Network HSM Evaluation

DNS Working Group @ RIPE'62

Jakob Schlyter – jakob@kirei.se

Review performed by Certezza on commission from .SE.

Why?

- Assist in procurement process
- Encourage product development

Requirements & Scope

- Network connected appliance
- FIPS 140-2 level 3 (or better)
- Decent performance
- PKCS#11 interface

Vendors

- AEP Keyper v2

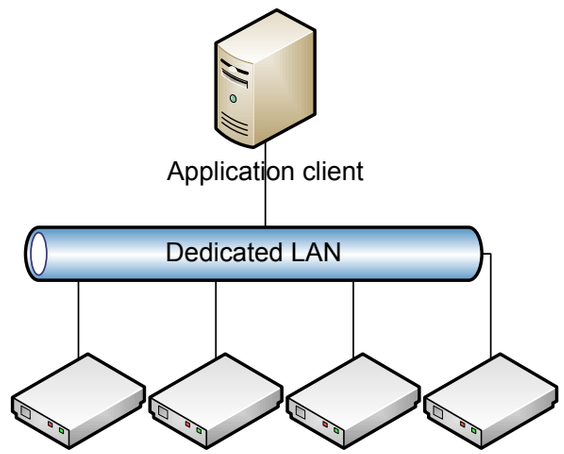
- Safenet Luna SA 4

- Thales nShield Connect

- Ultimaco CryptoServer Se1000

Test Setup & Tools

- All devices tested using
  - ods-hsmspeed
  - pkcs11-testing



- Test software available from the OpenDNSSEC code repository

Common Features

- Primary UI via front panel (no web GUI)
- Remote administration via CLI
- Role-based administration
- Smart card authentication

Results

Algorithm Support

Function	AEP Keyper	Safenet Luna	Thales nShield	Utimaco CryptoServer
AES*	128-256	128-256	128-256	128-256
AES modes	ECB,CBC,MAC	ECB,CBC,MAC	ECB,CBC,MAC	ECB,CBC,CTR,MAC
3DES modes	ECB,CBC,MAC	ECB,CBC,MAC	ECB,CBC,MAC	ECB,CBC,MAC
RSA	1024-4096	512-4096	1024-4096	512-8192
ECDSA	-	112-571	-	112-521
DSA*	512-4096	512-1024	512-2048	512-4096
ECDH*	-	112-571	-	112-521
SHA-1	SHA1	SHA1	SHA1	SHA1
SHA-2*	SHA256-SHA512	SHA256-SHA512	SHA256-SHA512	SHA256-SHA512
HMAC	SHA1	SHA1-SHA512, MD5	MD5	SHA1-SHA512, MD5

*Part of NSA Suite B [NSASuiteB]

Performance

Key size	AEP Keyper	Safenet Luna	Thales nShield	Utimaco CryptoServer*
1024	1020	7000	4375	2730
1536	580	1896	3560	1800
2048	410	1225	2760	1120
4096	23	45	410	260

Communication

- Supported operating systems
- Backup functionality
- Synchronization and clustering
- Network communication protocol

Security Features

- Certification levels
- Supported authentication methods
- Support for division of command (m-of-n)
- Remote administration
- Setup procedures
- Multiple security domains
- Time synchronization

Other Results

- Status and monitoring
  - Logging and auditing
  - SNMP
- Usability
  - Setup and ease of use
  - Software administration
  - Documentation

http://goo.gl/05rpM

Open
DNSSEC

www.opendnssec.org