Follow us on:

cryptosec

PCI VERSION 1.1

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

VERSIÓN 1.1

THE SOLUTION

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

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 1.1

THE SOLUTION

cryptoSign VERSION 1.1

GSA Schedule Contract GS-35F-121BA

Functional Features

The system consists of a cryptographic module with flexible software that transmits its functionality to the server and is equipped with the following capabilities:

- Symmetric-key encryption: Data Encryption Standard (DES), two-key Triple DES, three-key Triple DES, AES and Secure And Fast Encryption Routine (SAFER) 64 and 128 bits in K and SK modes. All of these algorithms can be executed in the following modes:
  - Electronic Code Block (ECB).
  - Cipher Block Chaining (CBC).
  - 64-bit Cipher FeedBack (CFB-64).
  - 64-bit Output FeedBack (OFC-64).
- Hash Functions: MD5, SHA-1, SHA-2 and RIPEMD (128 and 160 bits).
- RSA public key standard with key length up to 4096.
- Key generation based on FIPS 186-2 validated Random Number Generator (with Change Notice) and FIPS 140-2 approved.

Security Levels

- The module's firmware prevents output of confidential data.
- Access prevention to different parts of the cryptographic card using sensors that detect intrusions or anomalies and delete information (zeroization).
- All components are covered by an opaque epoxy resin and a metal casing to protect them all.
- TAMPER-RESPONSIVE: highest tamperization level. >>> State of the art anti-tamper mechanisms <<<
- Secure system for protection and key loading of externally generated keys through a secure direct connection using an asynchronous terminal.
- Possibility of assigning key ownership by users REALSEC.

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 capability. Configurable as: RS-232, I2C, USB, etc., isolated from CPU and memory.
- PCI Express Interface.
- Real-time clock.
- Epoxy resin protective covering and reinforced metal casing made of 0.9 mm steel plate.
- Intrusion sensors (temperature, physical access, voltage, etc.).

Certifications

- Common Criteria EAL 4+ (with ALC_FLR.1 augmentation)


In accordance with the authority granted under Act 11/2002, regulating the National Intelligence Centre, and applying articles 1 and 2, second paragraph, letter c, of Royal Decree 421/2004, 12th March, regulating the National Cryptologic Centre, I hereby:

Certify that the security of the CRYPTOSEC+FIRMWARE PKCS#11, version 1.0, developed by REALIA TECHNOLOGIES S.L., C/ Orense, 68, planta 11ª izda. 28020 Madrid , fulfills its Security Target identified as "Declaración de Seguridad de CRYPTOSEC+FIRMWARE PKCS#11-v1.0, version 1.0", 2010/06/21, to the extent defined by the evaluation assurance level EAL4+ (ALC_FLR.1), using the norms "Common Criteria for Information Technology Security Evaluation" and "Common Methodology for Information Technology Security Evaluation", version 3.1 R2.

Claimed Protection Profiles: None
Evaluation Facility: LGAI-APPLUS
Certification Report: INF-541

This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las T.I.C." at PRE/2740/2007, september the 19th.

The above-mentioned Security Target and Certification Report are available at the National Cryptologic Centre.

Madrid, August 25th 2010
Secretary of State Director

Félix Sanz Roldán