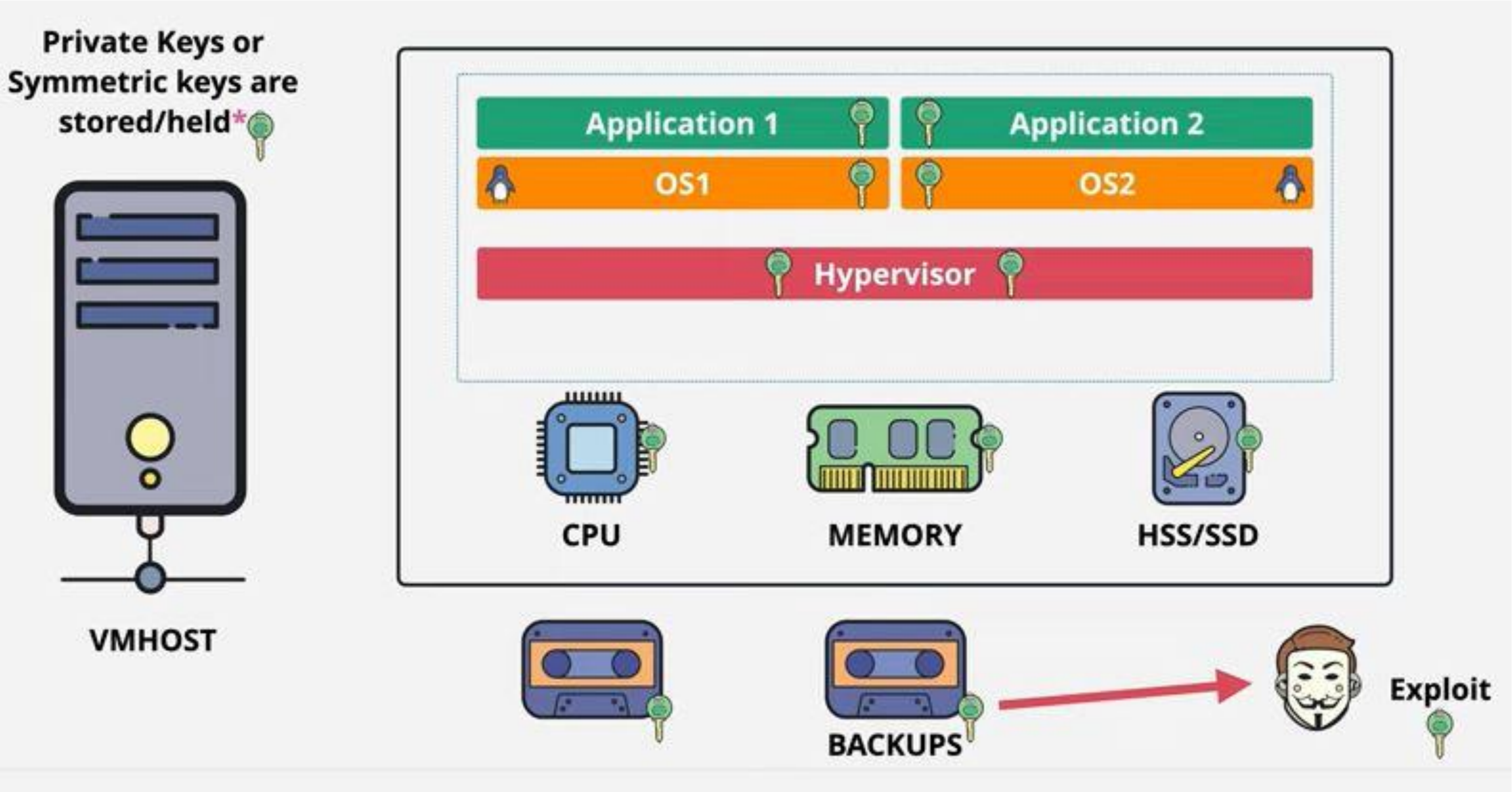
Hardware Security Module (HSM)

Hardware Security Module

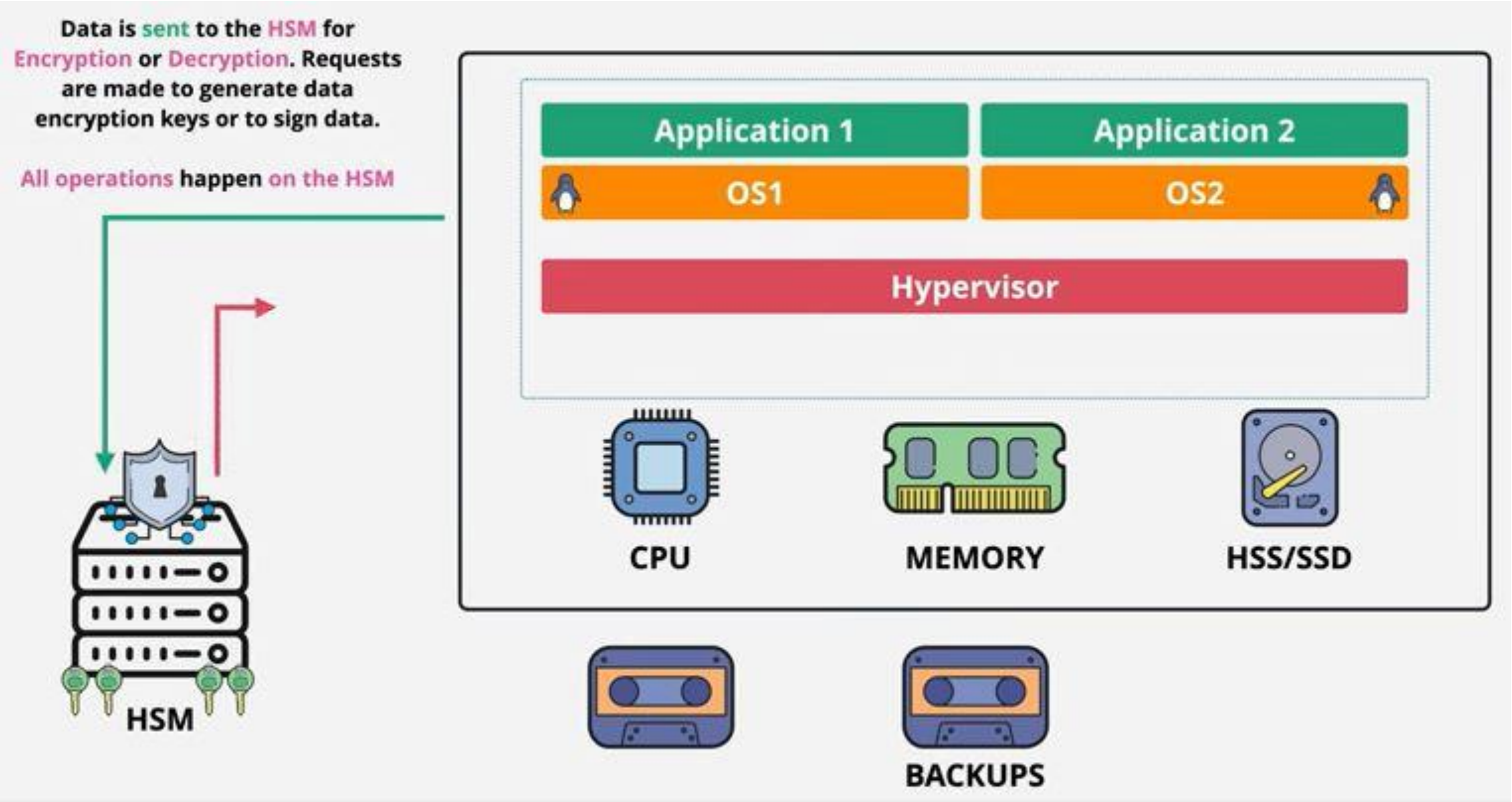
- A hardware security module (HSM) is a physical device that provides secure storage and management of cryptographic keys and performs cryptographic operations.

- It is designed to enhance the security of sensitive data and cryptographic operations in various applications, such as financial transactions, secure communications, digital signatures, and authentication systems.

Virtualized Environment without HSM



Virtualized Environment with HSM


Data is sent to the HSM for Encryption or Decryption. Requests are made to generate data encryption keys or to sign data.
All operations happen on the HSM
Application 1
Application 2
OS1
OS2
Hypervisor
CPU
MEMORY
HSS/SSD
HSM
BACKUPS

Development of HSM

- Initially it was invented for military deployment.
- Security modules were developed at a time when running cryptographic operations required special hardware.
- In the late ’70s and early ’80s IBM then introduced an algorithm to the market that developers could implement efficiently in hardware.
- Storing cryptographic keys securely in HSM was used later on.
- ATMs were the first to use Hardware security modules commercially.

Features of HSM

1. Role Separation: Different users/admins have different role by which they can access the HSM for different purposes.
   - No one should be given full access to HSM

2. Access through APIs: HMS are allowed to be accessed through Industry Standard APIs only.
   - PKCS#11, Java Cryptography Extensions, Microsoft CryptoNG (CNG) libraries etc..

3. Authentication: Objects on HSM are encrypted by the by each owner application and can be decrypted by means of specific secret key.
   - It takes place inside the device isolated security radius.

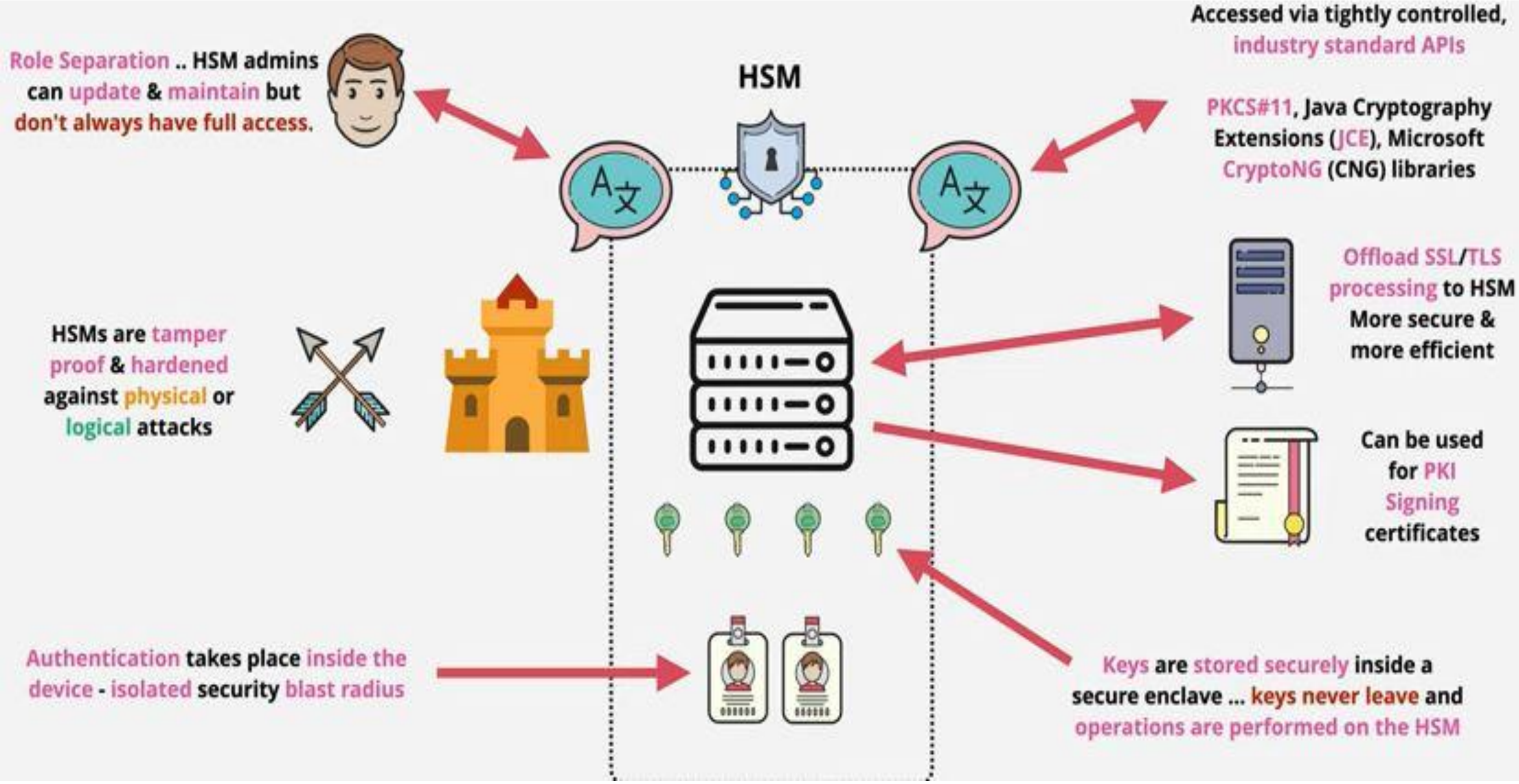
Features of HSM

4. Key Storage: All the secret key generated inside a HSM are to be forever stay in the HSM device.
   - They are stored inside a secure enclave.

5. Tamper proof: HSMs are also tamper-resistant and tamper-evident devices.
   - One of the reasons HSMs are so secure is because they have strictly controlled access, and are virtually impossible to compromise.

6. Keyless SSL/TLS: In addition to private keys stored on disk, Keyless SSL supports keys stored in a Hardware Security Module (HSM) via the PKCS#11 standard.
   - Keyless uses PKCS#11 for signing and decrypting payloads without having direct access to the private keys.

Features of HSM



Role Separation .. HSM admins can update & maintain but don't always have full access.

HSMs are tamper proof & hardened against physical or logical attacks

Authentication takes place inside the device - isolated security blast radius

Accessed via tightly controlled, industry standard APIs

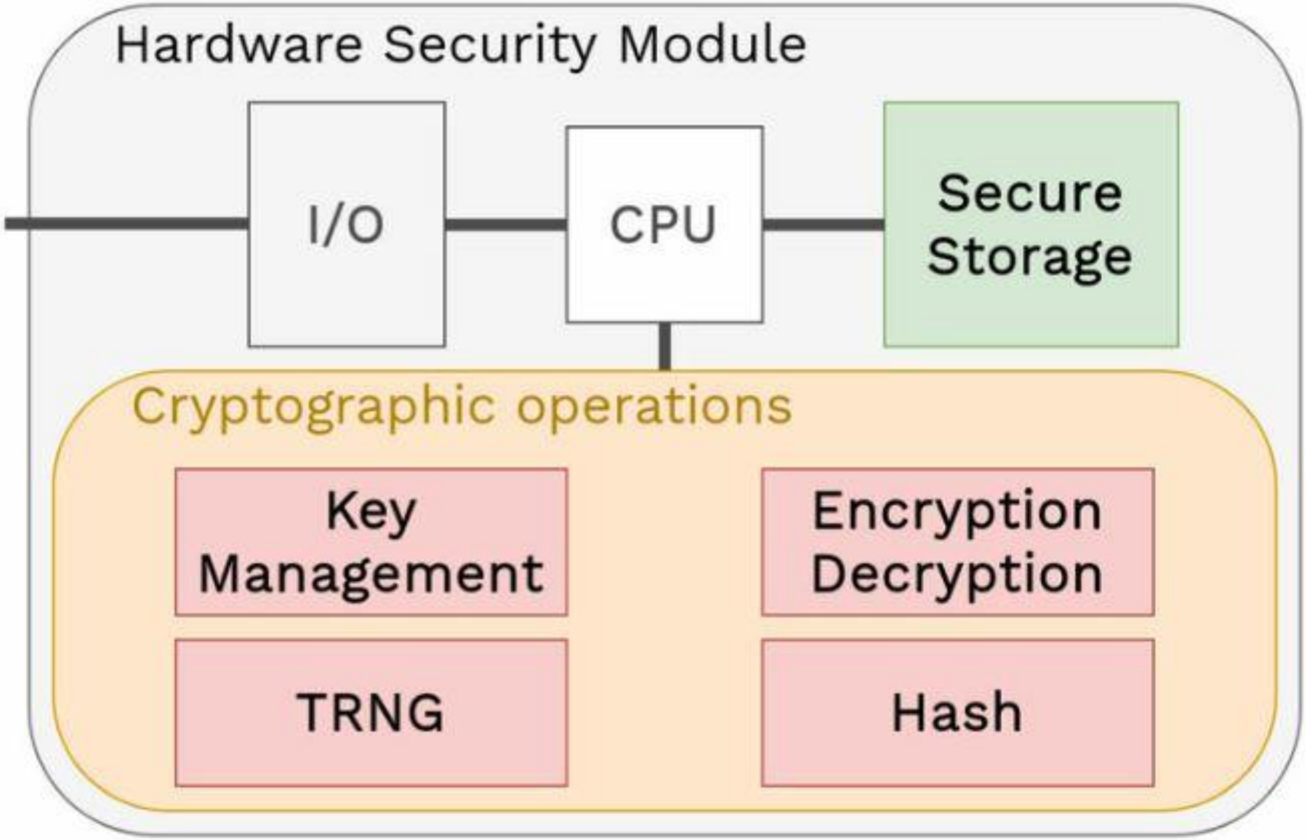
PKCS#11, Java Cryptography Extensions (JCE), Microsoft CryptoNG (CNG) libraries

Offload SSL/TLS processing to HSM More secure & more efficient

Can be used for PKI Signing certificates

Keys are stored securely inside a secure enclave ... keys never leave and operations are performed on the HSM

HSM General Architecture



Types of HMSs

Two main types

- **General Purpose:** General Purpose HSMs can utilize the most common encryption algorithms, such as PKCS#11, CAPI, CNG, and more, and are primarily used with Public Key Infrastructures, cryptowallets, and other basic sensitive data.

- **Payment and Transactions:** The other type of HSM is a payment and transaction HSM.
  - types of HSM are created with the protection of payment card information and other types of sensitive transaction information in mind.
  - These types of Hardware Security Module are narrower in the types of organizations they can work within, but they are ideal to help comply with **Payment Card Industry Data Security Standards (PCI DSS)**.

Functions of HSMs

1. **Key Generations:**

- The HSM has a built-in random number generator (RNG) that generates cryptographic keys.
- These keys are created within the secure environment of the HSM, ensuring their confidentiality and integrity.
- The keys can be asymmetric (such as RSA or ECC keys) or symmetric (such as AES keys).

Functions of HSMs

2. Key Storage:

- The HSM securely stores the generated cryptographic keys within its hardware components.

- The keys are encrypted and protected using encryption algorithms and access control mechanisms.

- The key storage area is isolated from the external environment, making it difficult for unauthorized parties to access or extract the keys.

Functions of HSMs

3. Cryptographic Operations:

- The HSM provides a range of cryptographic operations that can be performed securely within its protected environment.

- These operations include encryption, decryption, digital signatures, key exchange, and key derivation.

- The HSM's hardware is designed to accelerate these operations, making them more efficient and faster than software-based implementations.

Functions of HSMs

4. Access Control:

- Access to the HSM and its stored keys is tightly controlled.

- Authorized users, typically administrators or trusted applications, must authenticate themselves using authentication mechanisms such as passwords, smart cards, or biometrics.

- Access control mechanisms ensure that only authorized individuals or processes can utilize the HSM's functions.

Functions of HSMs

5. Tamper Detection and Response:

- HSMs are designed with tamper-evident and tamper-resistant features to detect and respond to physical attacks.
- These features include sensors, seals, and secure enclosures that can detect tampering attempts.
- If tampering is detected, the HSM can automatically erase its cryptographic material or enter a tamper-resistant state to protect the keys and prevent unauthorized access.

Functions of HSMs

6. Audit and Logging:

- HSMs maintain logs and records of all activities performed within the device.

- These logs include information such as key usage, cryptographic operations, authentication attempts, and configuration changes.

- Audit logs are critical for monitoring and compliance purposes, allowing organizations to track and review all actions performed with the HSM.

Functions of HSMs

7. Redundancy and Failover:

- To ensure high availability and fault tolerance, HSMs can be deployed in redundant configurations.

- Multiple HSMs can be synchronized to share cryptographic keys and configurations.

- If one HSM fails, another can seamlessly take over its operations, ensuring continuity of cryptographic services without interruption.

Compliance for HSMs

- HSMs often undergo rigorous certifications and evaluations to meet industry and regulatory standards. These certifications, such as **FIPS 140-2** or **Common Criteria**, validate the security and integrity of the HSM and provide assurance that it meets the required levels of protection.

- FIPS 140-2 (Federal Information Processing): This a standard that validates the effectiveness of hardware performing cryptographic operations. It is a recognized in both public and private sectors
  - It has 4 different level of compliance:

Compliance for HSMs

- **Level 1:** It is the lowest level, focuses on ensuring the device has basic security methods, such as one cryptographic algorithm, and it allows the use of a general purpose model with any operating system.
  - FIPS 140-2 level 1 requirements are limited just to provide some amount of security for sensitive data

- **Level 2:** In addition to level 1 it also provide tamper-evident device, role based authentication and OS that is Common Criteria EAL2(Evaluation Assurance Levels) approved. There is 7 levels of Common Criteria.

Compliance for HSMs

- Level 3: Level 3 requires everything that level 2 does along with tamper-resistance, tamper-response, and identity-based authentication.
  - Private keys can only be imported or exported in their encrypted form, and a logical separation of interfaces where critical security parameters leave and enter the system.
  - This is the most commonly sought compliance level.

- Level 4: Level 4 is the most restrictive FIPS level, advanced intrusion protection hardware and is designed for products operating in physically unprotected environments.

Key Management in HSMs

- Securing the keys in a cryptographic system is critical to maintaining a secure system.
- Key management is subject to individual design and preference. Diverse approaches have been take by the manufacturers of HSMs for key management:
  - some ensuring that the keys never leave the physical confines of the HSM.
  - others allowing for key export (safely encrypting the keys before doing so).

Cryptographic Key’s Lifecycle

- HSMs manage different cryptographic keys by following six steps:
- 1. **Provisioning.** Keys are created by an HSM, another type of key management system or a third-party organization that does this. A true random number generator should be used to create keys.
- **Backup and storage.** A copy of a keys should be made and securely stored, in case the key is compromised or lost. They can be stored in the HSM or on external media. Private keys must be encrypted before being stored.

Cryptographic Key’s Lifecycle

3. **Deployment.** This involves installing the key in a cryptographic device such as an HSM.

4. **Management:** Keys are controlled and monitored based on industry standards and an organization's own internal policies.
   - The encryption key management system handles key rotation where new keys are deployed as existing keys expire.

- The hardware security module protects cryptographic keys and handles the encryption and decryption processes.

Cryptographic Key's Lifecycle

5. **Archiving.** Decommissioned keys are put in offline, long-term storage for when they may be needed to access existing data that was encrypted with that key.

6. **Disposal:** Keys should be securely and permanently destroyed only after it is determined that they are no longer needed.