HSM Buyers' Guide

On this Page

Introduction

The purpose of this document is to provide a set of guidelines for purchasing a Hardware Security Module (HSM) for use with OpenDNSSEC.

Types of HSMs

Hardware Security Modules come in a variety of shapes, forms and sizes:

- PCI cards
- Separate units that communicate via various channels (networks, SCSI, …)
- Smart cards
- USB tokens
- Software tokens
- etc.

The main purpose of a HSM is to safeguard cryptographic key material and/or to speed up cryptographic operations (a HSM can have either one or both of these purposes).

For the purpose of this document, HSMs are divided into four categories:

1. Software tokens

Characteristics of this category are:

- Low price (probably free)
- Almost unlimited storage capability
- Speed for cryptographic operations is limited by the computer hardware
- Lower security because the keys are not protected by hardware
- Can be used if an HSM is not necessary, or to set up a testbed before purchasing a real HSM

SoftHSM is an example of a software token. It is provided by OpenDNSSEC.

2. Low-cost small form-factor (smart cards and USB tokens)

Characteristics of this category are:

- Low price (sub €100/unit)
- Portable
- Limited storage capability for key material (less than 20 RSA key-pairs)
- Limited or no support for symmetric cryptographic algorithms
- Limited speed for cryptographic operations

3. Medium- to high-cost cryptographic accelerators (PCI cards/separate units)

Characteristics of this category are:

- Medium to high price (€2500 – €30000 per unit)
- Fixed location
- Emphasis is on acceleration of cryptographic operations not on key storage (typical product names: “SSL accelerator” or “Crypto accelerator”, etc.)
- High speed cryptographic operations both symmetric as well as asymmetric

4. Medium- to high-cost traditional hardware security modules (PCI cards/separate units)

Characteristics of this category are:

- Medium to high price (€2500 – €30000 per unit)
- Fixed location
- Large storage capability for key material (thousands of RSA keys or more)
- Cryptographic acceleration

Of these four types of HSMs, three types are suitable for use with OpenDNSSEC (types 1, 2, and 4). Type 3 HSMs (cryptographic accelerators) are less suited for use with OpenDNSSEC because they do not always provide the means to securely and efficiently store cryptographic key material.

Supported algorithms and key sizes

Most HSMs support both RSA as well as DSA key generation and signing. RSA is recommended for use with OpenDNSSEC. The RSA support should at least comply with the following guidelines:

- On-board key generation and key storage must be supported
- The minimum key size should be 1024 bits or less
- The maximum key size should be at least 2048 bits or more

DSA is not recommended for use with DNSSEC in general for the following reasons:

- The maximum key size is limited to 1024 bits
- Validation of DSA signatures requires significantly more processing than validation of RSA signatures, thus imposing additional load on validating resolvers.

APIs for access

Most HSMs will support one or more of the following APIs for access to their cryptographic functionality:

- PKCS #11
  This is an open standard from RSA laboratories. It is also known as “Cryptoki”.
- OpenSSL engine
  This is not really a standard, but more of a plug-in for the OpenSSL library.
- Microsoft CryptoAPI
  This is a closed standard that is only used on Windows systems.

To be interoperable with OpenDNSSEC a HSM must support the PKCS #11 API. The minimum supported version of the PKCS #11 API is version 2.11. A compliancy tool will be made available that tests whether the PKCS #11 module supplied with a HSM is compatible with OpenDNSSEC.

Speed of cryptographic operations

When comparing HSMs in order to decide which one to purchase it is useful to compare the speed of cryptographic operations. There are two important benchmarks to look for:

- Signing speed for RSA
  This is usually measured in 1024-bit signing operations with public exponent 3 or 65537 per second.
- Key generation speed for RSA
  This is usually the average key generation time for 1024-bit and 2048-bit keys measured in seconds.

In general, separate unit HSMs and PCI cards will outperform smart cards and USB tokens by a large factor.

Security certifications

It is common for HSM manufacturers to have the security of their devices evaluated by a third party auditor. These audits are usually performed against internationally recognised standards for security evaluation. The two most important standards are:

Federal Information Processing Standard (FIPS) 140-2

This standard is maintained by the National Institute of Standards and Technology (NIST) which is a United States governmental body. The FIPS 140-2 standard recognises four levels to which a module can be evaluated (for a more detailed description see FIPS 140-2):

- Level 1 – the lowest level; basic security requirements are specified
- Level 2 – includes requirements for tamper evidence, user authentication
- Level 3 – includes requirements for tamper detection/resistance, data zeroisation, splitting user roles
- Level 4 – the highest level; penetration of the module has a very high probability of being detected, has requirements on environmental protection

For use with OpenDNSSEC, a HSM that has at least a FIPS 140-2 level 2 certification is recommended. Note that operating a HSM in FIPS 140-2 level 3 or higher mode may impose restrictions on on-board key generation through the PKCS #11 API that may be incompatible with OpenDNSSEC.

Common Criteria Evaluation Assurance Levels (CC-EAL)

The Common Criteria are an internationally recognised set of standards for evaluating security hardware and software. It is a highly regulated process with the following characteristics:

- The product or system under evaluation is referred to as the “Target of Evaluation” or TOE for short
- The TOE is evaluated against a Protection Profile (PP); a profile defined by a user or user community, examples of which include the Secure Signature Creation Device (SSCD) which is one of the bases of the European Digital Signature Directive
- The evaluation is performed on the basis of a so-called “Security Target” (ST) which is a detailed document describing the security functions of the TOE and refers to the PP

When a product has been evaluated the depth of and confidence in the evaluation is expressed as an Evaluation Assurance Level (EAL) ranging from 1 to 7 where 1 is the lowest and 7 the highest qualification.

If a HSM that is to be used with OpenDNSSEC has been evaluated according to Common Criteria it is recommended that the EAL is at least 4 or up.

Please note: a Common Criteria certification only has value if the Protection Profile is strict enough. Therefore, a Common Criteria certification can only really be trusted if the Protection Profile that was used for the evaluation is checked (this is very difficult for outsiders). Within the EU, the Protection Profile for Secure Signature Creation Devices (SSCD) (European standard CWA 14169) is a valuable profile for evaluation.

Backup and synchronisation

The key material used by OpenDNSSEC and stored in a HSM is extremely valuable as it guarantees the continued signed presence of a domain in the Domain Name System. It is therefore important to check the backup mechanisms supported by your HSMs.

Unfortunately, there are no specific standards for backing up key material in HSMs at the moment. Most manufacturers, however, will provide a [vendor specific] way for backing up key material. When evaluating a HSM product, attention should be paid to the security, ease of use and above all robustness of the backup method(s) provided by the HSM manufacturer.

A good example of a backup strategy is a HSM which maintains a key database (on disk) that is secured using (a) [set of] master key(s). These can be stored on smart cards that can be distributed among multiple security officers. An N out of M model can then be used to restore the master key(s) in a new HSM if a backup needs to be restored where at least N out of M security officers need to present their card to restore the master key(s). The new HSM can then access the key database stored on disk which could have been backed up using readily available backup tools.

Matching HSM types to typical usage scenarios

This section provides guidelines for the features to look for in an HSM given a specific usage scenario in combination with OpenDNSSEC

Scenario 1: organisation with a few small to medium size static zones

For this scenario a USB token or smart card should suffice to store the Key Signing Keys; Zone Signing Keys could be stored in a soft token that is protected using a key on the USB token or smart card.

Scenario 2: organisation with one or a few large static zones

For this scenario a USB token or smart card should suffice to store the Key Signing Keys; Zone Signing Keys could be stored in a soft token that is protected using a key on the USB token or smart card.

Scenario 3: organisation with many small to medium size static zones

For this scenario a simple HSM should suffice. Both Key Signing Keys as well as Zone Signing Keys could be stored in the HSM. It is important to pay attention to the number of keys the HSM can store. This should be a large multiple of the number of zones.

Scenario 4: organisation with many large static zones

It is recommended to use a HSM in this scenario. Both Key Signing Keys as well as Zone Signing Keys could be stored in the HSM. It is important to pay attention to the number of keys the HSM can store. This should be a large multiple of the number of zones. In addition to this, key generation speed and signing speed are important parameters.

Scenario 5: organisation with (many) dynamic zones

It is recommended to use a HSM in this scenario. Both Key Signing Keys as well as Zone Signing Keys could be stored in the HSM. It is important to pay attention to the number of keys the HSM can store. This should be a large multiple of the number of zones. In addition to this, key generation speed and signing speed should both be very high.

Checklist

The checklist below can help determine whether or not a HSM is suitable for use with OpenDNSSEC:

Feature	**Required/Optional**
PKCS #11 API	Required
MS CryptoAPI	Not required
OpenSSL engine support	Not required
Minimum key size 1024 bits	Required
Maximum key size 2048 bits	Required
RSA algorithm support	Required
DSA algorithm support	Optional
Symmetric algorithm support (AES, DES, etc.)	Optional
FIPS 140-2 (level 2 or 3)	Recommended*
Common Criteria (EAL 4 or up)	Recommended*
Backup mechanisms	Required

*Having at least one of these two certifications is recommended