

How to Choose a Hardware Security Module (HSM)

When choosing a hardware security module (HSM) for your organization, there are 9 simple points to consider. While not all are obvious, they are critical make-or-break factors for the smooth implementation, management and use of such a system, impacting every aspect of your business processes. Whether you are considering the purchase of an HSM solution for your organization, or replacing an existing HSM, use the points below as guidelines to ensure you are implementing the highest levels of security and reliability for mission critical cryptographic applications.



Security - This is a fundamental and obvious requirement of an HSM solution. The solution must guarantee that sensitive data such as keys are not exposed and that unauthorized users will not gain access to data.

Tip: Be certain that all access to the HSM is authenticated and that the key material inside the HSM is encrypted. Additionally, make sure that the case itself will provide reliable tamper-evidence and audit mechanisms.



Multiple Application Support - Numerous applications may require cryptographic services. While some HSMs are application specific, other HSMs can enable multiple applications to simultaneously access the HSM. Via this second option, an organization can use the same HSM for multiple purposes.

Tip: Make sure it is possible to define a set of keys for each individual application to assure that all keys are exclusive to their specific application.



Performance - This is another critical issue as it influences the number of HSMs required for deployment. A high-performance HSM will require fewer additional units, and therefore reduces costs.

Tip: Evaluate HSM performance according to your operational requirements (i.e., symmetric and a-symmetric operations).



High Availability & Disaster Recovery - An HSM is typically regarded as a mission critical system that should work 24/7/365. Therefore, it must seamlessly overcome any technical problem. This is achieved with high availability configuration and backing up all critical data stored in the HSM.

Tip: Make sure that a high availability mechanism is automatically achieved without user intervention and that the HSM supports a secured backup and restoration procedure.



Compliance - Each regulation has its own specific requirements that should be addressed by the cryptographic module. For example, HSM regulations for Europay, MasterCard, and VISA (EMV) applications require that the HSM is FIPS 140 certified. It is also mandatory that the key management conforms to VISA and MasterCard policies.

Tip: Review the regulations for your industry and make sure that the HSM complies with all of the necessary requirements.



Centralized Key Management - Applications may typically use multiple keys. These keys can be managed while encrypted in an external DB, or secured inside the HSM. Externally-managed keys are vulnerable to exposure when sent across the network to the HSM for each transaction, and it is more difficult to control and limit access to the keys. When keys are managed inside the HSM, there is only one copy of the key in the system and it is protected in the internal database. This guarantees that only authorized users can access the system.

Tip: Make sure the HSM can store multiple keys in an internal encrypted database and that it is possible to load/read keys in an encrypted format as well as in clear/encrypted parts.



Network Attached and Secure Access Control - An HSM can be a PCI card plugged into a computer that serves that local computer only, or a dedicated hardware that is connected to the network and processes cryptographic requests from more than one station.

Tip: Make sure that access to the HSM is authenticated and encrypted in order to prevent unauthorized users from processing requests. It is also important to assure that authorization mechanisms exist for administrators so they can define the actions that can be performed by each user.



Flexible and Easy to Upgrade - There are HSMs that provide different interfaces, a variety of functionalities, and many supported platforms. This allows 3rd party applications maximum flexibility when using the HSM in their complete solution (e.g., using applications for EMV personalization or applications for a PKI solution).

Tip: Make sure that the HSM can be accessed from different operating systems, applications, and programming languages. Additionally, select an HSM that has the ability to upgrade when necessary in order to meet newer standards, and support new applications and algorithms.



Compliance to Standards - In order to allow for easy integration with applications, the HSM should provide common standards for cryptographic applications such as PKCS #11, Microsoft CAPI/CNG, and Sun JCA/JCE.

Tip: The HSM should be able to provide cryptographic operations suitable for a changing world of standards and applications. Verify that the HSM is in line with the most up-to-date cryptographic standards and has a built-in capability for extending its functionality with the same hardware.