Chapter 16
Hardware Security Module

Maria Sommerhalder

16.1 Introduction

This chapter provides an analysis of hardware security modules (HSMs). HSMs are specialized devices that perform cryptographic operations and store private-public key pairs and their associated secret values. They are widely used in various industries, such as banking, insurance, digital identity, and blockchain, to secure data. The chapter begins with defining HSMs and explaining their function and use in the cryptographic process. It also discusses trends in the use of HSMs until 2025, including the rise of cloud computing, double-key encryption, and the increasing demand for HSMs in the banking, financial services, and insurance industries. The chapter concludes by mentioning some of the key players in the global HSM market.

16.2 Analysis

Various industries use hardware security modules (HSMs) to secure data, including banking, insurance, digital identity, and blockchain applications. Their functions include key generation, key management, encryption, decryption, and hashing.

M. Sommerhalder (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Maria.Sommerhalder@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_16

16.2.1 Definition

A vital component of the cryptographic process is collecting and storing private-public key pairs and their associated secret values. HSMs are typically used in critical infrastructure such as payment solutions, encryption systems on the Internet, and certificate management systems [1]. HSMs are specialized devices used to conduct cryptographic operations and use a random number source to generate public-private key pairs and subsequently store them. Most HSM systems are designed to store information on the device itself. However, some systems can back up secret values outside the HSM perimeter, such as on USB storage devices, hard disks, smart cards, or other digital media [2]. In addition to providing logical protection for keys, HSMs also provide physical protection. For example, some devices are equipped with tamper-proofing features such as logging and alerting mechanisms and more intrusive features such as wiping the entire contents when tampering is detected, making it inoperable [3]. In addition, HSMs have the advantage of isolating cryptographic processes from other operations, resulting in more efficient processing and additional security [3].

16.2.2 Trends

For over 20 years, HSMs have been used to protect cryptographic material in multiple applications [4]. However, a Ponemon Institute survey of 580 IT and security practitioners worldwide (55% from organizations with 1000 or more employees) found that HSMs are primarily used for key management or payment. A survey made in 2014 found that Organizations typically utilize 13 modules for key management, followed by eight for payment purposes [5].

The advent of cloud computing has increased the complexity of securing critical data. Data is now stored in the cloud: the percentage of corporate data stored in the cloud in organizations worldwide has doubled from 30% in 2015 to 60% by 2022 [6]. Many companies are concerned that their data will be unprotected from unauthorized access by the cloud provider or the US government in case of a subpoena, as most of the renowned cloud providers operate from the United States. As a result, double-key encryption has become increasingly popular, which encrypts data using two keys. A copy is stored on an HSM, and a copy is stored in the cloud. Before storing the data in the cloud, the owner of the data or the HSM vendor encrypts it so that the cloud provider cannot decrypt it. Parties can only access the data with both keys [7]. The use of double key encryption is widespread in highly regulated industries such as banking, health, and the public sector to comply with privacy and data protection laws [7].

Global payment markets are expanding, resulting in a higher demand for HSM machines to secure payment-related cryptographic operations. Many other factors are driving the growth of the HSM market, including the rise of cybersecurity

threats and the need for confidentiality in the banking, financial services, and insurance industries [8]. There is also an increase in demand for HSMs from other sources, such as the automotive industry, where they are used to enable secure communication, verify and authenticate software updates [9].

Several key players in the global HSM market include Gemalto, Inc., IBM Corporation, Ultra Electronics Group Holdings, Utimaco GmbH, Futurex L.P., Thales e-Security, Inc., Hewlett Packard Enterprise Development L.P., SWIFT C.S., and Yubico, Inc. [8].

In EPFL's School of Computer and Communication Sciences, there is a research domain entitled "Security and Privacy", which publishes papers on the topic [10]. The area of research involving the development of post-quantum hardware security modules is also present. The possibility of seeing some of them be available shortly, combined with embedded hardware accelerators, see Chap. 20 [11]. The area of combining Iot devices and Hardware Security modules is also explored. For example, the HSM can achieve the integrity of the key injection [12].

16.3 Consequences for Switzerland

Due to the political stability and the availability of skilled labor, a specialist ecosystem has developed in Switzerland, with many HSM providers having branch offices here and Swiss providers establishing themselves on the international stage. The Swiss branch of Securosys SA and the Swiss branch of Thales Suisse SA are examples of this.

16.3.1 Maturity

Due to the maturity of the HSM market, it is possible to find machines suitable for a wide range of applications. However, HSMs should be purchased from reputable vendors, preferably ones that have already been certified (see below).

16.3.2 Recommendation and Options

Three recommendations are presented in this section regarding the use of HSMs.

- Geo-redundant setup and Clustering

  HSMs must be stored in secure data centers, but even then, hardware failures, natural disasters, or human error can destroy an HSM. This would result in the irreversible loss of all key material. Typically, a company has two to three devices with the same build and data (i.e., replicated) located geographically. Therefore,

there must be operational failover procedures (switching operations to a backup recovery facility in case of primary system failure) between these devices [4].

- Key ceremony auditability

  Companies in regulated industries may be required to audit the generation of asymmetric key material [13]. The auditor must be able to obtain evidence of the entire process, including the hardware used, as well as verify the location and ownership of all key components during key generation and management. As a result, additional policies regarding access and change management must be prepared, as well as documents relating to the transport, storage, and management of keys, tokens, smart cards, and any related hardware. In light of the number of steps that could potentially compromise the private key, it is essential to have a solid runbook. The runbook describes the step-by-step process and the roles of all personnel involved in key generation. This ensures that auditors and all involved parties understand the process and serves as an audit trail [13].
- HSM Security Certification

  Generally, HSMs are certified following internationally recognized standards, such as FIPS-PUB 140-2 [3], 140-3 [14], or Common Criteria (CC) [15]. In addition, four security levels are defined by the FIPS certification [16]. An HSM certificate is issued only for the HSM device itself. It does not automatically guarantee secure keys since the operation of a key management system is equally critical to security. Regardless of certification, a system must address the single point of failure problem. It is a legal and compliance requirement that custodial services in the financial sector must be enforced to implement governance and policy regulation throughout the entire key lifecycle.

16.4 Conclusion

HSMs provide adequate cryptographic key protection throughout their lifecycles by enabling the secure generation of keys within an isolated hardware environment without revealing their identity. Furthermore, as HSMs can manage keys and enable users to manage keys, they provide significant security benefits to applications utilizing cryptography.

References

1. Norbert Pohlmann. Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen. page 5, 2012. Datenschutz und Datensicherheit.
2. William Mehuron. SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES. page 69, May 2001.
3. National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. Technical Report Federal Information Processing Standard (FIPS) 140-2, U.S. Department of Commerce, December 2002.

4. Michael Suby. An Anchor of Trust in a Digital World: Risk Management Strategies for Digital Processes - Whitepaper. March 2020.
5. Ponemon Institute LLC. HSM Global Market Study. July 2014.
6. Statista. Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2022. https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/, March 2022.
7. Mustapha Hedabou. Cloud Key Management Based on Verifiable Secret Sharing. In Min Yang, Chao Chen, and Yang Liu, editors, *Network and System Security*, volume 13041, pages 289–303. Springer International Publishing, Cham, 2021. Series Title: Lecture Notes in Computer Science.
8. Bloomberg. Hardware Security Modules Market size worth $ 7.9 Billion, Globally, by 2028 at 12.4% CAGR: Verified Market Research. February 2022.
9. Claudius Pott, Philipp Jungklass, David Jacek Csejka, Thomas Eisenbarth, and Marco Siebert. Firmware Security Module: A Framework for Trusted Computing in Automotive Multiprocessors. *Journal of Hardware and Systems Security*, 5(2):103–113, June 2021.
10. EPFL. Security & Privacy. https://www.epfl.ch/schools/ic/research/security-privacy/, August 2022.
11. Wen Wang and Marc Stöttinger. Post-Quantum Secure Architectures for Automotive Hardware Secure Modules, 2020. Report Number: 026.
12. Simranjeet Sidhu, Bassam J. Mohd, and Thaier Hayajneh. Hardware Security in IoT Devices with Emphasis on Hardware Trojans. *Journal of Sensor and Actuator Networks*, 8(3):42, September 2019. Number: 3 Publisher: Multidisciplinary Digital Publishing Institute.
13. Capital Markets and Technology Association. Digital Assets Custody Standard. https://cmta.ch/content/77ea8b352579fd35f28e246cec6c4c46/cmta-digital-assets-custody-standard-v-12-final-october-2020-1.pdf, October 2020.
14. National Institute of Standards and Technology. Security requirements for cryptographic modules. Technical Report NIST FIPS 140-3, National Institute of Standards and Technology, Gaithersburg, MD, April 2019.
15. Common Criteria Portal. Certified Products. https://www.commoncriteriaportal.org/products/, August 2022.
16. NIST. FIPS General Information. https://www.nist.gov/itl/fips-general-information, May 2018.