SoftHSM

A BRIEF OVERVIEW

ICANN 50, London - June 25th 2014

Roland van Rijswijk-Deij (SURFnet)

Introduction

- SoftHSM is a software-only implementation of PKCS #11 (Cryptoki)
- Developed by the OpenDNSSEC project
- Goals:
  - serve as test PKCS #11 library for OpenDNSSEC (note: we test with real HSMs as well)
  - provide a free alternative for users that do not need a real HSM for DNSSEC

SoftHSM v1

- SoftHSM v1 was introduced in September 2009
- Developed with focus on PKCS #11 functions required for DNSSEC signing
- Stores key material "in the clear", just like BIND
- Uses SQLite database as storage backend
- Supports import of BIND-style key material
- Uses Botan as underlying cryptographic library

SoftHSM v1

- Slowly extended over time beyond bare features required for DNSSEC, e.g. support for:
  - Storing X.509 certificates
  - Newer signature schemes like RSA-PSS
- Current (2014-05-25) version is 1.3.7

SoftHSM v1

- Source available on GitHub: https://github.com/opendnssec/SoftHSMv1
- Tarball from: http://www.opendnssec.org/download/
- Pre-built packages available for:
  - Debian
  - Red Hat/CentOS (EPEL)
  - FreeBSD
  - Gentoo
  - NetBSD
  - Ubuntu
  - Windows
  - OpenBSD (in the works)

SoftHSM v2

- Started in 2011
- Re-design from the ground up, to be "as secure as we can make it in software"
- Security features:
  - All sensitive material stored in encrypted form
  - Only decrypted in memory when needed
  - Optionally suppress paging (swap) of sensitive data

SoftHSM v2

- Designed to scale better for large deployments (> 100K objects stored, for large DNSSEC deployments)
- Cryptographic abstraction layer to support multiple backends (currently: Botan and OpenSSL)
- Multiple storage backends (file-based, SQLite)
- Comprehensive support for PKCS #11 features
- Supports GOST

SoftHSM v2

- Currently under development
- Feature complete but needs further testing
- Alpha release available from:
  http://www.opendnssec.org/download/
- Sources on GitHub:
  https://github.com/opendnssec/SoftHSMv2
- We could use some help with further development (mostly funding)

Questions/comments?

roland.vanrijswijk@surfnet.nl

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

Visit our website

http://www.opendnssec.org/

http://www.softhsm.org/