HSM

Hardware Security Modules

Jakob Schlyter – jakob@kirei.se

kirei

What is an HSM?

kirei

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

kirei

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

kirei

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

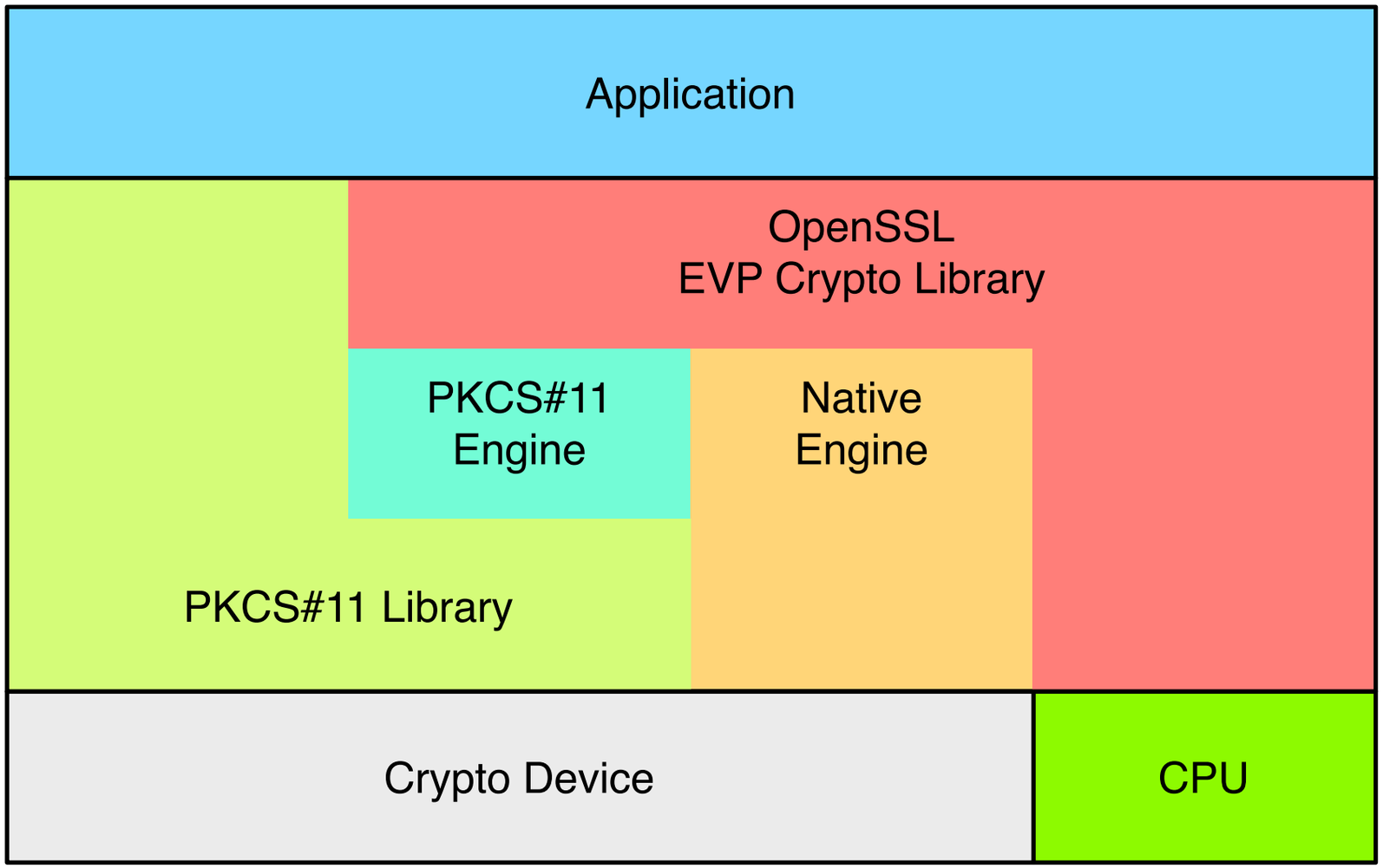
kirei

API

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

kirei

Stacked APIs are possible…



kirei

Why use a HSM?

kirei

What is the risk?

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

kirei

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

kirei

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

kirei

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)

kirei

The Buyer's Guide to Hardware Security Modules

kirei

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

kirei

Algorithms and key sizes

- What algorithms are supported
  - RSA recommended, DSA optional
- What key sizes are supported
  - Minimum key size ≤ 1024 bits recommended
  - Maximum key size ≥ 2048 bits recommended

kirei

Capacity

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

kirei

API

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

kirei

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.

kirei

Security Certifications

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

kirei

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, Enviromental protection

kirei

CC-EAL

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

kirei

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?

kirei

Examples of HSMs

kirei

SCA 6000

Sun Crypto Accelerator 6000

Interface	PCI-Express x8
Certification	FIPS 140-2 level 3
Performance RSA-1024	13,000 sign/s
System Support	Solaris, Linux
Approx price	€ 960

kirei

AEP Keyper 9720

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

kirei

IBM 4764 PCIXCC

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

kirei

SoftHSM

Interface	software
Certification	none
Performance RSA-1024	CPU-dependent
System Support	Unix
Approx price	€ 0

Note: Not really a HSM – just looks like one…

kirei

Other vendors

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

kirei

jakob@kirei.se

kirei