

TECHNICAL INFORMATION

HSM Server

Technical Specifications

HSM System

- Processor with RISC, ARM7TDMI architecture at 50MHz
- Cryptographic acceleration: two RSA co-processors and a symmetrically and hash encrypted co-processor.
- Specific address bus for very high speed symmetrically encrypted operations
- 128 Kbytes of high security internal memory (this memory is automatically erased upon intrusion).
2,1 Mbytes of high security internal storage.
- Random numbers generator compliant with FIPS 186-2 with modification note and hardware seed generation.
- Asynchronous communications port RS-232 separate from the processor and the memory.
- Real time clock
- Protection cover with epoxy resin and reinforced metal casing of 0,9mm steel sheets.
- Intrusion sensors (physical access, temperature and pressure).

Server System

- Processor with Intel architecture of 3.06GHz
- 512MB of internal memory
- Two ETHERNET connections 10/100/1000 Mbps

Cryptographic Capacities

- Symmetric cipher encryption:
 - simple DES, triple DES with double length cipher, triple DES with triple length cipher
 - SAFER in 64 and 128 bits and in K and SK modes; and in the following modes: ECB, CBC, CFB-64 and OFC-64.
- Hash Functions
 - MD5
 - SHA-1
 - RIPEMD in 128 and 160 bits
- RSA standard public cipher with cipher length up to 4.096 bits
- Time control, for Time Stamping
- Cipher generation via a random numbers generator, in accordance with the specifications of FIPS 186-2 with modification note and approved by FIPS 140-2.

Security

- The HSM complies with the FIPS 140-2 certification standard, level 3.
- The module's firmware impedes the outflow of confidential data.
- Access to diverse areas of the HSM is prevented with sensors which detect intrusions or anomalies, erasing the information.
- The HSM is covered by an opaque epoxy resin; a metal cover protects the whole ensemble.
- Secure system for the loading and storage of ciphers of external origin via a direct connection to the control board of an asynchronous terminal.

Functional Characteristics

System Access

The server allows access to the HSM via a network. To send a command the client application must form a TCP packet in accordance with the format of the chosen command. In the case of the PKCS#11 interface a layer of software is delivered compliant with the standard required for network communication. In all cases, the system allows the receipt of concurrent requests from one or various clients.

In addition to access via network, there is a series connection, direct to the HSM, for a VT100 terminal. Via this connection administrative tasks are carried out such as up-dates, registration and cancellation of users and loading of ciphers, amongst others.

Functionalities Included

CryptosecLan is a product oriented towards general use cryptography. It allows user administration, the loading, erasing and up-dating of ciphers and generic cryptographic calculation such as encryption/decryption or calculation/verification of signatures.

Extension of the Functions

In accordance with Client requirements, it is possible to incorporate into CryptosecLan functions of interest, such as the operation of PIN blocking, of Validation codes or of any other function either based on a standard or of their own design.

Similarly it is possible to incorporate other cryptographic or hash algorithms, such as DSA or different algorithms of the SHA family.

These extensions can be incorporated into the server at any time, via an update of the firmware.

Performance

There follows an illustration of operational capabilities under symmetric, hash encryption and asymmetric encryption. The performance of the server is limited by ETHERNET connections and depends in any event on network traffic. To obtain performance information on any of the specific server functions, contact REALSEC.

- *Asymmetric Cipher*

<i>Function</i>	<i>Maximum performance (Mbps)</i>			
	<i>ECB</i>	<i>CBC</i>	<i>OFB64</i>	<i>CFB64</i>
DES	400	355	355	355
3DES 2 or 3 ciphers	400	128	128	128
SAFER K64 6 repeats	533	457	457	457
SAFER SK64 8 repeats	400	355	355	355
SAFER K128 10 repeats	320	291	291	291
SAFER SK128 10 repeats	320	291	291	291

- *Hash:*

<i>Function</i>	<i>Performance (Mbps)</i>
MD5	393
RIPEMD-128	393
RIPEMD-160	316
SHA-1	316

- *Asymmetric Cipher:*

The performance of the symmetric cipher operation depends to a large degree on the length of the ciphers and specifically on their values.

<i>Function</i>	<i>Performance (exp/s)¹⁾</i>	
	<i>Without embedded</i>	<i>With embedded⁵⁾</i>
Exponentiation 1024 bit public cipher ²⁾	7240	ND ⁶⁾
Exponentiation 2048 bit public cipher ²⁾	2275	ND ⁶⁾
Exponentiation 1024 bit private cipher ³⁾	337	688
Exponentiation 2048 bit private cipher ⁴⁾	43	166

Notes:

- 1) The modules used with the public ciphers are odd, not even
- 2) The exponent of the public cipher is 216+1
- 3) The private cipher is of 1024 bits and contains approximately the same number of "0" and "1"
- 4) The private cipher is of 2048 bit and contains approximately the same number of "0" and "1"
- 5) For the CRT performance test, the public and private ciphers are of the same length
- 6) The CRT algorithm can only be used when both the public and private ciphers are known