What is a General Purpose Hardware Security Module (HSM)?

Hardware Security Modules (HSMs) are hardened, tamper-resistant hardware devices that strengthen encryption practices by generating keys, encrypting and decrypting data, and creating and verifying digital signatures. Some hardware security modules (HSMs) are certified at various FIPS 140-2 Levels. Hardware security modules (HSMs) are frequently used to:

* Meet and exceed established and emerging regulatory standards for cybersecurity
* Achieve higher levels of data security and trust
* Maintain high service levels and business agility

What is a Payment Hardware Security Module (HSM)?

A payment HSM is a hardened, tamper-resistant hardware device that is used primarily by the retail banking industry to provide high levels of protection for cryptographic keys and customer PINs used during the issuance of magnetic stripe and EMV chip cards (and their mobile application equivalents) and the subsequent processing of credit and debit card payment transactions. Payment HSMs normally provide native cryptographic support for all the major card scheme payment applications and undergo rigorous independent hardware certification under global schemes such as FIPS 140-2, PCI HSM and other additional regional security requirements such as MEPS in France and APCA in Australia for example.

Some of their common use cases in the payments ecosystem include:

* PIN generation, management and validation
* PIN block translation during the network switching of ATM and POS transactions
* Card, user and cryptogram validation during payment transaction processing
* Payment credential issuing for payment cards and mobile applications
* Point-to-point encryption (P2PE) key management and secure data decryption
* Sharing keys securely with third parties to facilitate secure communications

What Is Remote HSM Management?

Remote hardware security module (HSM) management enables security teams to perform tasks linked to key and device management from a central remote location, avoiding the need to travel to the data center. A remote HSM management solution delivers operational cost savings in addition to making the task of managing HSMs more flexible and on-demand.

Depending on the HSM solution used, remote HSM management enables:

* Greater, more flexible control
* Strong access control based on digital credentials rather than physical keys
* Stronger audit controls from tracking activities to individual card credentials
* Quicker identification of remote HSM status issues
* Simpler software and license upgrade installation
* Reduced risk of errors
* Simplified logistics

Related Articles

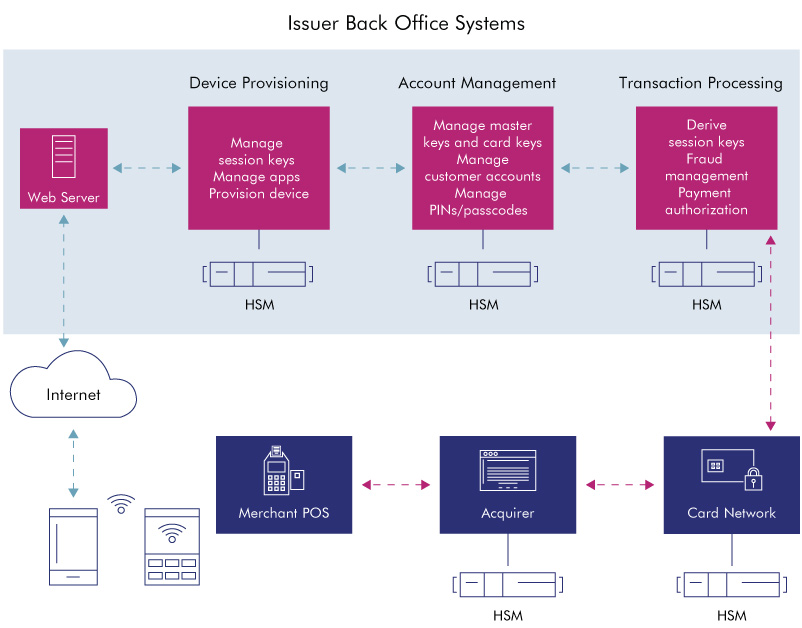
* [Payment HSMs](https://cpl.thalesgroup.com/encryption/hardware-security-modules/payment-hsms)
* [HSM Management and Monitoring](https://cpl.thalesgroup.com/encryption/hardware-security-modules/hsm-management-and-monitoring)
* [Thales Announces Major Update To Remote HSM Manager For Its Line Of Payments Hardware Security Modules](https://cpl.thalesgroup.com/encryption/hardware-security-modules)

What is Host Card Emulation (HCE)?

Host card emulation (HCE) is a technology for securing a mobile phone such that it can be used to make credit or debit transactions at a physical point-of-sale (POS) terminals. With HCE, critical payment credentials are stored in a secure shared repository (the issuer data center or private cloud) rather than on the phone. Limited use credentials are delivered to the phone in advance to enable contactless transactions to take place.

This approach eliminates the need for Trusted Service Managers (TSMs) and shifts control back to the banks. However, it brings with it a different set of security and risk challenges.

* A centralized service to store many millions of payment credentials or create one-time use credentials on demand creates an obvious point of attack. Although banks have issued cards for years, those systems have largely been offline and have not requiring round-the-cloud interaction with the payment token (in this case a plastic card). HCE requires these services to be online and accessible in real-time as part of individual payment transactions. Failure to protect these service platforms places the issuer at considerable risk of fraud.
* Although the phone no longer stores payment credentials, it still plays three critical security roles, all of which create opportunities for theft or substitution of credentials or transaction information.
  + It provides the means for applications to request card data stored in the HCE service.
  + It is the method by which a user is authenticated and authorizes the service to provide the payments credentials.
  + It provides the communications channel over which payment credentials are passed to the POS terminal.
* All mobile payments schemes are more complex than traditional card payments, yet smart phone user expectations are extremely high.
  + Poor mobile network coverage can make HCE services inaccessible.
  + Complex authentication schemes lead to errors.
  + Software or hardware incompatibility can stop transactions.



Related Articles

* [Thales Host Card Emulation](https://cpl.thalesgroup.com/encryption/host-card-emulation)

### What is Root of Trust?

Root of Trust (RoT) is a source that can always be trusted within a cryptographic system. Because cryptographic security is dependent on keys to encrypt and decrypt data and perform functions such as generating digital signatures and verifying signatures, RoT schemes generally include a hardened hardware module. A principal example is the hardware security module (HSM) which generates and protects keys and performs cryptographic functions within its secure environment.

Because this module is for all intents and purposes inaccessible outside the computer ecosystem, that ecosystem can trust the keys and other cryptographic information it receives from the root of trust module to be authentic and authorized. This is particularly important as the Internet of Things (IoT) proliferates, because to avoid being hacked, components of computing ecosystems need a way to determine information they receive is authentic. The RoT safeguards the security of data and applications and helps to build trust in the overall ecosystem.

RoT is a critical component of public key infrastructures (PKIs) to generate and protect root and certificate authority keys; code signing to ensure software remains secure, unaltered and authentic; and creating digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments.

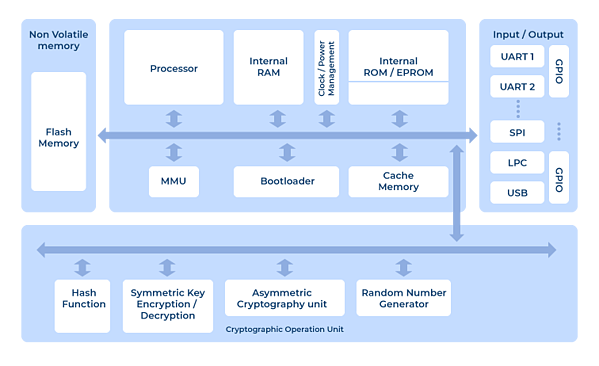
# **Hardware Security Module (HSM): What is it, and what is its role in protecting payment card data?**



David E. Acosta April 23, 2020

One of the main problems arising from the use of cryptography for the protection of sensitive data during storage and transmission **is the complexity of managing the life cycle of encryption keys**(generation, storage, import/export, distribution, rotation, replacement, backup, revocation, suspension, destruction, auditing, etc.). **The security of the cryptographic system must lie in the security of the key**([Kerckhoffs' principle](https://es.wikipedia.org/wiki/Principios_de_Kerckhoffs" \t "_blank)). This key must be managed as securely as possible since it is assumed that the potential attacker can know or have access to all the other parameters of the cryptographic system (the algorithm used, encrypted text, clear text). If the key is compromised, the entire cryptographic system is compromised ("a cryptosystem should be secure even if everything about the system except the key, is in the public knowledge").

In this sense, one of the most recommended alternatives to manage the cryptographic keys is through the use of a **Hardware Security Module (HSM)**. An HSM is also known as Secure Application Module (SAM), Secure Cryptographic Device (SCD), Hardware Cryptographic Device (HCD), or Cryptographic Module. It is a secure, tamper-resistant cryptographic processor designed specifically to protect the life cycle of cryptographic keys and to execute encryption and decryption routines. It provides a high level of security in terms of confidentiality, integrity, and availability of cryptographic keys and any sensitive data processed.

***Figure 1***. Schematic diagram of a hardware safety module (HSM). Source: University of Patras.

HSMs can be found in smart cards, portable devices, dedicated cards (cryptographic cards), self-contained devices (appliances) or offered as a cloud service (HSM-as-a-Service).

***Figure 2. Different types of HSM: cryptographic card, appliance, USB (nano) HSM and smart card***

## **HSM Types**

Depending on requirements, HSM devices can be classified into two types:

1. **General Purpose HSM:** HSM devices that include a variety of standard encryption algorithms (symmetric, asymmetric and hash functions) with support for API interconnectivity using Public-Key Cryptography Standard (PKCS) #11, Microsoft Cryptographic Application Programming Interface (CAPI), Cryptography API Next Generation (CNG), Java Cryptography Architecture (JCA), Java Cryptography Extension (JCE) and others. These devices are typically used in PKI environments, HTTPS channels, DNSSEC, generic sensitive data protection, and crypto-wallets, among others.

2. **Transaction and Payment HSM:** Specific HSM devices for the protection of payment transactions which include the use of PIN (generation, management, validation and translation of the PIN Block in transactions carried out at POS and ATMs), the protection of electronic fund transfers (EFT), the generation of data for magnetic strips and EMV chips in card production and personalization processes, the processing of payment transactions with debit and credit cards and the validation of cards, users and cryptograms. These devices typically provide cryptographic support for the payment applications of most brands of cards, and their interconnection interfaces are usually more limited than the generic use HSMs.

## **Validation of the security levels of HSM devices**

A series of international standards have been defined to validate the security levels of this type of device, among which we find the following:

1. [FIPS (Federal Information Processing Standard) 140-2](https://csrc.nist.gov/publications/detail/fips/140/2/final) (Security Requirements for Cryptographic Modules): It is a standard aimed at validating the effectiveness of cryptographic hardware. Despite being a federal standard in the USA and Canada, it is recognized worldwide in both the government and private sectors. This certification defines four levels of security, from the lowest (Level 1) to the most restrictive (Level 4):

* Level 1: Includes basic security requirements (at least one approved algorithm or function must be used), allowing the software and firmware components of the cryptographic module to be executed on a general-purpose system using an untested operating system. No physical security mechanisms are included. Example: encryption card of a personal computer.
* Level 2: This level enhances level 1 security by requiring the use of mechanisms for tamper-evidence detection and role-based authentication. Software implementations must run on a Common Criteria EAL2 approved operating system.
* Level 3: This level requires additional requirements for tamper-resistance, tamper-response, and identity-based authentication. It also requires a logical separation between interfaces through which critical security parameters enter and exit the system. Private keys can only be imported or exported in encrypted form.
* Level 4: This last level includes advanced intrusion protection (tamper-active) and is designed for products operating in physically unprotected environments.

2. [Common Criteria](https://www.commoncriteriaportal.org/products/) (ISO/IEC 15408): Common Criteria for Information Technology Security Evaluation is an internationally recognized certification standard for IT product and system security. It was developed by Canada, France, Germany, the Netherlands, the UK, and the USA in the 1990s. Products evaluated under Common Criteria are categorized into levels (Evaluation Assurance Level - EAL), with EAL1 being the lowest and EAL 7 the strictest.

3. [Payment Card Industry (PCI) PTS HSM Security Requirements](https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true) (PCI HSM): The PCI HSM standard is part of the PCI SSC PIN Transaction Security (PTS) group of standards and defines the security controls required during the manufacturing, shipment, use, and dismantling of HSM devices used in financial transactions.

Additionally, some countries such as Germany, France (CB MEPS), Australia (APCA CECS), or Italy have developed specific standards for key and algorithm management in HSM devices, which may require special certifications.

## **HSM devices and their relationship to PCI SSC standards**

Cryptography is one of the primary mechanisms used for the protection of transactional data related to payment cards. Because of this, many of the controls in the PCI SSC standards (PCI DSS, PCI PIN, PCI P2PE, PCI 3DS, PCI Card Production, etc.) require formal management of cryptographic keys and - in some cases - require the use of specific HSMs and certificates. Listed below are some of the PCI SSC standards and their requirements in terms of HSM device usage:

## **PCI DSS v3.2.1**

## **Related requirements:**

3.5.x, 3.6.x

## **Comments:**

The PCI DSS standard does not require the use of an HSM device to manage encryption keys. However, the use of these devices facilitates the processes of secure key storage (3.5.3 and 3.6.3), key generation (3.6.1), key distribution (3.6.2), rotation/crypt periods (3.6.4), key replacement (3.6.5), implementation of "dual control" and "split knowledge" (3.6.6), key replacement prevention (3.6.7) and custodian management (3.6.8).

## **PCI PIN v3.0**

## **Related requirements:**

1-x

## **Comments:**

The PCI PIN standard requires that:  
  
- The PIN data is processed in devices that are classified as Secure Cryptographic Device (SCD) and certified as PCI HSM or FIPS 140-2 Level 3 or higher  
  
- All cryptographic keys used for PIN encryption/decryption must be generated in devices certified as PCI HSM, FIPS 140-2 Level 3 or higher or using a NIST 800-22 aligned random number generator.  
  
- Key injection processes must be performed on devices certified as PCI HSM or FIPS 140-2 Level 3 or higher.

## **PCI P2PE v3.0**

## **Related requirements:**

4A-1  
5-1

## **Comments:**

The PCI P2PE standard requires that  
  
- The devices used in the decryption environment are HSMs certified as PCI HSM or FIPS 140-2 Level 3 or higher.  
  
- All cryptographic keys used for PIN encryption/decryption must be generated in devices certified as PCI HSM, FIPS 140-2 Level 3 or higher or using a NIST 800-22 aligned random number generator.  
  
- Key injection processes must be performed on devices certified as PCI HSM or FIPS 140-2 Level 3 or higher

## **PCI 3DS v1.0**

## **Related requirements:**

P2-6.1.2

## **Comments:**

The PCI 3DS standard requires that entities offering Access Control Server (ACS) or Directory Server (DS) services employ a PCI HSM or FIPS 140-2 Level 3 or higher certified HSM.

For entities that offer services such as 3DS Server (3DSS), the use of an HSM is not mandatory but highly recommended.

## **PCI Card Production (Logical) v2.0**

## **Related requirements:**

8.5 (Key generation)  
8.7 (Key loading)  
8.14 (Key-Management Security Hardware)

## **Comments:**

The PCI Card Production (Logical) standard requires the use of HSMs certified as PCI HSM or FIPS 140-2 Level 3 or higher for key generation, key loading and sensitive data protection processes.

## **Cloud HSM and HSM-as-a-Service (HSMaaS)**

In addition to the locally deployed (on-premise) HSM model, many cloud service providers and HSM device manufacturers are offering Hardware Security Module "as a Service" or managed services. This new model offers many advantages over the traditional model, including high scalability, availability, and additional integration options. Some examples of these services are:

* Microsoft Azure: [Azure Dedicated HSM](https://azure.microsoft.com/en-us/services/azure-dedicated-hsm/#overview) and [Azure Key Vault](https://azure.microsoft.com/en-us/services/key-vault/)
* Google Cloud Platform: [Cloud HSM](https://cloud.google.com/hsm/) and [Cloud Key Management Service](https://cloud.google.com/kms)
* Amazon Web Services: [AWS Key Management Service (KMS)](https://aws.amazon.com/es/kms/) and [AWS CloudHSM](https://aws.amazon.com/es/cloudhsm/)
* IBM [Cloud Hardware Security Module](https://www.ibm.com/cloud/hardware-security-module)
* Utimaco [HSM-as-a-Service](https://hsm.utimaco.com/products-hardware-security-modules/form-factor/cloud-hsm-as-a-service/)
* nCipher [nShield-as-a-Service](https://www.ncipher.com/products/general-purpose-hsms/nshield-as-a-service" \t "_blank)
* Thales [CipherTrust Cloud Key Manager](https://www.thalesesecurity.com/products/key-management/ciphertrust-cloud-key-manager" \t "_blank)

However, it is essential to note that the use of these managed or cloud services offer general-purpose HSM devices that may be useful for integration with PCI DSS environments but not for use in PCI PIN, PCI P2PE or PCI 3DS environments. These standards require transactional HSMs with special cryptographic support and additional physical and device lifecycle security controls that none of these vendors offer today.

## **Conclusion**

Bruce Schneier, in his book "[Applied Cryptography](https://www.schneier.com/books/applied_cryptography/2preface.html)," said: "The management of cryptographic keys is the most difficult part of cryptography and often the Achilles' heel of a secure system." A safe and not so complicated way to perform this management is by using hardware security modules (HSM). These devices allow secure key management, secure processing of sensitive data, and meet strict certifiable security requirements and are a secure alternative to the use of generic cryptographic software libraries.