Cryptosec 2048
Realia Technologies S.L. (Realsec)
http://www.realsec.com/

FIPS 140-2 Level 3 Validation
Non-Proprietary Security Policy

INDEX

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cryptosec 2048 cryptographic accelerator from Realia Technologies S.L. This security policy describes how the Cryptosec 2048 meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 3 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Realia Technologies S.L. website, http://www.realsec.com/, contains information on the full line of products from Realia Technologies S.L.
- The NIST Validated Modules website, http://csrc.ncsl.nist.gov/cryptval/, contains contact information for answers to technical or sales-related questions for the module.
- Technical or sales-related questions can also be sent to info@realsec.com.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

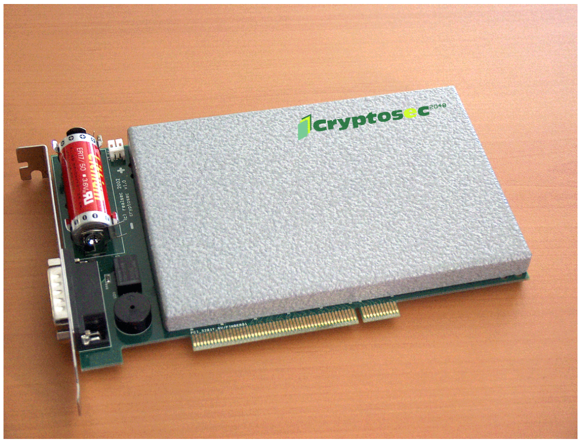
- Realia Technologies S.L. Vendor Evidence document.
- Finite State Machine.
- Module Source Code Listing.
- Hardware Schematics.
- Crypto Officer/User Guides.
- Other supporting documentation as additional references.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Realia Technologies S.L. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Realia Technologies S.L.

2 CRYPTOSEC 2048

2.1 Overview

The Cryptosec 2048 is a high-end PCI cryptographic accelerator card that provides cryptographic services and secure storage of cryptographic keys. The module is built to perform cryptographic processing and features a tamper-protective case to physically protect sensitive information contained within the card.



The Cryptosec 2048 supports the following algorithms approved for use in a FIPS mode of operation:

- RSA key generation, signature generation/verification, and key wrapping.
- DES (only to be used in legacy systems) and TDES (2-key and 3-key) generation, encryption and decryption. In many cases below, the Security Policy refers to “DES” as the cryptographic services provided in FIPS PUB 46-3, that includes the DEA and TDEA, commonly referred to as DES and TDES. Unless explicitly stated, DES should imply both algorithms defined FIPS PUB 46-3.
- SHA-1 hashing.

The Cryptosec 2048 also supports the following algorithms for use in a non-FIPS mode of operation:

- RSA encryption/decryption.
- MD5 hashing.
- RIPEMD hashing.

The Cryptosec 2048 product design, development, test and production has satisfied the requirements to ensure a secure product. Security has been the focus of the development team, and the Cryptosec 2048 product has been designed from the ground up to incorporate security in all design and development steps.

The Cryptosec 2048, Hardware Model 1.0, firmware version 01.04.0010 is tested to meet the FIPS 140-2 security requirements for the levels shown in the following table. The overall module is tested FIPS 140-2 Security Level 3.

FIPS 140-2 Security Requirements	Section Level
1. Cryptographic Module Specification	3
2. Module Ports and Interfaces	3
3. Roles, Services, and Authentication	3
4. Finite State Model	3
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	3
8. EMI / EMC	3
9. Self Tests	3
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A

Cryptosec 2048 is comprised of the module itself and the supplied software drivers outside module boundary to access the functionality of the product. A special serial cable is also included.

2.2 Module Interfaces

The Cryptosec 2048 is classified as a multi-chip embedded module for FIPS 140-2 purposes. The FIPS 140-2 cryptographic boundary is defined by the perimeter of the protection covers. The battery system (battery clips, auxiliary battery connector), DB-15 power supply pin, power supply relay, the DB-15 connector and the buzzer are excluded from the security requirements of FIPS 140-2. The module is accessible only through well-defined interfaces.

The physical interfaces of the Cryptosec 2048 are: PCI port, buzzer (unused, disabled by firmware), RS-232 port, I2C port (unused, disabled by firmware), DB-15 power supply pin and battery system.

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Module Physical Interface	FIPS 140-2 Logical Interface
PCI, RS-232	Data Input Interface
PCI, RS-232	Data Output Interface
PCI	Control Input Interface
PCI	Status Output Interface
PCI, battery system and DB-15 power supply pin	Power Interface

All sensitive information that is entered to the module in plaintext form (like authentication data, cryptographic key components and cryptographic key component check values) is entered through the RS-232 port. All sensitive information that leaves the module in plaintext form (like cryptographic key components and cryptographic key component check values) is output through the RS-232 port. A trusted VT-100 or VT-100-like system must be connected to that port.

2.3 Roles and Services

The Cryptosec 2048 performs identity-based authentication. Operators are identified by a username and authenticated by a password. The role of an operator is assigned when the operator is created.

The strength of the authentication mechanism with 255 possible characters with repetition and a minimum of a 8-character password is 1 in 17,878,103,347,812,890,625 (255^8). The module delays a replay for five seconds when an incorrect password is entered. After three incorrect entries the session is closed and must be reestablished.

The status of the module can be viewed from two registers on the PCI bus. When using the supplied software drivers to access the module, the status is returned as the function call return value.

The roles supported by the module are two: Superuser (or Crypto-Officer) and User. The Superuser is a normal User with administrative privileges. There are unauthenticated services that do not provide any security functionality, those services are available to all roles.

2.3.1 Crypto-Officer Role

The following table summarizes the services available only to superusers:

Service	Description	Input	Output	CSP	Type of Access to CSP
Create User	Initializes a new User	User's ID, User's password	Status	User's password	Write
Delete User	Erases an existing User	Session ID and User's ID	Status		
Set time and date	Adjusts the module's RTC	Session ID and time and date info	Status		
Load work key	Loads the work key. (Not used in FIPS mode)	Session ID, number of custodians, work key components, users' ID and password	Status	Work key	Write
				Users' password	Read
Retrieve work key's CV	Computes the work key's CV (Not used in FIPS mode)	Session ID	Status and CV	Work key	Read
Work key exists	Checks work key existence (Not used in FIPS mode)	Session ID	Status and key existence	Work key	Read
Load back-up key	Loads the module's back-up key	Session ID, number of custodians, users' ID and password	Status	Back-up key	Write
				Users' password	Read
Get back-up key	Retrieves the back-up key	Session ID, number of custodians, users' ID and password	Status and back-up key components	Back-up key	Read
				Users' password	Read
Retrieve back-up key's CV	Computes the back-up key's CV	Session ID	Status and CV	Back-up key	Read
Create back-up	Creates a module's back-up	Session ID	Status and Back-up data	Every CSP apart form back-up key and work key	Read
Restore back-up	Restores a module's back-up	Session ID and Back-up data	Status	Every CSP apart form back-up key and work key	Write
Reset firmware	Clears the program memory	Session ID	Status	Every CSP	Lost
Load license	Loads a license file (Not used in	Session ID and License data	Status		

Service	Description	Input	Output	CSP	Type of Access to CSP
	FIPS mode)				
Generate license info file	Generates a license information file (Not used in FIPS mode)	Session ID	Status and license data		

2.3.2 User Role

The following table summarizes the services available to any User:

Service	Description	Input	Output	CSP	Type of Access to CSP
Power-up Test	Forces the execution of the power-up tests	Session ID	Status		
Create session	Logs an operator and creates a session ID	Session ID==NULL	Status and Session ID	User's password	Read
Close session	Closes a session	Session ID	Status		
RSA key generation	Generates a RSA key pair	Session ID, public exponent and modulus length	Status and key ID	Private key	Write
RSA key generation and no store	Generates a RSA key pair and exports it	Session ID, public exponent and modulus length	Status and key data		
RSA key generation, no store and cipher	Generates a RSA key pair and exports it in VIS format	Session ID, public exponent, modulus length and the exporting key ID	Status and ciphered key data		
RSA private	Performs a RSA private encryption	Session ID, key ID, data	Status and encrypted data	Private key	Read
RSA public	Performs a RSA public encryption	Session ID, key ID, data	Status and encrypted data		
Get public key	Retrieves a public key	Session ID and key ID	Status and key data		
Get private key	Retrieves a private key	Session ID and key ID	Status and key data	Private key Transport key	Read Read
Write private key	Loads a private key	Session ID and key data	Status and key Id	Private key Transport key User's DES key	Write Read Read
Erase RSA key	Deletes a User's RSA key	Session ID and key ID	Status	Private key	Lost
List RSA keys	Returns the User's RSA key IDs	Session ID	Status and key ID list	Private key	Read
Get users	Returns the users' ID	Session ID	Status and User info		
Set password	Sets a new User's password	Session ID and new password	Status	User's password	Write
Random24	Returns a 24-bit random number	Session ID	Status and data		
Get date and time	Reads the module's RTC	Session ID	Status and RTC data		
Hash finish	Terminates a hash session and returns the hash value	Session ID	Status and hash value		

Service	Description	Input	Output	CSP	Type of Access to CSP
Delete DES key	Deletes a User's DES key	Session ID and key ID	Status	DES key	Lost
Get DES key ID	Returns User's DES key Ids and their length	Session ID	Status and key ID list and lengths	DES key	Read
Get DES key parts	Returns a User 's DES key in n parts	Session ID, key ID and number of custodians	Status and key components	DES key	Read
Get DES key cipher	Returns a User's DES key ciphered	Session ID, DES key ID	Status and key data	DES key	Read
				Transport key	Read
Get CV DES key	Computes a User's DES key's CV	Session ID, DES key ID	Status and CV	DES key	Read
Load DES key parts	Loads a DES key in n parts	Session ID, number of custodians and users' ID and password	Status and key ID	DES key	Write
				Users' password	Read
Get CV transport key	Computes the transport key's CV	Session ID	Status and key's CV	Transport key	Read
Get transport key	Returns a User 's transport key in n parts	Session ID and number of custodians	Status and key components	Transport key	Read
Load transport key	Loads the User's transport key	Session ID, number of custodians and key components	Status	Transport key	Write
Derivate DES key	Performs the VISA key diversification algorithm	Session ID, Derivation key, Export key and derivation data	Status	Derivation key	Read
				Export key	Read
BCHU config	Configures the symmetric ciphering and hashing unit	Session ID and config data	Status		
Datab	Controls traffic to and from the symmetric unit	Session ID	Status		
Generate DES key	Generates a DES key	Session ID and key length	Status	DES key	Write
Get DES key ciphered	Returns a User's DES key ciphered with another User's DES key	Session ID, ciphering key ID and exported key ID	Status and ciphered key	Exported key	Read
				Ciphering key	Read
IV values	Returns the chain values of the active DES operation	Session ID	Status and chain values		
Load DES key list parts	Similar to Load DES key parts, but with n keys	Session ID, number of custodians, keys' lengths and users' ID and password	Status and key IDs	DES keys	Write
				Users' passwords	Read
Write private key CB2000®	Imports a private key in CB2000® format	Session ID and key info	Status and key ID	Transport key	Read
				Private key	Write
Use license	Makes use of a card emission item (Not used in FIPS mode)	Session ID	Status		
Read partial counter	Reads the number of licenses ready to be used	Session ID	Status and number of licenses		
Read total counter	Reads the number of licenses used	Session ID	Status and number of licenses		
Load DES key cipher	Loads a ciphered user's DES key	Session ID	Status and key ID	DES key	Write
				Transport key	Read
Load DES key ciphered	Loads a User's DES key ciphered with	Session ID, ciphering key ID and key data	Status and key ID	Ciphering DES key	Read

Service	Description	Input	Output	CSP	Type of Access to CSP
	another User's DES key			DES key	Write
Get OMR	Recovers the symmetric ciphering and hashing unit configuration	Session ID	Status and config data		
Get DES key public	Recovers a User's DES key ciphered with a public key	Session ID, key ID and public key	Status and export data	DES key	Read
Load DES key private	Loads a DES key ciphered with a public key	Session ID and public key	Status and key ID	DES key Private key	Write Read
Change mode	Switches between FIPS and non-FIPS mode	Session ID	Status		
RSA sign	Performs a RSA signature (partially)	Session ID, key ID, hash data, hash algorithm and signature format	Status, signature block length and signature block	Private key	Read
RSA verify	Performs a RSA signature verification (partially)	Session ID, public key length, public key data and signature block	Status, signature block length, signature block in clear, hash algorithm and signature format		

2.3.3 Unauthenticated Services

The following table shows the unauthenticated services:

Service	Description	Input	Output	CSP	Type of Access to CSP
Firmware Version	Returns the firmware version	Session ID if any, else, Session ID==NULL	Status and the firmware version, in the form MM.mm.bbbb, where MM is the major version number, mm is the minor version number and bbbb is the build number		
Get HSM Identification	Returns a unique 64-bit identification code	Session ID if any, else, Session ID==NULL	Status and the identification code		

2.4 Finite State Machine Model

The Cryptosec 2048 is designed around a FSM which is detailed in a proprietary document. Parties interested in reviewing this document should contact Realia Technologies S.L. via the sources listed in the Introduction section of this document.

2.5 Physical Security

The module provides tamper evidence and tamper response mechanisms. The metallic casing and the epoxy resin conform the tamper evidence mechanism. The tamper response is based on a zeroization circuitry.

The metallic non-removable covers are made of 0.9mm steel and they cover both sides of the PCB. The space between them is completely filled with epoxy resin, making the module more protected.

A wire runs inside both sides of the module. In case the wire is cut or broken in any way, the main processor tamper response mechanism is launched. The internal 128 KB memory is actively erased. This memory contains the main processor firmware and the Master Firmware key.

2.6 Operational Environment

This section does not apply. The Cryptosec 2048 does not provide a modifiable operational environment.

2.7 Key Management

2.7.1 Key Storage & Protection

Secret Keys:

The module can store up to 15000 general use DES and TDES (2-key and 3-key) keys. They are kept ciphered in the SRAM of the module. They are owned by their respective users. A User can have several keys. Secret keys can be exported and imported in several ways. They are also part of the back up.

There are also some special secret keys, with specific purposes:

- Backup key: it is a 3-key TDES. The back up file is encrypted/decrypted with this key. The Superuser can load and save this key. This is done by means of split knowledge key entry. It is stored in the internal processor memory.
- Transport key: it is a 3-key TDES, used to import and export keys, although other keys can be used with this purpose. Each User has a transport key, and is able to administrate it on its own. They are stored in the SRAM memory, protected by the Master Firmware key.
- Work key: it is a DES key, a TDES 2-key or a TDES 3-key. It is not used in FIPS mode. It is stored in the internal processor memory.
- Master Firmware key: it is a TDES 3-key. It is used to cipher the SRAM protected contents. It is generated automatically by the module, and it is never exported or revealed in any way. It is stored in the internal processor memory.

Private keys:

The module can store up to 1000 RSA keys. Their modulus may vary in length from 512 to 2048 bits. Take into account that in FIPS mode, the minimum accepted modulus length is 1024 bits. They are kept, into a PKCS#1 structure, ciphered by the Master Firmware key in the SRAM of the module. They are owned by users. A User can have several keys. Private keys can be exported and imported in several ways. They are also part of the back up.

The firmware protects the secret, private and public keys against unauthorized disclosure, unauthorized modification and unauthorized substitution requiring owner's authentication.

No one, not even the owner, can modify a key, but only the owner can delete its keys.

The administrators can erase users and other administrators, this implies the deletion of all the keys owned by that user.

2.7.2 Key Generation

The key generation algorithms differ from DES keys to RSA key pairs.

In the DES key case, the process starts generating a random number of the specified length. This value is compared with weak keys and semi-weak keys, if they do not match, the number is accepted as a DES key. Note that the parity bits are not set, although they can be set when exporting the key. This is to keep compatibility with some PIN block management functions (not included in this firmware version).

In the RSA key pair case, the process starts generating the prime numbers *p* and *q*, with length according to the specified modulus length. There are different possibilities regarding primality tests, they can be selected by the User. In FIPS mode, FIPS 186-2 specifications are followed.

2.7.3 Key Import and Export

There are three methods to import a symmetric key:

1. Split knowledge.

   Each custodian of each component is authenticated (one by one) before typing its part of the key. The key component is entered along with a corresponding CV. The cryptographic module calculates a CV and compares it to the CV entered. If the values do not match, an error occurred during key entry and the key is rejected.

   The n components are needed to restore the key imported. The key is assigned to the owner of the session.

2. Ciphered with a DES key.

   The owner of the key is authenticated before giving its key, which is ciphered with the Transport Key of the owner or with other key owned by the User.

3. Ciphered with a RSA key pair.

   The User can import the DES key previously ciphered with a public key, if the User owns the key pair.

There are three methods to export a symmetric key:

1. Split knowledge.

   Each custodian is authenticated (one by one) before getting its part of the key. The cryptographic module gives the CV of each part to be verified next time it was imported.

2. Ciphered with a DES key.

   The key is ciphered with the Transport Key of the owner.

3. Ciphered with a RSA key pair.

   The User can select a RSA key pair and export the DES key ciphered with the public part.

RSA key pairs are exported or imported ciphered with the transport key in a PKCS#1 RSA Private structure. The public parts are exportable freely and in clear, in a PKCS#1 RSA Public structure.

Although it is not an import/export mechanism, note that every key is saved and restored in the back-up process.

2.7.4 Key Zeroization

If the physical security mechanisms are activated, the back-up key, the work key and the Master Firmware key are actively zeroized, together with the firmware and other processor's internal memory contents. The User information, the rest of the secret keys and the private keys are not erased but retained in encrypted format, but they are unusable, as the Master Firmware key is zeroized.

The delete firmware command, followed by a reset, forces the activation of the process described in the former paragraph.

Key deletion and user deletion processes include the zeroization of key and user information.

2.7.5 Random Number Generator

The Cryptosec 2048 uses the FIPS approved RNG specified in FIPS 186-2 with change notice DSA-RNG using SHA-1 for generation of cryptographic keys and other purposes in FIPS mode. This RNG is seeded with the internal hardware-based RNG.

In non FIPS mode, the module only uses the internal hardware-based RNG.

A continuous test is performed on both.

2.8 EMI/EMC

The module conforms to FCC Part 15 Class B requirements for home use.

2.9 SELF TESTING

The Self-Tests that the module can perform are:

- Power-Up Tests
  - Integrity of Firmware Test (CRC-32).
  - TDES KAT (3-key, 2-key, single key (DES)).
  - SHA-1, MD5, RIPEMD-128, RIPEMD-160 KAT.
  - RSA KAT.
  - RNG KAT (FIPS 186-2 RNG).
- Conditional Tests
  - Pair-wise consistency Test (RSA).
  - Signature Generation/Verification Test (RSA).
  - Manual Key Entry Test.
  - Continuous RNG Test (applicable to the hardware-based RNG and also to the FIPS 186-2 RNG in FIPS mode).

The events that can produce the conditions are as follows:

EVENT (E) or FUNCTION (F)	CONDITION
Power up (E)	Firmware integrity test
Power up (E)	DES test
Power up (E)	Hash test
Power up (E)	RSA test
RSA key generation (F)	Pair wise consistence test
RSA key generation no store(F)	
RSA key generation, no store and cipher (F)	
Write private key(F)	
RSA key generation (F)	Sign verify test
RSA key generation no store (F)	
RSA key generation, no store and cipher (F)	
Write private key (F)	
Load backup key (F)	Manual key entrance test
Load transport key (F)	
Load DES key parts (F)	
Load DES key list parts (F)	
Load work key (F)	
First time the firmware is loaded (E)	Continuous RNG test
Create session (F)	
RSA public (F)	
Get backup key (F)	
Get transport key (F)	
Get DES key parts (F)	
RSA key generation (F)	
RSA key generation no store (F)	
RSA key generation, no store and cipher (F)	

If a power-up self-test error has occurred, the module displays an appropriate indicator via the status output interface. The module must be reset to clear the error condition, and then can resume normal operation. If the Error continues (hard-error) to occur, the module must be returned to the manufacturer for repair or the firmware must be replaced. If a conditional error occurs, the module clears the soft-error and resumes normal operation.

2.10 DESIGN ASSURANCE

Each release of the hardware is stored in a separate repository named by release number. Each hardware build is named, e.g.: v0.0, v0.1, v1.0, v1.1, v2.0, etc. The hardware version is shown on the space between the battery and the module's cover. It is also shown by means of the VT-100 terminal when the module is started.

Each release of the firmware is stored in a separate repository named by release number. Each hardware build is named, e.g.: v00.00.0000, v00.01.0001, v01.00.0010, v01.01.0000, v02.00.0004, etc. The firmware version is shown invoking a specific command. As the hardware version, it is also shown by means of the VT-100 terminal when the module is started.

User documentation is versioned like source. Each release of the documentation is stored in a separate repository named by release number. The documentation states the firmware version that it refers to.

2.11 MITIGATION OF OTHER ATTACKS

The Cryptosec 2048 does not employ any technology that mitigates against other attacks.

3 SECURE OPERATION OF THE CRYPTOSEC 2048

3.1 Secure administration

3.1.1 Initialization

When the module is received, the Superuser must check the module's case for evidence of tampering. Such indications include prying, bending, or cutting of the metal casing.

After checking the module for evidence of tampering, the Superuser must connect the module to the PCI port on the computer to be used. The RS-232 connection must also be established, using the supplied cable, with a VT-100 terminal or equivalent. Although it is not mandatory, the Superuser should connect the supplied battery, in order to keep the module's contents in absence of PCI power supply. The installation CD contains all the setup files needed to access the Cryptosec 2048 module.

The module is delivered in a blank state, this is, with no firmware loaded. It is necessary to load the firmware into the module. The firmware is supplied in a *.emb file. Once the firmware is loaded, the module resets and the CRC-32 check of the firmware is performed, along with other self-test. If they pass the module asks, through the RS-232 connection, for an unlock PIN. This value, with a length of 8 bytes, is sent to the client separately, and it is unique for that version of the firmware and that particular module. This unlock PIN is not retained in the module, and it is not needed after the firmware installation.

When the unlock PIN is correctly typed, the module asks for the login and password of the first User. This User will have Superuser privileges. The module must have at least one User, and that User must be Superuser. Nevertheless, the User created at this point can be deleted in the future, provided that there is another Superuser already created. In other cases, the module will start the Superuser creation automatically. This implies that there can be as many superusers as needed, and all of them operate as administrators without distinction.

3.1.2 Management

The module can be administered using the supplied managing User interface. This software allows the User to access all the functions supported by the module, and check the status of the module. Superuser and User guides are available from Realia Technologies S.L.

The Superuser can create Users up to the limit of 1000 accounts, including both users and superusers. Each User should modify the initial password given by the Superuser. The passwords do not expire.

As the users can create and load both RSA and DES keys, the Superuser should check how many keys each User owns, and define a policy regarding this subject. Superusers can delete a User, which deletes all of its keys, but can not directly delete keys of other users.

It is compulsory to make a back-up before upgrading the firmware, as this operation erases the memory of the module. Once the upgrade is finished, the back-up should be restored. A back-up scheme should be established by the organization using the module.

The Superuser is responsible for keeping track of the module and must routinely check the module for signs of physical tampering. If strange activity or damage to the case is apparent, the Superuser should take the module offline and investigate.

The battery must be changed every two years. It can be done while the module is working. If it is done in absence of PCI power supply, the operation should not last more than a minute.

3.1.3 Termination

When a module's usage has been completed, the module should be zeroized by the Superuser in order to wipe all sensitive data. This zeroization should be done by deleting the module's firmware, using the appropriate command, and taking apart the battery, if applicable. The module should then be stored in a secure location.

3.2 Secure operation

The User behavior with respect to the secure operation of the module is mainly related to the secret of the password and the keys or keys components that the User custodies. The User should be careful not to provide private keys and secret keys to other parties. The User should also not provide the User password to anyone.

4 FIPS 140-2 MODE OF OPERATION

FIPS 140-2 mode of operation is defined as a mode in which only FIPS allowed or approved security methods are used.

Whether the module operates in a FIPS Approved Mode of Operation or not is selected by the User. This is done by invoking the change mode service.

Any User can access the information regarding the FIPS or not FIPS state, its flag is part of the status of the module shown in the PCI port registers.

Note that there are some services not available in FIPS mode: those related to work key and licensing. Refer to 2.3.1 Crypto-Officer Role and 2.3.2 User Role for details.

4.1 Security Functions

4.1.1 Approved Security Functions

The following are the approved Security functions for FIPS 140-2 Mode of Operation:

The approved cryptographic algorithms are:

- FIPS 186-2 with change notice DSA-RNG using SHA-1.
- SHA-1 bit oriented.
- DES ECB.
- DES CBC.
- DES CFB64.
- DES OFB64.
- 2-key TDES ECB.
- 2-key TDES CBC.
- 2-key TDES CFB64.
- 2-key TDES OFB64.
- 3-key TDES ECB.
- 3-key TDES CBC.
- 3-key TDES CFB64.
- 3-key TDES OFB64.
- RSA signature generation/verification and key wrapping.

Note that DES is only to be used in legacy systems.

4.1.2 Non-Approved Security Functions

Non Approved Security Functions:

- Hardware-based RNG.
- RSA for general encryption/decryption.
- MD5.
- RIPEMD-160.
- RIPEMD-128.

The module's DES implementation includes a mechanism that can be used for calculating a DES-MAC: the module can output the appropriate DES blocks and an external application can used them to calculate the MAC value. Although the module does not implement the DES-MAC algorithm, it can be used for the calculation of the MAC.

As previously stated, the Cryptosec 2048 comes with the certified firmware revision compliant, tested and validated with FIPS 140-2.

5 GLOSSARY OF TERMS

The following table lists the terms discussed in this security policy and their respective definitions:

Term	Definition
DES	Data Encryption Standard
CB2000®	Crypto Board 2000
CBC	Cipher Block Chaining
CD	Compact Disk
CFB64	Cipher FeedBack (64-bit feedback data)
CRC	Cyclic Redundancy Checksum
CSP	Critical Security Parameter
CV	Check Value
CVV	VISA Card-Verification Value
DB-15	Sub D 15-pin connector
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FSM	Finite State Machine
I2C	Inter-Integrated Circuit
ID	Identification
MAC	Message Authentication Code
MD5	Message Digest 5
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OFB64	Output Feedback (64-bit feedback data)
PCB	Printed Circuit Board
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standard
RIPEMD	Race Integrity Primitives Evaluation Message Digest
RNG	Random Number Generator
RS-232	Recommended Standard 232
RSA	Rivest, Shamir and Adleman
RTC	Real Time Clock
SAFER	Secure And Fast Encryption Routine
SHA-1	Secure Hash Algorithm
SRAM	Static Random Access Memory
VIS	VISA Information Source
VT-100	DEC's Video Terminal 100