HSM
Hardware Security Modules

Jakob Schlyter – jakob@kirei.se
What is an HSM?
What is an HSM?

• Protected keystore
  ▸ Private keys can never be extracted in clear

• Crypto hardware
  ▸ Sometimes increases speed (but not always)

• Well-defined software interface
Protected Keystore

- Keys stored in tamperproof memory
  - If you mess with the chip, the device will (try to) detect it and zeroize

- Implemented using
  - Covering components in epoxy
  - Thin wires covering sensitive components
Crypto Hardware

- Hardware to assist accelerate symmetric and asymmetric crypto
  - RSA, DSA, AES, 3DES
- Good random number generator
- Hashing is often implemented in the host
API

- PKCS#11 (aka Cryptoki)
- OpenSSL Engine
- Microsoft CAPI
- Java Cryptography Extension
Stacked APIs are possible…
Why use a HSM?
What is the risk?

- Keys can be compromised by...
  - Compromised hosts
  - Disgruntled staff
  - Math
How do we lower the risk?

• Protect the host itself
  ▸ But some sort of remote management is usually needed anyway

• Protect the private keys
  ▸ Move keys to HSM
Residual risk

• Keys can still be misused
  ▸ If you can use a key, you can also misuse it

• Garbage in $\Rightarrow$ Garage out
  ▸ If you feed it a bad zone – the result is still a signed bad zone
Increase trust?

• Using an HSM increases trust – Why?
  ▶ Standards compliance
  ▶ Verifiable security – e.g. FIPS 140-2

• Also provides a clean cut between keystore and signing software
  ▶ You know where your keys are (and not are)
The Buyer’s Guide to Hardware Security Modules
Types of HSMs

- Local interface – e.g. PCI cards
- Remote interface – e.g. Ethernet
  - Sharable between multiple hosts
- Smart cards
- USB tokens
  - usually a smart card with integrated reader
Algorithms and key sizes

• What algorithms are supported
  ‣ RSA recommended, DSA optional

• What key sizes are supported
  ‣ Minimum key size $\leq 1024$ bits recommended
  ‣ Maximum key size $\geq 2048$ bits recommended
Capacity

• How many keys can be stored?
• Where are the keys stored?
  ▸ Internal keystore
  ▸ External keystore (encrypted by master key)
API

• What API do you need?
  ▸ PKCS#11, OpenSSL, MS-CAPI, JCE

• What platforms are supported?
  ▸ Mind details like Linux kernel versions, distributions etc.
Speed

• Signing speed – RSA
  ▶ Usually measured in 1024-bit signing operations (with public exponent 3 or 65537) per second.

• Key generation speed – RSA
  ▶ Usually the average key generation time for 1024-bit and 2048-bit keys per second.
Security Certifications

• FIPS 140-2
  ▸ Federal Information Processing Standard

• CC-EAL
  ▸ Common Criteria Evaluation Assurance Levels
## FIPS 140-2

<table>
<thead>
<tr>
<th>Level</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Basic security requirements</td>
</tr>
<tr>
<td>2</td>
<td>Tamper evidence, user authentication</td>
</tr>
<tr>
<td>3</td>
<td>Tamper detection/resistance, data zeroisation, splitting user roles</td>
</tr>
<tr>
<td>4</td>
<td>Very high tamper detection/resistance, Environmental protection</td>
</tr>
</tbody>
</table>
CC-EAL

- What Protection Profile (PP) has been used for the Target of Evaluation (ToE)?
  - CMCKG-PP – Key Generation
  - CMCSO-PP – Signing Operations
Key Backup

• How do you backup your keystore?
• Can you restore a backup elsewhere?
  ▸ e.g. on a hot-standby site
• Split key backup possible?
• Well-known backup format?
Examples of HSMs
### SCA 6000

**Sun Crypto Accelerator 6000**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>PCI-Express x8</td>
</tr>
<tr>
<td><strong>Certification</strong></td>
<td>FIPS 140-2 level 3</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>13,000 sign/s</td>
</tr>
<tr>
<td><strong>RSA-1024</strong></td>
<td></td>
</tr>
<tr>
<td><strong>System Support</strong></td>
<td>Solaris, Linux</td>
</tr>
<tr>
<td><strong>Approx price</strong></td>
<td>€ 960</td>
</tr>
</tbody>
</table>
## AEP Keyper 9720

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Ethernet</td>
</tr>
<tr>
<td>Certification</td>
<td>FIPS 140-2 level 4</td>
</tr>
<tr>
<td>Performance</td>
<td>1,200 sign/s</td>
</tr>
<tr>
<td>RSA-1024</td>
<td></td>
</tr>
<tr>
<td>System Support</td>
<td>Solaris, Linux, Windows</td>
</tr>
<tr>
<td>Approx price</td>
<td>€ 17,500</td>
</tr>
</tbody>
</table>
# IBM 4764 PCIXCC

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>PCI-X</td>
</tr>
<tr>
<td>Certification</td>
<td>FIPS 140-2 level 4</td>
</tr>
<tr>
<td>Performance</td>
<td>1,200 sign/s</td>
</tr>
<tr>
<td>RSA-1024</td>
<td></td>
</tr>
<tr>
<td>System Support</td>
<td>Solaris, Linux, Windows, AIX, i5/OS</td>
</tr>
<tr>
<td>Approx price</td>
<td>€ 6,600</td>
</tr>
</tbody>
</table>
## SoftHSM

<table>
<thead>
<tr>
<th></th>
<th>software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification</td>
<td>none</td>
</tr>
<tr>
<td>Performance</td>
<td>CPU-dependent</td>
</tr>
<tr>
<td>RSA-1024</td>
<td></td>
</tr>
<tr>
<td>System Support</td>
<td>Unix</td>
</tr>
<tr>
<td>Approx price</td>
<td>€ 0</td>
</tr>
</tbody>
</table>

*Note: Not really a HSM – just looks like one...*
Other vendors

- Thales (formerly nCipher)
  - netHSM, nShield
- SafeNet
  - Luna SP, Luna CA, Luna PCI
jakob@kirei.se