

OpenDNSSEC > HSM

Hardware Security Modules

- [List of HSM products](#)
- [Guidelines for purchasing a Hardware Security Module](#)

Key Storage

Two major types of HSM:s has been identified:

- Keys stored on host, encrypted with HSM master key. Suitable for large number of keys, e.g. DNS hosting providers.
- Keys stored on HSM Suitable for a smaller number of keys, e.g. enterprise?

Hardware Interface

The HSM:s differ in the type of interface used between the host and the HSM.

- Local interface (typically via PCI), high speed link between a single host and the HSM.
- Remote interface (typically via Ethernet), HSM possibly sharable between multiple hosts.

It should also be noted that it is possible to design a system with a locally connected HSM, but shared among multiple hosts using a separate API (e.g. XML-RPC, SOAP, ONC-RPC). Hence, the choice of hardware interface is not directly tied to whether a single or multiple systems should be able to access the HSM itself.

Software Implementations

The interface can also be entirely provided by a software implementation, so called [soft tokens](#).

Requirements

Some [requirements](#) have been identified for a decent HSM to be able to comply with the [project requirements](#).

Application Program Interface

The most common Application Program Interfaces (API) for HSMs are:

- [PKCS#11](#)
- [OpenSSL](#)
- [API Comparison](#)

Using an HSM

- [Creating Keys](#)
- [Finding Keys](#)

- [Using Keys](#)
- [An introduction to the use of HSM](#) by Jelte Jansen, NLNetLabs ([PDF version](#))

Interesting technical reports and presentations about HSMs

- [Luna CA3 compromise](#) (note: the Luna CA3 has reached end-of-life)
- [Hardware Token compromises](#)