Want a faster payment HSM?

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT (SCD)

HSMs are primarily focused on security but they also need to be fast. crypto operations are very demanding operations and require important processing power. Crypto processors used by the HSMs are fast because the cryptographic routines are implemented in the hardware directly but they need to cope with eventual high-volume requests.

Here we look at the AT1000 and check what it takes to be a fast payment HSM.

The factors to consider for an HSM to be fast

HSMs are modern digital computers so the factors that impact their speeds will generally be the factors that impact a modern digital computer speed plus other factors related to cryptography.

- Operating System
- Ram
- CPU power
- Crypto-CPU power
- Network and I/O

Fast Operating System

An HSM has no 'ordinary' operating system. There must be a guarantee that it cannot be infected by computer viruses, trojans, or malware. This prevents the usage of operating systems such as Windows, Linux, or OsX - at least in their "normal" versions.

An operating system may slow down a computer. For instance, if many services are launched at startup or if some module from the OS needs to perform some costly background tasks like backups, updates, etc…

Many ATMs for instance are equipped with Windows embedded or Windows XPE. Usually, these OS will run from a read-only media and copy themselves in a RAM drive, to get maximal speed.

A very fast Operating System is an operating system that is built from sources to prevent performance issues. That way everything can be tailored and only what is needed by the HSM can be kept. There are several ways to do this such as using the Platform builder and similar tools to build a Windows Embedded OS or to use the "Linux From Scratch" project to make a dedicated distribution of Linux.

The HSM may have no operating system at all but firmware (e.g. a BIOS) loaded in ROM. HSMs OS are often built on specific (minimal) kernels without the concept of user mode.

When Buying a new HSM, one may want to question the vendor about the nature of the operating system (or firmware).

An important amount of RAM

Ram is a key factor for an HSM to work fast. Ideally, only physical RAM should be used. HSMs typically use different sorts of RAM such as Non-volatile RAM, DDRAM, etc… These memory modules should have enough capacity to handle a large amount of operations.

Again, make sure the HSM has important RAM because in the years coming, HSM may have to act with more demand and may have to process more operations so it may be adequate to make sure the amount of RAM will be enough.

CPU power

As we mentioned, an HSM is a digital computer like the others. If it is equipped with a "weak" CPU it will perform poorly. Also, recall that the CPU must perform well - the same as with the RAM - during the lifetime of the HSM and eventually have to support increasing demand for operations. Therefore make sure the CPU is adequate and do not hesitate to question the vendor about this. What kind of CPU is it? What kind of architecture? (X86, ARM,Risc-V etc…) Does the CPU need a fan or a cooling device in general?

Crypto-CPU power

The crypto-processor of HSMs allows a significant offload when it comes to ciphering/deciphering, especially for asymmetric cryptography.

The crypto-processors are performing RSA or Elliptic curves encryption/decryption in the processor itself. Crypto-processors are generally perceived as accelerating cryptographic operations.

These processors can also come with various architectures: MIPS or ARM for instance and they can use either FPGA or ASIC hardware.

Their power is measured by the quantity of ciphering/deciphering that they can perform by seconds, for a given algorithm of course.

It is a good idea to ask for a benchmark of the capacities of the crypto-processor of the HSM.

Here is a typical example of such a benchmark.

	Se12		Se52		Se500		Se1500	
	PCIe	LAN	PCIe	LAN	PCIe	LAN	PCIe	LAN
RSA signature generation (tps*)								
2048 Bit	16	16	80	75	690	580	960	780
4096 Bit	2	2	11	11	100	90	160	150
RSA bulk signature generation (tps*)								
2048 Bit	16	16	85	80	2200	2100	3400	3200
4096 Bit	2	2	11	11	220	220	360	360
Elliptic Curve signature generation (tps*)								
224 Bit	150	140	1000	880	1300	1040	1900	1400
384 Bit	50	50	450	390	950	790	1400	1100
Elliptic Curve bulk signature generation (tps*)								
224 Bit	160	160	1400	1300	1800	1700	3500	3100
384 Bit	54	54	490	490	1300	1200	2400	2200

Network and I/O

Finally, the speed of the HSM depends also greatly on the I/O operations and especially the network speed. An HSM should be ideally configured with a network latency of 0.5 ms.

Ask also the vendor about the type of disk storage used, SSD or Flash for instance, and the overall I/O performances. Make sure you buy a "beast" and not a weak HSM which will not perform fast enough for your ever-increasing demanding operations.

Conclusion

We aimed here to give some tips for those who wish to acquire a modern and fast HSM. It is a good practice to enquire about the hardware specifications of the HSM and make sure it is fast and will stay fast during its lifetime. If you are buying an expensive product, you have the right and should inquire about its detailed specifications to make sure that you're buying a fast HSM.