HSM Solutions for the Financial Vertical

Financial Services Message

Since 1983, SafeNet Hardware Security Modules (HSMs) have led the market in protecting the most sensitive financial transactions for the world's most important financial services institutions. SafeNet has specific HSM products to protect and secure the transactions of payment processors, card issuers, acquirers, switches, merchants, leading banks, central banks, governments, and e-payment solution providers. In fact, SafeNet HSMs are trusted to protect over 80% of the world's fund transfers- $1 trillion per day. SafeNet's proven technology provides these institutions with the assurance that their financial assets are protected and that regulatory compliance is not only met, but exceeded. Typical financial services applications include funds transfer, PIN mailers and generators, PIN management, online banking transactions, root key protection, and smart card issuance.

Market Drivers

- Privacy
  - External Driver- breaches in current security raise publicity and create external push to improve data security and privacy protection.
  - Internal Driver- push from within to strengthen security

- Mandates
  - Payment Card Industry Data Security Standard (PCI-DSS)- developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or they risk losing the ability to process credit card payments
  - Sarbanes-Oxley- (SOX) US federal law passed in 2002 in response to corporate scandals around accounting and reporting. Some of the numerous requirements under SOX include:
    - Enough information about the flow of transactions to identify where material misstatements due to error or fraud could occur
    - Controls designed to prevent or detect fraud, including who performs the controls and the regulated segregation of duties
    - Controls over safeguarding of assets
  - Gramm-Leach Bliley- allowed commercial and investment banks to consolidate. Goal is to protect the clients. Must have safeguards in place:
    - Denoting at least one employee to manage the safeguards,
    - Constructing a thorough risk management assessment on each department handling the nonpublic information,
    - Develop, monitor, and test a program to secure the information, and
    - Change the safeguards as needed with the changes in how information is collected, stored, and used.

Types of Organizations

- Major Banks
- Check Clearing Houses
- Payment Processors

Sample Applications

- Funds transfer
- PIN mailers
- PIN generators
- Online banking transactions,
- Banking PIN management
- Root key protection
- Electronic funds transfer
- Document signing
- Database encryption
- Certificate Validation
- Document rights management
- SSL web and application servers
- Web services XML

Financial Industry Associations - Banking

Trade Organizations/Associations

- International
  - BAFT - Bankers' Association for Finance and Trade – Global - www.baft.org
  - BAI - Bank Administration Institute - www.bai.org
  - www.ncba.com, etc. – great for contact names – and payment center co's
  - ICBA – Independent Community Bankers Assoc. - www.icba.org
- NALA
  - ABA- American Bankers Association - www.aba.com
  - FIBA - Florida International Bankers Association - www.fiba.net
  - State Level – www.floridabankers.com , www.gabankers.com, www.nyba.com, www.tnbankers.org,
- APAC
  - Asia Pacific Economic Cooperation - www.apec.org

Publications

- *ABA Banking Journal*
- *ABA Journal*
- *American Banker*
- *Banking Strategies - BAI*
- *Bank Systems and Technology*
- *Bank Technology News*
- *ID Focus* newsletter www.cardtechnology.com (really for any vertical)
- *National Underwriter*
- *US Banker*
- *Wall Street Directory*
- *Wall Street Journal*

Websites

- www.bankingtech.com - great place to look at Trade Shows of interest

Trade Shows

- NALA
  - BAFT 85th Annual Meeting - April 22-24, 2007 Scottsdale
  - ABA Information Security Forum -May 7-9, 2007, Scottsdale
  - ABA Banking Leaders Forum and Annual Convention - October 7-10, 2007, San Diego
  - BAI Audit, Compliance & e-Security Conference April 23 – 25, 2007, New Orleans
- APAC
  - China Info World Bank
  - Banking Vietnam Conf.

Financial Industry Associations - Payment

Trade Organizations/Associations

- International
  - BAI - Bank Administration Institute - www.bai.org
  - PCI Security Standards Council- www.pcisecuritystandards.org
  - PCISVA- PCI Security Vendor Alliance- www.pcialliance.org
  - MasterCard- www.mastercard.com
  - Visa Partner Network http://partnernetwork.visa.com
  - RILA Retail Industry Leaders Association www.retail-leaders.org
- NALA
  - Interac Association- www.interac.ca
- EMEA
  - APACS- UK Payment Association- www.apacs.org.uk

Publications

- *Banking Strategies - BAI*
- *Nilson Report* (must have a subscription)
- *Wall Street Directory*
- *Wall Street Journal*
- Retail Industry Buying Guide- lists payment and access control companies http://www.stores.org/ribg/
- www.smartbrief.com

Websites

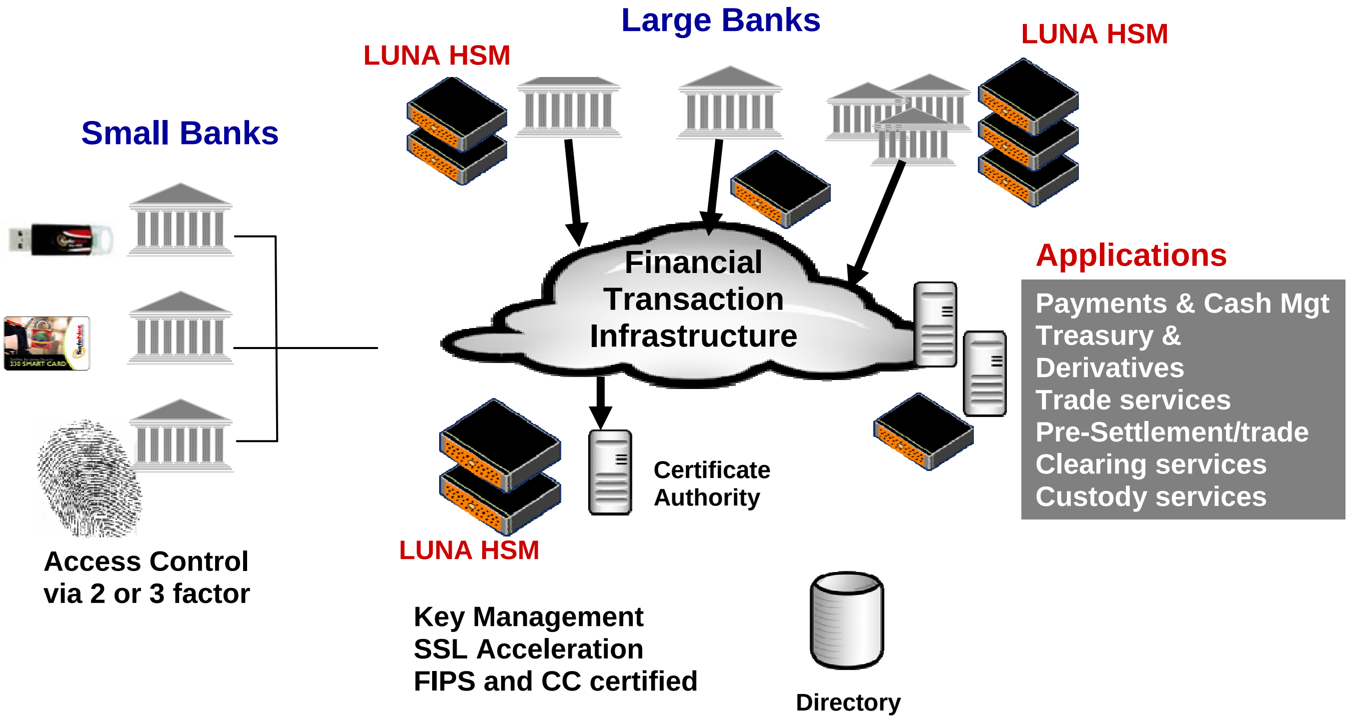
- www.bankingtech.com - great place to look at Trade Shows of interest
- www.paymentsnews.com
- www.theretail-it-bulletin.com
- www.stores.org

Trade Shows

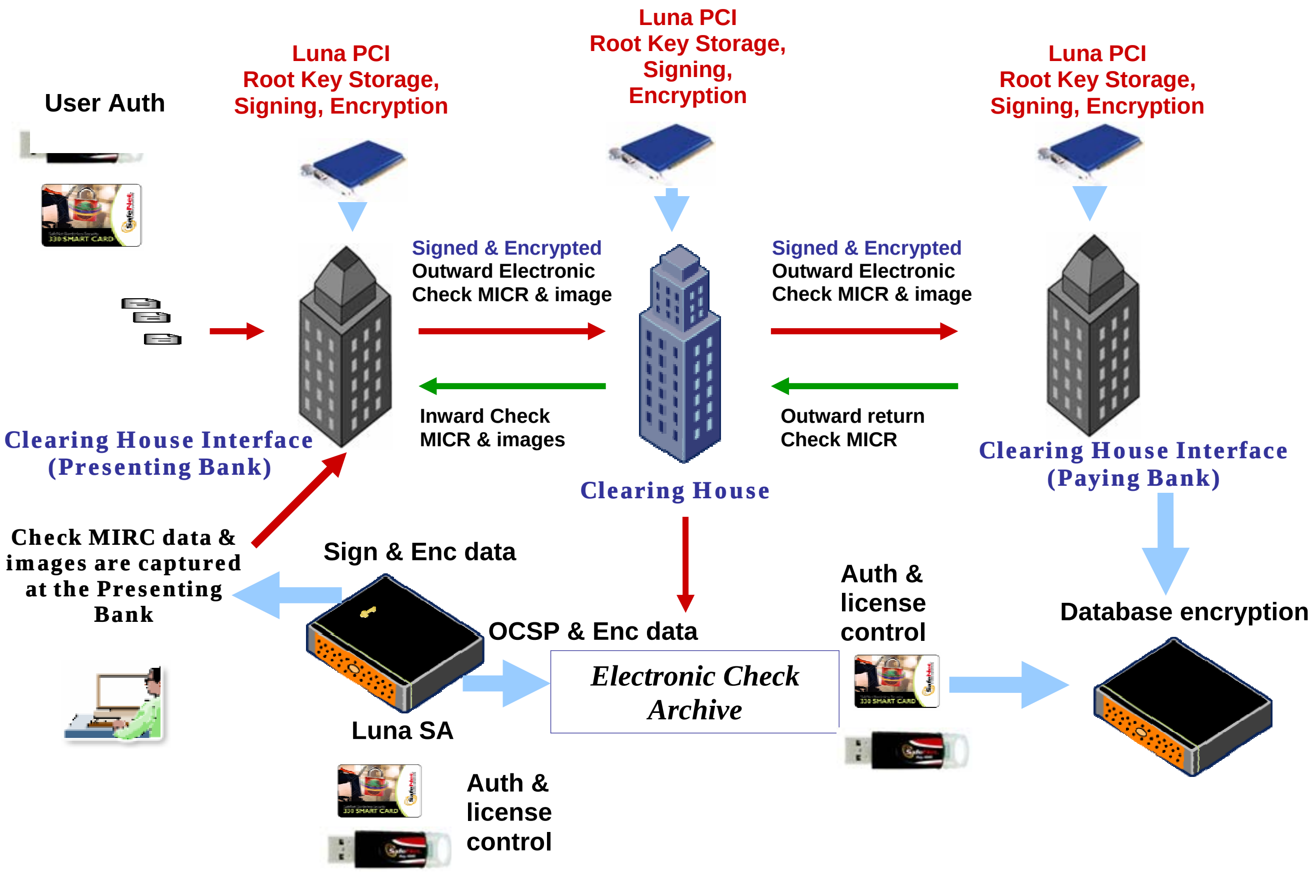
- NALA
  - BAI Retail Delivery Conference & Expo Las Vegas, November 13-16, 2007
  - MasterCard Risk Conferences- Cancun, Mexico - April 23 – 27, 2007
  - MasterCard Risk Conferences- Huntington Beach, CA - May 21 – 24, 2007
  - Glenbrook Payment Book Camp- New York City, NY April 24-25, 2007
  - Glenbrook Payment Book Camp- San Francisco, CA May 2-3, 2007
  - Glenbrook Merchants Payment Boot Camp Santa Clara, CA March 21-22, 2007
- APAC
  - CardsAsia- Suntec,Singapore- April 25- 27
  - MasterCard Risk Conferences- Bangkok, Thailand - September 3 – 7
  - Visa Smart Global Vendor Conference- TBD
- EMEA
  - MasterCard Risk Conferences- Algarve, Portugal - October 17 - 19
  - MasterCard Risk Conferences- Cape Town, South Africa - November 5 - 7

Common Financial Service Applications of HSMs

Securing Banking Transactions (Appliance Example)



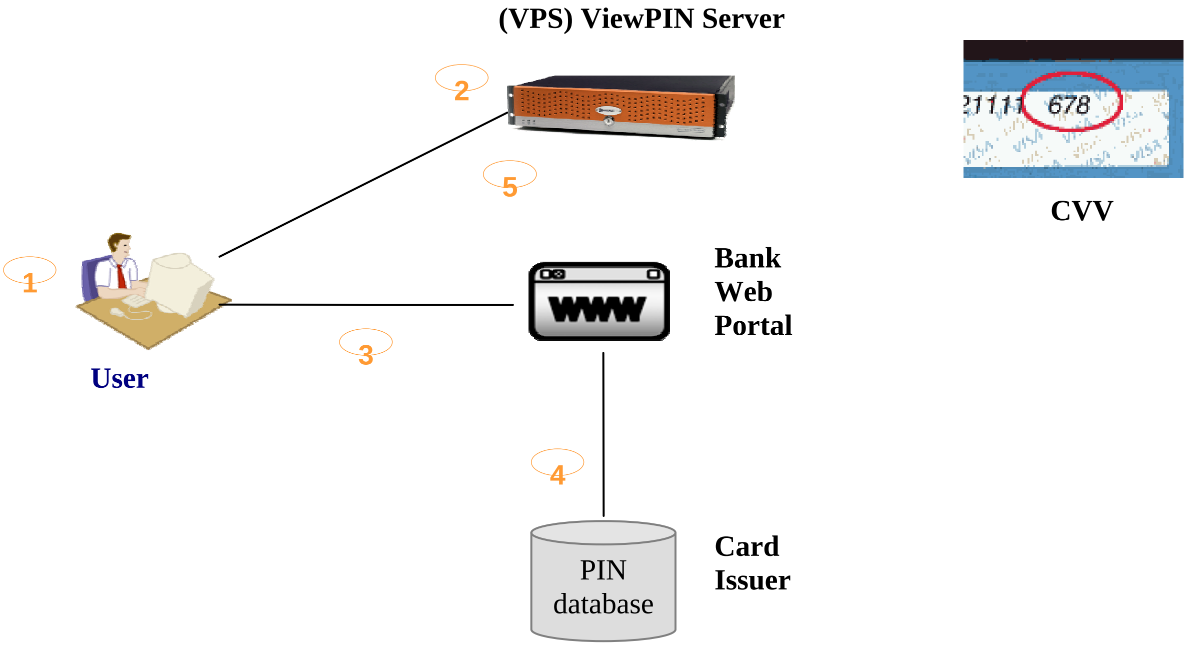
Check Clearing Process (Embedded Example)



A defined asymmetric key pair is established for each bank-to-bank relationship. The individual bank, within this relationship, uses the key pair to sign and verify documentation and transactions from the other bank. The key pairs for each of these relationships are secured, stored, and managed with an HSM.

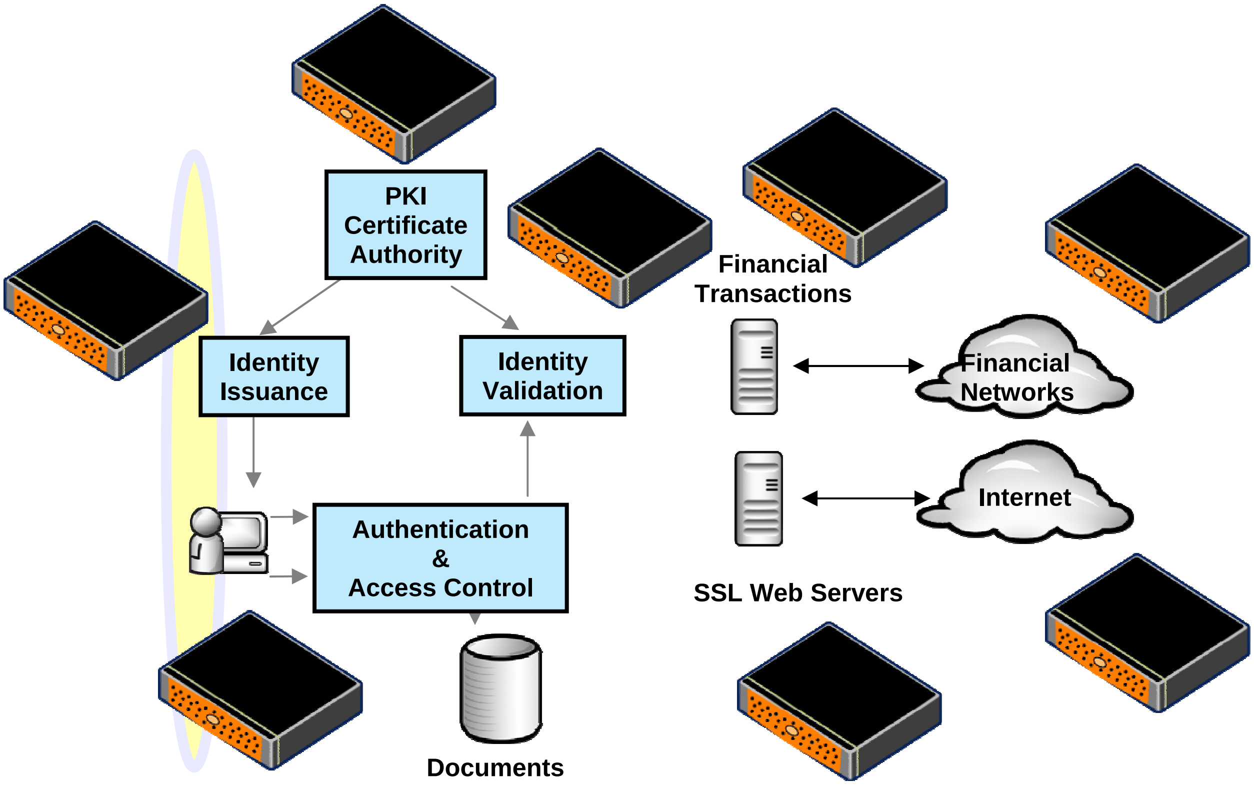
Here, to transfer funds, the presenting bank encrypts the message, containing the electronic check Magnetic Ink Character Recognition (MICR) and image, with the public key associated with the relationship, and signs it with their signing key. The clearing house takes the message and verifies the Online Certificate Status Protocol (OCSP) to ensure it has not been revoked, time-stamps the transaction, archives a copy of the electronic check, and then signs the message before forwarding it to the paying bank. The paying bank then verifies that the message is from the clearing house and decrypts the message with the private key associated with the relationship. The paying bank then encrypts a message containing the return electronic check MICR & image with the public key, which goes through the clearing house and back to the presenting back through the same process.

Egg’s ViewPIN (Programmable Appliance Example)



(1) The user, when prompted by the bank webpage, enters the Card Verification Value (CVV) found on the back of the card. (2) The ViewPin Server (VPS) then encrypts the CVV for the card issuer, and then (3) forwards the encrypted CVV to the card issuer via the bank web portal. (4)The card issuer then decrypts the CVV and looks up the PIN associated with the account, encrypts the PIN for VPS decoding via the bank web portal. (5) The VPS then decrypts the PIN and displays the pin to the user over the SSL sever.

Financial Networks (Appliance Example)



Here, the PKI certificate authority issues the identity. The user's identity allows for them to have access to secured documentation once the identity is authenticated and validated by the certificate authority. The process of identity issuance, authentication and access, and identity validation is conducted by an HSM for both inter and intra-bank financial networks, as well as internet transactions.

HSM Case Studies for the Financial Vertical

HSM Solutions for the Government Vertical

Government Message

SafeNet is the leading vendor of Hardware Security Modules (HSM), allowing government organizations to reliably protect data against compromise and to meet government and industry requirements for compliance and confidentiality. SafeNet's robust FIPS-140 Level 2 and Level 3, FIPS-201/PIV, and Common Criteria validated HSMs offer the highest level of security, featuring in hardware key management and storage, support for major cryptographic API standards, and a tamper-resistant chassis. SafeNet provides the world's only high-performance HSM solutions, with form factors to meet any customer requirements, including database encryption, key storage, root key protection, PKI key generation, certificate validation, smart card issuance, time stamping, document signing, secure authentication, EFT transaction processing, and hardware acceleration of cryptographic algorithms.

Market Drivers

- Mandates
  - Homeland Security Presidential Directive 12 (HSPD-12)- After September 11, 2001, President Bush issued Homeland Security Presidential Directives or HSPDs, with the consent of the Homeland Security Council. The first such directive created the Homeland Security Council while the second changed immigration policies to combat terrorism
  - US Visa Waiver Program- E-passport- border control
  - Other International, Federal, State, and Local directives
  - X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework States that…
    "CAs that issue certificates under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CAs that do not issue certificates under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. RAs shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. "

    Best practices dictate that private CA keys should be stored in an HSM; however, this is not always the case. This is an example of how regulation and compliance create the need for HSMs. All federal PKIs, and PKIs that are cross-certified to the federal bridge, must meet this guidance. This policy creates an expectation that HSMs will be used to protect sensitive keys in other types of federal civilian, DoD, and IC accredited systems

- Privacy
  - Internal Driver- push from within to strengthen security
  - External Driver- breaches in current security raise publicity and create external push to improve data security and privacy protection. (i.e. Veterans Affairs breach)

Types of Organizations

- International, Federal, State and Provincial, and Local Governments
- Government Institutions (i.e. Universities)

Sample Applications

- E-passport
- E-driver’s license
- E-voting
- Time stamping
- Database encryption
- Smartcard issuance
- Root key protection
- Gaming
- Root key protection
- Certificate validation
- Document rights management
- Electronic funds transfer
- Document signing
- SSL web and application servers

Government Industry Associations

Trade Organizations/Associations

- International
    - AFCEA International – Armed Forces Communications and Electronics Association – www.afcea.org - local chapters also.
    - IACP - International Association of Chiefs of Police - www.theiacp.org
    - APCO - The Association of Public –Safety Communications - www.apcointl.org
- NALA
    - ACT - American Council for Technology - www.actgov.org Industry. Advisory Council
    - NASTD - National Association of State Telecommunications Directors - www.nastd.org
    - GMIS - Government Management Information Sciences - www.gmis.org
    - CSG - Council of State Governments - www.csg.org
    - PTI - Public Technology, Inc. - www.pti.org – local gov.
    - NASACT - National Association of State Auditors, Comptrollers and Treasurers - www.nasact.org
    - APCO Canada - The Association of Public –Safety – Canada - www.apco.ca
    - URISA - The Urban and Regional Information Systems Association - www.urisa.org

Publications

- *Government Computer News*
- *Government Security News*
- *Federal Computer Week*
- *Homeland Defense Journal*
- *Government Security*
- *Government Technology*
- *Washington Technology*
- *Access Control & Security Systems*
- *Defense News*
- *eWeek*
- *Federal Times*
- *Government Executive*
- *Government Leader*
- *Homeland Security Today*
- *Information Week*
- *InfoWorld*
- *ITSecurity*
- *National Defense*
- *SIGNAL*
- *URISA Journal*

Websites

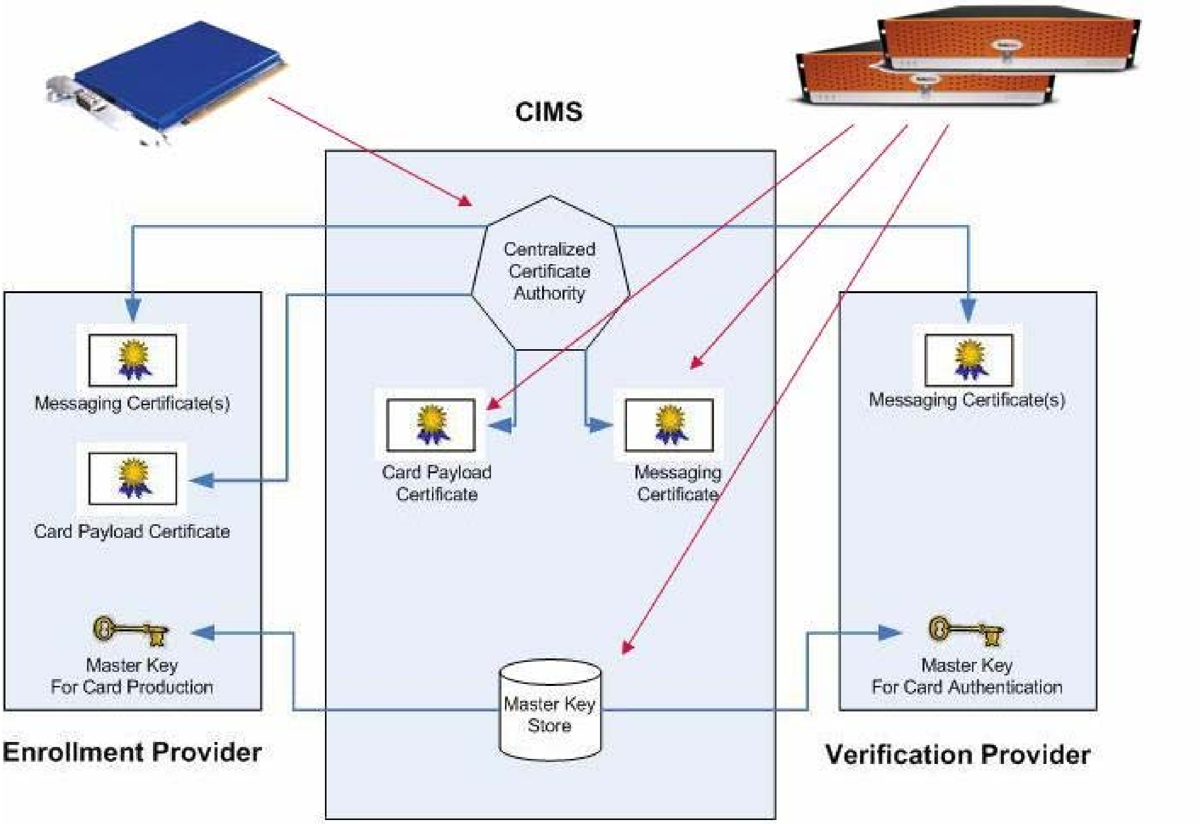
- www.einnews.com/news-Government-Politics
- www.INPUT.com
- www.gnn.gov.uk

Trade Shows

- NALA
    - Identity Protection & Management Conference 2007 – 4/16-4/20 – Dallas
    - Biometrics Technology Expo 2007 – 9/11-9/13 – Baltimore
    - Federal Information Security Conference (FISC) - 8/1-8/2, Colorado Springs
    - Dept. of Homeland Security Exposition – Date TBD
    - Federal Information Assurance Conf – www.fbcinc.com show – date TBD
    - NIST PKI R&D Workshop: Applications-Driven PKI – 4/17-4/19 – Gaithersburg
    - NIST IT Security Day – 4/10 – Gaithersburg
- APAC
    - Government Tech NZ – 8/20-8/22 – New Zealand

Common Government Applications for HSMs

Secure Biometric Clearing Network



For the highest level of security available to protect America's transportation system, SafeNet provided a key management and cryptographic acceleration solution. A dedicated SafeNet Luna SA HSM is used to secure the highly sensitive Root Certification Authority. Two additional SafeNet Luna SAs are used to secure other critical cryptographic keys, including the Subordinate Certification Authorities, XML, and SSL encryption keys, and other application-specific keys. The network-attached HSMs are configured in a cluster to provide high-availability to meet the necessary SLAs, as well the current performance requirements. This architecture provides scalability for future performance needs as the system grows.

The SBCN CIMS architecture uses PKI certificates for authentication, digital signature, non-repudiation, and data encryption. SafeNet HSMs and Security Consulting Services helped SBCN deploy a multi-tiered Certification Authority with Microsoft Certificates Services in less time than it would have taken to outsource it, and at a lower cost, all while meeting the strict security requirements imposed by the Transportation Security Administration. The CIMS architecture requires the use of SSL for securing data in motion. Both the initiator and the responder must verify each others identity when establishing this connection. Certificates are issued to each Service Provider for this purpose and are presented whenever attempting to establish a secure connection. SafeNet HSMs are used by CIMS to issue and store these SSL certificates. The CIMS security architecture requires that all sensitive data that is exchanged between system components be encrypted to prevent leakage of sensitive or personal information. SafeNet HSMs are used by CIMS to issue and store XML encryption certificates, and to encrypt and decrypt the XML data fields.

HSM Solutions for the Healthcare Vertical

Market Drivers

- Privacy
  - Internal Driver- push from within to strengthen security
  - External Driver- breaches in current security raise publicity and create external push to improve data security and privacy protection.

- Mandates
  - SAFE- Industry
  - HIPAA- Government

Types of Organizations

- Pharmaceutical Companies
- Hospitals
- Insurance Providers

Sample Applications

- Database encryption
- Smartcard issuance
- Root key protection
- Digital signatures
- Certificate validation
- Document rights management

Healthcare Industry Associations

Trade Organizations/Associations

- International
  - SAFE BioPharma Association - www.safe-biopharma.org
  - HIMSS -Healthcare Information and Management Systems Society – www.himss.org
  - Bio IT Coalition.org – www.bioitcoalition.org
  - AAMI - Association for the Advancement of Medical Instrumentation - www.aami.org
  - ABC - Association of Biotechnology Companies
  - Biotechnology Industry Organization - www.bio.org
  - IFPMA - International Federation of Pharmaceutical Manufacturers Associations - www.ifpma.org
- NALA
  - AMA – American Medical Association - www.ama-assn.org
  - ACIL -American Council of Independent Laboratories - www.acil.org
  - AAPS - American Association of Pharmaceutical Scientists - www.aapspharmaceutica.com
- EMEA
  - ABPI - Association of British Pharmaceutical Industries - www.abpi.org.uk
  - EFPIA – European Federation of Pharmaceutical Industries and Associations www.efpia.org
- APAC
  - KPMA - Korea Pharmaceutical Manufacturers Association - www.kpma.or.kr/kpma/ENG/greeting.asp
  - JPMA – Japan Pharmaceutical Manufacturers Association www.jpma.or.jp/english

Publications

- *Pharmaceutical Technology*
- *Healthcare Finance News*
- *Healthcare IT News* e-newsletter
- *Medical Design Technology Magazine* -www.mdtmag.com
  Medical Device Technology – www.devicelink.com/mdt -for European medical product designers

Websites

- www.safe-biopharma.org
- www.bioitcoalition.org
- www.pharmaceuticalonline.com
- www.pharmaceutical-drug-manufacturers.com
- www.pharmabiz.com - India

Trade Shows

- NALA
  - Interphex – 4/24-4/26 NYC
  - Bio IT World Conference and Expo - www.bio-itworldexpo.com 4/30 – 5/2 Boston

HSM Solutions for the Technology Vertical

Market Drivers

- Privacy
  - Internal Driver- push from within to strengthen security
  - External Driver- breaches in current security raise publicity and create external push to improve data security and privacy protection.

- Mandates
  - SOX

Types of Organizations

- Wireless Communication Providers
- IP Telephone
- High Tech Mfg
- Storage Providers
- Network Equipment Manufacturers
- Identity Stamping Devices

Sample Applications

- Database encryption
- Smartcard issuance
- Root key protection
- Certificate validation
- Document signing
- Electronic funds transfer
- Document rights management
- SSL web and application servers
- Time stamping
- Code signing
- Trusted manufacturing
- Gaming

Technology Industry Associations

Trade Organizations/Associations

- International
  - Software Developer, Publisher and Author Trade Organizations can be found at- www.softwaremarketingresource.com/tradeorganizations.html
  - SIIA – Software and Information Industry Association - www.siia.net
  - AISIP - Association of Independent Software Industry Professionals - www.aisip.com – member list
  - IEEE - Institute of Electrical and Electronics Engineers, Inc. – www.ieee.org
  - ISSA - Informatin Systems Security Association - www.issa.org
  - InfiniBandta.org - www.infinibandta.org
  - ISACA - Information Systems Audit and Control Association - www.isaca.org
  - ITGI - IT Governanace Institute - www.itgi.org
  - (ISC)2 - International Information Systems Security Certification Consortium - www.isc2.org
  - GSMA- GSM Association- www.gsmworld.com

Publications

- *SC Magazine*
- *IT News*
- *Network Computing*
- *TechNet Mag*
- *ITDefense*
- *Modern Applications News*
  Information Security Magazine
- *Software Business eNewsletter*

Websites

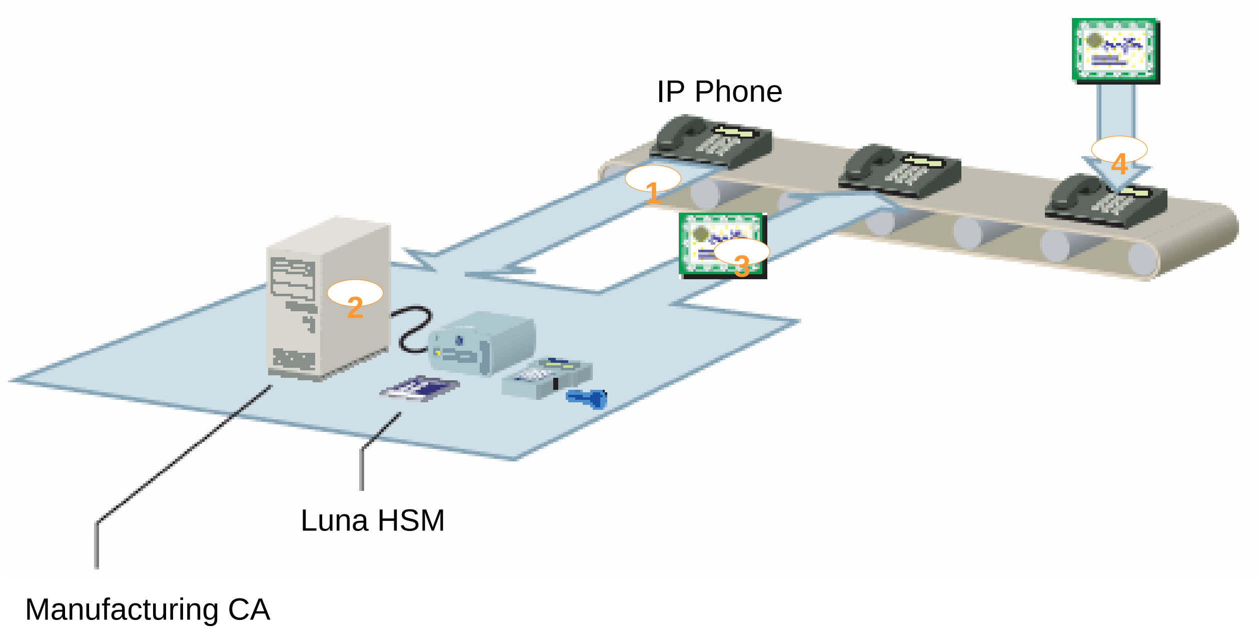
- www.computer.org
- www.infiniBandta.org
  www.searchsecurity.com – same as www.techtarget.com
- www.itsecurity.com
- www.itsecuritysource.com
- www.softwarebusinessonline.com
- Certified Information Systems Security Professionals - www.cissps.com - Web Portal

Trade Shows

- NALA
  - Sys Admin Technical Conf. 5/7-5/8 – Baltimore
  - Information Security Decisions Conf. 11/5-11/7 – Chicago
- APAC
  - Japan Computerworld

Common Technology Applications for HSMs

Manufacturing PKI for Cisco IP Phones



(1) The IP phone requests a certificate from the manufacturing certificate authority. (2) The certificate authority generates a new certificate that the Luna HSM signs with the root key. (3) The certificate is sent to the IP phone. (4) The IP phone now has a unique digital identity that is stamped into the phone by Cisco's.

Technical HSM Applications by Vertical- Customer Overview

FINANCIAL SERVICES		
Business Driver	**Company**	**Technical Application**
-Privacy -Security Breach -Industry Mandates (PCIDSS) -FIPS/CC	Federal Reserve Bank, Citibank, TD Bank, Barclays	Root Key Protection
	Bank of Canada	EFT
	UBS	Document Signing, Document Rights Management, SSL Web and App Servers
	Egg Bank	Web Services XML
	Bank of Central Asia, Westpac	Bank Pin Mgmt
	NCR (E-check)	Time stamping

TECHNOLOGY		
Business Driver	**Company**	**Technical Application**
-Security Breach -Local Regulations -FIPS/CC	Cisco	Root Key Protection Certificate Validation
	Adobe, Verisign, Entrust, Symantec	Root Key Protection
	Penn State, University of Chicago	Document Signing Document Rights Mgmt
	Partnership: Protegrity, Oracle	Database Encryption
	G&D, Active Identity	Smartcard Issuance
	Symantec, Verisign.	SSL Web & App Serv
	RIM, Motorola, Symante, Verisign	Code Signing
	T-Mobile	Web Services XML
	Cisco IP Phones & Scientific Atlanta Cable Modems	Trusted Mfg
	Sony	Gaming

GOVERNMENT		
Business Driver	**Company**	**Technical Application**
-Government Mandate (HSPD-12) -Security Breach -FIPS/CC	US DoD, Cdn Dnd, State Dept, NASA, DEA, State of Illinois, SSA, US Marines, White House,	Root Key Protection
	FRB, Reserve Bank of India	EFT
	Government Printing Office	Document Signing
	Protegrity and Oracle Partnership	Database Encryption
	FRB & DoD	Smartcard Issuance
	DoD	Certificate Validation
	Government Printing Office	Document Rights Mgmt
	Several EMEA countries with Authentidate & UPS	Time stamping
	US Fed, Aus Government (14 Countries)	E-Passport
	Westlotto; Lottery Hamburg	Gaming

HEALTHCARE		
Business Driver	**Company**	**Technical Application**
-Industry Mandate (SAFE) -Security Breach -Government Mandate (HIPAA) -FIPS/CC	P&G, Merck, Novartis,Bayer	Root Key Protection
	SAFE	Document Signing & Document Rights Mgmt
	Protegrity and Oracle Partnership	Database Encryption
	P&G	Certificate Validation

SafeNet®
The Foundation of Information Security