



# OpenDNSSEC Hardware Security Modules

**.se**



What is an HSM?

**.se**



# 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

**.se**



# 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

**.se**



# 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

**.se**

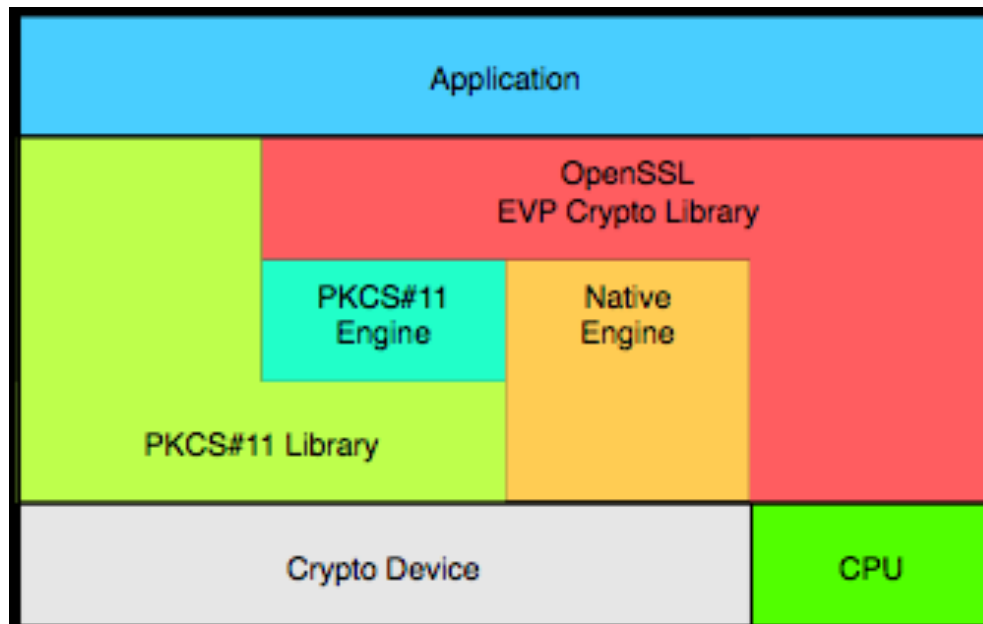


# API

- PKCS#11 (aka Cryptoki)
- OpenSSL Engine
- Microsoft CAPI
- Java Cryptography Extension

**.se**

# Stacked APIs are possible...



**.se**



# PKCS#11

E.g:

- C\_Initialize
- C\_GetSlotList
- C\_OpenSession
- C\_Login
- C\_GenerateKeyPair
- C\_FindObjectsInit, C\_FindObjects, C\_FindObjectsFinal
- C\_SignInit, C\_Sign
- C\_Finalize

**.se**





Why use an HSM?

**.se**



# What is the risk?

- Keys can be comprimised by...
  - Compromised hosts
  - Disgruntled staff
  - Math

**.se**



# 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

**.se**



# Residual risk

- Keys can still be misused
  - If you can use a key, you can also misuse it
- Garbage in -> Garage out
  - If you feed it a bad zone – the result is still a signed bad zone

**.se**



# 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)

**.se**



# The Buyer's Guide to Hardware Security Modules

**.se**



# 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

**.se**



# Algorithms and key sizes

- What algorithms are supported
  - RSA recommended, DSA and GOST optional
- What key sizes are supported
  - Minimum key size  $\leq 1024$  bits recommended
  - Maximum key size  $\geq 2048$  bits recommended

**.se**





# Capacity

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

**.se**



# API

- What API do you need?
  - PKCS#11, OpenSSL, MS-CAPI, JCE
- What platforms are supported?
  - Mind details like Linux kernel versions, distributions etc.

**.se**



# 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.

**.se**



# Security Certifications

- FIPS 140-2
  - Federal Information Processing Standard
- CC-EAL
  - Common Criteria Evaluation Assurance Levels

**.se**



# FIPS 140-2

Level	Requirement
1	Basic security requirements
2	Tamper evidence, user authentication
3	Tamper detection/resistance, data zeroisation, splitting user roles
4	Very high tamper detection/resistance, Environmental protection

**.se**



# CC-EAL

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

**.se**



# 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?

**.se**



# Examples of HSMs

**.se**



# SCA 6000

## Sun Crypto Accelerator 6000



Interface	PCI-Express x8
Certification	FIPS 140-2 level 3
Performace (RSA-1024)	13,000 sign/s
System support	Solaris, RHEL, SUSE
Approx price	€ 960

**.se**

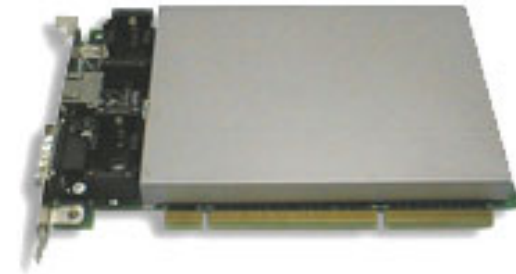
# AEP Keyper 9720



Interface	Ethernet
Certification	FIPS 140-2 level 4
Performace (RSA-1024)	1,200 sign/s
System support	Solaris, Linux, Windows
Approx price	€ 17,500

**.se**

# IBM 4764 PCIXCC



Interface	PCI-X
Certification	FIPS 140-2 level 4
Performace (RSA-1024)	1,200 sign/s
System support	Solaris, Linux, Windows, AIX, i5/OS
Approx price	€ 6,600

**.se**

# SoftHSM



Interface	Software
Certification	None
Performace (RSA-1024)	CPU-dependent
System support	UNIX
Approx price	Free

**.se**



# Other vendors

- Thales (formerly nCipher)
  - netHSM, nShield
- SafeNet
  - Luna SP, Luna CA, Luna PCI
- Aladdin eToken

**.se**



# Thank you

- Questions?

**.se**