SafeNet

THE
DATA
PROTECTION
COMPANY

Security in Mumbai CTS

Ruchin Kumar

Security Evangelist – India & SAARC

18th Jan 2013

Benefits of Public Key Cryptography

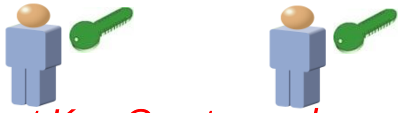
- **Entity Authentication** – Validates the identity of machines and users.
- **Data Confidentiality** – Encodes data to ensure that data cannot be viewed by unauthorized users or machines.
- **Data Integrity** – Protect data to ensure that data cannot be alter by unauthorized users or machines.
- **Digital Signature** – Provides the electronic equivalent of a hand-written signature
- **Non Repudiation** – Ensures that communications, data exchanges, and transactions are legally valid and irrevocable.

Not other security technologies or standards available today can provide the same level of benefits as PKI.

Public Key Cryptography

- Based on two mathematically related keys – commonly known as public key and private key
- Public key is published and known to everyone while private key is kept secret to oneself
- Based on mathematic problem – given a public key, it is mathematically difficult to derive the corresponding private key
- Based on mathematic relationship –
  - whatever that is encrypted by the public key can only be decrypted by the private key
  - whatever that is decrypted by the private key can only be encrypted by the public key

- Advantages of Public Key vs Secret Key Cryptography
  - Resolve key distribution issues since no one share the same secret key

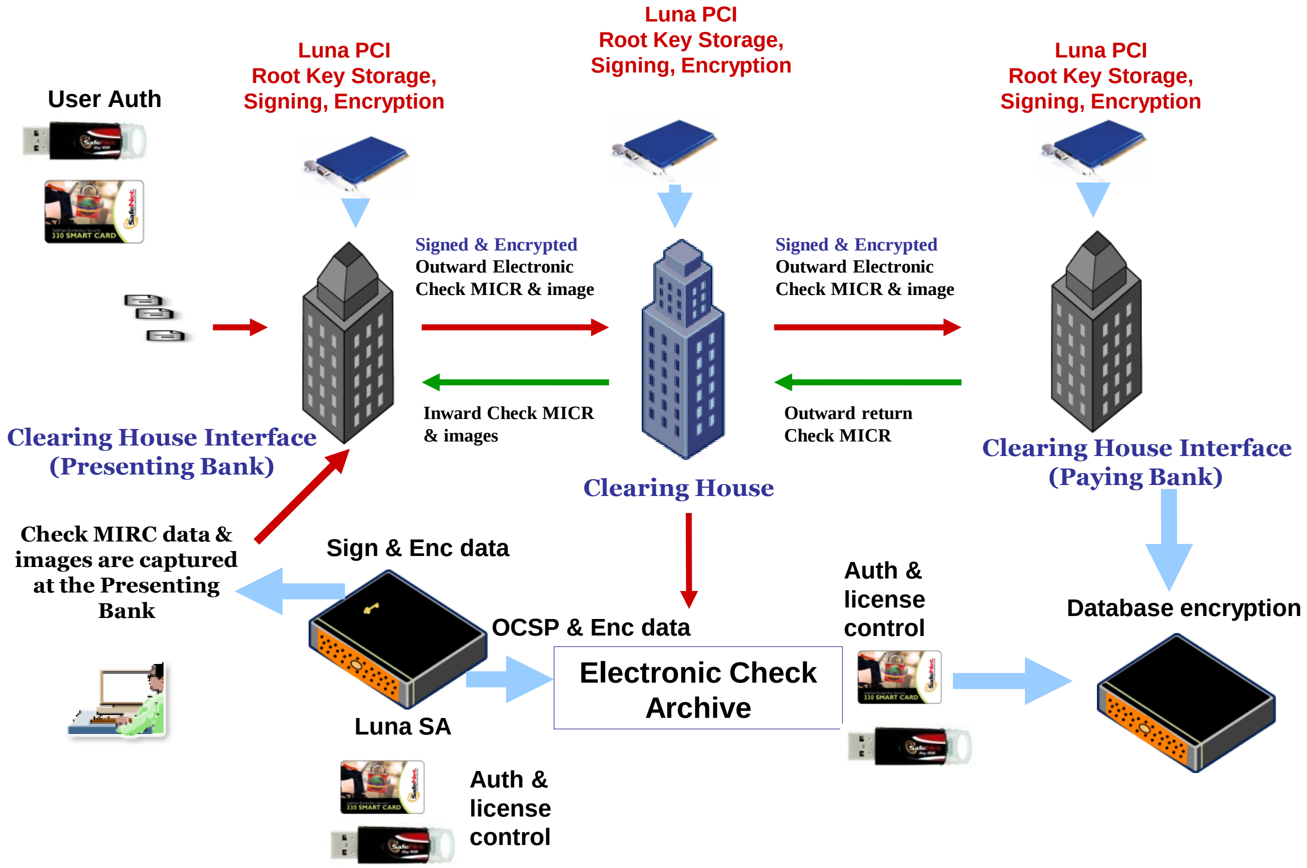


Secret Key Cryptography –
sender and recipient hold the same key

Public Key Cryptography -
sender and recipient each hold a pair of public/private key

Cheque Clearing Process

Embedded Example



User Auth

Luna PCI
Root Key Storage,
Signing, Encryption

Luna PCI
Root Key Storage,
Signing, Encryption

Luna PCI
Root Key Storage,
Signing, Encryption

Signed & Encrypted
Outward Electronic
Check MICR & image

Signed & Encrypted
Outward Electronic
Check MICR & image

Inward Check MICR
& images

Outward return
Check MICR

Clearing House Interface
(Presenting Bank)

Clearing House

Clearing House Interface
(Paying Bank)

Check MIRC data &
images are captured
at the Presenting
Bank

Sign & Enc data

OCSP & Enc data

Auth &
license
control

Database encryption

Electronic Check
Archive

Luna SA

Auth &
license
control

security perspective

- Proof of endpoints
- Unique sequence numbering
- Encryption
- Authentication
- Integrity
- duplicate detection
- digital signature based non-repudiation of both source and origin
- complete, secure audit trail.

Security for the CTS Solution

- Large amount of data to be processed at CH
- Heavy digital signings/hr is required at CH.
- All the data traveling between CHI-CLHS should be encrypted.
- High availability so each application server need to be equipped with a crypto module.
- Key management requirements for all individual banks.

Value of
Hardware Security Module (HSM)
in PKI

Role of HSM in PKI

Luna PCI

- HSM
  - manages the lifecycle of private key securely
  - provides multilevel role-based authentication
  - provides two factor authentication using token plus PIN
  - accelerates cryptographic process
  - offloads burden from application server
  - backups and restores root/private keys securely
  - provide high assurance level with FIPS 140 level 2 or level 3 validation

Luna PCI helps in Symmetric Encryption

- For encrypting the data a session key is generated, which is used to encrypt the data to be sent to recipient.
- Symmetric key is also encrypted using the public key of recipient and attached with the encrypted data.
- The session key can be generated on HSM if parameters are passed accordingly in the application.
- Luna PCI 7000 is having an onboard accelerator for doing symmetric encryption using this session key

Deployment Scenario in CTS

- Server running a CHI will have the Luna PCIe HSM
- Keys will be generated onboard inside the temper resistant HSM
- Certificate request or the certificate from old
- Digital Signing of the images and other instruments will be done inside the secure boundaries of HSM
- Keys inside the HSM will be never exposed in the S/W
- Backup is done from secure H/W HSM to secure H/W HSM
- Remote backup is possible

Deployment Scenario in CTS Contd..

- 2 Luna PCI for the cluster servers at production site
- 1 Luna PCI for the DR CHI
- 1 Remote backup HSM to ensure backup is securely done from H/W to H/W from any centralized location.
- Software development kit

ashesh.thanawala@safenet-inc.com

9820193422