

Crypto board (HSM)

Technical specifications

- ARM7TDMI Risc CPU.
- 50 or 60 MHz bus speed (it depends on version).
- Two RSA co-processors.
- DES symmetric co-processor.
- Extreme speed dedicated bus for symmetric operation.
- 128 Kbytes top security RAM (400 mbps) (erased immediately after intrusion detection) .
- Up to 2 Mbytes CPU-external protected storage.
- Hardware True Random Number Generator (RNG).
- Asynchronous communications port capabilities. It can be configured to meet different protocols (RS-232, I2C, USB etc...) fully isolated from CPU and memory.
- PCI 2.2 interface.
- Real Time Clock (RTC).
- Epoxy filled hard steel cover.
- Intrusion detection sensors (temperature, physical access, voltage...)



Functional characteristics

The system is composed of a cryptographic board with flexible internal software, allowing the host to access its functionality, with the following capabilities:

- Symmetric key encryption, Data Encryption Standard (DES), two keys triple DES, three keys triple DES, and Secure And Fast Encryption Routine (SAFER) with 64 and 128 bit and with K and SK modes, all of them can be run in:
 - Electronic Code Book (ECB),
 - Cipher Block Chaining (CBC),
 - Cipher Feedback 64 bit (CFB-64),
 - Output Feedback 64 bit (OFC-64).
- HASH Functions: MD5, SHA-1 y RIPEMD (128 and 160 bits)
- RSA Public key standard with up to 4098 bit key length.
- Time Stamping.
- Robust key generation, using a true Random Number Generator RNG following FIPS 140-2, according to FIPS 186-2 specifications and FIPS 140-2 approved.

Security levels

This hardware is fully FIPS 140-2 level 3 compliant and is certified by NIST.

- The module firmware protects any confidential data to be outputted of the HSM.
- Accessing the protected cryptographic boundary is impossible due to the intrusion detection systems incorporated, actively clearing all information. All the cryptographic boundary is covered with an epoxy resin and covered with a 1 mm thick steel covering.
- Secure system allowing key uploads and safe key custody via asyna terminal conection.
- Possibility to assign key properties per user.

Other characteristics

Another interesting aspects are:

- One of the firmware versions support PKCS#11 standard. Due to this compliancy the HSM is available to be integrated with any application using this standard. There are specific versions for other environments and with its specific protocols.
- Banking PINBLOCK management functions included.
- It is possible to use several boards in parallel allowing any speed requirement to be met.
- The firmware is upgradeable, using a secured authentication system, and providing a mechanism for having the HSM always up to date.
- The internal design of the HSM allows future implementation of new algorithms, as for example asymmetric algorithms up to 4096 bits and elliptic curve algorithms.
- The HSM can be upgraded with client specific applications, enabling users to create its own security environment.

Performance

Symmetric Key Algorithms:

The following speeds are valid with a sustained data flow. The real world speed depends on the access mode user implemented in each application and the application itself.

Function	Throughputs (Mbps)			
	ECB	CBC	OFB64	CFB64
DES	400	355	355	355
3DES 2 or 3 keys	400	128	128	128
SAFER K64 6 loops	533	457	457	457
SAFER SK64 8 loops	400	355	355	355
SAFER K128 10 loops	320	291	291	291
SAFER SK128 10 loops	320	291	291	291

Hash:

The same as in the latter explanation. It depends on specific user implementation.

Function	Throughputs (Mbps)
MD5	393
RIPED-128	393
RIPED-160	316
SHA-1	316

Asymmetric Key Algorithms:

The performance of these algorithms depends mainly on the key length. The HSM has two independent co-processors, and the following are performance data of one of these units. The full performance depends on the complete usage of the two units in parallel, allowing in the best case the double of the capacity in the table.

Function	Throughputs (exp/s) ¹⁾	
	Without CRT	With CRT ⁵⁾
1024 bit exponentiation public key ²⁾	7240	ND ⁶⁾
2048 bit exponentiation public key ²⁾	2275	ND ⁶⁾
1024 bit exponentiation private key ³⁾	337	688
2048 bit exponentiation private key ⁴⁾	43	166

The following table shows RSA key generation times with several Miller-Rabin test runs, thus assuring a false positive probability below 2^{-100} .

Tamaño del módulo	Rendimiento (parejas de claves/hora)
768 bit	13.846
1024 bit	7.826
2048 bit	1.358