Version 1

The first version of SoftHSM was developed for OpenDNSSEC using the general requirements for DNSSEC. It uses the library Botan for the crypto operations and the keys are stored in a database backend using SQLite.

On this Page

- Pros and Cons
- Documentation
- Limitations
- Performance
- Requirements
- Design

Pros and Cons

There are some arguments why or why not you should use SoftHSM in your environment compared with regular HSM:s.

Documentation

The documentation of SoftHSM is documented in another part of the wiki.

Limitations

SoftHSM v1 has a number of limitations regarding the number of concurrent sessions and the number of stored objects. It also has some limitations on the algorithm support. Only the RSA algorithm can be used for public key operations. Outside the scope of DNSSEC, there is also support for X.509 certificates.

Performance

The performance of SoftHSM has been compared with OpenSSL on various platforms.

Requirements

The development was based on a number of requirements.

Design

SoftHSM implements functions in accordance with the PKCS#11 v2.20 specified by RSA Security Inc. But you can read more about the design here.