Incognito TSM410 Security Policy

Document number	PR-D2-0504
Revision	1.1
Authors	Giovanni Gallus, Richard Pitchers, Gary Rolfe, Trevor Davel
Date	August 2004
Synopsis	The Incognito TSM410 is a multi-chip embedded Tamper Responsive Security Module with a PCI interface that meets the Level 3 requirements laid down by FIPS PUB 140-2 (with Level 4 for physical security). This module supports cryptographic operations for Electronic Payment Systems including TDEA, SHS and rDSA. This document details the cryptographic module security policy for the Incognito TSM410, being a precise specification of the security rules under which the module will operate.

1. Contents

1.1 Figures

1.2 Tables

2. Overview

The Incognito TSM410 is a PCI bus multi-chip embedded security module housed in a hard opaque case. This Tamper Responsive Security Module (TRSM) is targeted at Electronic Payment Systems (EPS) including Electronic Funds Transfer (EFT) switches and mobile commerce.

The TSM410 is firmware upgradeable, with the firmware being split into a Boot Loader and an Application. Exactly one Boot Loader and at most one Application may be present in the module at any time. The Boot Loader's main purpose is to load authenticated applications.

This document refers to the Incognito TSM410 Module (Part Number 5520-00091 Rev 2) with FIPS Boot Loader (firmware version 1.1.1.0). Firmware Applications are not included in this security policy and will be evaluated separately.

Figure 1 is a photographic image of the Incognito TSM410. A block diagram of the module indicating the functional components, cryptographic boundary and physical interfaces is presented in Figure 2 (on page 8).

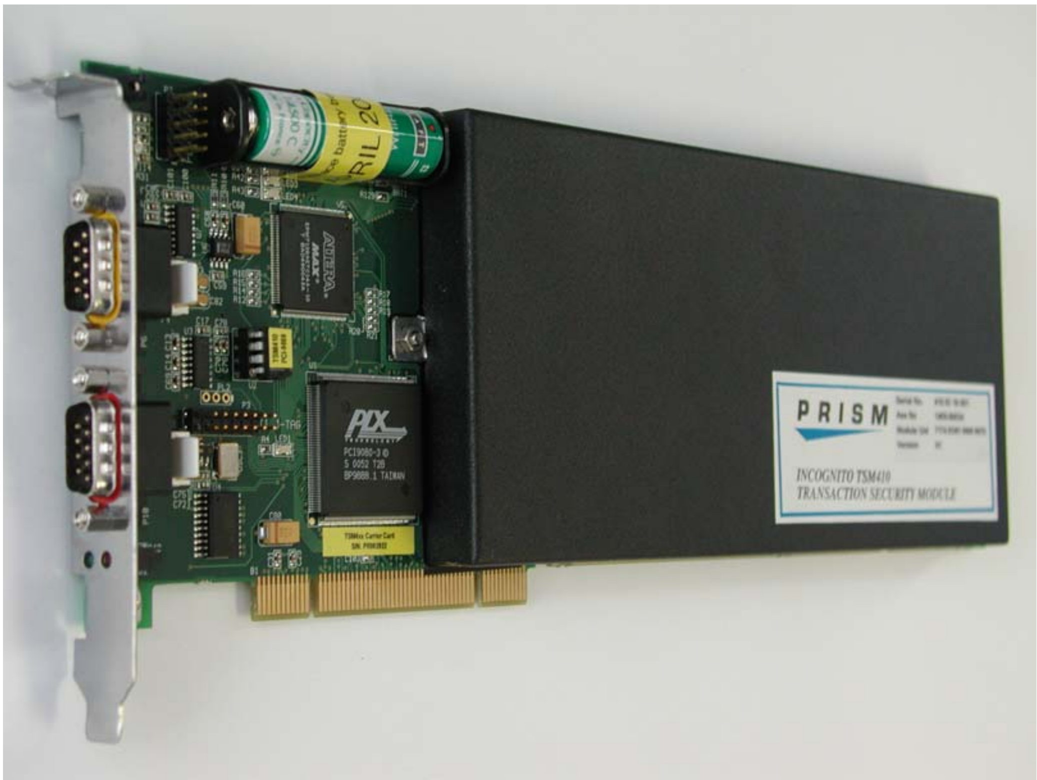

Figure 1. Incognito TSM410 on its PCI carrier card

3. Security Level

The TSM410 meets the overall requirements of Level 3 for FIPS 140-2 [1], as well as the Level 4 requirements for Physical Security.

A detailed breakdown of the FIPS requirements met by the TSM410 is given in Table 1.

FIPS 140-2 Security Requirement	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 1. Security Levels met for FIPS security requirements

3.1 Operational Environment

The FIPS 140-2 [1] Operational Environment requirements for cryptographic security modules are not applicable to the TSM410 as it qualifies as a limited operating environment.

There is no operating system running below the FIPS Boot Loader or Application firmware.

4. Modes of Operation

The user can determine the overall mode of operation of the TSM410 by executing the "Get Status" service.

4.1 FIPS Approved mode

The FIPS Boot Loader always executes in Approved mode [1]. This does not necessarily mean that the overall mode of operation of the TSM410 is always in an Approved mode.

The FIPS Boot Loader supports the FIPS Approved security functions given in Table 2 (on page 7).

Loading an Application that has been separately validated to FIPS 140-2 [1] shall result in a FIPS-validated TSM410 module that may operate in Approved mode, depending on the modes of operation of the Application. The "Get Status" service will indicate whether or not the module is operating in FIPS Approved mode.

4.2 Non-approved modes

The FIPS Boot Loader has no non-approved modes of operation.

Loading an Application that has been separately validated to FIPS 140-2 [1] shall result in a FIPS-validated TSM410 module that may operate in Approved mode, depending on the modes of operation of the Application. Loading an application that is not separately validated to FIPS 140-2 [1] shall result in a non-validated TSM410 module that may not operate in FIPS mode.

[1] "Approved mode of operation" as defined by FIPS PUB 140-2 [1] in the Glossary and Function Security Objectives.

FIPS Approved security function	Certification
Triple-DES (Triple DEA, TDEA, TDES) Triple Data Encryption Standard (Algorithm) per FIPS PUB 46-3 [2] and ANSI X9.52-1998 [3]. Support for encryption and decryption in ECB and CBC modes.	Certificate 259
DES (DEA) Data Encryption Standard (Algorithm) per FIPS PUB 46-3 [2] and FIPS PUB 81 [4]. Support for encryption and decryption in ECB and CBC modes.	Certificate 261
SHA-1 The SHA-1 algorithm of the Secure Hash Signature Standard (SHS) FIPS PUB 180-2 [5].	Certificate 241
Triple-DES MAC The Data Authentication Algorithm described in FIPS PUB 113 [6], using Triple-DES as the e() function (as permitted by FIPS 140-2 Annex A).	Vendor affirmed (TDES Cert. 259)
Enhanced Security DES MAC (Retail MAC, rMAC) The MAC algorithm described in Annex C of ANSI X9.19-1996 [7] ("Procedure To Prevent Exhaustive Key Determination"), equivalent to MAC Algorithm 3 of ISO 9797-1 (1999) [8].	Vendor affirmed (DES Cert. 261)
DAA (DES MAC) The Data Authentication Algorithm described in FIPS PUB 113 [6] and referred to as a MAC algorithm in ANSI X9.9-1994 [9], equivalent to MAC Algorithm 1 of ISO 9797-1 (1999) [8].	Vendor affirmed (DES Cert. 261)
rDSA Digital signature algorithm using reversible public key cryptography (based on RSA) per ANSI X9.31-1998 [10]. Support for key generation, digital signature creation and verification using various key sizes in the range 1024 to 2048 bits.	Vendor affirmed
FIPS-Approved random number generator	**Certification**
Deterministic Random Number Generator [1] (PRNG) Pseudo Random Number generation using the DEA in accordance with Appendix A to ANSI X9.31-1998 [10].	Vendor affirmed

Table 2. Approved security functions for FIPS Approved mode of operation

[1] The deterministic random number generator is used in the generation of all cryptographic keys.

5. Ports and Interfaces

Figure 2 illustrates the logical components of the Incognito TSM410 and their relationship to the cryptographic boundary. Each port (a physical interface, depicted outside the boundary) allows limited communication across the Security Boundary. The limits of this communication are governed by the logical interface associated with the port.

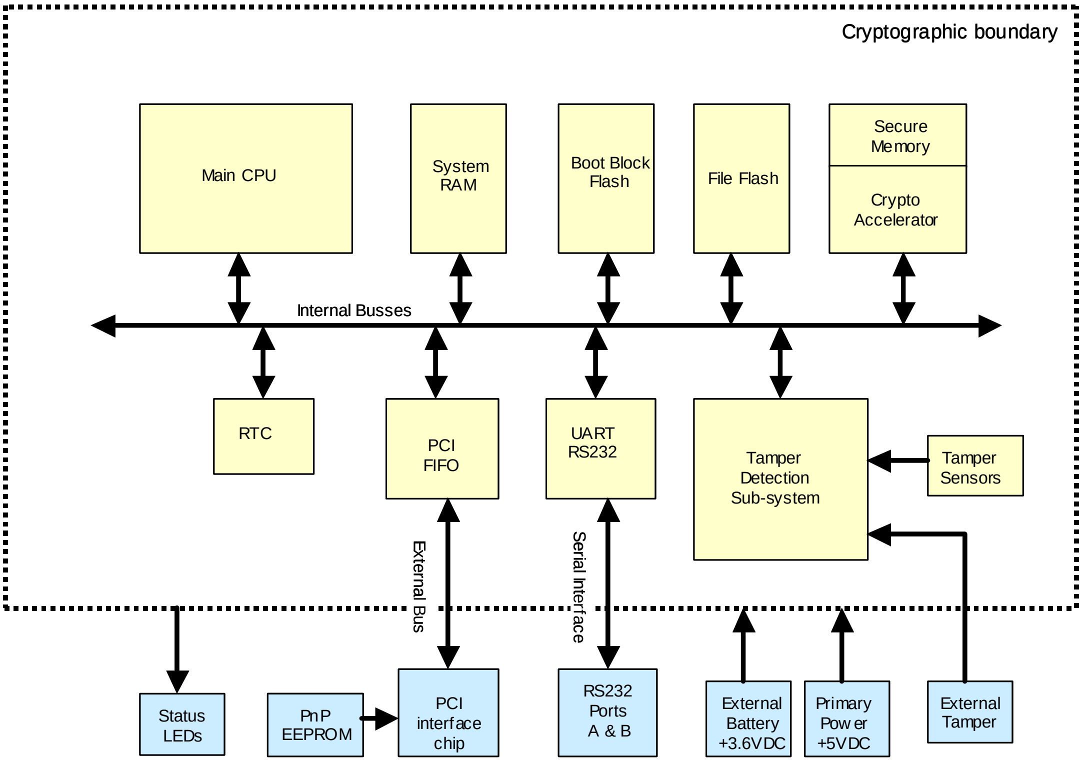

Figure 2. Incognito TSM410 functional components and cryptographic boundary

The relationships between the TSM410's ports and the FIPS Boot Loader's logical interfaces (as defined by FIPS PUB 140-2 [1]) are presented in Table 3.

FIPS 140-2 Logical Interface	Ports (physical Interfaces)
Data Input	External Bus (PCI); Serial Interface (RS232 Port B) [1]
Data Output	External Bus (PCI); Serial Interface (RS232 Port B)
Control Input	External Bus (PCI); External Tamper
Status Output	External Bus (PCI); Status LEDs
Power Port	Primary Power; External Battery
N/A	Serial Interface (RS232 Port A) [2]

Table 3. Physical and logical interfaces

[1] Serial Port B is dedicated for the entry of Critical Security Parameters (CSPs)

[2] Serial Port A is logically disconnected in the FIPS Boot Loader

6. Services

A service is a processing operation of the TSM410 that may be performed on demand by an operator. Not all services are available to all operators. The Access Control Policy (in section 7) restricts the availability and execution of services. The services that are authorised for each operator role are presented in Table 6 (on page 13).

All services require a control input (to execute the service) and produce a status output (the result of the operation). Some services may require data input or produce data output and/or additional status output. A summary of the data input and output requirements for each service is provided in Table 9 (on page 15).

The following services are provided by the TSM410 in conjunction with the FIPS Boot Loader.

6.1 Change Own Password

Allows the operator to change his/her password. This service only applies to operators acting in roles that employ a Username and Password authentication mechanism (see Table 4 on page 12). The operator's existing password must be supplied to authorise the change.

6.2 External Tamper

Any operator may activate the External Tamper control input (a port presented in Table 3 and Figure 2). This service does not require authentication of the operator, and otherwise has the same effect as the Force Tamper service.

6.3 Force Tamper

Forces the TSM410 into the Tampered state, immediately causing the zeroisation of Secure Memory (and thus the destruction of Critical Security Parameters).

6.4 Get Random Bytes

Uses the Deterministic Random Number Generator Approved algorithm (see Table 2) to generate an operator-defined number of random bytes. These bytes are then returned to the operator.

6.5 Get Status

Allows the operator to query the current status of the module's hardware and firmware. This service does not require authentication of the operator. The service returns detailed status information in addition to the "result of operation" status output that all services return.

The status LEDs by comparison indicate limited status information, but do so continuously.

Status information may include protected items other than Critical Security Parameters (CSPs), or information about protected items (other than CSPs) such as their presence, absence or identification.

6.6 Load Authenticated Application

The operator may use this service to introduce Application firmware to the module. Existing Application firmware (if any) will be erased in the process. Application firmware is signed by the Manufacturer to guarantee integrity and to authenticate its origin.

The act of updating an Application may qualify as an upgrade. This occurs when the firmware being loaded has the same distinguishing name (or identifier) as the existing Application and a version number greater than or equal to that of the existing Application, or when there is no existing Application.

To upgrade an Application requires authentication of the Manufacturer *only*, which is provided by the digital signature over the Application firmware. Protected items are not affected by an upgrade.

Loading an Application that is not an upgrade requires authorisation from a Cryptographic Officer *in addition to* authentication of the Manufacturer. Critical Security Parameters are zeroised by loading an Application in this manner, but other Protected Items are not affected.

In the instance that authentication (of the Manufacturer and/or Cryptographic Officer) fails, the existing Application firmware, if any, will not be erased.

6.7 Load Authenticated Public Key

Allows the Manufacturer to change a public key that is stored in the TSM410, and which is one of the keys used to authenticate the Manufacturer. The change must be authorised by the Manufacturer, and this process utilises the (existing) Manufacturer's Authentication Public Key.

6.8 Load Boot Loader

The operator may use this service to replace Boot Loader firmware in the module. Existing Boot Loader firmware will be erased in the process. Boot Loader firmware is signed by the Manufacturer to guarantee integrity and to authenticate its origin.

Replacing the Boot Loader requires authentication of the Manufacturer, which is provided by the digital signature over the Boot Loader firmware. Critical Security Parameters will be zeroised during the execution of this service, and various other protected items (excluding public keys) will be reset to factory default values.

6.9 Reset

Restarts the TSM410 causing the Boot Loader to execute and, in the process, invoke a suite of self-tests. Any operator may execute a reset, and no authentication is required.

The results of the self-tests may be obtained by executing the "Get Status" service, and any critical failure(s) will be indicated by the Status LEDs.

6.10 Reset Tamper

Forces the TSM410 out of the Tampered state, allowing it to resume normal operation. This operation can only complete successfully if there are no active tamper events at the time the service is executed.

The operator must inspect the module's opaque enclosure for evidence of tampering before executing this service.

6.11 Set Date and Time

This service sets the state of the Real-Time Clock (that is, the date and time).

6.12 Set Lost Password

Allows an operator having a role specified by the Manufacturer to enter a new password. The Manufacturer may authorise this service if an operator has lost his/her password.

7. Access Control Policy

The Access Control Policy for the TSM410 defines the operator roles, security-relevant protected data items, and the relationships between roles, protected items and services. In particular it is possible to identify for each service within each applicable role the protected items that may be accessed and the nature of this access.

7.1 Operator roles

The TSM410 supports three operator roles (presented in Table 4): Manufacturer, Cryptographic Officer and User.

Each role is entered separately for each execution of a service, and left when the service completes executing.

7.1.1 Manufacturer role

The Manufacturer role exists to allow the manufacturer of the TSM410 the ability to upgrade the module's firmware and security parameters, and to assist in recovery if operators have lost their passwords.

7.1.2 Cryptographic Officer role

The Cryptographic Officer role allows trusted operators to modify certain protected items, such as the Tamper state and Real-Time Clock (RTC) state. A Cryptographic Officer can also authorise the loading of Application Firmware (see section 6.6 for details).

This role matches the FIPS [1] definition for a Crypto Officer Role.

7.1.3 User role

The User role allows trusted operators to modify certain protected items, such as the Tamper state. A User can also obtain random data from the PRNG.

This role matches the FIPS [1] definition for a User Role.

7.2 Identification and Authentication

All roles require identity-based authentication using a sufficiently strong authentication mechanism. The supported roles, nature of authentication and authentication mechanisms are summarised in Table 4, while the strengths of the various authentication mechanisms are presented in Table 5.

Since a role is entered only for the period of execution of a single service (see section 7.1), the operator must identify and authenticate him/her-self every time a service (that requires a particular role) is executed.

7.2.1 rDSA digital signature mechanism

Operators having the Manufacturer role are authenticated by means of rDSA digital signatures. Public keys are stored in the module as protected data items; the Manufacturer has access to the corresponding private keys (which are never available to the module). A private key may be used to generate an rDSA signature over an instruction or data item (as described in ANSI X9.31-1998 [10]) providing identification and authentication of the operator.

Each rDSA key pair is generated in accordance with the provisions of ANSI X9.31-1998 [10], and length of the modulus of each key is at least 2048 bits.

7.2.2 Username and password mechanism

Cryptographic Officers and Users must supply a Username to identify themselves. An alphanumeric password is used for authentication. The operator must know the Username and password, while the module stores the Username along with a SHA-1 hash of the password. To identify and authenticate him/her-self, the operator presents his/her Username and password to the module. A SHA-1 hash of the operator-supplied password is performed, and the result compared against the stored password.

The password is randomly selected by the operator, and must be at least 7 characters long.

There are two predefined Cryptographic Officers Usernames (“CryptoOfficer1” and “CryptoOfficer2”) and one predefined User Username (“User1”) in the FIPS Boot Loader. Each Username must be assigned to a unique individual, and may not be treated as a general-purpose role-based name. The individual must be the only person to know the password that is associated with the Username, and must not share the password or store it (which could place it at risk of unauthorised disclosure and use).

Role	Nature of authentication	Authentication mechanism	Predefined identities
Manufacturer	Identity-based operator authentication	rDSA digital signature	Manufacturer
Cryptographic Officer	Identity-based operator authentication	Username and password	CryptoOfficer1 CryptoOfficer2
User	Identity-based operator authentication	Username and password	User1

Table 4. Operator roles, identities and authentication

7.2.3 Strengths of authentication mechanisms

The minimum security requirement of an authentication mechanism is that the maximum probability of falsifying an authentication in 1 minute is 1 in 100,000 (as required by FIPS [1]).

The cryptographic strengths of the authentication mechanisms that are employed are presented in Table 5. The overall strength of the mechanism has been enhanced by the implementation of a 2 second delay after a failed authentication, limiting the speed at which an attack can progress to at most 30 attempts per minute.

Authentication mechanism	Description and strength of mechanism
rDSA digital signature	The length of each key is at least 2048 bits, but the strength of the mechanism is limited to the strength of the SHA-1 hash (160 bits offering a 1 in 2^{80} chance of collision). At a possible 30 attempts per minute the probability of falsifying authentication in 1 minute is approximately 30 in 2^{80}, which is less than 1:100,000.
Username and password	Assuming a worst-case with only numeric passwords of minimum length (7 digits), the number of possible passwords is 10^7. At a possible 30 random attempts per minute the probability of falsifying authentication in 1 minute is 30 in 10^7, which is less than 1:100,000.

Table 5. Strengths of authentication mechanisms

7.3 Service access by role

Table 6 cross-references the authorised services of the FIPS Boot Loader with the supported roles that are permitted to access those services.

A tick indicates that the service is available to the corresponding role. Services indicated as “Role Independent” are not associated with a role and are always available to any operator. A blank space indicates that the service is unavailable to that role.

Authorized Service	Manufacturer Role	Cryptographic Officer Role	User Role	Role Independent [1]
Change Own Password		✓	✓	
External Tamper				✓
Force Tamper		✓	✓	
Get Random Bytes			✓	
Get Status				✓
Load Authenticated Application	✓	✓ [2]		
Load Authenticated Public Key	✓			
Load Boot Loader	✓			
Reset				✓
Reset Tamper		✓		
Set Date and Time		✓		
Set Lost Password	✓			

Table 6. Authorised services for operator roles

7.4 Protected items

Protected items are security-relevant data that are contained within the Cryptographic boundary, and must be protected against unauthorised access. Critical Security Parameters are a class of protected items.

7.4.1 Critical Security Parameters

Critical Security Parameters (CSPs) are protected against unauthorised substitution, modification or disclosure. The CSPs under the control of the FIPS Boot Loader are presented in Table 7.

Critical Security Parameter	Description and purpose
User1 password	This password exists temporarily when the operator “User1” submits his/her password to the TSM410.
CryptoOfficer1 password	This password exists temporarily when the operator “CryptoOfficer1” submits his/her password.
CryptoOfficer2 password	This password exists temporarily when the operator “CryptoOfficer2” submits his/her password.
PRNG parameters	Parameters include the state of the PRNG (K and V values) and the seed (which exists temporarily during processing).

Table 7. Critical Security Parameters

[1] Not associated with a role; always available to any operator.

[2] Always authenticated by the Manufacturer, but authentication of a Cryptographic Operator may *also* be required. See section 6.6 for further explanation.

7.4.2 Public Keys and other protected items

Protected items (other than CSPs) are protected against unauthorised substitution or modification. Public keys fall into this category of security-relevant data. The non-CSP protected items under the control of the FIPS Boot Loader are presented in Table 8.

Protected item	Description and purpose
Manufacturer's Authentication Public Key	The public part (exponent and modulus) of a 2048-bit RSA key that is used with the rDSA Approved security function. The key is used to authenticate the Manufacturer by verifying a signature over Application firmware, Boot Loader firmware and/or public keys.
Manufacturer's Licensing Public Key	The public part (exponent and modulus) of a 2048-bit RSA key that is used with the rDSA Approved security function. The key is used to authenticate the Manufacturer by verifying a signature over a license certificate that forms part of the Application firmware.
Manufacturer's Set Password Public Key	The public part (exponent and modulus) of a 2048-bit RSA key that is used with the rDSA Approved security function. The key is used to authenticate the Manufacturer by verifying a signature over an instruction to change an operator's password.
User1 password hash	A hash over the password of operator "User1", calculated using the SHA-1 Approved function. This hash is used to authenticate the "User1" operator.
CryptoOfficer1 password hash	A hash over the password of operator "CryptoOfficer1", calculated using the SHA-1 Approved function. This hash is used to authenticate the "CryptoOfficer1" operator.
CryptoOfficer2 password hash	A hash over the password of operator "CryptoOfficer2", calculated using the SHA-1 Approved function. This hash is used to authenticate the "CryptoOfficer2" operator.
RTC state	The state of the Real-Time Clock, that is, the date and time.
Tamper state	The state of the Tamper circuitry, which indicates whether the module is in a Tampered state or not. Entering the Tampered state causes the immediate zeroisation of Secure Memory (and hence the destruction of all Critical Security Parameters).
PRNG comparison hashes	Hashes over the last blocks of output from the random number generators; used in the Continuous Random Number Generator Test. The hashes are calculated using the SHA-1 Approved function.
Application firmware binary	The executable code comprising the Application firmware. Integrity of the code is protected by a hash that is calculated using the SHA-1 Approved function.
Boot Loader firmware binary	The executable code comprising the Boot Loader firmware. Integrity of the code is protected by a 32-bit Cyclic Redundancy Check (CRC) value.

Table 8. Public keys and other protected items

7.5 Modes of access to protected items

Different services access various protected items in a variety of ways. Table 9 indicates the ways in which protected items are accessed by each service, that is, the modes of access. This section describes the mode of access and indicates precisely what protected items are accessed, how, and why.

Authorised Service	Approved security functions used	Service Inputs	Service Outputs	Roles	Auth. required	Protected Item modes of access
Change Own Password	SHA-1	New password	Status	Crypto. Officer *or* User	Yes Yes	Verify operator password Overwrite operator password hash
External Tamper	None	None	Status		No	Set tampered state
Force Tamper	SHA-1	None	Status	Crypto. Officer *or* User	Yes Yes	Verify operator password Set tampered state
Get Random Bytes	PRNG	Length requested	Status Random bytes	User	Yes	Verify operator password Generate random number
Get Status	None	None	Status		No	Read disclosable protected items
Load Authenticated Application	SHA-1 *and* rDSA (verification)	Signed Application - Firmware binary	Status	Manufacturer (*and* Crypto. Officer [1])	Yes Yes	Verify digital signature (Authentication Key) Verify digital signature (Licensing Key) Verify operator password Overwrite Application Firmware
Load Authenticated Public Key	SHA-1 *and* rDSA (verification)	Signed Public Key	Status	Manufacturer	Yes	Verify digital signature (Authentication Key) Overwrite public key (Authentication Key, Licensing Key or Set Password Key)
Load Boot Loader	SHA-1 *and* rDSA (verification)	Signed Boot Loader - Firmware binary	Status	Manufacturer	Yes	Verify digital signature (Authentication Key) Overwrite Boot Loader Firmware
Reset	None	Reset control	Status		No	Verify integrity of protected items
Reset Tamper	SHA-1	None	Status	Crypto. Officer	Yes	Verify operator password Clear tamper state
Set Date and Time	SHA-1	Date and time	Status	Crypto. Officer	Yes	Verify operator password Set Real Time Clock
Set Lost Password	SHA-1 *and* rDSA (verification)	Signed instruction *and* New password	Status	Manufacturer	Yes	Verify digital signature (Set Password Key) Overwrite operator password hash

Table 9. Summary of authorised services and their security relationship

[1] When the Application is *not* an upgrade, authentication of *both* a Cryptographic Officer and the Manufacturer is required (see section 6.6 for full details).

7.5.1 Clear tamper state

Tamper state	Write

Takes the module out of the Tampered state. This operation can only complete successfully if there are no active tamper events at the time the service is executed.

The FIPS Boot Loader allows the normal execution of services and the execution of Application firmware only when it is not in the Tampered state.

7.5.2 Generate random number

PRNG parameters	Read
PRNG comparison hashes	Read + Write

Generates a random number by reading a seed from a hardware random number generator and using it as input to an Approved Deterministic Random Number Generator. The seed and the state of the deterministic generator are PRNG parameters. The PRNG comparison hashes are used and updated by the Continuous Random Number Generator Test that is performed as part of this operation.

When processing is complete the PRNG seed is destroyed and the pseudo-random number is returned.

7.5.3 Overwrite Application firmware

Application firmware binary	Write
All Critical Security Parameters	Write

Stores executable binary code as Application firmware. Existing Application firmware (if any) is erased and/or replaced during this operation.

Optionally Secure Memory may be erased during this operation (thus destroying all Critical Security Parameters). The conditions under which this will occur are described in section 6.6.

7.5.4 Overwrite Boot Loader firmware

Boot Loader firmware binary	Write
All password hashes	Write
All Critical Security Parameters	Write

Stores executable binary code as Boot Loader firmware. Existing Boot Loader firmware is erased and/or replaced during this operation, and Secure Memory is erased (thus destroying all Critical Security Parameters).

All operator password hashes (User1, CryptoOfficer1 and CryptoOfficer2) are reset to factory default values.

7.5.5 Overwrite operator password hash

Operator's password	Read
Operator's password hash	Write

Accepts the clear password of the identified operator (User1, CryptoOfficer1 or CryptoOfficer2) and calculates the SHA-1 hash of the password. The result is stored as the operator's password hash.

When processing is complete the clear password is destroyed.

7.5.6 Overwrite public key

Purpose Public Key	Write

Stores the supplied public key as the Manufacturer's Public Key for the indicated purpose (Authentication, Licensing, or Set Password). The existing public key (if any) is overwritten.

7.5.7 Read disclosable protected items

All Public Keys	Read
RTC state	Read
Tamper state	Read

Reads and returns the values of and/or information about various protected items (including all Manufacturer's Public Keys, the date and time and the Tamper state).

7.5.8 Set Real Time Clock

RTC state	Write

Sets the date and time that is maintained by the Real-Time Clock to the supplied values.

7.5.9 Set tampered state

Tamper state	Write
(all Critical Security Parameters)	Write

Forces the module to enter a Tampered state. This action immediately causes the zeroisation of Secure Memory (and hence the destruction of all Critical Security Parameters). The Main CPU (see Figure 2) is reset and its internal memory is erased immediately after coming out of reset (resulting in any temporarily stored information being erased).

Once in the Tampered state the FIPS Boot Loader prevents the execution of Application firmware, and the only role-dependent services that may be executed are Reset Tamper and Load Boot Loader (all role-independent services may be executed).

7.5.10 Verify digital signature

(Purpose) Public Key	Read

Verifies a signature over an instruction or data item using a Manufacturer's Public Key. The key to be used is indicated by the authentication requirements of the executing service.

7.5.11 Verify integrity of protected items

(all non-temporary protected items)	Read

Uses integrity checking algorithms and stored integrity data to verify that no stored protected items have been corrupted, modified or substituted. All stored (non-temporary) protected items (thus excluding Critical Security Parameters) can be read in their entirety by this **function**, but are not in the process disclosed beyond the **function**.

7.5.12 Verify operator password

(Operator's) password	Read
(Operator's) password hash	Read

Accepts the clear password of the identified operator (User1, CryptoOfficer1 or CryptoOfficer2) and calculates the SHA-1 hash of the password. The result is compared against the stored password hash for that operator.

When processing is complete the clear password is destroyed.

8. Physical Security Policy

This security policy details the physical security mechanisms that protect the cryptographic module, and the actions operators must take to ensure that physical security is maintained.

8.1 Physical security mechanisms

The TSM410 is a multi-chip embedded cryptographic module that includes the following physical security properties and mechanisms. Standard passivation techniques are used on the PCB.

8.1.1 Tamper-evident enclosure

The module is contained within an opaque tamper-evident enclosure. The enclosure does not have any ventilation holes or slits. The module (and enclosure) does not have any removable covers or doors, or a maintenance role, and is not designed to permit access to its contents.

Unauthorised attempts at physical access, use or modification have a high degree of being detected as a result of visible signs that will be left by such an attempt.

8.1.2 Tamper-detection envelope and response circuitry

The module is encapsulated by an envelope that detects tampering by means such as cutting, drilling, milling, grinding, or dissolving of the enclosure to an extent sufficient to access Critical Security Parameters.

The module contains tamper response and zeroisation circuitry that continuously monitors the tamper-detection envelope, and upon detecting tampering will enter the Tampered state and immediately zeroise the Secure Memory.

The Status LEDs clearly indicate when the module is in the Tampered state.

8.1.3 Environmental Failure Protection

The module includes Environmental Failure Protection (EFP). The internal temperature and voltage are monitored constantly; if the internal temperature or voltage falls outside the tamper thresholds for these parameters the module enters the Tampered state and immediately zeroises the Secure Memory.

The Status LEDs clearly indicate when the module is in the Tampered state.

8.2 Inspection by operators

To maintain the physical security of the module it must be inspected periodically. The actions that operators must perform are given in Table 10.

Physical security mechanism	Inspection details	Recommended frequency
Tamper-evident enclosure	Inspect the enclosure for signs of tampering.	When commissioned and every 12 months thereafter
Tamper-detection and response circuitry	Inspect the Status LEDs (located at the base of the back-plate on the PCI carrier) to confirm that the module is not in the Tampered state.	When commissioned and every 3 months thereafter

Table 10. Inspection of physical security mechanisms

9. Mitigation of Other Attacks Policy

The TSM410 provides additional protection mechanisms that are not specifically required by FIPS [1]. These mechanisms and the attacks they mitigate are listed in Table 11.

Attack	Mitigation mechanism	Specific limitations
Simple Power Analysis (SPA)	Power supply filtering	None
Differential Power Analysis (DPA)	Power supply filtering	None

Table 11. Mechanisms for the mitigation of other attacks

The mitigation mechanisms listed in Table 11 have been verified by design analysis.

10. Security Rules

This section presents rules that apply to the TSM410, its use and environment, as required by FIPS 140-2 [1]. Section 10.7 lists additional rules not required by FIPS [1] that have been imposed by the vendor.

10.1 General rules

- The security module employs physical security mechanisms in order to restrict unauthorized physical access to the module and to deter unauthorized modification of the module. All hardware and firmware components within the cryptographic boundary are protected.
- There is no maintenance role: the module does not allow operators to perform physical or logical maintenance.
- The module does not implement a bypass capability.
- The module conforms to the EMI/EMC requirements specified by Code of Federal Regulations Title 47 [11], Part 15, subpart B: Unintentional radiators (Class B: digital devices). Certificate #2287-1 from EMCE Engineering Inc..

10.2 Interface rules

- The security module restricts all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module.
- Interfaces are logically distinct from each other.
- The module distinguishes between data and control for input, and between data and status for output.
- All input data entering the security module via the "data input" interface only passes through the input data path.
- All output data exiting the security module via the "data output" interface only passes through the output data path.
- The output data path is logically disconnected from processes while performing key zeroisation.

10.3 Approved security function rules

- The security module employs one approved and one non-approved random number generator (RNG). The non-approved hardware random number generator (part of the Crypto Accelerator, see Figure 2) is used to seed the Approved Deterministic Random Number Generator.

10.4 Protected item rules

- Critical Security Parameters are protected within the security module against unauthorized disclosure, modification, or substitution.
- The security module provides a method to zeroise all Critical Security Parameters within the module.
- Critical Security Parameters are input to the security module via serial port B, which is dedicated to this purpose.
- Public keys and other protected items are protected from unauthorized modification or substitution. Such items are stored as plaintext (unencrypted) in the security module and are not subject to zeroisation.

- The module associates each public key with a specific use or purpose, and will not permit a public key to be used other than for the intended purpose.

10.5 Authentication rules

- The security module contains authentication data required to authenticate the operator for the first time the module is accessed.
- The module does not support multiple concurrent operators.
- The results of previous authentications are not maintained between power cycles.
- No feedback or output is provided during authentication that could reduce the strength of the authentication mechanism. The result of authentication is reported as success or failure, without any further reason or detail being provided.

10.6 Self tests

- Power-On Self Tests (POST) are performed by the security module when power is applied to it. These tests verify the integrity of the module and its firmware, and employ Known Answer Tests to ensure the correct behaviour of the Approved security functions.
- The Power-On Self Tests are initiated automatically and do not require operator intervention.
- The operator can initiate the Power-On Self Tests by resetting the security module.
- All data output via the data output interface is inhibited while the Power-On Self Tests are performed.
- When the Power-On Self Tests are completed the results are output via the “status output” interface. The results may thus be obtained by observing the Status LEDs or by executing the “Get Status” service.

10.6.1 Error state

- If the security module fails a self-test the module enters the Error state. An error result is output via the “status output” interface, and may be obtained by observing the Status LEDs or by executing the “Get Status” service.
- No cryptographic operations may be performed while in the Error state.
- All data output via the data output interface is logically inhibited while in the Error state. The data output interface is physically combined with the status output interface on the External Bus. Status information can be returned in the Error state.
- It is possible to leave the Error state by removing power from the security module or by using the “Reset” service.

10.6.2 Integrity tests

The following integrity tests are part of the Power-On Self Tests:

- A Boot Loader firmware integrity test is performed using a 32-bit Cyclic Redundancy Check (CRC) algorithm. If the integrity verification fails the only recourse is for the Manufacturer to destroy the module’s enclosure and refurbish the module.
- An Application firmware integrity test is performed (if Application firmware is present in the module) using the SHA-1 Approved security function. If the integrity verification fails the module behaves as if there is no Application firmware present.

10.6.3 Critical Function tests

The following Critical Function tests are part of the Power-On Self Tests:

- Test the non-approved hardware random number generator to ensure that it is toggling.

10.6.4 Known Answer Tests

The following Known Answer Tests of Approved security functions are part of the Power-On Self Tests:

- Triple-DES Known Answer Test (encryption and decryption)
- DES Known Answer Test (encryption and decryption)
- SHA-1 Known Answer Test
- Triple-DES MAC Known Answer Test
- Enhanced Security DES MAC Known Answer Test
- Data Authentication Algorithm (DES MAC) Known Answer Test
- rDSA signature verification Known Answer Test
- Deterministic Random Number Generator (PRNG) Known Answer Test

10.6.5 Conditional tests

The security module features the following Conditional tests:

- A Continuous Random Number Generator Test is performed on the output of the hardware random number generator and on the output of the Deterministic Random Number Generator (PRNG). Each block of output (from either generator) is hashed using the SHA-1 algorithm and the result is compared to the hash of the previous block, ensuring that each randomly generated block is different. This test is executed whenever the PRNG is used.
- A Software Load Test is performed to verify the integrity of Boot Loader and/or Application firmware that is loaded into the module (via the “Load Boot Loader” or “Load Authenticated Application” services). This test requires rDSA verification of the signature over the firmware, and is always executed whenever firmware is loaded.

10.7 Vendor specific rules

- Each module contains a unique identification number (UID).
- Only a Cryptographic Officer may adjust the state of the Real-Time Clock.
- DES and DAA (DES MAC) are permitted in order to interface with legacy systems, and may only be used for this purpose. This rule is in compliance with FIPS 46-3 [2].
- All public keys required and used by the FIPS Boot Loader must have different values, so that each key is limited to one defined purpose.
- All TSM410 modules use the same set of public keys for the authentication of the Manufacturer.

11. References

[1] FIPS PUB 140-2: Federal Information Processing Standards Publication 140-2
National Institute of Standards and Technology (NIST), 2001
"Security Requirements for Cryptographic Modules"

[2] FIPS PUB 46-3: Federal Information Processing Standard Publication 46-3
National Institute of Standards and Technology (NIST), 1999
"Data Encryption Standard (DES)"

[3] ANSI X9.52-1998: Financial Services standard X9.52
American National Standards Institute (ANSI), 1998
"Triple Data Encryption Algorithm Modes of Operation"

[4] FIPS PUB 81: Federal Information Processing Standard Publication 81
National Institute of Standards and Technology (NIST), 1980
"DES Modes of Operation"

[5] FIPS PUB 180-2: Federal Information Processing Standard Publication 180-2
National Institute of Standards and Technology (NIST), 2002
"Secure Hash Signature Standard (SHS)"

[6] FIPS PUB 113: Federal Information Processing Standard Publication 113
National Institute of Standards and Technology (NIST), 1985
"Standard on Computer Data Authentication"

[7] ANSI X9.19-1996: Financial Services standard X9.19
American National Standards Institute (ANSI), 1996
"Financial Institution Retail Message Authentication"

[8] ISO 9797-1 (1999): Information technology – Security techniques standard 9797
International Organization for Standardization, 1999
"Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher"

[9] ANSI X9.9-1994: Financial Services standard X9.9
American National Standards Institute (ANSI), 1994
"Financial Institution Message Authentication (Wholesale)"

[10] ANSI X9.31-1998: Financial Services standard X9.31
American National Standards Institute (ANSI), 1998
"Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)"

[11] CFR47-2003: Code of Federal Regulations Title 47
Federal Communications Commission (FCC), 2003
"Code of Federal Regulations Title 47: Telecommunication"

12. Glossary

ANSI	American National Standards Institute
CBC	Cipher Block Chaining (DES or TDES mode of operation)
CPU	Central Processing Unit
CRC	Cyclic Redundancy Calculation
CSP	Critical Security Parameter
DEA	Data Encryption Algorithm, also known as DES
DES	Data Encryption Standard, also known as DEA
DPA	Differential Power Analysis
ECB	Electronic Code Book (DES or TDES mode of operation)
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFP	Environmental Failure Protection
EFT	Electronic Funds Transfer
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPS	Electronic Payment System
FCC	Federal Communications Commission
FIFO	First In First Out, a hardware buffer
FIPS	Federal Information Processing Standard
I/F	Interface
ISO	International Organisation for Standardization
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PCB	Printed Circuit Board
PCI	Peripheral Component Interconnect, a type of bus
PnP	Plug and Play
POST	Power-On Self Test
PRNG	Pseudo-Random Number Generator
RAM	Random Access Memory (readable and writable)
rDSA	Reversible Digital Signature Algorithm
rMAC	Retail Message Authentication Code (an algorithm also known as the Enhanced DES MAC)
RNG	Random Number Generator
RS232	Recommended Standard 232, a wire protocol
RSA	Rivest Shamir Adleman, a cryptographic algorithm
RTC	Real-Time Clock
SHA	The SHA-1 algorithm, also known as the Secure Hash(ing) Algorithm
SHS	Secure Hashing (Signature) Standard, see also SHA
SPA	Simple Power Analysis
TDEA	Triple-DEA (Data Encryption Algorithm), see also TDES
TDES	Triple-DES (Data Encryption Standard), see also TDEA
TRSM	Tamper Responsive Security Module, also known as a cryptographic security module
TSM410	The Incognito TSM410 cryptographic security module
UART	Universal Asynchronous Receiver-Transmitter, a communication interface
UID	Unique Identifier
VDC	Voltage Direct Current