Appendix 09
HSM: Hardware Security Module

1 Introduction

The term HSM refers to an internal or external peripheral device for the efficient and secure execution of cryptographic operations or applications for sensitive data, including the highly secure storage of the required cryptographic keys[1] . This enables the implementation of security mechanisms for data confidentiality, integrity, and authenticity using cryptographic methods.

An HSM can efficiently protect the keys used both through software and against physical attacks and side-channel attacks. In addition to highly secure key protection, an HSM implements all essential cryptographic methods, such as symmetric encryption methods (AES, One-Time-Pad, etc.), asymmetric methods for encryption and/or signature calculation (e.g., RSA, ECDSA, Diffie-Hellman key exchange), and hash functions (SHA-1, SHA-2, SHA-3). In addition, HSMs typically include their own random number generator (deterministic and/or non-deterministic) and comprehensive functions for the secure management of the device and the keys.

A key feature of many HSMs is their ability to actively defend against attacks, which allows them to be described as “tamper-responsive” (i.e., reacting to attempts at manipulation).

HSMs are available with USB interfaces, in PCIe form factors, and for networks. HSMs are used in smart cards, USB drives, portable devices, standalone devices, IoT devices, hosted solutions, or offered as a cloud service (HSM as a Service). In the context of QKD, RKD, and MKD, all these types of HSMs are of interest.

[1] https://en.wikipedia.org/wiki/Hardware_security_module

Some HSMs feature so-called "tamper-responsive" or "tamper-evident" functions. These include physical measures such as sealing and shielding against electromagnetic radiation, as well as self-destruction in the event of tampering. If the housing is opened or damaged, the HSM detects this via sensors and can automatically erase the memory (zeroization).

Today, HSMs are designed almost exclusively for mathematical cryptography. They are used for the highly secure storage of many cryptographic keys and for the implementation of cryptographic functions. However, because one-time pads do not play a role in this context, while the storage is highly secure (with zeroization, etc., see above), it typically has a storage capacity of only 4 to 16 GB, which is very little for MKD.

However, the storage space is sufficient for the amount of key material provided by QKD and MKD. Since the OTPH encryption method is designed for this amount of key material and requires an HSM, HSMs are ideally suited for OTPH.

HSMs for mathematical cryptography currently start at around $1,100, while models with automatic memory erasure (zeroization) start at around $1,600. Because in MKD with a one-time pad, the secret key bits are only stored in a highly secure storage medium , HSMs are not required for MKD, and zeroization plays no major role, particularly in telecommunications applications.

HSMs are certified to higher security standards, such as FIPS 140-1 and 140-2, as well as Common Criteria (CC, e.g., EAL4+).

The following list includes only HSMs suitable for MKD, i.e., cost-effective options. However, there are numerous other HSMs on the market for various application scenarios. In addition to “general-purpose HSMs,” which are universally applicable, there are HSMs for specialized applications, such as in the financial sector (primarily banks and payment service providers). HSMs for pure network applications are also available, such as IPsec VPN gateways with a hardware encryption unit, like the German SINA-Box.

The global HSM market is estimated at $2 billion in 2025 and is projected to grow to $9.4 billion by 2035 (CAGR: 16.7%).

2 Market Overview of HSMs

HSMs with a USB interface are cost-effective and typically resemble a USB flash drive; they have a capacity of only a few hundred keys at most and a low transaction rate (up to about 30 transactions per second). They are priced between $550 and $1,600.

HSMs with a PCIe interface are usually the size of a PCIe card, are significantly faster (up to several thousand transactions per second), can process several thousand keys, and cost between $2,200 and $5,500.

- YubiHSM 2: It costs between $250 and $550 and has a USB interface
- Nitrokey HSM2: It costs approximately $110, has a USB interface, and is programmable
- Feitian ePass Security Key – K9 / K10: It costs between $30 and $70, has an NFC interface and a USB interface, and is programmable

More expensive HSMs, e.g., for QKD and RKD in conjunction with the OTPH encryption method, include:

- Rohde & Schwarz SITLine: The SITLine ETH4G model costs approximately $900
- Utimaco CryptoBox: The SecurityServer CSe LAN v5 costs between approximately $22,000 and $27,000 and is available in network and PCIe versions
- Thales SafeNet Luna HSM: The Luna PCIe HSM A700 costs between approximately $10,000 and $12,000

References

[HSM 1] Andreas Philipp: Hardware Security Modules (HSM) for Dummies. Published by: Wiley-VCH Verlag GmbH & Co. KGaA, Weinheim. 1st edition. Weinheim, pp. 11–20.

[ISO] ISO/IEC 13491-1:2024 Financial services — Secure cryptographic devices (retail) Part 1: Concepts and requirements