

CRYPTOSEC 2048

The objective of this laboratory is the analysis and evaluation of Cryptosec 2048 from Realia Technologies S.L. (REALSEC). Cryptosec 2048 consists of a hardware security module (HSM, Hardware Security Module) and a complete interface which facilitates the integration process with any system, as well as the development of new systems which need to use some of the services provided by Cryptosec. The system consists of a cryptographic module whose main functions are the generation, storage and protection of cryptographic ciphers but, also, it provides hardware acceleration for cryptographic operations such as encryption/decryption. The hardware integrates easily into the server via a PCI interface. In addition, it complies with the FIPS 140-2 certification standard, level 3, which certifies the security of the product.

IDENTIFICATION OF THE PRODUCT

Cryptosec provides support to cryptographic operations securely and with high performance.

Product: Cryptosec 2048

Company: Realia Technologies S.L. (REALSEC)

Contact details: www.realsec.com

Increasingly, cryptography is a key factor in the business processes of organizations. The appropriate use of cryptography facilitates the resolution of the main problems of security: privacy, integrity, authentication and non repudiation. The bases of cryptography are cryptography ciphers. The protection of these ciphers is found in the model of procedural security based on cryptography. From there follows the importance of secure storage of the cryptographic ciphers, as well as the necessity of high security support for cryptographic operations. The modules of hardware security, also known as HSM (Hardware Security Module) are currently the most appropriate solutions to the problem of storage and management of cryptographic ciphers and other sensitive data. Hardware solutions provide a greater level of protection than the standard ones based on software, and that is why they are the ones most used in environments with high security requirements.

The product evaluated in this laboratory, HSM from Realsec, is a module of hardware security, which includes hardware acceleration for encryption operations such as the generation of symmetric and asymmetric cryptographic ciphers via a random numbers generator, export and import of cryptographic ciphers, encryption/decryption operations with different cryptographic algorithms, public cipher (PKI) cryptography function via different summary or HASH functions, amongst others. The hardware acceleration enables the cryptographic operations to be carried out efficiently avoiding the slow-down that these processes tend to incur in systems based on cryptography.

The hardware product HSM is accompanied by an application, Criptosec, which acts as an interface for tests with the hardware module. Said application allows the testing of all the functions provided by the hardware security module.

Cryptosec 2048 is a high capacity product which provides a powerful high security solution and performance for the recurring problems of all systems based on cryptography of the storage and management of cryptographic ciphers.

Amongst the main applications of Cryptosec 2048 we can find:

- Public cipher (PKI) infrastructure
- Encrypted communications
- Mass encryption of files and disks
- Data protection
- Secure execution of application code
- Digital safes
- Development of encrypted systems using the cryptographic model: payment media (EMV cards – Visa, Mastercard -, encryption of TPV communications and cash-point machines), digital signature validation procedures.

PHYSICAL DESCRIPTION OF THE PRODUCT

The hardware model evaluated is a PCI card with must be installed in equipment with a free slot compatible with PCI 2.1. The connection to the hardware module is via an RS-232 connection.

The module has external protection in the form of epoxy resin, as well as a reinforced iron-clad metal casing of 0,9mm steel sheets. It also has sensors for temperature, physical access and pressure which are used to detect possible intrusions within the system, erasing information in the event of an intrusion to avoid unauthorised access (tamper-resistant).

The modules incorporate an auxiliary lithium battery (ER17/50) system and a DB-15 plug for the electrical supply. It is not necessary to connect the battery for the module to work although it is recommended in order to maintain access to the module contents in the absence of PCI feed. The battery can be replaced while the module is in operation.



Figure 1. Cryptosec

Hardware specifications

- Processor with RISC ARM7TDMI architecture
- 50 MHz Address Bus (depending on version)
- Two RSA co-processors
- Address bus specific to high speed symmetric encryption operations
- 128 Kbytes of high security internal memory (it automatically erases in the event of an intrusion)
- 2,1 Mbytes of high speed internal storage
- Random number generation hardware
- Asymmetric communications port capacity configurable as RS-232, I2C, USB, etc., separate from the processor and the memory.
- PCI 2.1 Interface
- Real time clock
- Protection cover with epoxy resin and reinforced iron-clad metal casing of 0,9mm steel sheets.
- Intrusion sensors (physical access, temperature and pressure).

FUNCTIONAL SPECIFICATIONS

The system is composed of a cryptographic module with flexible software which interacts with the server, with the following functions:

- Symmetric cipher encryption: Data Encryption Standard (DES), 2 and 3 cipher TDES, Secure And Fast Encryption Routine (SAFER) in 64 and 128 bits and in K and SK modes. All of the above can be carried out in the following modes:
 - 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 and RIPEMD in 128 and 160 bits.
- Standard RSA public cipher with cipher length up to 4096 bits.
- Time control in order to mark time (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. The module can store more than 15000 DES and TDES ciphers and more than 1000 RSA (up to 2048 bits).
- Generation of encrypted PIN blocks or EPB (Encrypt Pin Block) for operations in banking environments. The Cryptosec EPB support formats are:
 - ISO-0 (o ANSI X9.8, VISA-1, ECI)
 - ISO-1 (o ECI-4)
 - ISO-2
 - IBM 3624

All Cryptosec functions have been tested with positive results during the evaluation of the product. To do this, an application was used which is provided with the hardware module and which implements all of the functions available within it. The application requires a connection via a VT100 terminal. Some of the main functions are listed as follows:

1. Open/close sessions. The first thing to do each time Cryptosec is to be used is to open a session with the hardware module. To do this, Cryptosec 2048 carries out authentication based on identity (fig.2)
2. Load/delete firmware
3. User management. Cryptosec facilitates the inclusion of more than 1000 users. The users can thereby manage their own ciphers with the HSM.
4. Copy/recovery of data. It facilitates copies and cipher restoration. It also facilitates the copying and recovery of an image from the module content.
5. Adjust the RTC (Real Time Clock) of the module.
6. Operations with public ciphers. Public ciphers can be obtained, loaded or deleted.
7. Initial Verification. This starts the checks carried out when switching on, with the exception of that of the firmware. (See fig 3)
8. RSA Operation. It provides commands for generation, deletion, exportation, importation, encryption, decryption, signature generation, consistency checking, amongst others.
9. DES operation. Provides commands for generation, deletion, exportation, importation, encryption, decryption, hash operations and creation of transport cipher for the secure exportation of ciphers, amongst others.
10. Encrypt Pin Block operations or EPB for banking environments. It facilitates the generation and encryption of the PIN Block, EPB verification, change between different formats, etc. It also facilitates functions with VISA and American Express. Such as the generation and testing of the verification value of VISA cards (CVV, Card Verification Value) and American Express (CSC, Card Security Code).

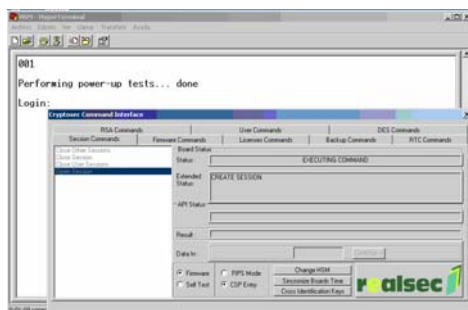


Figure 2.. Details of the “Open session” operation

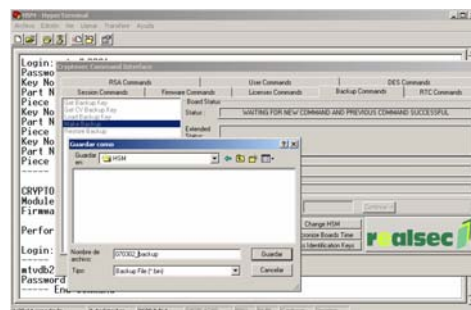


Figure 3. Detail of the security copy.

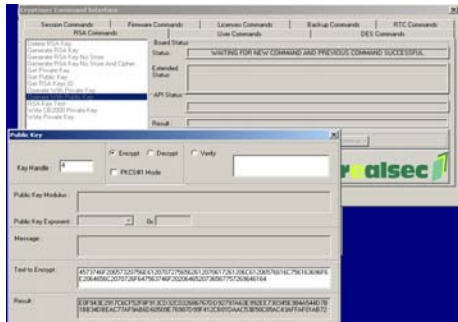


Figure 4. Detail of the text encryption with RSA.



Figure 5. Detail of the RSA cipher generation.

In relation to the integration of the HSM within Cryptosec with the security applications required for its use, Realsec provides interaction in its HSM via the PKCS#11 standard and a native API for the development of cryptographic applications. The PKCS#11 interfaces allow the use of hardware for a large range of cryptographic applications and this is, currently, the interface used in the majority of smart cards, for example. There is also the provision of a complete toolkit (API) which makes the integration process easier with any class of systems which need to use some or one of the services provided by Cryptosec. In fact, as well as the interface with the PKCS#1 standard, there are other interfaces specific to the HSM, such as for example interfaces for online banking operations, for card personalization or for motorway tolls. So, the functionality of the product can easily be extended with the ability to create interfaces to measure for whatever application it is required to integrate into the HSM, this way the integration is possible with existing products which do not use standard interfaces.

With regard to the hardware/software compatibility, the only product requirement is the availability of a PCI slot in the server in which the hardware module can be installed and that this server has a win32 operating system, as currently only drivers for these operating systems are available.

SECURITY

The two operational modes which Cryptosec provides have been identified and positively valued:

- **FIPS Mode.** In this mode the only functions which appear as available are those functions permitted and/or approved in the security evaluation carried out by the NIST (National Institute of Standards and Technology) where Cryptosec obtained a level 3 certification of security for the FIPS 140-2 standard. The supported algorithms in FIPS mode are: generation of RSA ciphers and signatures, DES and TDES generation and encryption/decryption and summary function SHA-1.
- **General Mode.** In this mode there is extended functionality not required in the FIPS 140-2 evaluation and, therefore, its security has not been evaluated by the NIST. In addition, in this mode Cryptosec has the following algorithms: encryption/decryption with RSA, summary functions MD5 and RIPEMD.

The NIST evaluates the security characteristics that a product must comply with in accordance with security levels 1 to 4. In the case of HSM it applies the security evaluation of FIPS 140-2 cryptographic modules. The level 3 verified for Cryptosec is the highest level awarded to cryptographic modules and corresponds to level EAL3 or above of the security evaluation standard Common Criteria 2.1 (ISO/IEC 15408).

FIPS 140-2 Level 3 Security represents:

Protection of the mechanism from unauthorized physical access (tamper-evidence). All the components of the HSM are covered with an opaque epoxy resin and, in addition, the whole ensemble is protected by a metal cover. Also, it has a response mechanism in the face of possible intrusions (tamper-response). In such cases, the internal memory is erased. This memory contains the firmware and the key cipher of the firmware, which prevents access to sensitive information.

- Authentication based on identity. The module authenticates the user by verifying his identity, with a robust authentication system, and also verifies his role in the system by checking if he has authorization to carry out the services requested. Cryptosec has two roles: super-user (or Crypto-Officer) and user, thereby distinguishing administrative tasks from others.
- Critical data is physically separated from the rest and the input and output of this data is encrypted. All sensitive information is entered into the module or sent from it via the RS-232 port (requires connection via console to the server in which the module is installed). Also, the firmware of the module prevents the output of confidential data.
- The server on which the module is installed must comply with the requirements of the Common Criteria level EAL3 or above. Currently the operating systems supported by Cryptosec (Microsoft Windows 2000 and 2003) comply with the requirements.
- A high level language is provided for interaction with the module. Cryptosec has complete documentation on the C++ categories used to hide the protocol from the user for low level communication with the module, so that code may be developed to programme applications which use the HSM without needing to know this protocol.



With the product, descriptive documentation is provided about the capacities of the product directly related to security, from a description of the product to the internal functioning of it. It should be noted that this documentation also includes recommendations for safe use of the product included within the security guidelines.

PERFORMANCE

In tables 1 to 41 the performance can be observed, assuming a continuous flow of data, for the supported algorithms.

Function	Maximum Performance (Mbps)			
	ECB	CBC	OFB64	CFB64
DES	400	355	355	355
3DES 2 or 3 length 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

Table 1. Performance for symmetric algorithms

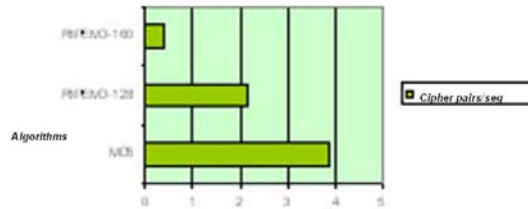


Table 2. Performance for hash functions

In the case of asymmetric algorithms, the performance depends in great measure on the cipher length. The HSM has two asymmetric cipher processing units. The data on table 3 shows the performance obtained with these two units (and one single HSM).

¹ The performance data has been collated in the controlled environment of the Realsec laboratory with Pentium III equipment at 700 MHz with 256 MB of RAM and Windows 2000 and XP operating systems.

Function	Performance (exp/s) ¹⁾	
	Without embedded CRT	With embedded CRT
Exponentiation 1024 bit public cipher	7240	ND
Exponentiation 2048 bit public cipher	2275	ND
Exponentiation 1024 bit private cipher	337	688
Exponentiation 2048 bit private cipher	43	166

Table 3. Performance for asymmetric algorithms

Finally, in Table 4 the generation of RSA cipher times are shown with an amount of passed Miller-Rabin tests to ensure a probability of false positives of less than 2^{100} .

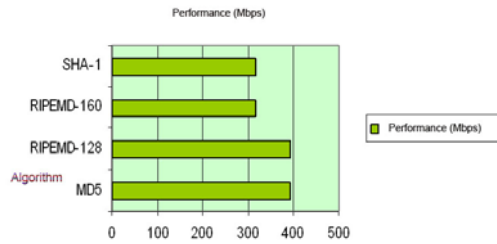


Table 4. The Generation of RSA cipher

OTHER CHARACTERISTICS

According to the evaluation methodology of the quality of software used, as well as the characteristics seen up to now, the reliability of the product and the ease of administration have also been evaluated due to their significance in the end quality of the software.

SATISFACTION WITH THE PRODUCT

By way of support for the results of the products external characteristics evaluation, surveys were also submitted to different companies using the module to measure the degree of satisfaction with Cryptosec 2048 and thereby try and obtain the degree of product quality whilst in use.

In table 5 the results of the surveys can be seen, in which the Cryptosec clients have awarded points from 1 to 10 for the different characteristics of the product. características dadas en el producto.

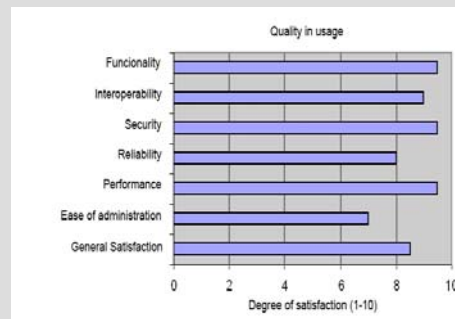


Table 5. Degree of Satisfaction of Cryptosec 2048 clients

EURO 6000 is one of the companies using Cryptosec 2048. EURO 6000 developed in conjunction with Realsec a specific interface to provide an adapted solution for the requirements of the EURO 6000 Savings Banks. Amongst the main applications of note is the support of sector standard management and administration operatives, as well as of the new operatives (EMV, e-commerce, Via T or the dynamic management of ciphers in the terminals, amongst others). Secure access is also possible for applets "on-line" and "off-line" and it has a precise interface for administrative tasks and for secure printing of the PIN codes and cipher components.

In relation to the reliability of the product, although Cryptosec does not provide specific fault tolerance mechanisms, it does offer the possibility of working with various HSM simultaneously, so that mechanisms of this type can be implemented at

a superior level to the HSM (software). On the other hand, the HSM does not have an operating system, or other characteristics such as dynamic memory management. This simplicity of design makes the HSM a highly robust device by avoiding all possible fault points related to these elements. Also, Cryptosec 2048 separates the areas of memory and temporary data from the storage area of critical data such as ciphers and users. With regard to the recovery capacity, it provides options to effect back-ups and data recovery. Finally, Cryptosec has a function which allows verification tests of the firmware integrity and the stored ciphers and which can be carried out from the interface at any time.

With regard to the administration of the product, the installation is very easy. The module need simply be installed in a PCI slot and thereafter install the drivers provided and load the firmware.

The administration is subsequently carried out via the interface with HSM provided by the product. This interface is a graphic application based on easy to use BSAFE of RSA. The initial configuration of the module is also very simple, the VT100 session need only be opened and then a session with the interface. From there, users, ciphers, etc can be created. The up-dating of the product is also very easy. The only thing to bear in mind is that a back up of data must be made as up-dating the firmware erases all data stored on the module. Finally, with regard to the usability of the interface, the application is very simple. For its use, full and complete documentation is provided: user and administrator manuals, as well as those already mentioned previously (programmer manual and documentation about security policy). It does not have on-line help or related help messages, for example, with errors in the entry of data into the application there are no messages which help correct this entry, and this can make the initial learning process of how to use it more difficult but, given the simplicity of the tool and how it is not oriented towards the user but towards the administrator for whom we may assume advanced knowledge on application use, it should not be a problem. The interface of the application is very austere and, in so being, is an accurate reflection of the simplicity on which the product is based in order to concentrate on security and reliability as the main objectives in its development.

EQUIPMENT USED IN THE EVALUATION	
✓	HSM Cryptosec 2048 with firmware version v.02.04 (Build 0001)
✓	PCs Pentium III 700 Mhz with 256 MB of RAM and 2800 Mhz with 1.8GB of RAM with operating systems Microsoft Windows 2000, 2003 and XP.
✓	As physical infrastructure local Ethernet 100BaseT networks have been used CISCO communications equipment (Catalyst 2950 and 2800 routers)
✓	Protocols analyzer for the monitoring of communications
✓	Application of tests to measure the performance of the HSM
✓	Application of simulation of intrusion attacks and security scanner

In relation to the mobility of the product, it is capable of exporting and importing ciphers towards and from modules from other manufacturers, which increases the ease with which it can replace other products of similar characteristics or be replaced by one of them.

CONCLUSIONS

Cryptosec 2048 is a high range cryptographic accelerator which provides cryptographic and secure storage services of encrypted ciphers, essential in all environments with very demanding requirements relating to security.

The results obtained after submitting the product to continuous evaluation tests during one month, demonstrate that the product is of high quality as much in the high

level of functionality that it provides, as well as in the stability and security demonstrated via the most important security certification currently available. Its high performance is also noteworthy both in the generation of ciphers and in the encryption/decryption of data. In addition, the simple design on which the product is based gives it a great versatility enabling it to be easily integrated and making possible the extension of its initial characteristics providing, for example, the possibility of implementing fault tolerance mechanisms to provide reliability to the applications which make use of it.

EVALUTATION TEAM
<p>Prof. Maite Villalba de Benito Prof. Dr. Luis Fernández Sanz DPRIS Investigation Group (Software programming and engineering) European University of Madrid</p> 