verification operations are performed within the HSM to deliver the highest levels of performance, availability, and security to ensure business processes and systems are running efficiently
- Stored on hardened and FIPS 140-2 Level 3 and Common Criteria EAL 4+ certified cryptographic modules, cryptographic keys never leave the confines of the HSM
- SafeNet HSMs are available in different form factors and performance classes to meet the unique design goals of any cryptographic key deployment - from PCI cards embedded in the server to highly scalable network-attached appliances that can be transparently shared by multiple servers

In addition SafeNet HSMs support key rollover functions, since DNSSEC keys do not have a permanent lifetime. The chances a key will be compromised, whether through accident, espionage, or cryptanalysis, increase the longer the key is used. Key rollover is the process by which a key is replaced with a new key and associated signatures are updated.

Implementing DNSSEC with Scalability & Robust Processing

A phased approach is recommended when deploying DNSSEC in your organization. Depending on the complexity of your environment, you might want to limit the initial deployment to a small number of domains before you deploy DNSSEC broadly. When responding to queries, the DNS server will respond with additional DNSSEC resource records. This will increase the number of packets on the network and can decrease the maximum query throughput of the DNS server. A DNS server that is performing validation of DNSSEC data can experience an increase in CPU usage. Configuring an HSM to the DNS server ensures that the server has sufficient processing capabilities. SafeNet HSMs can scale to meet the phased approach, but also keep up with the large number of incoming requests for domain name resolution in large zones, and can scale to thousands of signing operations per second.

A Recursive Query Being Secured Using SafeNet HSMs for DNSSEC


DNS Root Server Cluster
HSM
*FIPS 140-2 Level 4 Validated
Root zone records signed by private key in HSM
2
TLD Server Cluster
SafeNet HSM
TLD zone records signed by private key in SafeNet HSM
3
Authoritative Server Cluster
SafeNet HSM
Enterprise level zone key signed by SafeNet HSM (www.mybank.com)
4
Recursive (Caching) Name Server
5
1
Client-side of the DNS
DNS Query

SafeNet HSM stores the cryptographic keys that sign the DNS records: (DNSKEY, RRSIG, NSEC, and DS)

1 Client initiates query for www.mybank.com

2 ISP caching name server starts recursive search at root if no record found in cache

3 Recursive search referred to applicable TLD by root. If record does not exist in TLD zone, query referred to the Authoritative server. (Simplified example – additional zone searches may be required to identify Authoritative Name Server.)

4 Authoritative Server responds with signed DNS zone record

5 Recursive server returns verified IP address for “mybank.com” to DNS client

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

SURFnet Selects SafeNet HSMs to Secure DNSSEC Material

CASE STUDY

Business Challenges

- Find a DNSSEC solution that was standards-based and scalable for a phased install approach
- Securely store cryptographic keys without compromise
- Keep customer data safe from insider and hacker intrusion
- Find a dynamic and secure back-up system

SURFnet enables groundbreaking education and research—designing and operating the hybrid SURFnet6 network and providing innovative services in the field of trusted identities and electronic collaboration for institutions like universities, hospitals, research institutes, corporate research bodies, and libraries.

SafeNet HSMs Safeguard Thousands of DNS Zones for National Computer Network in the Netherlands

SURFnet enables groundbreaking education and research—designing and operating the hybrid SURFnet network, as well as providing innovative services in the field of trusted identities and electronic collaboration.

The SURFnet network is the national computer network for higher education and research in the Netherlands. Connecting to the SURFnet network is restricted to the following organizations:

- Universities
- Academic hospitals and teaching hospitals
- Institutes for higher professional education
- Research institutes
- Corporate R & D departments
- Libraries
- Other organizations funded by the Ministry of Education, Culture and Sciences

Business Challenge

Because SURFnet is a provider of network support for a large constituency of organizations, including universities, hospitals, research institutes, corporate research bodies, and scientific libraries, they needed to safeguard private key material used in DNS Security Extensions (DNSSEC).

With such large amounts of information in play for SURFnet's network and its large constituency, its network has opened itself up to standard DNS security flaws, where unsecured and vulnerable caching name servers are easy targets for hackers to hijack Web traffic containing sensitive data. SURFnet recognized the need to add DNSSEC to its repertoire to protect their network from many vulnerabilities, including cache poisoning, man-in-the-middle attacks, rerouting of e-mails, and denial-of-service attacks.

As a provider of a massive network of respected bodies and institutions in the Netherlands, SURFnet needed a DNS security solution that was:

- Compatible with OpenDNSSEC, an Open Source software that manages security for DNS.
- Compliant with the PKCS#11 standard, which calls for a platform-independent API to the HSM.
- Supported by world-class customer support.
- Provided by a reliable and reputable security provider.

> “SafeNet met the requirements for the robust security and availability needed to ensure integrity of the domain name space and matched our performance needs, which are based on our large number of supported network organizations across the Netherlands. SafeNet HSMs gave us the much-needed ability to back up data securely and quickly, as well as manage security keys to maintain their integrity.”
>
> Roland van Rijswijk
> SURFnet

Solution

SURFnet evaluated a number of security vendors’ solutions for DNSSEC and chose SafeNet’s HSMs for its standards-based DNSSEC solution.

After testing their DNSSEC options, SURFnet found SafeNet HSMs to:

- Secure digital signatures in order to ensure the validity of response to queries through every zone in the DNS hierarchy and establish the chain of trust.
- Control access so only authorized customers and internal staff can access sensitive applications and data.
- Scale to accommodate high-volume processing.
- Have secure backup features.
- Store all key material in hardware ensuring integrity and protection of all hardware keys.
- Provide standardized PKCS#11 support for application integration to the SafeNet HSMs.
- Be supported by superior customer service.

SURFnet will initially deploy DNSSEC for its own domain to pioneer the technology on its network. It will then deploy the technology for its large constituency, leveraging the scalability offered by SafeNet’s HSMs. SURFnet will operate the SafeNet HSMs in high-availability mode to ensure maximum redundancy for this critical infrastructure.

“SafeNet has proven to be an elite security vendor for our DNSSEC rollout. The SafeNet HSMs were scalable, easy to deploy, and let us install security through a phased approach, thus allowing for maintenance of ongoing network viability,” said Roland van Rijswijk, SURFnet. “The compliance to PKCS standards, as well as its FIPS 140-2 Level 3 and Common Criteria EAL 4+ certifications, combined with its compatibility to OpenDNSSEC, has shown our constituents that we are serious about protecting the vulnerabilities in DNS technology.”

Benefits

Since deploying SafeNet HSMs, SURFnet has revamped its key management capabilities through key generation, distribution, rotation, storage, termination, and archival—keeping the private DNSSEC signing key and DNS server secure at all time. SafeNet HSMs also boosted SURFnet’s cryptographic processing capabilities, by offloading it from application servers and storing cryptographic keys in a centralized, hardened device, thereby eliminating the risks associated with having these assets housed on poorly secured platforms. Using SafeNet HSMs has also allowed SURFnet to significantly streamline security administration.

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

< Table of contents

eDocuments

INTERNAL REFERENCE GUIDE

SafeNet Value

SafeNet Hardware Security Modules form a single auditable point of trust in eDocument deployments. In addition, SafeNet HSMs support the leading virtual platforms including Microsoft Hyper-V, Citrix XenServer, and VMware vSphere.

Types of eDocument Processes

- Invoicing
- Procurement
- Notary
- Mortgage
- Contracts

Overview

eDocuments are a type of paper-to-digital initiative, often including a digital signature. Digital signatures are required by some localities and are the preferred choice in others because they offer stronger security attributes.

eDocumentation involves the process of moving from paper bases systems, towards digitized invoice imagery, tracking, management based, and storage. When coupled with a digital signature, it offers robust security, non-repudiation, and trust between parties.

Gaining momentum worldwide, the highest rates of adoption and focus have been in Europe, followed closely by Latin American countries.

Customer Problem

- Meet Regulatory Mandate/Directives:
    - EU VAT directive (Value Add Tax)
    - Brazilian Nota Fiscal (NF-e)
    - Ordinance of the Federal Department of Finance on Electronic Data and Information (OEIDI)
    - Others
- Improve efficiencies for invoice processing, storage, and retrieval
- WW environmental "green" concerns
- Eliminate the cost of paper documents
- Reduce the cost and complexity of long-term storage of large amounts of paper-based documents

	Technical/Security Problem
▶	Establish trust as the invoice moves between parties
▶	Determine how to move the invoice to a digital format in a secure and timely manner
▶	Ensure the integrity of invoice content
▶	Provide non-repudiation of receipt and origin
▶	Secure electronic tracking, storage, and management
▶	Adequate performance requirement for signing/verifying large quantities of incoming invoices, as well as invoices retrieved from storage

SafeNet Partners:

- 4Point
- Azurian
- Certisign
- Complus
- Datasoft
- GlobalSign
- Identiga
- Mier Borda
- Netco
- Netsec

SafeNet Customers:

- Petrobras - Luna SAs (3)
- Acos Villares - PSEs (2)
- Oi - PSEs (3)
- Brasil Telecom - Luna SAs (3)
- Yamaha - PSEs (3)
- Allergan - PSGs (2)
- Antwerp Port Authority
- NF-e Brazil

HSM's Role

The key is to establish trust in the eDocument between all parties, ensuring that it remains unaltered throughout the document life cycle:

At the point of entry → By the digital processing → During the storage period → At the time of retrieval

SafeNet HSMs are the cornerstone for establishing this trust-safeguarding the cryptographic keys that will sign/verify the documents, providing security in the digital process, and ensuring trust across all parties.

Our high-performance SafeNet HSMs are the high security ENGINES that can meet the potentially large transaction volume requirements with real-time capabilities and high availability, expediting processes.

Benefits Gained

- Reduced cost of handling invoices
- Improved relationships with suppliers because the approval and payment cycle can be significantly reduced
- Increased productivity through seamless integration with back office systems
- Reduced storage space requirements and elimination of manual filing of paper invoices
- Reduced errors resulting in reduced reconciliation time
- Efficient retrieval of invoice records
- Meet regulatory mandates
- Adaptable solution for addressing future requirements
- Digital signature allows for multiple signatures per eInvoice

Targets

Industries:	Solution Providers:
• Retailers • Government • Postal organizations • Scanning and invoice management providers • Archive service providers • Electronic marketplaces • Banks and their service centers • Third-party billing services	• b_process • Logica • EDB • Anochron • Progrator • Tieto • Medidata • BBS • SETTCE

Use Case

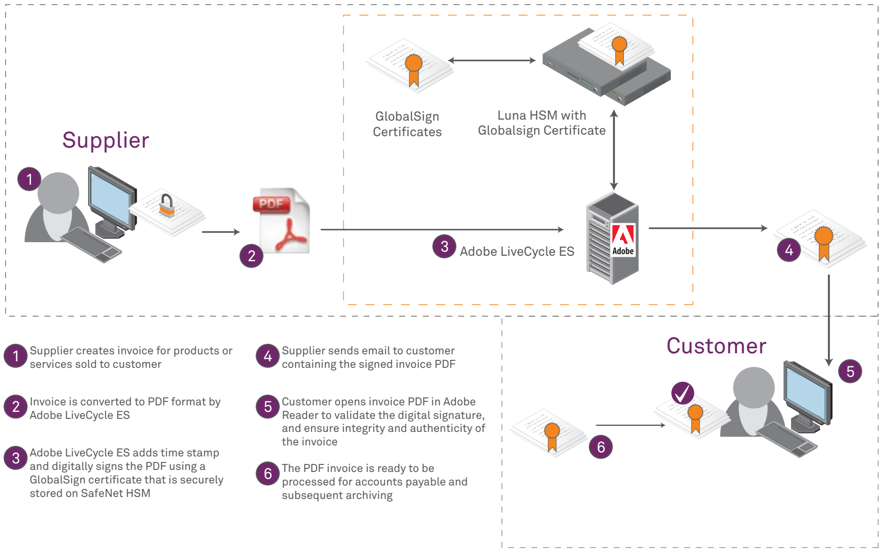
In order to comply with the VAT law, the Antwerp Port Authority implemented an advanced e-invoice solution based on digital signatures. The port authority leveraged its investment in Adobe's LiveCycle Enterprise Suite (ES) and GlobalSign's DocumentSign digital certificates by selecting an HSM that offered easy integration with these applications.

After Adobe LiveCycle ES converts an invoice into a PDF/A (Archive)-compliant document, digital signatures are applied using a digital certificate to ensure the authenticity and integrity of the PDF. The PDF invoices 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 lifecycle.

The HSM enables the organization to secure digitally-certified invoices and to cryptographically bind the identity of the certifying party to the invoice. The Adobe PDF Reader automatically verifies all of the embedded information, and visually highlights the authenticity and integrity of the document, allowing the recipient to easily detect whether the document has been altered after being certified. By applying digital signature and encryption technologies within a PKI network environment, the firm quickly brought digital invoicing processes online, thereby streamlining workflow, lowering costs, and meeting mandatory European directives for compliance.

Danish Public Authority saved $120 million Euros per year by accepting only digital eInvoices

Production Deployment



1 Supplier creates invoice for products or services sold to customer

2 Invoice is converted to PDF format by Adobe LiveCycle ES

3 Adobe LiveCycle ES adds time stamp and digitally signs the PDF using a GlobalSign certificate that is securely stored on SafeNet HSM

4 Supplier sends email to customer containing the signed invoice PDF

5 Customer opens invoice PDF in Adobe Reader to validate the digital signature, and ensure integrity and authenticity of the invoice

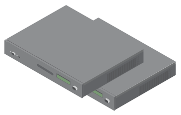
6 The PDF invoice is ready to be processed for accounts payable and subsequent archiving

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

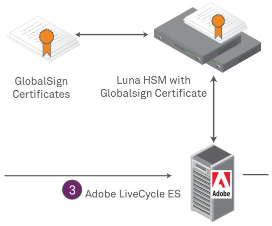
Typical HSM Opportunities

Production Deployment
Two HSMs

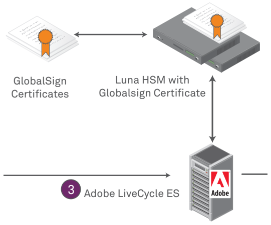


Product Units & Disaster Recovery/Business Continuity

Development Deployment
One HSM



User Acceptance Test Deployment
Two HSMs



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

SafeNet HSMs for eInvoicing

SOLUTION BRIEF

Features and Benefits

- Ensures integrity of electronic documents
- Provides non-repudiation of receipt and origin
- Secures electronic tracking and storage
- Scales to accommodate high volumes of important documents
- FIPS validated and Common Criteria certified

Powering eInvoicing systems with industry-compliant hardware security modules for maximum integrity, accuracy, and security

Overview

Trust is a critical requirement for the feasibility of eDocuments. Digital signatures, powered by encryption and public key infrastructure (PKI), represent the means for establishing trust in eDocuments. Digital signatures give all parties the confidence required to trust that documents 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 eDocument infrastructure will be compromised. This is where hardware security modules (HSMs) come into play.

The Role of HSMs in eDocuments

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:

- Lifecycle 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

eDocuments 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 lifecycle. The HSM enables the organization to secure digitally certified documents and to cryptographically bind the identity of the certifying party to the documents. 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 Benefits of eDocuments with SafeNet HSMs

SafeNet offers a broad set of HSMs that are ideally suited to the demands of eDocument 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 eDocuments implementations, ensuring optimal trust in the entire document lifecycle. SafeNet HSMs address the following critical requirements:

Certification. Many SafeNet HSMs meet the demanding requirements of FIPS and Common Criteria certification.

The Benefits of eDocuments with SafeNet HSMs

Enhance Security and Ensure Compliance

- Certification
- Compliance
- Multiple signatures

Optimize Operational Performance

- Efficient retrieval, processing
- Elimination of time-consuming, inefficient paper-based processes
- Improve vendor relations
- Reduced errors and reconciliation times
- Efficiency through back office integration

Reduce Cost

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.

Optimize Operational Performance

By leveraging SafeNet's secure HSMs in a secure eDocument 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 important documents.

Elimination of tiime-consuming, inefficient paper-based processes. Secure eDocument systems enable businesses to eliminate a host of manual, error-prone processes associated with the handling and distribution of paper documents.

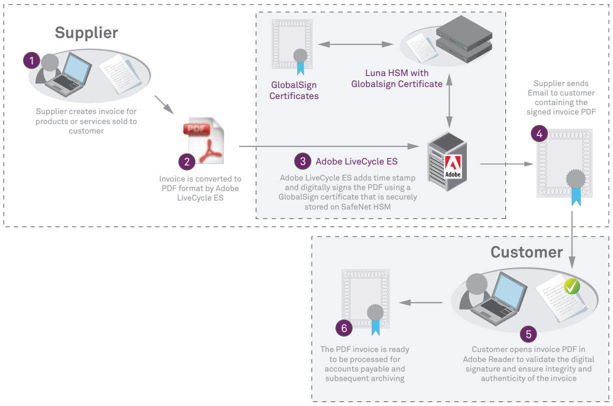
Improve relations. By ensuring trust and optimizing speed and efficiency throughout the document process, businesses can improve relationships with vendors customers, partners and other stakeholders.

Reduced errors, reconciliation times. With eInvoicing, businesses can improve accuracy in document 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 speedy payment cycles.

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

Reduce Cost

With SafeNet powering eDocument 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 documents, businesses can reduce the overhead and expense of paper document storage. Finally, the digitization of documents leads to significant reductions in the time and staffing costs associated with paper-based document processing.


Supplier
1
Supplier creates invoice for products or services sold to customer
PDF
2
Invoice is converted to PDF format by Adobe LiveCycle ES
GlobalSign Certificates
Luna HSM with Globalsign Certificate
3 Adobe LiveCycle ES
Adobe LiveCycle ES adds time stamp and digitally signs the PDF using a GlobalSign certificate that is securely stored on SafeNet HSM
Adobe
Supplier sends Email to customer containing the signed invoice PDF
4
Customer
5
Customer opens invoice PDF in Adobe Reader to validate the digital signature and ensure integrity and authenticity of the invoice
6
The PDF invoice is ready to be processed for accounts payable and subsequent archiving

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

Antwerp Port Authority Selects SafeNet

CASE STUDY

Customer Profile

- Antwerp Port Authority manages the 4th largest port in the world, including docks, berths, locks, and bridges.

Business Challenges

- Establish and maintain a secure and trusted e-invoicing solution
- Protect electronic invoices from being altered in transit
- Comply with European legislative mandates
- Integrate with existing technology partners

Solution

- Electronic invoice solution based on digital signatures that ensures authenticity and integrity of invoices
- SafeNet Luna SA HSM for secure storage of signatures and cryptographic keys
- Adobe LiveCycle Enterprise Suite
- GlobalSign Certified Document Services (CDS)

Secure Electronic Invoicing Solution

Business 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. Authenticity of origin ensures that the message content was actually created by the person or legal entity that signed it, while integrity assures that no changes have been made to the content of the invoice during transit.

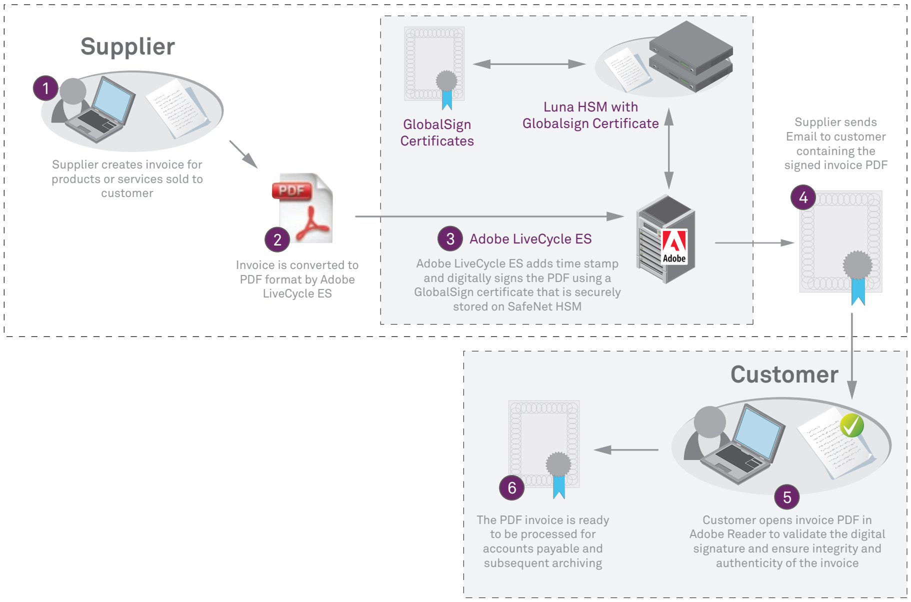
Solution

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.

After Adobe LiveCycle ES converts an invoice into a PDF/A (Archive)-compliant document, digital signatures are applied using a digital certificate to ensure the authenticity and integrity of the PDF. A secure, embedded time stamp locks down the exact time of signature creation, which meets a key VAT requirement for archival and storage. The Certified Document Service (CDS) digital certificates are provided by GlobalSign, a trusted Certificate Authority that delivers high-assurance digital identities to organizations and users worldwide.

The PDF invoices are digitally signed with a secure private signing key, which requires a cryptographic hardware security module (HSM) capable of performing certificate authority management tasks. The SafeNet Luna SA HSM stores the keys within the secure confines of the appliance throughout the key lifecycle. The integrity of both cryptographic keys and digital certificates is vital to the integrity of the overall security system—if the keys or digital certificates are compromised, the entire system is rendered obsolete. The SafeNet solution allows Antwerp Port Authority to secure digitally-certified invoices and to cryptographically bind the identity of the certifying party to the invoice. The Adobe PDF Reader automatically verifies all of the embedded information and visually highlights the authenticity and integrity of the document, allowing the recipient to easily detect whether the document has been altered after being certified.

> “We need a reliable partner to generate added value for our business and for our customers. SafeNet, with its security expertise and leading technology, is the best choice to ensure the authenticity of our invoices and bring peace of mind to us and all our customers.”
>
> -Jan Goosens
> Manager Software Development
> Antwerp Port Authority


Supplier
1
Supplier creates invoice for products or services sold to customer
PDF
2
Invoice is converted to PDF format by Adobe LiveCycle ES
GlobalSign Certificates
Luna HSM with Globalsign Certificate
3 Adobe LiveCycle ES
Adobe LiveCycle ES adds time stamp and digitally signs the PDF using a GlobalSign certificate that is securely stored on SafeNet HSM
Adobe
Supplier sends Email to customer containing the signed invoice PDF
4
Customer
6
The PDF invoice is ready to be processed for accounts payable and subsequent archiving
5
Customer opens invoice PDF in Adobe Reader to validate the digital signature and ensure integrity and authenticity of the invoice

Applying Security to the Automated PDF Work Flow for E-invoicing and E-archiving

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. All parties recognize the need to reduce their carbon footprint throughout the supply chain, as well as leverage the financial savings to reduce billing costs. By applying digital signature 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. For the party relying on the e-invoice, the secure Adobe PDF Reader allows for easy validating, processing, and archiving. Viewing and validating the e-invoices is also automated thanks to the out-of-the-box integrated trust solution between Adobe Reader and the Adobe Certified Document Services platform.

About Antwerp Port Authority

The Antwerp Port Authority manages Europe’s second biggest port, which offers an ideal gateway to Europe. More than 200 forwarding companies based in Antwerp help to secure shipping contracts across multiple market sectors, including steel, fruit, coffee, and tobacco. Numerous companies handle more than 16,000 seagoing ships and 65,000 barges that call at the port annually.

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

< Table of contents

Secure Credential Delivery

INTERNAL REFERENCE GUIDE

SafeNet Value

SafeNet's award-winning ViewPIN+ is the only secure Web-based PIN issuance and management solution that delivers unprecedented customer satisfaction and proven cost savings by eliminating expensive, less secure, and time-consuming paper-based authentication delivery to customers.

Overview

The Personal Identification Number (PIN) has existed since the invention of the Automated Teller Machine (ATM) in 1967 as a means to authenticate customers and authorize transactions, such as cash withdrawals, retail purchases, and account transactions. Until today, organizations involved in PIN issuance, (banks, retailers, universities, suppliers, etc.) have not found an easy and cost-effective way to securely deliver PINs to account holders. Most methods involve PIN mailers, which introduce waiting periods, mail house processing and postage costs, and risk factors inherent to paper-based processes.

Customer Problem

- Higher cost of operations
- Insecurity of authentication credential delivery
- Latency of authentication credential delivery system

Security Threat

▶ Existing protocols like SSL protect critical user data on public networks. However, once user data reaches a Web server, it is available in clear text, hence a variety of insider and external attacks are still possible. The solution is to devise a mechanism, such as ViewPIN+, that ensures that all critical user data remains encrypted all the time, until it enters a physically and logically secure HSM.

HSM's Role

With its hardware-based application security module, SafeNet ViewPIN+ offers hardware-based key management, and ensures that cryptographic keys and processes are, at all times, stored and managed exclusively within FIPS-validated hardware. Code signing, time stamping, and verification maintain the integrity of the Java application code and prevent unauthorized application execution. Additionally, strictly enforced access and usage policies prevent unauthorized access to sensitive applications or data.

Benefits Gained

- Massive cost savings compared to paper mailers
- Reduced security risks compared to paper mailers
- Faster PIN delivery. Cardholders begin using their card sooner, enabling greater bank revenue
- Increased customer satisfaction
- Significant "green" environmental benefits in moving from paper to digital

> "The SafeNet ViewPIN+ solution has helped us reduce our overhead costs significantly, as well as provide our customers with the convenience and security they not only expect, but deserve."
>
> ~ Lead Security Architect for Egg plc

SafeNet Partners:

- Gemalto

Targets

Industries:

- Postal organizations
- Scanning and invoice management providers
- Archive service providers
- Electronic marketplaces
- Banks and their service centers
- Third-party billing services

Solution Providers:

DNS ROOT Service Providers

- VeriSign
- ICANN (recommending body)
- U.S. Government

Top Level Domain Providers:

- VeriSign
- ISC
- RIPE NCC
- Cogent Systems
- Autonomica
- U.S. DOD

Use Case

In order to guard against forgery, many manufacturers are relying on HSMs to protect their intellectual property, such as chips, hard drives, printer components, among other, as well as protect against lost revenue. One such manufacturer wanted to protect their phones from snooping, identity forgery, and other forms of network abuse that plague the cellular phone and satellite television industries. An IP phone manufacturer needed to integrate secure identification and authentication into its devices. The business needed to integrate the issuance of digital identities and authentication into its manufacturing processes, which meant the organization would need to securely and cost-effectively create thousands of industry-compliant digital identities.

The IP telephone manufacturer selected Microsoft Certificate Services software for managing the issuance of the digital identities, but needed a hardware solution to deliver maximum security and performance. A highly secure hardware system was required to protect the certificate issuance root key—the basis of trust for all of the IDs issued to the phones—and prevent the possibility of a copy of that key being used to create illegitimate device identities. The solution also had to meet high performance standards to ensure that the computationally-intensive certificate issuance process did not create bottlenecks in the manufacturing process.

SafeNet Customers:

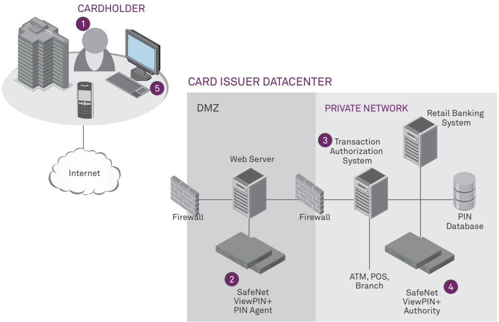
- Citi/Egg Bank

The manufacturer selected an HSM as the foundation for their digital identity issuance system for IP telephones. Their selected HSM held both FIPS 140-2 and Common Criteria certification. With each IP telephone containing a unique, trusted digital identity, users can be sure that the IP telephone they are connecting with is definitely the telephone it claims to be. This IP telephone manufacturer's use of HSMs demonstrates how high-volume, high-speed digital ID issuance can be seamlessly integrated into the manufacturing process without sacrificing security.

> "ViewPIN+ is a perfect example of how we strive to make banking secure and convenient for our customers. We are constantly seeking to adapt our products and services such that they fit in with their modern lifestyles."
>
> ~Head of Architecture and Innovation for Citi's UK Consumer Business

Production Deployment

1. Using a browser (PC or mobile device), the user authenticates to an application server and then supplies unique identifying credentials, which are sent to the ViewPIN PIN Agent.
2. PIN Agent generates a symmetric key. This key is used to encrypt the credentials that were sent to PIN Agent. This key is then wrapped using the wrapping certificate of PIN Authority. All this information is then timestamped and signed using the signing key of the PIN Agent.
3. PIN Agent redirects the user to an application on the private network web server, along with the encrypted session key.
4. The flow is as follows:
   1. PIN Authority first un-wraps the symmetric session key.
   2. PIN Authority then verifies the signed, and time stamped information submitted by the PIN Agent using the signing key certificate of the PIN Agent.
   3. Once verified, the PIN Authority decrypts the user credentials and then time stamps, signs, and encrypts the user authentication credential information, returns it to the private network web server, and back to the PIN Agent.
5. PIN Agent then validates the digital signature and time stamp of the encrypted user credential information and sends it to the user's web browser.



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

ViewPIN+ Revolutionizing Web-based PIN Issuance and Management

PRODUCT BRIEF

Benefits

- Safe, fast, easy, and cost-effective PIN issuance
- Winner-2008 Network Product Guide Best in Security Solution Finance
- Highest security available
- Increases customer satisfaction
- Increases competitive advantage
- Increases profitability
- Environmentally responsible
- Easy to integrate and deploy

PINs are just a click away with ViewPIN+. For banks, credit card issuers, telecom operators, and retailers with membership/PIN cards, SafeNet's award-winning ViewPIN+ is the only secure Web-based PIN issuance and management solution that delivers unprecedented customer satisfaction and proven cost savings by eliminating expensive, insecure, and time-consuming paper-based PIN delivery to customers.

Highest Security Available

Paper-based mailers are easy to intercept by fraudsters, while voiced-based systems cannot be effectively secured. Traditional SSL-secured websites are also not entirely secure because they require encrypted data to be decrypted at the Web server as part of the delivery process. A key advantage of ViewPIN+ is that it overcomes this vulnerability by establishing a secure end-to-end encrypted tunnel between the cardholder and the card issuer.

This best-of-breed solution includes SafeNet HSM Luna SP – a FIPS 140-2 Level 3-validated hardware security module (HSM) that provides an integrated, secure application environment, including hardware key management, at the customer's site/data center/back end. Cryptographic keys and processes are stored and managed exclusively within FIPS-validated hardware at all times, protecting against physical, logical, and operational threats. In addition, code signing and verification maintain the integrity of the ViewPIN+ Java application code, which is only executed within the confines of the appliance to prevent unauthorized application execution. To further enhance security, ViewPIN+ maintains a separation between the cardholder identity and the PIN to protect against compromise - the two are never linked.

Increased Customer Satisfaction

ViewPIN+ is easy to use and provides instant results for the end user through an intuitive Web interface for self-service PIN issuance and management - convenient and instantaneous. By comparison, delivery of PINs by mail is slow, resulting in a waiting period, during which a cardholder could use a competitor's card.

Increased Profitability

ViewPIN+ reduces operational costs, increases revenue, and saves resources for banks, credit card companies, and retail program membership card issuers. The first ViewPIN+ customer was U.K.-based financial services provider Egg Banking, plc, a Citigroup company, and the world's largest online bank. Using ViewPIN+, Egg eliminated paper-based PIN issuance, saving thousands of resource hours and upwards of $5 million dollars in expenses the first year alone.

Technical Specifications

Performance and Scalability

- Services up to 2 million PIN requests per day
- Supports load balancing
- Running on fastest HSMs in the market

Physical characteristics

- 1U

Platform

- SafeNet Luna SP

Transport

- Hardware-secured accelerated SSL
- Any browser that supports Javascript 1.1 or higher
- IE, Firefox, Safari, Opera, iPhone

Compliance

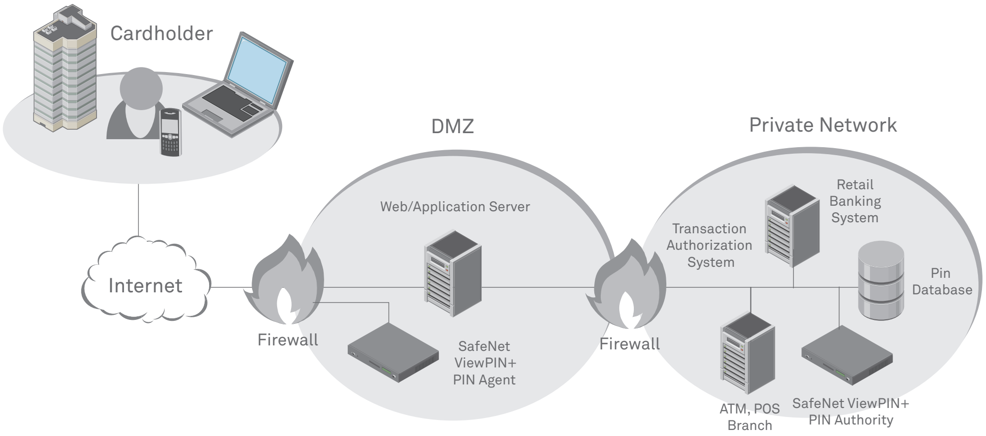
- FIPS 140-2 Level 3
- APACS guidelines
- RoHS
- ISO 9002 certification

Network Connectivity

- 2x10/100 Ethernet

Secure Integration & Administration

- Secure remote administration
- Hardware-secured RSA and 3DES/AES crypto keys
- Strongest cryptographic algorithm



Easy to Deploy

ViewPIN+ integrates into the bank's existing website and user authentication system without any requirement for applets or browser plug-ins on the client side. The browser requirements are basic and standards-based, making ViewPIN+ available from any browser, including on mobile devices.

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

Egg Bank Eliminates Costs and Expedites PIN Issuance with SafeNet Solution

CASE STUDY

Solution & Benefits

- SafeNet ViewPIN+ Web-based PIN management platform for secure PIN issuance
- Secure PIN issuance solutions reduce credit card fraud from stolen PIN mailers, improve customer satisfaction, and lower operational costs significantly

Business Challenges

- Issuance of PINs efficiently, securely, and in a manner that improves the overall customer experience
- Needed a way to allow customers to securely obtain PINs over the Internet

The world's largest online bank securely issues PINs online to save money, reduce fraud, and improve the customer experience with SafeNet's award-winning ViewPIN+ Web-based PIN management platform.

Customer Profile

Egg, the UK's leading online bank and a member of Citi, became the U.K.'s first Internet-only bank in 1998. Today, it is the world's largest online bank with 3.2 million customers. Egg is a savvy, agile organization that leverages the Internet in innovative ways to improve both efficiency and customer experience.

Business Challenge

Personal Identification Numbers (PINs) are increasingly used to authenticate customers and authorize credit card transactions, such as ATM withdrawals or retail purchases. Before the introduction of ViewPIN+, Egg used to issue millions of new PIN mailer letters through the postal service. In addition, every time a customer forgot a PIN, another letter was mailed. In short, sending PINs through the traditional mail delivery channel was very costly, time consuming, and highly insecure. Egg was looking for a better solution.

Egg wanted their customers to experience the best service possible by being able to use their cards immediately after receiving them, rather than having to wait seven to ten days for their PIN to follow by mail. Egg also wanted to lower the risk of fraud that typically occurs when PIN mailer letters are intercepted en route to customers, as well as decrease the costs associated with providing up to three million new PINs a year. Leveraging the Internet seemed like an obvious solution for this online bank. However, allowing customers to retrieve their PINs via the Internet seemed dangerous, even to some of the company's own security experts.

In 2006, Egg began a search for a highly secure, automated, and convenient method of delivering PINs to customers over the Internet. The Web-based PIN management system had to be not only absolutely secure, but also fast and reliable. One of the biggest challenges of the project was ensuring that the customer was the only person able to view their PIN. "We insisted on a solution that would prevent anyone or anything from being able to gain knowledge of the PIN number as it traveled to the rightful owner of the card. It was imperative that we could demonstrate to our peers within the payment industry that we were improving the security of the payment network rather than weakening it," said Horler. Preventing disclosure of the PIN across the entire transaction would be difficult. The third-party card issuer holding Egg's customer PIN data had doubts as to whether a technology actually existed to achieve this goal.

> "The SafeNet ViewPIN+ solution has helped us reduce our overhead costs significantly, as well as provide our customers with the convenience and security they not only expect, but deserve."
>
> -Stuart Horler
> Lead Security Architect
> Egg plc

"ViewPIN+ is a perfect example of how we strive to make banking secure and convenient for our customers. We are constantly seeking to adapt our products and services such that they fit in with their modern lifestyles."

-Ken Woghiren Head of Architecture and Innovation for Citibank UK Consumer

Solution

Egg knew they would need an experienced security technology partner, so they approached SafeNet about the project. SafeNet's award-winning PIN management platform ViewPIN+ perfectly suited the challenge. With its hardware-based application security module, ViewPIN+ would offer hardware key management, and would ensure that cryptographic keys and processes were, at all times, stored and managed exclusively within FIPS-validated hardware. Code signing and verification would maintain the integrity of the Java application code and prevent unauthorized application execution. Additionally, strictly enforced access and usage policies would prevent unauthorized access to sensitive applications or data. With tamper-resistant hardware, network connectivity, and secure remote administration, only SafeNet ViewPIN+ would make it possible for Egg to deploy sealed high-assurance Java Web service applications, which proved to be a critical, project-enabling capability.

The Benefits

Stuart Horler, said the technology, which has been in use since 2004, has had a 100% success and reliability rate. Another major benefit of the Web-based PIN issuance solution is the hard cost savings. For every card customer, Egg saves in postage and fulfillment costs, while providing the customer with better service—a win-win situation for the bank and its customers.

Time savings are also a significant factor. A PIN request through the Egg website is fulfilled instantly and the customer can use their card immediately. In contrast, a PIN request that has to go through the postal system can take up to 10 days, assuming it is not subject to interception fraud and actually arrives to the rightful account owner.

"That's a week or more that the customer is either not using the card for purchases or is doing so with a card from another issuer," said Horler. "Multiplied by the large number of credit card customers we have, that is a huge potential loss of revenue and an unnecessary inconvenience for our customers."

"Egg continues to pride itself on being at the core of a very small number of financial institutions that really understand customer need. The critical connection between the services every bank provides and customer satisfaction is often assumed, a significant flaw in the planning arena for some and a major advantage for businesses like Egg. Online banking is simple, delivers excellent service through a digital channel, 24/7, and makes sure security is at the heart of every solution. With SafeNet and Egg working in partnership, you have security and customer service delivered in a neat, effective, and cost-efficient solution. Happy customers, CIO, and Finance Director, what more could anyone want!"

-Robin Young, CIO Citi UK

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.

About Egg

Egg is the UK's leading online bank, providing banking, insurance, investments, and mortgages through its Internet site and other distribution channels.

About Citi

Egg is a member of Citi, the leading global financial services company, has some 200 million customer accounts, and does business in more than 100 countries, providing consumers, corporations, governments, and institutions with a broad range of financial products and services, including consumer banking and credit, corporate and investment banking, securities brokerage, and wealth management. Citi's major brand names include Citibank, CitiFinancial, Primerica, Smith Barney, Banamex, and Nikko. Additional information may be found at www.citigroup.com or www.citi.com.

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

Secured Manufacturing

INTERNAL REFERENCE GUIDE

SafeNet Value

Using the HSM for key management ensures the IP is protected both internally and among third parties who may or may not have their own security policies. With SafeNet HSMs, manufacturers are able to leverage the HSM for centralized control to remote locations, and since each manufacturing environment is different, also customized features. In addition, SafeNet HSMs offer high availability, load balancing, and ECC key limit size constraints for smaller crypto footprints, to ensure production uptimes and efficient performance rates that will not bog down systems.

Overview

The goal of implementing a secured manufacturing environment is to protect intellectual property (IP). With a projected year-over-year increase in IT spending of 3.6 percent, companies are moving towards secured manufacturing environments in an effort to reduce manufacturing costs, improve supply chain efficiencies, and protect their IP. This especially holds true with third-party manufacturing sites that may not have security policies in place and cannot be trusted.

Customer Problem

Reasons vendors look to Offshore Manufacturing:

- Costs
- Lack of core competency
- Greater flexibility
- Higher volumes
- Higher quality
- Time to market

Risks/Concerns with Offshore:

- Lack of control
- Loss of IP
- Production of black market replicas
- IP laws are not equally enforced WW
- Complexity increases with distance
- Language barriers

	Security Threat
▶	Privacy of IP data
▶	Authentication of manufacturing tools
▶	Limits on manufacturing quantities
▶	Limits on license features, added at manufacturing time
▶	Authentication of manufactured components once deployed
▶	Enforcement of policy and procedures

HSM's Role

Using the HSM for key management ensures the IP is protected both internally and among third parties who may or may not have their own security policies. In addition, SafeNet Remote PED will provide centralized control.

Since each manufacturing environment is different, SafeNet Functionalities Modules and the Luna SP Java applet will allow manufacturers to customize their features/logic.

High availability and load balancing features will assure production uptimes and efficient performance rates that will not bog down systems. In addition, next-generation HSMs will include ECC keys limit size for smaller signed data footprints.

Benefits Gained

- Protection of IP
- Control of manufacturing process
- Remote operational control with cryptographic policies, regardless of distance
- Cost reduction
- Improved time to market
- Improved quantity capabilities
- Improved quality

Targets

Industries:	Solution Providers:
• Technology manufacturing • Automobile and machinery manufacturers • Textile manufacturers • Third-party suppliers	• b_process • Logica • EDB • Anochron • Progratror • Tieto • Medidata • BBS • SETTCE

SafeNet Customers:

- Seagate
- Intel
- John Deere
- Cisco
- Lexmark
- Sony
- Motorolla

IDC predicts a 3.6% increase in IT spend for process manufacturing and a 2.5% increase for discrete manufacturing in 2010.

Use Case

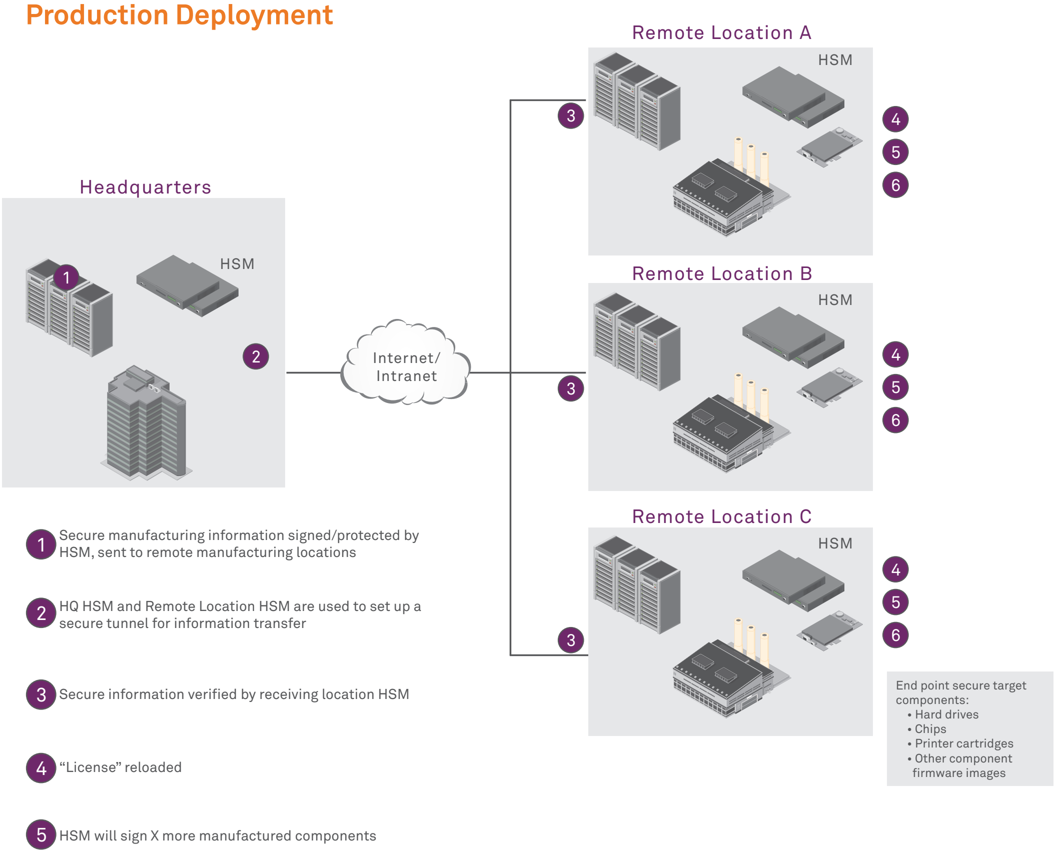
In order to guard against forgery, many manufacturers are relying on HSMs to protect their intellectual property, such as chips, hard drives, and printer components, as well as protect against lost revenue. One such manufacturer wanted to protect their phones from snooping, identity forgery, and other forms of network abuse that plague the cellular phone and satellite television industries. An IP phone manufacturer needed to integrate secure identification and authentication into its devices. The business needed to integrate the issuance of digital identities and authentication into its manufacturing processes, which meant the organization would need to securely and cost-effectively create thousands of industry-compliant digital identities.

The IP telephone manufacturer selected Microsoft Certificate Services software for managing the issuance of digital identities, but needed a hardware solution to deliver maximum security and performance. A highly secure hardware system was required to protect the certificate issuance root key—the basis of trust for all of the IDs issued to the phones—and prevent the possibility of a copy of that key being used to create illegitimate device identities. The solution also had to meet high performance standards to ensure that the computationally-intensive certificate issuance process did not create bottlenecks in the manufacturing process.

The manufacturer selected an HSM as the foundation for their digital identity issuance system for IP telephones. Their selected HSM held both FIPS 140-2 and Common Criteria certification. With each IP telephone containing a unique, trusted digital identity, users can be sure that the IP telephone they are connecting with is definitely the telephone it claims to be. This IP telephone manufacturer's use of HSMs demonstrates how high-volume, high-speed digital ID issuance can be seamlessly integrated into the manufacturing process without sacrificing security.

The black market projected value of counterfeit technology products is $100 billion and the value of counterfeit pharmaceutical products is $75 billion. Source: Havocscope Report

Production Deployment



End point secure target components:
- Hard drives
- Chips
- Printer cartridges
- Other component firmware images

1 Secure manufacturing information signed/protected by HSM, sent to remote manufacturing locations

2 HQ HSM and Remote Location HSM are used to set up a secure tunnel for information transfer

3 Secure information verified by receiving location HSM

4 “License” reloaded

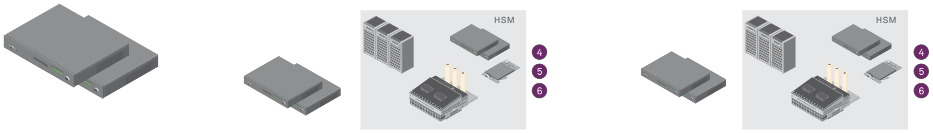
5 HSM will sign X more manufactured components

Typical HSM Opportunities

Production Deployment
Two HSMs

Development Deployment
One HSM

User Acceptance Test Deployment
Two HSMs



The black market projected value of counterfeit technology products is $100 billion and the value of counterfeit pharmaceutical products is $75 billion. Source: Havocscope Report

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

< Table of contents

Smart Grid Security (Smart Meters)

INTERNAL REFERENCE GUIDE

SafeNet Value

- Supports industry compliance requirements
- Supports best practices for key management/security

Overview

Smart Grid

The smart grid creates a network of links between customers and utility companies. This smart grid network then connects to computer systems at utility companies and will signal people or their appliances to take certain actions, such as reducing power usage when electricity prices spike. In order to implement trust in this system, a PKI infrastructure secured with HSM technology is deployed in smart meters as the first step to establishing a smart grid.

Smart meters are deployed in two phases:

1. Automated Meter Reading (AMR) allows meters to be read remotely, eliminating the need to send meter readers to each location.
2. Advanced Metering Infrastructure (AMI) technologies facilitate a two-way channel of communication between meters on the grid and the utility that, in turn, provides increased business intelligence to both the utility and the end consumer.

Utilities managed by the smart grid are a fundamental part of our everyday lives and must be protected. Protecting these assets will require the deployment of authentication, encryption, and integrity protection solutions throughout the smart grid architecture.

Customer Problem

Energy providers use a complex and decentralized system of applications to manage the delivery of the utility. Manipulation of one or all of these components in the smart grid could impede the delivery of energy to homes and businesses, with potentially disastrous consequences.

Assets managed at the application and communication layers of the grid require the most security:

The Application Layer

- Outage Management System (OMS). An Outage Management System is a computer system tasked with the management of the restoration of power in the event of an outage. These systems are used to estimate the location, size, and work force required to restore power.
- Geographical Information Systems (GIS). Geographical Information Systems allow utilities to visualize the electric and communications systems, and the relationship that exists between them. GIS provides a real-time picture of the health of the grid itself.

SafeNet Partners:

Solution providers

- Elster, Elster Group is a world leader in Advanced Metering Infrastructure (AMI)
- Landis+Gyr. Landis+Gyr, the world's largest electricity metering and smart meter solutions company (uses SafeNet us with RSA key mgmt)
- Itron (uses SafeNet with Certicom key mgmt)
- Sensus
- General Electric

SafeNet Customers:

- Southern California Edison
- Vectren (ProtectFile)

- Distribution Management Systems (DMS). A DMS is responsible for the allocation of utility assets and provide tools to anticipate future energy consumption.
- Energy Management Systems (EMS). An EMS is a system of computer-aided tools used by operators of electric utility grids to monitor, control, and optimize the performance of the generation and/or transmission system.
- Meter Data Management Systems (MDM). An MDM system performs long-term data storage and management for the vast quantities of data that are now being delivered by smart metering systems. This data consists primarily of usage data and events that are imported from the head end servers that manage the data collection in Advanced Metering Infrastructure (AMI) or Automatic Meter Reading (AMR) systems.
- Enterprise Resource Planning Systems (ERP). ERP systems manage internal and external resources, including tangible assets, financial resources, materials, customer information, and human resources data of utility organizations.

The Communications Layer

- Smart Meters. A class of meter that will not only measure kilowatt hours but also 'quality of supply' functions. It is capable of being read remotely.
- Network Gateways. LAN, WAN, FAN/AMI, and HAN networks facilitate the channels of communication between smart meter and the utility.

Security Threat

If not properly secured, smart grid attacks could lead to:

▶ **Grid Instability.** Large-scale manipulation of smart meters could be used to create instability in the power grid by falsifying the usage readings to be higher or lower than the actual demand. If meters were to simultaneously have a dramatic change in draw, it could cause outages across a large area.

▶ **Loss of Consumer and Enterprise Privacy.** A benefit of the Smart Grid is improved customer service relationships through more frequent communication between customers and utility companies. This requires an exchange of personal and account data at some level that could be exploited.

▶ **Actionable Energy Usage Data Exposure.** Electricity use patterns could lead to disclosure of not only how much energy customers use but also when they're at home, at work, or traveling. In residential deployments, it would be possible to deduce information about personal behaviors and what appliances are present by monitoring energy usage.

▶ **Utility Fraud.** Criminals can tap into the network, extract data that could contain executable codes, configuration information or cryptographic keys, all of which could be stolen or modified. These assets could be used to manipulate billing or usage data.

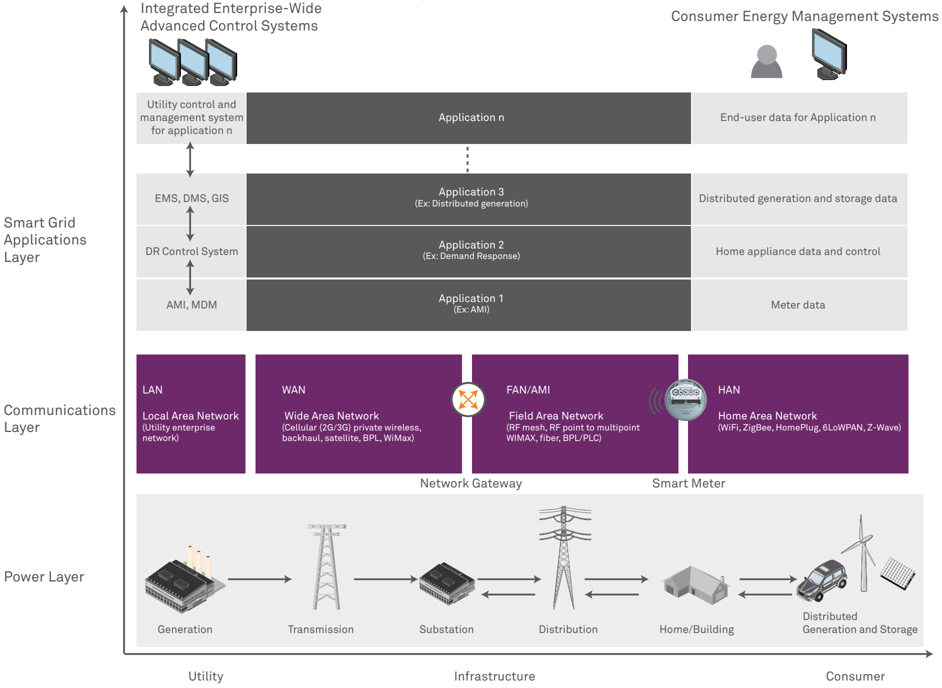
HSM's Role in the Smart Grid and Smart Metering

Smart Grid security solutions must be able to be deployed on a large scale, with minimal effect on application performance. Securing the smart grid requires a system to identify connected devices, to verify that these devices are configured correctly, and to validate these devices for network access. The recommended solution for this authentication process is a Public Key Infrastructure, as PKIs are ideal for large scale security deployments that require a high level of security with minimal impact on performance.

In a PKI environment, it is essential that private keys and certificates are guarded with a reliable key management solution that protects against ever-evolving data threats. SafeNet HSMs generate and store cryptographic keys in a tamper-proof, highly available appliance. HSMs provide the following security functions:

- Device Attestation. Using device attestation certificates, the HSM confirms the device manufacturer, model, and serial number, and that the device has not been tampered with. These certificates, coupled with the appropriate authentication protocol, can be used by the energy service provider to ensure that the device is exactly what it claims to be.
- PKI and EKM Key Management. HSMs provide significant cost savings, as HSM functionality (key generation/offline root/online root/key export) is made available with one device.
- Trust Anchor. A local policy database is a set of rules that define how the device can use its certificate, and what types of certificates it should accept when acting as a relying party. The LPD would be a signed object, signed and stored within the HSM.
- Encryption and Decryption of Information. AES 256 & ECC 256/384-bit. ECIES key management and ECDSA signing performance (256-bit curves)
- Transaction processing of usage and billing to customers. E-invoicing and secure billing.
- Compliance. Compliant with NIST, FIPS, and NERC audits

End-to-End Smart Grid
(High-Level Taxonomy)


Integrated Enterprise-Wide Advanced Control Systems
Consumer Energy Management Systems
Smart Grid Applications Layer
Utility control and management system for application n
Application n
End-user data for Application n
EMS, DMS, GIS
Application 3 (Ex: Distributed generation)
Distributed generation and storage data
DR Control System
Application 2 (Ex: Demand Response)
Home appliance data and control
AMI, MDM
Application 1 (Ex: AMI)
Meter data
Communications Layer
LAN
Local Area Network (Utility enterprise network)
WAN
Wide Area Network (Cellular {2G/3G} private wireless, backhaul, satellite, BPL, WiMax)
FAN/AMI
Field Area Network (RF mesh, RF point to multipoint WIMAX, fiber, BPL/PLC)
HAN
Home Area Network (WiFi, ZigBee, HomePlug, 6LoWPAN, Z-Wave)
Network Gateway
Smart Meter
Power Layer
Generation
Transmission
Substation
Distribution
Home/Building
Distributed Generation and Storage
Utility
Infrastructure
Consumer

Benefits Gained

Security Benefits

- Security
- Reliability
- Redundancy
- Privacy

Business Benefits

- Increased visibility and control over the power grid
- Compliance with PII (authentication, signing, encryption of data), NIST, FIPS, and NERC audits
- Improved budgeting. Accurate data improves budgeting and cash flow projections.
- Reduce administrative costs. Eliminate time spent checking and validating bills. Bills are based on accurate and up-to-date information
- Improved customer service

Technical Benefits

- Key management for deployment of keys
- Signing of messages/ software delivery to end points
- Encryption of data back to head end
- Transaction processing of usage & billing to customers

Targets

Industries:	Solution Providers:
Power utility companies, municipalities	

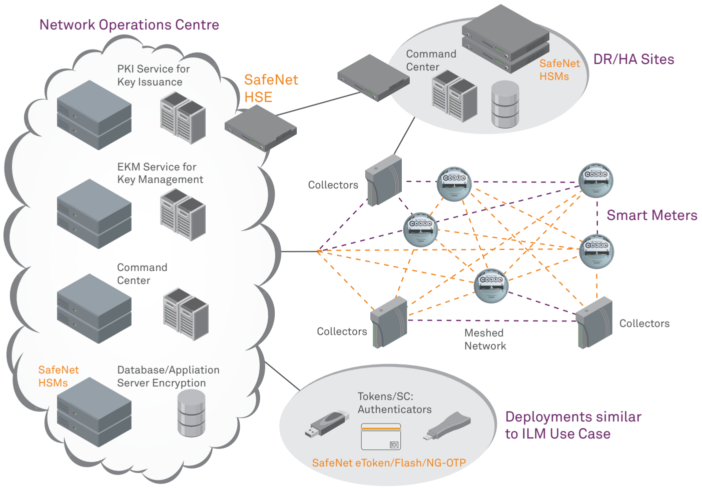
Use Case

The Smart Grid and HSMs

With Smart Metering, utility companies and consumers can gain increased insight into energy consumption, cost, and workload across the energy grid. While the two-way flow of information from meters to the utility company can provide cost savings, increase customer service, and bolster conservation efforts, the smart grid introduces new vulnerabilities to the utility infrastructure that could be used maliciously.

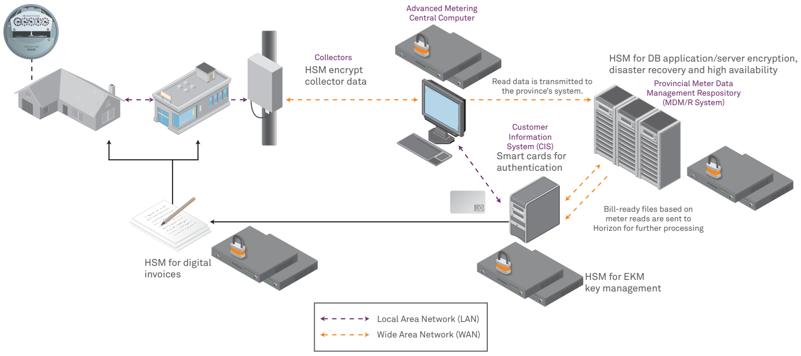
SafeNet HSMs are a cost-effective security solution for smart grid deployments. The SafeNet Luna SA HSM ensures the integrity and security of cryptographic operations in a robust, high-availability appliance. Luna SA is capable of up to 6,000 RSA and 400 ECC transactions per second and offers optional stand-alone authentication to protect the most demanding security applications. With the SafeNet Luna SA PKI Bundle solution, product and maintenance costs are dramatically reduced by combining HSM functionality that usually requires two or more HSMs into a single HSM "bundle" of modular functions. For CAs with certificates and root keys, for example, rather than requiring separate HSMs for key generation and key export for offline and online root CAs respectively, the requirements can be fulfilled by only one Luna SA HSM, which stores keys in hardware achieving FIPS 140-2-Level 3 security.

Secure Metering Grid Architecture Overview



Network Operations Centre
PKI Service for Key Issuance
EKM Service for Key Management
Command Center
SafeNet HSMs
Database/Appliation Server Encryption
SafeNet HSE
Command Center
SafeNet HSMs
DR/HA Sites
Collectors
Smart Meters
Collectors
Meshed Network
Collectors
Tokens/SC: Authenticators
SafeNet eToken/Flash/NG-OTP
Deployments similar to ILM Use Case

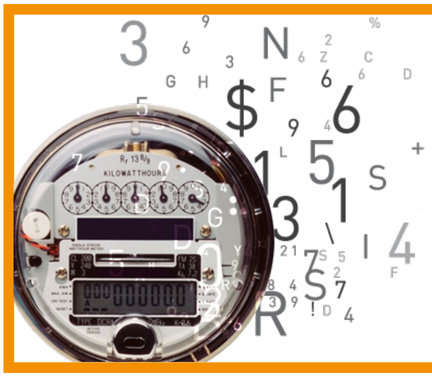
Production Deployment



Advanced Metering Central Computer
Collectors
HSM encrypt collector data
Read data is transmitted to the province's system.
HSM for DB application/server encryption, disaster recovery and high availability
Provincial Meter Data Management Respository (MDM/R System)
Customer Information System (CIS)
Smart cards for authentication
Bill-ready files based on meter reads are sent to Horizon for further processing
HSM for digital invoices
HSM for EKM key management
Local Area Network (LAN)
Wide Area Network (WAN)

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

< Table of contents



HSM for Securing the Smart Grid

SOLUTION BRIEF

Benefits of PKI

- Protect customers private data
- Protect power grid from manipulation
- Prevent large scale attacks on the grid
- Eliminate deployment of fraudulent meters

Building trust in the smart grid with hardware security modules for meter attestation, PKI and EKM management, and compliance with security mandates

Overview

The smart grid is the first major effort to modernize an energy infrastructure that has remained largely unchanged over the past several decades. The smart grid creates a network of links between customers and utility companies that provides increased insight into energy consumption, cost, and workload across the energy grid.

At a time when energy utilities play an increasingly important role in our everyday lives, smart grid technologies introduce new security challenges that must be addressed. Implementing a smart grid without proper security could result in grid instability, loss of private information, utility fraud, and unauthorized access to energy consumption data. Building a trusted smart grid will require robust security solutions that can be easily deployed at the communication and application layers of the smart grid infrastructure.

In the first phase of smart grid deployments, traditional meters will be replaced with smart meters that can be read remotely, called smart meters. The Advance Metering Infrastructure (AMI) is the second phase of the smart grid and uses smart meters to enable a two-way channel of communication between meters and the utility company. Securing this two-way line of communication is imperative, and will require a solution for authentication and device attestation to ensure the integrity of the grid.

HSMs Role in the Smart Grid

Smart grid security solutions must be able to deploy on a large scale, with minimal effect on application performance. Securing the smart grid at the communication layer will require a system to identify connected meters, to verify that these meters are configured correctly, and to validate thm for network access. The recommended solution for this authentication process is a Public Key Infrastructure (PKI). PKIs are ideal for large scale security deployments that require a high level of security with minimal impact on performance. In a PKI environment, it is essential that private keys and certificates are guarded with a reliable key management solution that protects against ever-evolving data threats.

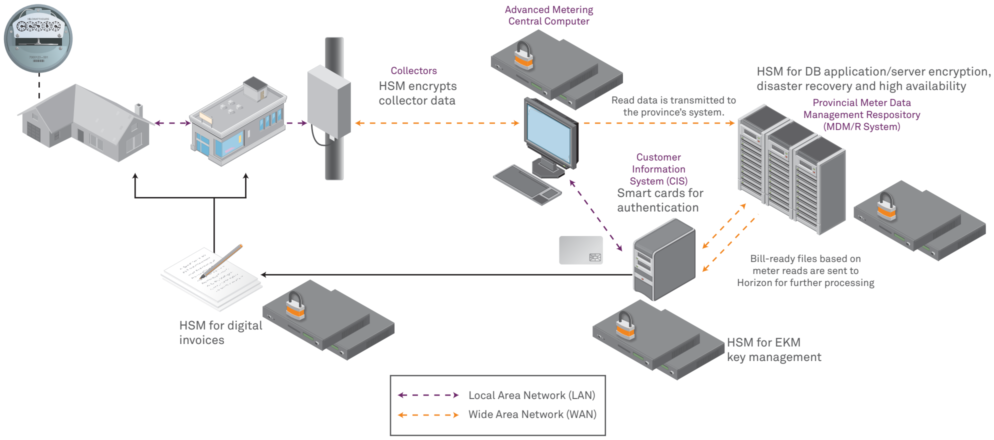
SafeNet HSMs offer a cost-effective PKI solution for easy deployment in smart grid infrastructures. With the SafeNet PKI Bundle, product and maintenance costs are dramatically reduced by combining HSM functionality that usually requires two or more HSMs into a single HSM “bundle” of modular functions. For CAs with certificates and root keys, for example, rather than requiring separate HSMs for key generation and key export for offline and online root CAs, the requirements can be fulfilled by only one SafeNet HSM that stores keys in hardware to achieve FIPS 140-2 L3 security. In addition, with processing speeds of up to 6,000 1024-bit RSA and 400 384-bit ECC transactions per second, SafeNet HSMs can keep up with the performance requirements of even the most complex smart meter deployments.

Why SafeNet HSMs?

- FIPS 140-2 Level 3-validated hardware
- Common Criteria EAL 4+ certified
- Ideal for disaster recovery readiness
- Scalable, easy installation and management
- High-availability mode

HSMs provide the following security functions:

- **Device Attestation.** Using device attestation certificates, the HSM confirms the device manufacturer, model, and serial number, and that the device has not been tampered. These certificates, coupled with the appropriate authentication protocol, can be used by the energy service provider to ensure that the device is exactly what it claims to be.
- **PKI and EKM Key Management.** HSMs provide significant cost savings, as HSM functionality (key generation/offline root/online root/key export) is made available with one device.
- **Trust Anchor.** A local policy database is a set of rules that define how the device can use its certificate, and what types of certificates it should accept when acting as a relying party. The LPD would be a signed object, signed and stored within the HSM.
- **Encryption and Decryption of Information.** AES 256 & ECC 256/384-bit. ECIES key management and ECDSA signing performance (256-bit curves).
- **Transaction processing of usage and billing to customers.** Provide a trusted path for energy usage for accurate and secure electronic billing.
- **Compliance.** Compliant with PII, NIST, FIPS, and NERC audits
- **Remote Management of Meters.** Securely update the metering settings, configuration, security credentials, and firmware of all devices in the AMI System.


Advanced Metering Central Computer
Collectors
HSM encrypts collector data
HSM for DB application/server encryption, disaster recovery and high availability
Read data is transmitted to the province's system.
Provincial Meter Data Management Respository (MDM/R System)
Customer Information System (CIS)
Smart cards for authentication
Bill-ready files based on meter reads are sent to Horizon for further processing
HSM for digital invoices
HSM for EKM key management
Local Area Network (LAN)
Wide Area Network (WAN)

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. For more information, visit www.safenet-inc.com.

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

< Table of contents

Trusted Virtual Infrastructure Platform

INTERNAL REFERENCE GUIDE

Cloud Service Types:

Virtualization Technology Providers - (VMWare, Microsoft, Oracle, Red Hat, Citrix, Xen)

Software as a Service (SaaS) providers - Delivers a single application through the browser to their enterprise customers (Amazon, Google Aps, Workday, Zoho, Salesforce.com, Netsuite)

Platform as a Service (PaaS) providers - Allows enterprises to deploy their own apps on the Cloud platform (Force.com, Microsoft Azure, Facebook, Salesforce AppExchange)

Infrastructure as a Service (IaaS) Providers - Computing Storage (Amazon Web Services, RackspaceCloud, Nirvanix, Terremark Enterprise Cloud)

Trusted Cloud Platform for Trusted Service Providers

Overview

In order for cloud service providers to expand their market share, and increase existing and potential customer confidence, they need to offer a level of security that accommodates organizations managing assets from all levels of data sensitivity. Widespread adoption is contingent on the ability to foster a level of trust matching that of existing internal enterprise resources.

SafeNet's trusted cloud platform, using a data-centric approach, protects these valuable information assets. Protecting assets at the data level allows for the same protection polices to be applied wherever the data resides or is used. Our solution achieves this by linking the cryptographic keys that protect the data to a hardware-based root-of-trust controlled by the data owner.

With a trusted cloud platform, a service provider can target enterprises requiring a level of security previously unavailable in the cloud, allowing them to offload sensitive information assets—saving money.

Customer Problem

Cloud Service Provider

- Need to accommodate organizations at all levels of data sensitivity
- Need to offer hardware-based cryptographic services
    - Centralized key management
    - Granular security polices
    - Data encryption
    - Digital signature
    - Strong authentication and access control
- Need to offer validated/certified hardwared-based security with auditing capabilities
- Need to offer trustworthy and efficient deployments to their enterprise customers

	Risks associated with shared resources
▶	Potential information leakage between users/processes
▶	Loss of physical and logical control over the storage and computing resources
▶	Potential for data and processes to change location without owner's knowledge

Trusted Cloud Platform for Enterprises

Overview

Issues of risk, data privacy, and compliance are the chief inhibitors to most organizations' adoption of cloud services. These concerns can outweigh the potential cost savings of cloud resources for many organizations. For an enterprise with highly sensitive data to transition to the cloud, they must first trust that a cloud environment will allow them to preserve their existing level of encryption and retain full control over security ownership.

With a trusted cloud platform, enterprises can leverage the cloud and get the level of security needed to stay compliant with all pertinent regulatory mandates and security policies. With features including robust encryption, secure remote key management, and granular access control, we create the foundation for a cloud-based infrastructure that meets the security objectives of every enterprise.

Customer Problem - Enterprise

- Protect an enterprises' virtual images as they are run in the cloud
    - Protecting applications
    - Protecting data
- Need to ensure data remains protected in the cloud
- Need to remain in control of their information assets, and maintain compliance with all mandates and policies—ensuring the enterprise knows exactly where those cloud applications they push out are running
- Need to safeguard the trust of their customers, business partners, and employees

	Security Threat
▶	Data location risk
▶	Data loss risk
▶	Data security (privacy) risk

HSM Role – Cloud Service Provider

Cloud providers start off by deploying something we call cryptography as a service via HSMs. The HSMs are FIPS certified and hold secrets (keys) for providing encryption as a service—actually doing the cryptographic operations. Service providers need HSMs to protect their TLS/SSL identities. To meet many clients' security requirements, these HSMs should be FIPS 140-2 Level 3-validated. Luna SA supports 100 clients, enabling organizations to deploy servers on a large scale, through virtualization and infrastructure clouds, without needing to scale their physical HSMs. Today, it's not unheard of to have 100 virtual machines running on a single cluster of virtualization servers. Luna SA can keep pace!

Types of Organizations:

Existing HSM Customers

Any enterprise that may have an on-premise key vault (HSM) and will be moving toward a virtualized data center

Organizations Wanting Cloud Benefits of IaaS with No Risk involved

Non-sensitive data can be transferred into the cloud as is; for example, for disaster recovery or archival purposes. Will migrate an application to the cloud when the processing capacity of its corporate cloud or data center is exceeded

Platform as a Service (PaaS) providers

Allow enterprises to deploy their own apps on the Cloud Platform (Force.com, Microsoft Azure, Facebook, Salesforce, AppExchange)

Organizations Migrating Business Services to the Cloud

Hosting provider deployments requiring limited trust

Trusted Cloud Platform - Cryptography as a Service

Benefits Gained

Scalable solution that will grow with your business and cloud needs

- Partitioning. A single set of Luna SA devices serve as the highly available HSM for twenty separate security domains for virtual machines (VM). Up to 100 VMs can share these 20 security domains - including multiple instances of each VM. Future releases will increase available partitions from 20 to 100.
- Migration Support. Given the network-attached nature of the client-HSM connection, can move to any server that is registered with the same Luna SA.
- Elastic Scalability. Luna SA's partitioning and client registration fully supports multiple instances of the same VM. Client registration can be scripted and invoked from a secure management console to automate an elastic response to performance demands.
- Hypervisor Support. Luna SA supports the leading hypervisors, including VMware vSphere, Microsoft Hyper-V, and Citrix XenServer.

Ease of management for lower administrative and operational costs

- Remote PED Authentication and Management. Luna SA implements a trusted-path, multi-factor authentication method for its HSM partitions. This enables flexible remote management, consistent with virtualized infrastructures. In addition, the Luna PED can logically connect to an HSM across any network using a secured trusted path.
- Secure Transport Mode. Using secure transport mode, Luna SA can be pre-configured, securely shipped, racked and stacked, and remotely activated for secure deployments in a third-party data center.

Trusted security

- Strong Access Control and Authorization. Luna SA uses industry proven TLS with full client authentication to provide strong network access controls and authorization for each client requesting HSM access. To simplify the deployment of this technology, the Luna SA includes its own internal CA to certify and authorize each client's certificate. Therefore, no external PKI is required.
- Secure Authentication. In addition to the client-level authentication and access control, each user or process must authenticate using a secure challenge-response mechanism to gain access to the keys in a particular HSM partition.
- In-Hardware Key Storage. Luna SA secures more keys, deeper in the hardware than ever before by utilizing a special, SafeNet-designed, tamper-proof ASIC cryptographic processor.

Performance and reliability helping to keep up with demands to the cloud infrastructure

- Marketing Leading Performance. A single Luna SA 5.0 device is capable of up to 6,000 RSA 1024-bit transactions per second and up to 1,200 RSA 2048-bit transactions per second. Luna SA 5.0 processes over 400 384-bit ECC transactions per second (the security equivalent of RSA 7680-bit).
- High Availability and Load Balancing. Luna SA has a high-availability and load-balancing mode that allows multiple Luna SA units to group as a logical set. This feature aids in the deployment of virtual services by delivering the reliability and performance required in a highly virtualized infrastructure. A three unit, high-availability setup can triple transaction performance, enabling processing speeds of up to 18,000 RSA 1024-bit, 3,600 RSA 2048-bit, and 2,400 384-bit ECC transactions per second. Clients communicate to partitions in the group as if it is a single HSM, and the Luna SA automatically keeps key material synchronized and load-balances requests across the set.

SafeNet Partners

Several partners (Amazon, Adobe, Microsoft, NetApps, and others) have asked about the possibility of SafeNet providing a HSM-as-a-Service offering. This would concentrate the skills associated with configuring and managing cryptographic devices, while making them generally available to enterprise customers – for both on-premises and in-the-cloud applications.

Use Case – HSMs and Cryptography-as-a-Service

Cloud providers have been moving towards the concept of enabling on-premise HSMs for securing their cloud-hosted applications. Bringing the security benefits of a HSM onto virtualized platforms can greatly reduce the costs of traditional in-house deployment, making cloud solutions a viable and cost-effective option for organizations with even the most sensitive data. With SafeNet's Luna SA, providers can offer their clients a solution for central key and policy management, robust encryption support, and flexible integration that we define as Cryptography-as-a-Service.

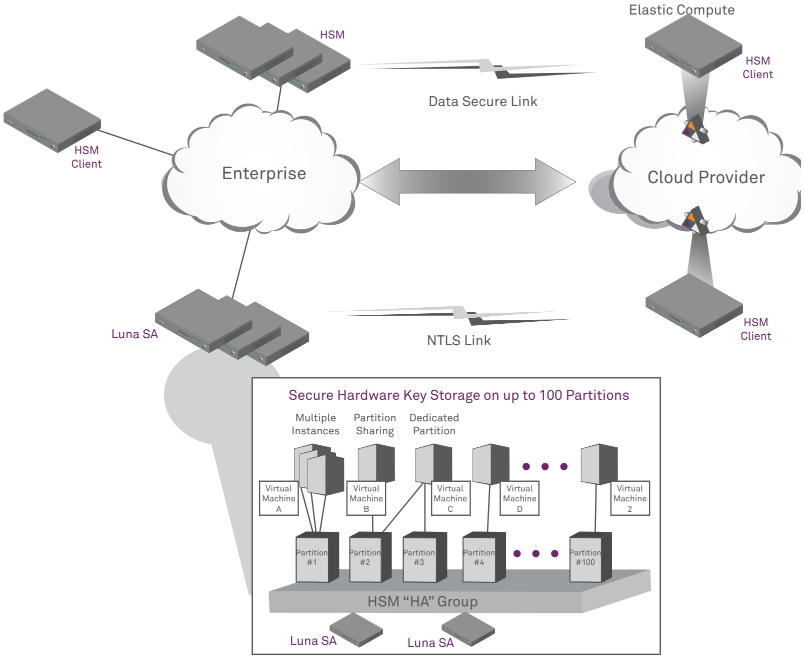
For enterprise organizations, as they look to the cloud to reduce costs, increase reliability, and provide flexibility with cloud solutions, HSMs in the cloud infrastructure provide a strong foundation of protection. The Luna SA HSM, manages cryptographic keys, access control, and other security policies. Deployed in a cloud environment, the Luna SA protects assets at the data level while allowing for full remote security administration through the use of a remote PIN entry device (PED).

The Luna SA HSM is ideally suited for use in a virtualized infrastructure. The Luna SA includes multiple features to enable virtualization:

- Support for 100 client machines independent of their physical or virtual nature
- Support for 20 partitions that directly map to distinctly separate logical HSMs for virtual machines (100 in future releases)
- Support for high availability and load balancing to deliver the reliability and scalable performance demanded by a virtualized infrastructure
- Remote management capabilities enabling strong separation between infrastructure administration and security roles associated with HSMs
- Supports the leading hypervisors, including VMware vSphere, Microsoft Hyper-V, and Citrix XenServer
- Support for elastic scaling of identical VM instances and concurrent re-use of client registrations

SafeNet Value

SafeNet's network-based HSM, the Luna SA, has been architected in a manner that enables virtualization and cloud deployments—offering customers advanced future sets that will scale with their business needs, high levels of certification, auditability, non-repudiation, and ease of remote management. SafeNet HSMs also support the leading virtual platforms including Citrix XenServer, Microsoft Hyper-V, and VMware vSphere.



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

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