17.10. Hardware Security Modules

Objective

17.10.1. Hardware Security Modules are used where additional security of cryptographic functions is desirable.

Context

Scope

17.10.2. This section covers information relating to Hardware Security Modules (HSMs). Detailed key management guidance is provided in Section 17.9 – Key Management.

Hardware Security Module

17.10.3. Hardware Security Modules (HSMs) are defined as a hardware module or appliance which provides cryptographic functions. HSM's can be integrated into a design, installed in a host or be externally connected. HSM's can be packaged as discrete appliances, PCI cards, USB devices, smartcards or other form factors.

17.10.4. Functions include (but are not limited to) encryption, decryption, key generation, signing, hashing and cryptographic acceleration. The appliance usually also offers some level of physical tamper-resistance, has a user interface and a programmable interface for key management, configuration and firmware or software updates.

Usage

17.10.5. HSMs are used in high assurance security solutions that satisfy widely established and emerging standards of due care for cryptographic systems and practices—while also maintaining high levels of operational efficiency. Traditional use of HSMs is within automatic teller machines, electronic fund transfer, and point-of-sale networks. HSMs are also used to secure CA keys in PKI deployments, SSL acceleration and DNSSEC (DNS Security Extensions) implementations.

Physical Security

17.10.6. HSM's usually describe an encapsulated multi-chip module, device, card or appliance, rather than a single chip component or device. The nature of HSM's requires more robust physical security, including tamper resistance, tamper evidence, tamper detection, and tamper response.

Tamper Resistance

17.10.7. Tamper Resistance is designed to limit the ability to physically tamper with, break into or extract useful information from an HSM. Often the boards and components are encased in an epoxy-like resin that will destroy any encapsulated components when drilled, scraped or otherwise physically tampered with.

Tamper Evidence

17.10.8. The HSM is designed so that any attempts at tampering are evident. Many devices use seals and labels designed break or reveal a special message when physical tampering is attempted. Tamper evidence may require a regular inspection or audit mechanism.

17.10.9. HSMs can include features that detect and report tampering attempts. For example, embedding a conductive mesh within the epoxy-like package; internal circuitry monitored the electrical proper-ties of this mesh — properties which physical tamper would disrupt. Devices can also monitor for temperature extremes, radiation extremes, light, air and other unusual conditions.

Tamper Response

17.10.10. HSMs can include defensive features that activate when tampering is detected. For example, cryptographic keys and sensitive data are deleted or zeroised. A trade-off exists between availability and security as an effective tamper response essentially renders the HSM unusable.

References

17.10.11. Further references can be found at:

Reference	Title	Publisher	Source
	Payment Card Industry (PCI) Hardware Security Module (HSM) - Security Requirements	PCI	Official PCI Security Standards Council Site - Document PCI HSM Frequently Asked Questions (pcisecuritystandards.org)
FIPS PUB 140-2	**FIPS PUB 140-2 Security Requirements for Cryptographic Modules**	NIST	FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov)

Rationale & Controls

Hardware Security Modules

17.10.12.R.01. **Rationale**

Where high assurance or high security is required or high volumes of data are encrypted or decrypted, the use of an HSM should be considered when designing the network and security architectures.

17.10.12.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:3103]

Agencies MUST consider the use of HSMs when undertaking a security risk assessment or designing network and security architectures.

17.10.12.C.02. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:3105]

Agencies MUST follow the product selection guidance in this manual. See Chapter 12 – Product Security.

17.10.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3108]

Agencies SHOULD consider the use of HSMs when undertaking a security risk assessment or designing network and security architectures.

17.10.12.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3110]

Agencies SHOULD follow the product selection guidance in this manual. See Chapter 12 – Product Security.