WIKIPEDIA

Hardware security module

A **hardware security module** (**HSM**) is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. A hardware security module contains one or more secure cryptoprocessor chips.[1][2][3]

A FIPS 140-2 Level 4 certified PCIe HSM

Contents

Design

HSMs may have features that provide tamper evidence such as visible signs of tampering or logging and alerting, or tamper resistance which makes tampering difficult without making the HSM inoperable, or tamper responsiveness such as deleting keys upon tamper detection.[4] Each module contains one or more secure cryptoprocessor chips to prevent tampering and bus probing, or a combination of chips in a module that is protected by the tamper evident, tamper resistant, or tamper responsive packaging.

A vast majority of existing HSMs are designed mainly to manage secret keys. Many HSM systems have means to securely back up the keys they handle outside of the HSM. Keys may be backed up in wrapped form and stored on a computer disk or other media, or externally using a secure portable device like a smartcard or some other security token.[5]

HSMs are used for real time authorisation and authentication in critical infrastructure thus are typically engineered to support standard high availability models including clustering, automated failover, and redundant field-replaceable components.

A few of the HSMs available in the market have the capability to execute specially developed modules within the HSM's secure enclosure. Such an ability is useful, for example, in cases where special algorithms or business logic has to be executed in a secured and controlled environment. The modules can be developed in native C language, .NET, Java, or other programming languages. Further, upcoming next-generation HSMs[6] can handle more complex tasks such as loading and running full operating systems and COTS software without requiring customization and reprogramming. Such unconventional designs overcome existing design and performance limitations of traditional HSMs. While providing the benefit of securing application-specific code, these execution engines protect the status of an HSM's FIPS or Common Criteria validation.

Security

Due to the critical role they play in securing applications and infrastructure, HSMs and/or the cryptographic modules are typically certified to internationally recognized standards such as Common Criteria or FIPS 140 to provide users with independent assurance that the design and implementation of the product and cryptographic algorithms are sound. The highest level of FIPS 140 security certification attainable is Security Level 4 (Overall). When used in financial payments applications, the security of an HSM is often validated against the HSM requirements defined by the Payment Card Industry Security Standards Council.[7]

Uses

A hardware security module can be employed in any application that uses digital keys. Typically the keys would be of high value - meaning there would be a significant, negative impact to the owner of the key if it were compromised.

The functions of an HSM are:

- onboard secure cryptographic key generation
- onboard secure cryptographic key storage, at least for the top level and most sensitive keys, which are often called master keys
- key management
- use of cryptographic and sensitive data material, for example, performing encryption or digital signature functions
- offloading application servers for complete asymmetric and symmetric cryptography.

HSMs are also deployed to manage transparent data encryption keys for databases and keys for storage devices such as disk or tape.

HSMs provide both logical and physical protection of these materials, including cryptographic keys, from disclosure, non-authorized use, and potential adversaries.[8]

HSMs support both symmetric and asymmetric (public-key) cryptography. For some applications, such as certificate authorities and digital signing, the cryptographic material is asymmetric key pairs (and certificates) used in public-key cryptography.[9] With other applications, such as data encryption or financial payment systems, the cryptographic material consists mainly of symmetric keys.

Some HSM systems are also hardware cryptographic accelerators. They usually cannot beat the performance of hardware-only solutions for symmetric key operations. However, with performance ranges from 1 to 10,000 1024-bit RSA signs per second, HSMs can provide significant CPU offload for asymmetric key operations. Since the National Institute of Standards and Technology (NIST) is recommending the use of 2,048 bit RSA keys from year 2010,[10] performance at longer key sizes is becoming increasingly important. To address this issue, most HSMs now support elliptic curve cryptography (ECC), which delivers stronger encryption with shorter key lengths.

PKI environment (CA HSMs)

In PKI environments, the HSMs may be used by certification authorities (CAs) and registration authorities (RAs) to generate, store, and handle asymmetric key pairs. In these cases, there are some fundamental features a device must have, namely:

- Logical and physical high-level protection
- Multi-part user authorization schema (see Blakley-Shamir secret sharing)
- Full audit and log traces
- Secure key backup

On the other hand, device performance in a PKI environment is generally less important, in both online and offline operations, as Registration Authority procedures represent the performance bottleneck of the Infrastructure.

Card payment system HSMs (bank HSMs)

Specialized HSMs are used in the payment card industry. HSMs support both general-purpose functions and specialized functions required to process transactions and comply with industry standards. They normally do not feature a standard API.

Typical applications are transaction authorization and payment card personalization, requiring functions such as:

- verify that a user-entered PIN matches the reference PIN known to the card issuer
- verify credit/debit card transactions by checking card security codes or by performing host processing components of an EMV based transaction in conjunction with an ATM controller or POS terminal
- support a crypto-API with a smart card (such as an EMV)
- re-encrypt a PIN block to send it to another authorization host
- perform secure key management
- support a protocol of POS ATM network management
- support de facto standards of host-host key | data exchange API
- generate and print a "PIN mailer"
- generate data for a magnetic stripe card (PVV, CVV)
- generate a card keyset and support the personalization process for smart cards

The major organizations that produce and maintain standards for HSMs on the banking market are the Payment Card Industry Security Standards Council, ANS X9, and ISO.

SSL connection establishment

Performance-critical applications that have to use HTTPS (SSL/TLS), can benefit from the use of an SSL Acceleration HSM by moving the RSA operations, which typically requires several large integer multiplications, from the host CPU to the HSM device. Typical HSM devices can perform about 1 to 10,000

1024-bit RSA operations/second.[11] Some performance at longer key sizes is becoming increasingly important. To address this issue, some HSMs [12] now support ECC. Specialized HSM devices can reach numbers as high as 20,000 operations per second.[13]

DNSSEC

An increasing number of registries use HSMs to store the key material that is used to sign large zonefiles. An open source tool for managing signing of DNS zone files using HSM is OpenDNSSEC.

On January 27, 2007 deployment of DNSSEC for the root zone officially started; it was undertaken by ICANN and Verisign, with support from the U.S. Department of Commerce.[14] Details of the root signature can be found on the Root DNSSEC's website.[15]

Cryptocurrency wallet

Cryptocurrency can be stored in a cryptocurrency wallet on a HSM.[16]

See also

- Electronic funds transfer
- FIPS 140
- Public key infrastructure
- PKCS 11
- Secure cryptoprocessor
- Security token
- Transparent data encryption
- Security switch
- Trusted Platform Module

Notes and references

1. Ramakrishnan, Vignesh; Venugopal, Prasanth; Mukherjee, Tuhin (2015). *Proceedings of the International Conference on Information Engineering, Management and Security 2015: ICIEMS 2015* (https://books.google.com/books?id=Gw9pCwAAQBAJ&pg=PA9). Association of Scientists, Developers and Faculties (ASDF). p. 9. ISBN 9788192974279.
2. "Secure Sensitive Data with the BIG-IP Hardware Security Module" (https://www.f5.com/pdf/solution-profiles/hardware-security-module-sp.pdf) (PDF). F5 Networks. 2012. Retrieved 30 September 2019.
3. Gregg, Michael (2014). *CASP CompTIA Advanced Security Practitioner Study Guide: Exam CAS-002* (https://books.google.com/books?id=LKPCBwAAQBAJ&pg=PA246). John Wiley & Sons. p. 246. ISBN 9781118930847.
4. "Electronic Tamper Detection Smart Meter Reference Design" (http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=RDELECTRONICTAMPER). freescale. Retrieved 26 May 2015.
5. "Using Smartcard/Security Tokens" (http://www.mxcsoft.com/Man_Securing%20Privkeys.htm). mxc software. Retrieved 26 May 2015.
6. "World's First Tamper-Proof Server and General Purpose Secure HSM" (http://enforcerserver.com). Private Machines. Retrieved 7 March 2019.

7. "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards" (https://www.pcisecuritystandards.org). *www.pcisecuritystandards.org*. Retrieved 2018-05-01.
8. "Support for Hardware Security Modules" (https://web.archive.org/web/20150526064340/https://www.paloaltonetworks.cn/documentation/pan-os/newfeaturesguide/section_2/chapter_1.html). paloalto. Archived from the original (https://www.paloaltonetworks.cn/documentation/pan-os/newfeaturesguide/section_2/chapter_1.html) on 26 May 2015. Retrieved 26 May 2015.
9. "Application and Transaction Security / HSM" (http://www.provision.ro/access-management/application-and-transaction-security-hsm#pagei-1). Provision. Retrieved 26 May 2015.
10. "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" (https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final). NIST. January 2011. Retrieved March 29, 2011.
11. F. Demaertelaere. "Hardware Security Modules" (https://web.archive.org/web/20150906093444/http://secappdev.org/handouts/2010/Filip%20Demaertelaere/HSM.pdf) (PDF). Atos Worldline. Archived from the original (http://secappdev.org/handouts/2010/Filip%20Demaertelaere/HSM.pdf) (PDF) on 6 September 2015. Retrieved 26 May 2015.
12. "Barco Silex FPGA Design Speeds Transactions In Atos Worldline Hardware Security Module" (http://www.electronicspecifier.com/design-automation/adyton-barco-silex-ip-atos-worldline-fpga-design-speeds-transactions-hardware-security-module). Barco-Silex. January 2013. Retrieved April 8, 2013.
13. "SafeNet Network HSM - Formerly Luna SA Network-Attached HSM" (https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/safenet-network-hsm/). *Gemalto*. Retrieved 2017-09-21.
14. "ICANN Begins Public DNSSEC Test Plan for the Root Zone" (http://www.circleid.com/posts/20100127_icann_begins_public_dnssec_test_plan_for_the_root_zone/). *www.circleid.com*. Retrieved 2015-08-17.
15. Root DNSSEC (http://www.root-dnssec.org/)
16. "Gemalto and Ledger Join Forces to Provide Security Infrastructure for Cryptocurrency Based Activities" (https://www.gemalto.com/press/Pages/Gemalto-and-Ledger-Join-Forces-to-Provide--Security-Infrastructure-for-Cryptocurrency-Based-Activities-.aspx). *gemalto.com*. Retrieved 2020-04-20.

External links

- Current NIST FIPS-140 certificates (https://web.archive.org/web/20141226152243/http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm)
- A Review of Hardware Security Modules (https://www.opendnssec.org/wp-content/uploads/2011/01/A-Review-of-Hardware-Security-Modules-Fall-2010.pdf)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Hardware_security_module&oldid=1003464215"

This page was last edited on 29 January 2021, at 02:43 (UTC).