v2 Requirements

The requirements for the SoftHSM v2 are based on the original requirements for SoftHSM v1. New or changed requirements are marked with <new> and <changed>.

On this Page

General

- Must be a library that can be linked with other software.
- Must implement the PKCS #11 interface v2.30, as specified by RSA Laboratories. <changed>
- Must be licensed under a BSD license.
- Must be able to use a cryptographic library that is licensed under a BSD license.
- Must support multiple security realms. <new>
- Must be auditable; events should be traceable to the specific role using the SoftHSM. <new>
- Must be flexible enough to use different underlying cryptographic libraries. <new>
- When designing and implementing SoftHSM v2 secure coding guidelines and design principles shall be applied. <new>

The applicable secure coding standards are:
The CERT C Secure Coding Standard and
The CERT C++ Secure Coding Standard

Algorithms

- Must support the following cryptographic algorithms: RSA, DSA <changed>
- Should support the following cryptographic algorithms: GOST <new>
- Must support the following hash algorithms: SHA-1, SHA-256, SHA-512 <changed>
- Must support the following padding mechanisms: PKCS #1 v1.5
- Should support the following padding mechanisms: PKCS #1 PSS <new>

Key management

- Sensitive key material should only be exposed when necessary to perform cryptographic operations. <new>
- It must be possible to create backups of the SoftHSM v2 backend store. <changed>
- The implementation must not limit the number of keys the SoftHSM v2 supports. <changed>

Performance

- The performance of SoftHSM v2 in relation to the number of objects stored on a token should in the worst case degrade linearly. <new>

Key generation

- Must support RSA key-pairs from 1024-bits to at least 2048-bits. <changed>
- Should support RSA key-pairs up to 4096-bits. <new>
- The user must be able to specify the exponent when generating the RSA keys.

Sessions

- The number of concurrent sessions must not be limited by the implementation. <changed>

Functions

- Must support stand-alone digesting.
- Must support stand-alone signing.
- Must support combined-mechanism signing (digesting and signing in one operation).
- Must support raw signing (PKCS#11 CKM_RSA_X509) <new>

- Must support stand-alone verification. <changed>
- Must support key wrap and unwrap. <new>
- Should support decryption and encryption. <new>

Object types <new>

- Must support public key objects as token objects
- Must support private key objects as token objects
- Must support symmetric key objects as session objects
- Must support data objects as token objects
- Should support certificate objects as token objects

Support program: softhsm <changed>

softhsm and softhsm-keyconv have been merged into one tool in the requirements.

- Must be able to initialise a token with SO PIN, user PIN and label using PKCS#11
- Must be able to show which tokens are available using PKCS#11
- Must be able to support importing PKCS#8 formatted keys using PKCS#11
- Must be able to support importing BIND .private formatted keys using PKCS#11
- Must be able to dynamically load any PKCS#11 library
- Must NOT support export in BIND format