Follow us on:

cryptosec

PCI VERSION 1.0

THE SOLUTION

Hardware Security Module (HSM)

"In order to ensure the security of applications that perform digital signature, e-billing and encryption operations among others, organizations demand the advantages of hardware-based cryptographic systems, in other words, HSMs."

CryptoSign

VERSION 1.0

THE SOLUTION

A PCI compliant **Hardware Security Module (HSM)**. High performance, versatility and ease of deployment make it suitable for integrators.

realsec

The key to protecting your business

www.realsec.com

USA
303 Twin Dolphin Dr. Suite 600 Redwood City, CA 94065
Tel. +1 (650) 632 4240 • sales@realsec.com

HEADQUARTER
C/ Infanta Mercedes - Planta 4, 28020 Madrid (Spain)
Tel. +34 91 449 03 30 - Fax.+34 91 579 56 06
info@realsec.com

MEXICO
C/ Homero, 1.425, Planta 11. Col. Las Palmas. POLANCO
C.P. 11540 MEXICO DF. Tel. +52 (55) 44 35 00 46
infomexico@realsec.com

cryptosec

PCI VERSION 1.0

THE SOLUTION

GSA Schedule Contract GS-35F-121BA

> **"Hardware-based encryption systems are considered highly secure due to their integrity and independence from the systems they interact with."**

Functional Features

The system consists of a Cryptosec cryptographic hardware module (v.1.0) and a PKCS#11 firmware (v01.00.0308) with the following capabilities:

- RSA: signature, verification, encryption and de-cryption. Key length between 1024 and 4096 bits.
- DES, Triple DES-EDE, Triple DES-EEE: encryption and decryption.
- MD5 and SHA-1 hash functions.
- RNG.
- Key generation based on FIPS 186-2 validated Random Number Generator (with Change Notice) and FIPS 140-2 approved.

Security Levels

The HSM is equipped with self-protection mechanisms against physical attacks:

- Tampering.
- Fault injection.
- Processing emanation analysis.

Three types of users:

- Superuser.
- Operator.
- Custodian.

Two running modes:

- FIPS.
- Non-FIPS.

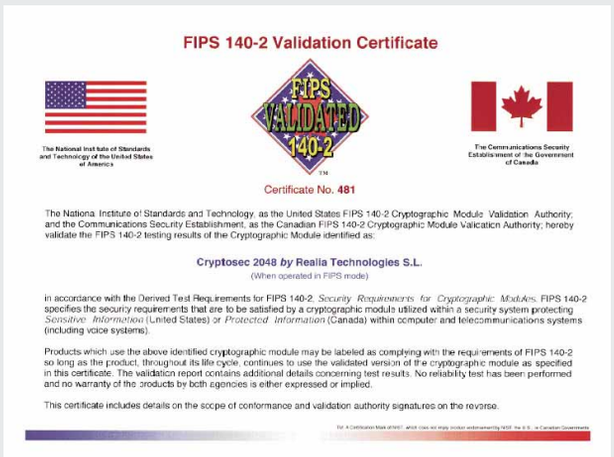
realsec
The key to protecting your business

Technical Specifications

- Two RSA coprocessors.
- Symmetric DES coprocessor.
- Special-purpose bus for high-speed symmetric encryption operations.
- 128 Kbytes of high-security internal memory (this memory is automatically deleted if a tampering attempt is detected).
- 2.1 Mbytes of high-security internal storage.
- Hardware Random Number Generator.
- Asynchronous communication port. Configurable as: RS-232, I2C, USB, etc., isolated from CPU and memory.
- PCI interface.
- Real-time clock.
- Epoxy resin protective covering and reinforced metal casing made of 0.9 mm steel plate.

Certifications

- FIPS 140-2, Level 3



FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

FIPS VALIDATED 140-2

The Communications Security Establishment of the Government of Canada

Certificate No. 481

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Cryptosec 2048 *by* Realia Technologies S.L.

(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.