Hardware Security Modules

SecAppDev 2009

F. Demaertelaere
Let’s introduce myself…

Filip Demaertelaere

>>>>> Head of Service Data Encryption Peripheral (DEP) <<<<<
Head of End-to-End Security
T&P/ENG/DEP - T&P/ENG/ES - Atos Worldline SA/NV
filip.demaertelaere@atosorigin.com
Phone: +32 (0)2 727 61 67
GSM: +32 (0)495 59 69 05
Fax: + 32 (0)2 727 62 50
DEP Hotline: dep.hotline-atosworldline@atosorigin.com
Atos Worldline is an Atos Origin company: www.atosworldline.be
Haachtsesteenweg 1442 Chaussée de Haecht- 1130 Brussels Belgium
Agenda (1)

- Cryptography: a short history
- HSM
  - Definition
  - Why?
  - Form factors
  - Application areas
  - Typical configuration
  - Tamper security
  - Logical security
  - Cryptography
  - Random generators
Agenda (2)

- HSM
  - Performance ideas
  - Key management
  - Standard interfaces/APIs
  - Standards/certifications
  - FIPS 140-2
  - Common Criteria
  - PCI HSM
  - Manufacturers

- Q&A
Cryptography - Short History (1)

- Classical Cryptography
  - 3300 BC, Sumer: first writing system: Cuneiform script

- 1600 BC, Irak: the oldest cryptographical «document» ever found, a jar!
Cryptography - Short History (2)

- Classical Cryptography
  - 1000 BC, Greece: transposition ciphers (change order of characters) with the scytale (Plutarque’s stick)
    
    WE ARE DISCOVERED FLEE AT ONCE
    
    W R I O R F E O E
    E E S V E L A N J
    A D C E D E T C X

- 600 BC, Hebrew: substitution ciphers (change characters)
  
  WE ARE DISCOVERED FLEE AT ONCE
  
  VA ZOA RFPBLUAOAR SIAA ZQ LKBA
  
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
  
  ZEBRASCDFGHJKLMNOPQRSTUVWXYZ
Cryptography - Short History (3)

- Classical Cryptography
  - 100 BC, Caesar’s ciphers
    
    \[ E_n(x) = (x + n) \mod 26. \]
    \[ D_n(x) = (x - n) \mod 26. \]

- Medieval, Substitution with multiple substitution alphabets
  
  WE ARE DISCOVERED FLEE AT ONCE
  
  YG CTG FHUEQXGTF HNGG CV QPEG

  WEAREDISCOVEREDFLEEATONCE
  LEMONLENONLENONLENONLENON
  HIMFRO...
Cryptography - Short History (4)

- Enigma Cipher Machine, 1920, Arthur Scherbius (World War II):
  Polyalphabetic substitution (continually changing substitution alphabet)
Cryptography and HSMs

- What have we learned?
  
  **Cryptography uses SECRET keys**

- So we need something to protect these keys...
  
  **A Hardware Security Module**
HSM – Definition (1)

- **HSM**
  - Hardware Security Module
  - Host Security Module

- **Definition**
  - Black box combination hardware and software/firmware
  - Attached (or inside) a PC or server
  - Provides cryptographic functions
  - Physical/logical tamper protection (security)
  - (Increased performance)
HSM – Definition (2)

- **Purpose**
  - (1) Secure generation (and entry)
  - (2) Secure storage (and backup)
  - (3) Secure use (i.e. cryptographic algorithms)
  - Of cryptographic and sensitive data material
  - Note: HSM never allows plaintext key export!

- **Other names**
  - PCSM – Personal Computer Security Module
  - SAM – Secure Application Module
  - SCD – Secure Cryptographic Device
  - SSCD – Secure Signature Creation Device
  - Hardware Cryptographic Device, Cryptographic Module…
HSM – Why?

SECURITY SECURITY SECURITY SECURITY

PERFORMANCE PERFORMANCE SECURITY SECUTRY

SECURITY PERFORMANCE SECURITY
HSM – Form Factors

- SafeXcel IP - Trusted Module
- Silicon and Software IP
- Trusted Chips
- Portable and Economical
- Offline Key Archive
- Perfect for OEMs
- Networked, Scaleable
HSM – Definition

- HSM
  - Hardware Security Module
  - Host Security Module

- Definition
  - Black box combination hardware and software/firmware
  - Attached (or inside) a PC or server
  - Provides cryptographic functions
  - Physical/logical tamper protection (security)
  - (Increased performance)
HSM – Typical Configuration (1)
HSM – Typical Configuration (2)
HSM – Application Areas (1)

- PKI Environments
  - Certification Authority (CA) and Registration Authority (RA)
  - Generate, store and handle key pairs

- Card Payment Systems
  - Authentication and integrity checking of messages
  - Confidentiality (e.g. PIN)
  - On-line PIN verification
  - Checking card security codes
  - Re-encryption of PIN blocks
  - Card creation: PIN mailers, generation of magnetic stripe data, personalization of chip cards
  - E-commerce and M-commerce
  - Home banking
HSM – Application Areas (2)

- Others
  - Key Distribution Centers
  - SSL connectivity
  - PayTV
  - Access control: one time passwords, user authentication
  - (Qualified) Digital signatures
  - Time-stamping
  - Trusted Platform Modules (TPM)
  - Document protection
  - Army
HSM – Application Areas: Card Production

Data Generation

PIN Distribution

Card Personalization

An Atos Origin Company
HSM – Application Areas: Key Distribution

Key Generation

Acquiring System

(Derived) Keys

(Derived) Keys
HSM – Application Areas: Card Payment

- VPN Router
- Dedicated network
- TELCO System
- Issuing System
- Open network
- EPIN Transaction Data
- EPIN Transaction Data
- EPIN Transaction Data
- TELCO network
- VISANET/EPSONET/EUFISERV/...
HSM – Definition

- **HSM**
  - Hardware Security Module
  - Host Security Module

- **Definition**
  - Black box combination hardware and software/firmware
  - Attached (or inside) a PC or server
  - Provides cryptographic functions
  - **Physical/logical tamper protection (security)**
  - (Increased performance)
HSM – Tamper Security (1)

- Tamper security terminology
  - Tamper Evidence
    - Unauthorised access to the protected object is easily detected
    - E.g. tamper seals, tamper stickers
  - Tamper Detection and Responsiveness
    - Automatic action by the protected object when a tamper has been detected (Tamper Detection) by the protected object itself
    - E.g. temperature sensors
  - Tamper Resistance
    - Resistance to tampering by normal users or others with physical access to the protected object
    - E.g. special screws
HSM – Tamper Security (2)

- Tamper security in HSM
- Opaque epoxy
- Wiring
  - Detection of mechanical penetration
  - Detection of chemical penetration
- Temperature manipulation
  - Low: freezing (liquid nitrogen) memory attack
  - High: guarantee correct working
- Voltage variation
- Movement
- Light sensors
HSM – Tamper Security (3)

- **Zeroization**
  - Definition: erase sensitive data and secret keys after Tamper Detection
  - Data remainance: residual representation of data that has been in some way nominated erased or removed
  - HSM requires active erasure of all memory containing sensitive data and secret keys
    - Fast!
    - Overwrite memory: zeroes, random or combination
HSM – Logical Security (1)

- Software/Firmware update: integrity and authentication
- Access control: grant access to functions with
  - Count limit
  - Time limit
  - No limit
- Real time clock: accuracy
- Communication: host authentication
- Logical HSM partitions
- Audit trails
HSM – Logical Security (2)

- Side Channel Attacks: attacks based on side channel information
- Timing Attacks: based on measuring the time it takes for the HSM to perform an operation
- Power Consumption Attacks: attacks based on analyzing the power consumption of the HSM during encryption operations
  - SPA (Single Power analysis): visual representation of the power consumption
  - DPA (Differential Power Analysis): statistical analysis of the power consumption
- Fault Analysis Attacks: investigate ciphers and extract keys by generating faults
HSM – Definition

- HSM
  - Hardware Security Module
  - Host Security Module

- Definition
  - Black box combination hardware and software/firmware
  - Attached (or inside) a PC or server
  - Provides cryptographic functions
  - Physical/logical tamper protection (security)
  - (Increased performance)
HSM – Cryptography (1)

- Cryptography mostly accelerated by hardware accelerators (performance)
- Symmetric cryptography
  - (T)DES, AES
  - Key generation
  - Encryption/decryption
  - Message Authentication Code
- Asymmetric cryptography
  - RSA, ECC
  - Key generation
  - Data signing (optionally verification)
  - Data decryption
HSM – Cryptography (2)

- Hashing
  - SHA-1, SHA-2, MD5
  - Mostly integrated in other cryptographic functions such as data signing

- Random generator
  - True random generator
  - Pseudo random generator
HSM – Random Generators (1)

- True random generator
  - Undeterministic
  - Uses physical processes which are unpredictable, as far as known ("Noice"), e.g. mouse movements, keyboard input, ...
  - (FIPS) outside human control
  - FIPS 140-2: No approved true random number generator

- Pseudo random generator
  - Deterministic
  - Uses computational algorithms (e.g. cryptographic algorithms) that produce long sequences of apparently random results
  - Initiated by a short initial value ("Seed")
  - E.g. (FIPS 140-2) NIST Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using 3-Key Triple DES and AES Algorithms
HSM – Random Generators (2)

- Statistical tests
  - Define the quality of random numbers

- Tests
  - FIPS 140-2
    - Undeterministic: no approved
    - Deterministic: known-answer-tests (KAT)
  - Diehard measures quality of set of random numbers
HSM – Definition

- HSM
  - Hardware Security Module
  - Host Security Module

- Definition
  - Black box combination hardware and software/firmware
  - Attached (or inside) a PC or server
  - Provides cryptographic functions
  - Physical/logical tamper protection (security)
  - *(Increased performance)*
HSM – Performance Ideas

- Almost no public information available
  - Internal versus external
  - Cryptographic module versus ethernet box
  - Asynchronous or synchronous
  - No raw cryptography
  - Optimal situations

- RSA 1024 bit Private Key operation: 100 – 7000 operations/second
- ECC 160 bit ECDSA signatures: 250 – 2500 operations/second
- 3DES: 2 - 8 Mbytes/second
- AES: 6 - 40 Mbytes/second (256 bit key)
ISO-11770: Information Technology – Security Techniques - Key Management

Key generation (random generation!!):
- Cleartext keys stored inside HSM protected memory («key storage»)
- Special key properties:
  - (T)DES: weak/semi-weak keys and parity bits!
  - RSA: prime number generation, output Public Key

Output for key exchange:
- Key components (XOR2/XOR3)
- Secret sharing
- Key cryptogram (transport key)

(Manual) key entry
- Key components (XOR2/XOR3)
- Secret sharing
- Key cryptogram (transport key)
HSM – Key Management (2)

- Key storage/backup
- Key space backup: backup of complete key space guaranteeing the confidentiality and integrity of the whole backup
- Individual key storage: cryptograms with confidentiality & integrity protection

<table>
<thead>
<tr>
<th>Date</th>
<th>Min. of Strength</th>
<th>Symmetric key algorithms</th>
<th>Asymmetric</th>
<th>Discrete Logarithm Key</th>
<th>Elliptic Curve</th>
<th>Hash (A)</th>
<th>Hash (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009 to 2010</td>
<td>80</td>
<td>2TDEA*</td>
<td>1024</td>
<td>160</td>
<td>1024</td>
<td>160</td>
<td>SHA-1**,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-224</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-256</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-384</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-512</td>
</tr>
<tr>
<td>2011 to 2030</td>
<td>112</td>
<td>3TDEA</td>
<td>2048</td>
<td>224</td>
<td>2048</td>
<td>224</td>
<td>SHA-224</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-256</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-384</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-512</td>
</tr>
<tr>
<td>&gt; 2030</td>
<td>128</td>
<td>AES-128</td>
<td>3072</td>
<td>256</td>
<td>3072</td>
<td>256</td>
<td>SHA-256</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-224</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-384</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-512</td>
</tr>
<tr>
<td>&gt;&gt; 2030</td>
<td>192</td>
<td>AES-102</td>
<td>7680</td>
<td>384</td>
<td>7680</td>
<td>384</td>
<td>SHA-384</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-512</td>
</tr>
<tr>
<td>&gt;&gt;&gt; 2030</td>
<td>256</td>
<td>AES-256</td>
<td>15360</td>
<td>512</td>
<td>15360</td>
<td>512</td>
<td>SHA-384</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SHA-512</td>
</tr>
</tbody>
</table>
HSM – Key Management (3)

- Key management devices: direct connection to cryptographic hardware (trusted path)
HSM – Standard Interfaces/API

- Standard API defining generic interfaces to cryptographic tokens (e.g. HSM)
- Goal: applications independent from HSMs
- Interfaces:
  - PKCS #11 (Public Key Cryptography Standards) (also «cryptoki»)
  - MSCAPI (Microsoft Cryptography API)
  - JCE (JAVA Cryptographic Engine)
- Examples of applications using PKCS#11:
  - Mozilla Firefox/Thunderbird
  - OpenSSL
  - OpenVPN
  - …
ISO-13491-1:2007 Banking – Secure Cryptographic Devices
- Specifies Requirements for Secure Cryptographic Devices
- Based on cryptographic processes defined in
  - ISO-9564: Banking – Personal Identification Number
  - ISO-16609: Banking – Requirements for Message Authentication
  - ISO-11568: Banking – Key Management

Protection Profile – Secure Signature Creation Device
- BSI-PP-0004-2002T 03.04.2002 – Type1
- BSI-PP-0005-2002T 03.04.2002 – Type2
- BSI-PP-0006-2002T 03.04.2002 – Type3
HSM – Standards / Certifications (2)

- Certifications:
  - FIPS 140-2; FIPS 140-3 (draft)
  - Common Criteria (CC)
  - PCI HSM (draft) from PCI SSC (Payment Card Industry Security Standards Council)
  - Local certifications: MEPS, ZKA, …
HSM – FIPS 140-2 (1)

- FIPS
  - Federal Information Processing Standard
  - US government computer security standard
  - Used to accredit cryptographic modules
  - Issued by NIST (National Institute of Standards and Technology)
  - Cryptographic Module Validation Program (CMVP)

- Security levels
  - Level 1: no specific physical security mechanisms
  - Level 2: tamper evidence requirement
  - Level 3: high probability of detecting and responding to attempts of physical access
  - Level 4: complete envelop of protection with the intent of detecting and responding to all unauthorized attempts of physical access
Requirement areas (11) for cryptographic modules

- Specifications: what has to be documented
- Parts/interfaces: which in/out information flows and how it must be segregated
- Roles, services and authentication: who can do what and how it is checked
- Final state model: documentation of high level states and transitions
- Physical security: tamper evidence/respondiveness/resistance
- Operational environment: which operating system
- Cryptographic key management: generation, entry, output, storage and destruction of keys
- EMI/EMC (Electromagnetic Interference/Compatibility)
- Self-tests: what must be tested and when; what when a test fails
- Design assurance: information to be provided
- Mitigation of other attacks: how it is done
HSM – FIPS 140-2 Certification Process

General Flow of FIPS 140-2 Testing and Validation

1. Vendor selects a lab; Submits module for testing; Module IUT
2. NVLAP Accredited FIPS 140-2 CMT Lab
   - Test for conformance to FIPS 140-2; Writes test report
   - CMT Test Report to NIST/CSE for validation; Module Review Pending
3. NIST/CSE
   - NIST submits comments from test report to lab for resolution
4. Lab submits questions for guidance and clarification
   - NIST/CSE issue testing and implementation guidance
5. List of Validated FIPS 140-2 Modules
   - Finalization; NIST adds module to validated modules list at www.nist.gov/cmvp

Cryptographic Module Vendor
- Issue validation certificate (via lab to the vendor)
- Cost Recovery Fee Received Prior to Validation
- Reviewer Assigned Module Under Review
HSM – Common Criteria (1)

- CC
  - Common Criteria for Information Technology Security Evaluation (evaluation methodology)
  - No security levels (FIPS), but Evaluation Assurance Levels (EAL1-EAL7)
  - National certification bodies with Common Criteria Recognition Agreement (CCRA)
  - Definition of security in Security Target (ST)
HSM – Common Criteria (2)

- 7 Classes
  - ACM – Configuration Management
  - ADO – Delivery and Operation
  - ADV – Development
  - ADG – Guidance documentation
  - ACL – Lifecycle support
  - ATE – Tests
  - AVA – Vulnerability Analysis
HSM – PCI HSM

- PCI SSC = VISA, MASTERCARD, JCB, AMEX, DISCOVERY
- Range of end-to-end security requirements: PCI PED, PCI UPT, PCI DSS, PCA PA DSS, PCI PIN and... PCI HSM
- Still draft
- Based upon FIPS, including payment functionality
- Own certification scheme
HSM – Manufacturers (1)

- Atos Worldline SA/NV
- Safenet
- Bull
- IBM
HSM – Manufacturers (2)

- Ncipher (now Thales)
- Utimaco
- Thales
- ARX
Filip Demaertelaere
Head of Service Data Encryption Peripheral (DEP)
Head of End-to-End Security
T&P/ENG/DEP - T&P/ENG/ES - Atos Worldline SA/NV
filip.demaertelaere@atosorigin.com
Phone: +32 (0)2 727 61 67
GSM: +32 (0)495 59 69 05
Fax: + 32 (0)2 727 62 50
DEP Hotline: dep.hotline-atosworldline@atosorigin.com
Atos Worldline is an Atos Origin company: www.atosworldline.be
Haachtsesteenweg 1442 Chaussée de Haecht- 1130 Brussels Belgium