The benefits of partitionable HSMs

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT (SCD)

Severe competition and increasingly volatile markets push CIOs and CISOs to rethink their IT and bring costs down. At the same time, many banks opt for a service platform strategy, which requires the banks' IT in general, and the crypto architecture in specific to be more flexible and sophisticated. In this article, we will look at how partitioned HSMs can reduce the total cost of ownership and at the same time make the architecture more flexible and able to rapidly embrace new applications.

Partitioned HSMs represent a new technology based on virtualization and hardware partitioning. This approach contributes to a reduction of TCO - Total Cost of Ownership.

The total cost of ownership of an HSM is a variable, which describes both the direct and indirect costs of an HSM. HSMs can be quite costly, and they also require service and maintenance. In what follows we will see how using HSM partitioning can help to significantly lower TCO.

An overview of HSM partitioning

An HSM is a computer, that has a motherboard with processors, usually crypto-processors, disks, and communication systems (USB, Ethernet etc…). These hardware resources can be partitioned to create several 'little' HSM instances from the hardware HSM.

In logical terms, these HSMs are identical to normal HSMs, they share the same characteristics and security.

Windows users know this process when creating a separate disk volume from an existing hardware disk. The Windows operating system sees the disk volume with all the characteristics and attributes of a real disk, while it is a logical abstraction on the top of a hardware device.

There are many ways to achieve hardware partitioning. Sometimes micro-partitioning can even be used by creating several logical processors from a unique physical processor.

Depending on the hardware capacities, hardware partitioning may even provide isolation between the partitions. For, it can create electrical isolation between two HSM instances: if one instance HSM is faulty, the other won't be affected!

Two of the HSM's many added values are the cryptoprocessor and an anti-tampering system to protect the 'cryptographic heart'. Sometimes the resources won't be used to their maximum capacity. Therefore, they can be shared between multiple partitioned HSMs. These partitioned HSMs will all use the cryptographic capacity and resources of the hardware HSM.

More technical details about HSM partitions

When partitioning a FIPS-140-based HSM, the instantiations will be also compliant with the standard.

Partitioning HSMs allows separate backup / restore procedures. They also allow separate specialization. For example, one HSM instance can be used as a Payment HSM, while another instance can be used for a general purpose.

HSM partitions are isolated (‘firewalled’) from each other

- by hardware (say, individual stacks registers),
- by cryptography - since they have different master keys,
- by memory process isolation (like all operating systems do)
- through modern virtualization machine isolation

... but they share the same cryptographic heart protected from intrusion by a secure grid.

Some manufacturers allow for micro-partitioning of partitioned HSMs. In such a case the partition system controls time slicing and manages

- all the hardware interrupts, dynamic movement of resources across multiple operating systems,
- and also the dispatching of logical partition workloads

Micro-partitioning allows for a finer granularity for creating HSM instances and can be an ideal solution but depends greatly on the hardware capacities.

Using HSM partitions

Using HSM partitions is very simple. First, they need to be created by the system administrator using remote access. The procedure for creating such partitions varies with the HSM vendors. Usually, a private key must be downloaded and the administrator must generate passwords for the selected security officers that will access the newly created partition HSM.

When creating a partition HSM, the administrator will require one or several of the following resources:

- The security officer who will use the HSM
- The partition password (must usually respect strong rules)
- The new TOKEN name for the HSM

- The domain, the storage size, and eventually other hardware data.

Advantages of partitioned HSM

The purely virtual deployment and its level of automation in creating and managing virtual HSM instances will have a direct impact on TCO

- All deployment can be done centrally in a highly automated process with a comfortable UI and with no need for additional hardware or physical installation. Rapid inclusion of new applications as required in a platform strategy is hence made easy.
- Key management procedures can also be modified purely virtually and from the same physical location
- Risks are minimized and time to deployment reduced as the system administrator does not have to deal with various vendor-specific procedures nor with additional hardware
- Time-consuming manual work is avoided. At the same time, the risk of errors is reduced.

Application of HSM partitions

Cloud Applications

HSM partitions involve multi-tenancy. An organization can deploy a smaller number of HSMs to run the same volume of cloud applications. This eliminates complexity and saves cost, space, and power supply.

In a public cloud, multi-tenancy enables firewalls inside the secure boundaries of the HSM to securely separate different tenants' partitions from one another. User authentication, key management, and key usage remain local to the partition and the company.

In the context of an organization using cloud applications, HSM partition is therefore ideal to lower TCO.

Consolidation of an HSM estate in an organization

HSM partitioning allows organizations to consolidate their HSM estate by replacing old or unsupported, phased-out HSMs with a partition HSM which leads to a reduction in TCO. Therefore, rationalizing the amount of HSMs and having but a few modern models of HSMs should be part of operationalized goals when implementing TCO strategies. This also lowers the TCO.

Reducing the cost of maintenance

If an HSM partition has a problem, it can be recreated and maintained remotely. Replacing a hardware-based HSM would be much more time and resource consuming This reduces the overall cost of maintenance and service, lowering the TCO.

Summary

We looked at the capacities of HSM partitioning. HSM partitions can significantly reduce the TCO of an organization. HSM partitioning is a relatively new technology and allows building "virtual HSMs" from a single hardware HSM which shares the exact security, cryptographic capacities, and anti-tampering as a hardware one.