Home

Welcome to the SoftHSM site for the OpenDNSSEC Project!!

SoftHSM is an implementation of a cryptographic store accessible through a PKCS#11 interface. You can use it to explore PKCS#11 without having a Hardware Security Module. It is being developed as a part of the OpenDNSSEC project.

On this Page

Background

OpenDNSSEC handles and stores its cryptographic keys via the PKCS#11 interface. This interface specifies how to communicate with cryptographic devices such as HSM:s (Hardware Security Modules) and smart cards. The purpose of these devices is, among others, to generate cryptographic keys and sign information without revealing private-key material to the outside world. They are often designed to perform well on these specific tasks compared to ordinary processes in a normal computer.

A potential problem with the use of the PKCS#11 interface is that it might limit the wide spread use of OpenDNSSEC, since a potential user might not be willing to invest in a new hardware device. To counter this effect, OpenDNSSEC is providing a software implementation of a generic cryptographic device with a PKCS#11 interface, the SoftHSM. SoftHSM is designed to meet the requirements of OpenDNSSEC, but can also work together with other cryptographic products because of the PKCS#11 interface.

SoftHSM v1

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.

Visit the SoftHSM v1 page for more information.

SoftHSM v2

It focuses on a higher level of security by encrypting sensitive information and using unswappable memory. There is also a more generalized crypto backend, where you can use Botan or OpenSSL. Visit the SoftHSM v2 page for more information.