# v1 Requirements

These are the requirements on SoftHSM v1.

**On this Page**



## General

- Must be a library that can be linked with other software.
- Must implement the PKCS#11 interface v2.20, specified by RSA Labratories.
- Must be licensed under a BSD license.
- Must use a cryptographic library that is licensed under BSD.
- The user must be able to specify the number of tokens to use and its corresponding slots.
- Should keep a log of important events.

## Algorithms

- Must handle RSA, SHA1, and SHA256.
- Should handle RIPEMD160, SHA384, and SHA512.

## Key management

- Must be able to protect the keys by using a PIN via the PKCS#11 interface.
- Must be possible to do backup of the keys.
- Must be able to manage 1000 1024-bit RSA key pairs.

## Key generation

- Must be able to generate RSA keys of length 1024 and 2048 bits.
- Should be able to generate RSA keys of length greater than 512 bits, but limited to maximum 4096.
- The user must be able to specify the exponent when generating the RSA keys.

## Sessions

- Must handle at least 2048 concurrent sessions.

## Functions

- Must be able to create a hash with a given algorithm.
- Must be able to sign with a given algorithm.
- Should be able to verify with a given algorithm.

## Support program: softhsm

- Must be able to initialize a token with SO PIN, user PIN, and label.
- Must be able to show which tokens that are available.
- Must be able to import/export RSA keys in PKCS#8 format.
- Must handle both encrypted and unencrypted PKCS#8 files.

## Support program: softhsm-keyconv

- Must be able to convert from BIND .private format to PKCS#8.
- Must be able to convert from PKCS#8 format to BIND .private and .key format.
- Must handle both encrypted and unencrypted PKCS#8 files.
- Must support the algorithms: RSAMD5, DSA, RSASHA1, DSA-NSEC3-SHA1, RSASHA1-NSEC3-SHA1, RSASHA256, RSASHA512