PRISM

TRUSTED TRANSACTIONS

A subsidiary of NET1 UEPS Technologies, Inc.

Incognito TSM500 Security Policy

Document number	PR-D2-0778
Revision	1.3
Authors	Richard Pitchers, Trevor Davel, Giovanni Gallus
Date	March 2010
Synopsis	The Incognito TSM500 is a multi-chip embedded Tamper Responsive Security Module 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 AES, TDEA, SHA-2, RSA (PKCS#1 and ANSI X9.31). This document details the cryptographic module security policy for the Incognito TSM500, 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 TSM500 is a multi-chip embedded Tamper Responsive Security Module (TRSM). Fitted on a PCI carrier card, the device offers high-performance, high-security services targeted at Electronic Payment Systems including EFT switches and mobile commerce.

The TSM500 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 TSM500 Module (Part Number 5520-00127 Rev 2) with "BL50" Boot Loader (Part Number 0610-00571 Rev 1.2). Firmware Applications are not included in this security policy and will be evaluated separately.

Figure 1 is a photographic image of the Incognito TSM500. The cryptographic boundary is indicated by the red border.

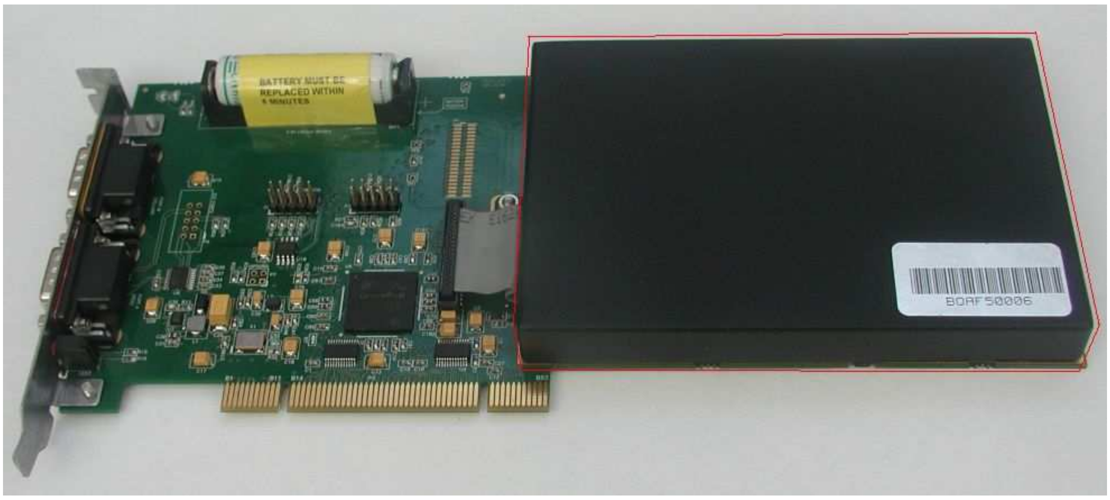

Figure 1. Incognito TSM500 on its PCI carrier card

3. Security Level

The TSM500 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 TSM500 is given in Table 1.

FIPS 140-2 Security Requirement	Level
Cryptographic Module Specification	3
Cryptographic 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 TSM500 as it qualifies as a limited operating environment.

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

4. Modes of Operation

The user can determine the overall mode of operation of the TSM500 by executing the "Get TSM Status" service.

4.1 FIPS Approved mode

The Boot Loader always executes in Approved mode [1]. This does not necessarily mean that the overall mode of operation of the TSM500 is always in an Approved mode. For the module to remain in FIPS mode, no Application firmware that is not FIPS 140-2 validated shall be loaded using the "Load Authenticated Application" service.

The "Get TSM Status" service will indicate whether or not the module is operating in FIPS Approved mode.

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

4.2 Non-approved modes

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

For the module to remain in FIPS mode, no Boot Loader firmware that is not FIPS 140-2 validated shall be loaded into the cryptographic boundary (via the "Manufacturer Load Authenticated Boot loader" service).

For the module to remain in FIPS mode, no Application firmware that is not FIPS 140-2 validated shall be loaded into the cryptographic boundary (via the "Load Authenticated Application" service).

4.3 Approved Security Functions

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 for 2-key and 3-key TDES.	TDES Certificate 801
AES Advanced Encryption Standard per FIPS 197 [12]. Support for encryption and decryption in ECB and CBC modes for 128, 192 and 256 bit keys.	AES Certificate 1100
Secure Hash Standard (SHS) The algorithms (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512) of the Secure Hash Standard (SHS) FIPS PUB 180-3 [5].	SHS Certificate 1023

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

FIPS Approved security function	Certification
Triple-DES MAC The Data Authentication Algorithm described in FIPS PUB 113 [6], using 2-key and 3 key Triple-DES as the e() function (as permitted by FIPS 140-2 Annex A).	Vendor affirmed (TDES Cert. 801)
RSA 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 4096 bits in conjunction with SHA-1, SHA-256, SHA-384 and SHA-512 hash algorithms.	RSA Certificate 515
RSA Digital signature algorithm using reversible public key cryptography (based on RSA) per PKCS#1 v2.1 [14]. Support for digital signature creation and verification for various key sizes in the range 1024 to 4096 bits, using the RSASSA-PSS and RSASSA-PKCS1_v1_5 schemes in conjunction with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 hash algorithms.	RSA Certificate 515
Deterministic Random Number Generator [1] (DRNG) FIPS-Approved Deterministic Random Number Generator using the AES with 128 bit key in accordance with [15].	RNG Certificate 612

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

4.4 Non-Approved Security Function allowed for use in FIPS Approved mode of operation

Non-Approved security function	
Hardware RNG The hardware seed generator is a nondeterministic RNG. FIPS 140-2 permits the use of a nondeterministic RNG to seed an Approved RNG in FIPS mode.	

Table 3. Non-Approved security function for use in FIPS Approved mode of operation

[1] The deterministic random number generator is used in the generation of all cryptographic keys. Within this security policy the term “DRNG” is used to describe the Approved deterministic random number generator validated with RNG Certificate 612.

5. Ports and Interfaces

Figure 2 illustrates the external interfaces of the Incognito TSM500. 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.

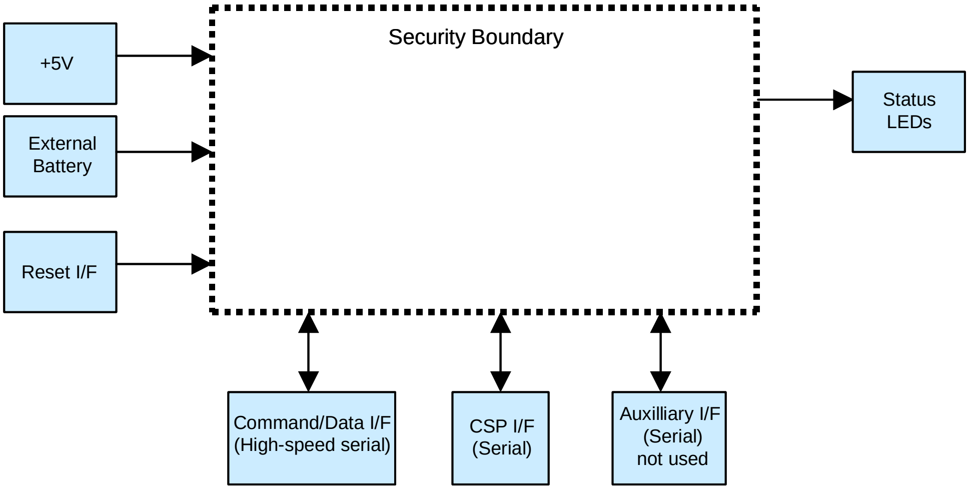

Figure 2. Incognito TSM500 external interfaces and cryptographic boundary

The relationships between the TSM500's ports and the Boot Loader's logical interfaces (as defined by FIPS PUB 140-2 [1]) are presented in Table 4.

FIPS 140-2 Logical Interface	Ports (physical Interfaces)
Data Input	Command/Data Interface (High-speed serial) CSP Interface (Serial) [1]
Data Output	Command/Data Interface (High-speed serial) CSP Interface (Serial)
Control Input	Command/Data Interface (High-speed serial) RESET
Status Output	Command/Data Interface (High-speed serial) Status LEDs Interface[2]
Power Port	Primary Power (+5V) External Battery
N/A	Auxiliary Interface (Serial) [3]

Table 4. Physical and logical interfaces

[1] CSP Interface is dedicated for the entry of Critical Security Parameters (CSPs)

[2] The TSM500 provides a signal to drive each Status LED outside the cryptographic boundary via the Status LEDs Interface.

[3] Auxiliary Interface is logically disconnected in the Boot Loader

5.1 Status LEDs Interface signals

Signal to RED LED	Signal to GREEN LED	Meaning
OFF	OFF	Not running / powered off
ON	OFF	Corrupt state
OFF (Flashes once as INIT sequence begins)	ON	Initialising, performing self tests
OFF	ON	Notice Me (waiting for password entery)
1-FLASH[1]	1-FLASH[1]	Error state
ON	1-FLASH[1]	Tampered state
OFF	1-FLASH[1]	Loader state (normal operational state)

Table 5. Status LEDs Interface signals

[1] A Red 1-FLASH or Green 1-FLASH sequence follows the pattern 101010 (500ms per state)

6. Services

A service is a processing operation of the TSM500 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 8 (on page 15).

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 11 (on page 19).

The following services are provided by the TSM5000 in conjunction with the 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 6 on page 14). The operator's existing password must be supplied to authorise the change.

6.2 Clear Tamper

Forces the TSM500 out of the Tampered state, allowing it to resume normal operation. The state of the Real-Time Clock will also be set.

The operator must inspect the module's opaque enclosure for evidence of tampering before executing this service. This service can only complete successfully if there are no active tamper events at the time the service is executed.

6.3 Echo

Echoes the data input back to the operator as data output, optionally delaying for a brief period of time. This service does not require authentication of the operator, and does not use security functions or interact with protected items.

This service is not available in the Error state.

6.4 Force Tamper

Forces the TSM500 into the Tampered state, causing immediate zeroisation of all Critical Security Parameters.

6.5 Get Boot Loader 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 Interface by comparison indicates limited status information, see Table 5, but does 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 Get Random Bytes

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

6.7 Get TSM Status

Allows the operator to query the current mode of operation of the module. 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.

Status information may include protected items other than Critical Security Parameters (CSPs).

6.8 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.

Digital signature verification of the entire set of executable code that constitutes the Application firmware is enforced through the Software/firmware Load Test (section 10.6.5), which uses the Manufacturer's Authentication Public Key to authenticate the origin and integrity of the firmware.

The operation must be authorised by the Manufacturer, and this process uses both the Firmware Licensing Public Key and the Firmware Load Authorisation Public Key to authenticate the Manufacturer.

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

For module to remain in FIPS mode, no Application firmware that is not FIPS 140-2 validated shall be loaded into the cryptographic boundary (via the "Load Authenticated Application" service)."

Upgrades to an existing Application

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.

If the operation does not qualify as an upgrade then:

- Authorisation from a Cryptographic Officer is required *in addition* to authentication of the Manufacturer; and
- Critical Security Parameters are zeroised (but other Protected Items are not affected).

6.9 Load Authenticated Management Public Keys

Allows the Manufacturer to change the management public keys that are stored in the TSM500, and which are used to authenticate the Manufacturer. All protected public keys described in Table 10 are considered management public keys.

The change must be authorised by the Manufacturer, and this process utilises the (existing) Manufacturer's Authentication Public Key. Critical Security Parameters (CSPs) will be zeroised during the execution of this service, and various other protected items will be reset to factory default values. The state of the Real-Time Clock will also be set.

6.10 Login Operator With Password

Verifies the identity of the operator by means of a password (entered via the CSP interface), and changes the TSM's state to make available (or deny) services according to the operator's role

6.11 Manufacturer Load Authenticated Boot loader

The operator may use this service to introduce boot loader firmware to the module. The existing boot loader will be erased in the process.

Digital signature verification of the entire set of executable code that constitutes the boot loader is enforced through the Software/firmware Load Test (section 10.6.5), which uses the Manufacturer's Authentication Public Key to authenticate the origin and integrity of the new boot loader firmware.

In the instance that authentication of the Manufacturer fails the existing boot loader will not be erased.

This service is only available in the Tampered state (all Critical Security Parameters (CSPs) will have been zeroised on entering the Tampered state). Various protected items will be erased or reset to factory default values during the execution of this service.

For the module to remain in FIPS mode, no Boot Loader firmware that is not FIPS 140-2 validated shall be loaded into the cryptographic boundary (via the “Manufacturer Load Authenticated Boot loader” service).

For module to remain in FIPS mode, no Application firmware that is not FIPS 140-2 validated shall be loaded into the cryptographic boundary (via the “Load Authenticated Application” service).

6.12 Read Audit Log

Reads recent entries from the tail of the Audit Log. Any operator may read the Audit Log, and no authentication is required.

6.13 Reset

Restarts the TSM500, causing the Boot Loader to execute and, in the process, perform all self tests described in section 10.6. Any operator may execute a reset, and no authentication is required.

The results of the self-tests may be obtained by executing the “Get Boot Loader Status” service, and the Status LEDs Interface will indicate any critical failure(s).

6.14 Reset Operator Password

Allows an operator to enter a new password. The Manufacturer may authorise this service if an operator has lost his/her password; this process utilises the Manufacturer’s Access Control Public Key.

6.15 Set Date and Time

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

7. Access Control Policy

The Access Control Policy for the TSM500 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 TSM500 supports three operator roles (presented in Table 6): Manufacturer, Cryptographic Officer and User.

7.1.1 Manufacturer role

The Manufacturer role exists to allow the manufacturer of the TSM500 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 6.8 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 DRNG.

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 6, while the strengths of the various authentication mechanisms are presented in Table 7.

7.2.1 RSA PKCS#1 digital signature mechanism

Operators having the Manufacturer role are authenticated by means of RSA PKCS#1 digital signatures (using RSASSA-PKCS1-v1_5 with SHA-256). 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 a RSA PKCS#1 signature over an instruction or data item providing identification and authentication of the operator.

Each RSA PKCS#1 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 3072 bits.

7.2.2 Operator ID and password mechanism

Cryptographic Officers and Users must supply an Operator ID to identify themselves. An alphanumeric password is used for authentication. The operator must know the Operator ID and password, while the module stores the Operator ID along with a SHA-256 hash of the password. To identify and authenticate him/her-self, the operator presents his/her Operator ID and password to the module. A SHA-256 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.

The Boot Loader uses up to two digits for the operator ID which allows for up to 99 operators. Each Operator ID 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 Operator ID, 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	RSA PKCS#1 digital signature	Manufacturer
Cryptographic Officer	Identity-based operator authentication	Operator ID and password	None
User	Identity-based operator authentication	Operator ID and password	None

Table 6. Operator roles, identities and authentication

7.2.3 Strengths of authentication mechanisms

The minimum security requirement of an authentication mechanism is that:

- The probability of a false acceptance for each use of the mechanism is less than 1 in 1,000,000; and
- 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 7. 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
RSA PKCS#1 digital signature	The length of each key is at least 3072 bits, which is given in NIST SP800-57 [13] as 128 bits of security. SP800-57 gives the security of the SHA-256 hash (used in a digital signature) as 128 bits. The effective security of the digital signature is thus 128 bits. For each use of the authentication mechanism the probability of a false acceptance is 1 in 2^{128}, which is less than 1:1,000,000. At a possible 30 attempts per minute the probability of falsifying authentication in 1 minute is approximately 30 in 2^{128}, 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. For each use of the authentication mechanism the probability of a false acceptance is 1 in 10^7, which is less than 1:1,000,000. 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 7. Strengths of authentication mechanisms

7.3 Service access by role

Table 8 cross-references the authorised services of the 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		✓	✓	
Clear Tamper		✓		
Echo				✓
Force Tamper[2]		✓	✓	
Get Boot Loader Status				✓
Get Random Bytes			✓	
Get TSM Status				✓
Load Authenticated Application	✓	✓ [3]		
Manufacturer Load Authenticated Boot Loader	✓			
Load Authenticated Management Public Keys	✓			
Login Operator With Password[4]		✓	✓	
Read Audit Log				✓
Reset				✓
Reset Operator Password	✓			
Set Date and Time		✓		

Table 8. 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.

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

[2] The Crypto. Officer role or User role can perform zeroisation via the "Force Tamper" service.

[3] Always authenticated by the Manufacturer, but authentication of a Cryptographic Officer may *also* be required. See section 6.8 for further explanation.

[4] Any operator can execute this service, but the service will only complete successfully through the authentication of a Cryptographic Officer or User.

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 Boot Loader are presented in Table 9.

Critical Security Parameter	Description and purpose
Operator password	Each password exists temporarily when the operator submits his/her password to the TSM500.
DRNG parameters	Parameters include the state of the DRNG (K , V and DT values).

Table 9. Critical Security Parameters

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 Boot Loader are presented in Table 10.

Protected item	Description and purpose
Manufacturer's Authentication Public Key	The public part (exponent and modulus) of a 3072-bit RSA key that is used with the RSA PKCS#1 Approved security function. The key is used to authenticate the Manufacturer by verifying a signature over Application firmware and/or public keys.
Firmware Licensing Public Key	The public part (exponent and modulus) of a 3072-bit RSA key that is used with the RSA PKCS#1 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 Access Control Public Key	The public part (exponent and modulus) of a 3072-bit RSA key that is used with the RSA PKCS#1 Approved security function. The key is used to authenticate the Manufacturer by verifying a signature over an instruction to change an operator's password.
Firmware Load Authorisation Public Key	The public part (exponent and modulus) of a 3072-bit RSA key that is used with the RSA PKCS#1 Approved security function. The key is used to authenticate the Manufacturer by verifying a signature over a load authorisation certificate that forms part of the Application firmware.
Operator password hashes	There is a hash over the password of each operator, calculated using the SHA-256 Approved function. This hash is used to authenticate the operator. The Boot Loader supports up to 99 operator password hashes.
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 all sensitive data (including all Critical Security Parameters).
DRNG 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-256 Approved function.

Protected item	Description and purpose
Boot loader	The executable code and data comprising the boot loader
Application firmware	The executable code and data comprising the Application firmware.
Audit log	The audit log contains in formation about events that includes power cycling, tamper latch and clear events, set date and time, operator login, password changes, password reset, public key changes and firmware changes. This information allows the operator to reconstruct a (recent) history of changes to the TSM. No CSPs are included in the audit log. Information about protected items (as may be retrieved with the Read Disclosable Protected Items mode of access) maybe included.

Table 10. 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 11 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-256	Service control [1] Operator password Password entry timeout New password	Status	Crypto. Officer *or* User	Yes Yes	Accept & verify operator password Accept new operator password & overwrite password hash
Clear Tamper	None	Service control Date and time	Status	Crypto. Officer	Yes	Clear tamper state Set Real Time Clock
Echo	None	Service control Echo data Sleep time	Status Echo data		No	None
Force Tamper	None	Service control	Status	Crypto. Officer *or* User	Yes Yes	Set tampered state
Get Boot Loader Status	None	Service control	Status Detailed Status		No	Read disclosable protected items
Get TSM Status	None	Service control	Status		No	None
Get Random Bytes	DRNG	Service control Number of bytes	Status Random bytes	User	Yes	Generate random number
Load Authenticated Application	SHA-256 and RSA PKCS#1 RSASSA-PKCS1-v1_5 with SHA-256 (verification)	Service control Signed Application Firmware	Status	Manufacturer (*and* Crypto. Officer [2])	Yes Yes	Verify digital signature (Manufacturer's Authentication Public Key) Verify digital signature (Firmware Licensing Public Key) Verify digital signature (Firmware Load Authorisation Public Key) Read disclosable protected items Overwrite Application Firmware

[1] Service control is a service invocation via the command/data interface

[2] When the Application is *not* an upgrade, authentication of *both* a Cryptographic Officer and the Manufacturer is required (see section 6.8 for full details).

Authorised Service	Approved security functions used	Service Inputs	Service Outputs	Roles	Auth. required	Protected Item modes of access
Manufacturer Load Authenticated Boot Loader	SHA-256 and RSA PKCS#1 RSASSA-PKCS1-v1_5 with SHA-256 (verification)	Service control Signed Application Firmware	Status	Manufacturer	Yes	Verify digital signature (Manufacturer's Authentication Public Key) Read disclosable protected items Replace Boot Loader
Load Authenticated Management Public Keys	RSA PKCS#1 RSASSA-PKCS1-v1_5 with SHA-256 (verification)	Service control Signed Public Keys Date and time	Status	Manufacturer	Yes	Verify digital signature (Manufacturer's Authentication Public Key) Overwrite public keys (Manufacturer's Authentication Public Key, Firmware Licensing Public Key, Manufacturer's Access Control Public Key, and Firmware Load Authorisation Public Key) Set Real Time Clock
Login Operator with Password	SHA-256	Service control Operator ID Operator password Password entry timeout	Status Role (Status output)	Any operator can execute this service, but the service will only complete successfully through the authentication of a Cryptographic Officer or User.	No	Accept & verify operator password
Read Audit Log	None	Service control Number of recent entries to skip Number of entries to read	Status Detailed Status		No	Read audit log
Reset	None	Reset control	Status		No	Verify integrity of protected items Append audit log
Reset Operator Password	SHA-256 and RSA PKCS#1 RSASSA-PKCS1-v1_5 with SHA-256 (verification)	Service control Signed reset instruction *and* New password Password entry timeout	Status	Manufacturer	Yes	Verify digital signature (Manufacturer's Access Control Public Key) Accept new operator password & overwrite password hash
Set Date and Time		Service control Date and time	Status	Crypto. Officer	Yes	Set Real Time Clock

Table 11. Summary of authorised services and their security relationship

7.5.1 Clear tamper state

Tamper state	Read + Write
Audit log	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 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 Set tampered state

Tamper state	Write
All Critical Security Parameters	Write
Audit log	Write

Forces the module to enter a Tampered state. This action causes immediate zeroisation of all sensitive data (including all Critical Security Parameters).

Once in the Tampered state the Boot Loader prevents the execution of Application firmware. All role-independent services may be executed, but only the following role-dependent services may be executed:

- Clear Tamper
- Load Authenticated Management Public Keys
- Login Operator with Password
- Reset Operator Password

7.5.3 Generate random number

DRNG parameters	Read + Write
DRNG comparison hashes	Read + Write

Generates a random number using the Approved Deterministic Random Number Generator. The DRNG parameters are the deterministic generator’s state and are updated by reading from the DRNG. The DRNG comparison hashes are used and updated by the Continuous Random Number Generator Test that is performed as part of this operation.

7.5.4 Set Real Time Clock

RTC state	Write
Audit log	Write

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

7.5.5 Accept & verify operator password

Operator’s password (transient)	Read
Operator’s password hash	Read
Audit log	Write

Solicits the operator's password (a Critical Security Parameter) via the CSP Interface, then computes the SHA-256 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.

7.5.6 Accept new operator password & overwrite password hash

Operator’s password (transient)	Read
Operator’s password hash	Write
Audit log	Write

Accepts the clear password (a Critical Security Parameter) of the identified operator via the CSP Interface, then computes the SHA-256 hash of the password. The hash is stored as the operator's password hash.

When processing is complete the clear password is destroyed.

7.5.7 Overwrite application firmware

Application firmware	Read + Write
All Critical Security Parameters	Write
Audit log	Write

Stores the 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 6.8.

7.5.8 Replace boot loader

Boot loader	Read + Write
All Critical Security Parameters	Write
Audit log	Write

Stores the boot loader. Existing boot loader is erased and replaced during this operation. The operator password hashes, Audit Log and Application firmware will also be erased.

7.5.9 Overwrite public keys

All Public Keys	Write
All Critical Security Parameters	Write
All other protected items	Write

Stores the supplied public keys. Secure Memory is erased (thus destroying all Critical Security Parameters), as are all operator password hashes. Existing Application firmware (if any) is erased during this operation. The existing public keys (if any) are overwritten.

7.5.10 Verify digital signature

(Purpose) Public Key	Read
Audit log	Write

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

7.5.11 Read disclosable protected items

All Public Keys	Read
RTC state	Read
Tamper state	Read
Application firmware	Read

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

Disclosable information may include checksums (fingerprints) of Public Key material using the Approved SHA-256 security function.

7.5.12 Read Audit Log

Audit log	Read

Reads and returns recent entries from the tail of the Audit Log (protected item).

7.5.13 Append Audit Log

Audit log	Write

Appends an event to the Audit log (protected item). The date & time, event type, operator identity, and a log message are recorded.

7.5.14 Verify integrity of protected items

All protected items	Read
All protected items (recovery)	Write

Uses integrity checking algorithms and stored integrity data to verify that selected stored protected items have not been corrupted, modified or substituted. Recovery of certain corrupted items may be attempted.

All stored protected items can be read in their entirety by this function, but are not disclosed beyond the function in the process.

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 TSM500 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 a hard 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 Interface clearly indicates 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. EFP is associated with both main voltage and battery voltage.

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

When the main voltage power is removed, the module will zeroise the volatile memory and power down.

8.2 Inspection by operators

The module relies on its Level 4 physical security to maintain security during distribution to operators. To maintain the physical security of the module it must be inspected periodically. The actions that operators must perform are given in Table 12.

Physical security mechanism	Inspection details	Recommended frequency
Tamper-evident enclosure	Inspect the hard, opaque, tamper-evident 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. **Note:** The module supplies a signal to drive each Status LED.	When commissioned and every 3 months thereafter

Table 12. Inspection of physical security mechanisms

9. Mitigation of Other Attacks Policy

The TSM500 provides additional protection mechanisms that are not specifically required by FIPS [1]. These mechanisms and the attacks they mitigate are listed in Table 13.

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

Table 13. Mechanisms for the mitigation of other attacks

The mitigation mechanisms listed in Table 13 have been verified by design analysis.

10. Security Rules

This section presents rules that apply to the TSM500, 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 #2833-1.

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 an Approved Deterministic Random Number Generator, which is seeded by a nondeterministic hardware seed generator[1].

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. The module performs active zeroisation of all internal memory locations where plaintext CSPs reside.
- Critical Security Parameters are input to the security module via serial port B, which is dedicated to this purpose.

[1] The hardware seed generator is a nondeterministic RNG. FIPS 140-2 permits the use of a nondeterministic RNG to seed an Approved RNG.

- 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 which are controlled by the Status LEDs Interface or by executing the "Get TSM 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 TSM 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.
- See Table 5 for details on signals output on the Status LEDs Interface.

10.6.2 Integrity tests

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

- An integrity test is performance on the FPGA configuration and Boot Loader firmware using a checksum. If the integrity verification fails the only recourse is for the Manufacturer to destroy the module's tamper-evident enclosure and tamper envelope, and refurbish the module.
- See Table 5 for details on signals output on the Status LEDs Interface.

- Application: SHA-256 verification integrity test (latent functionality; in its current form the module does not contain an application).

10.6.3 Critical Function tests

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

- Test the hardware seed generator to ensure that it is functional. This is also a continuous test.
- Integrity of essential protected items is verified as part of the Power-On Self Tests, as described in section 7.5.14.
- RTC tick test

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 in ECB and CBC modes with 2key and 3key)
- AES Known Answer Test (encryption and decryption in ECB and CBC modes with 128, 192 and 256 bit keys)
- SHA-1 Known Answer Test
- SHA-224 Known Answer Test
- SHA-256 Known Answer Test
- SHA-384 Known Answer Test
- SHA-512 Known Answer Test
- Triple-DES MAC Known Answer Test
- RSA (ANSI X9.31) key generation Known Answer Test
- RSA (ANSI X9.31) signature generation Known Answer Test
- RSA (ANSI X9.31) signature verification Known Answer Test
- RSA PKCS#1 RSASSA-PKCS1-v1_5 signature generation Known Answer Test
- RSA PKCS#1 RSASSA-PKCS1-v1_5 signature verification Known Answer Test
- RSA PKCS#1 RSASSA-PSS signature generation Pairwise Test
- RSA PKCS#1 RSASSA-PSS signature verification Known Answer Test
- Hardware Random Number Generator (HRNG) Known Answer Test
- Deterministic Random Number Generator (DRNG) 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 each RNG. Each block of output is hashed using the SHA-256 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 RNG is used.
- A Software/firmware Load Test is performed to verify the integrity of the Application firmware that is loaded into the module (via the “Load Authenticated Application” service). This test requires verification of the signature over the firmware, and is always executed whenever firmware is loaded.

- A Software/firmware Load Test is performed to verify the integrity of the Boot loader firmware that is loaded into the module (via the "Manufacturer Load Authenticated Boot loader" service). This test requires 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 Manufacturer or Cryptographic Officer may adjust the state of the Real-Time Clock.
- All public keys required and used by the Boot Loader must have different values, so that each key is limited to one defined purpose.
- All TSM500 modules may use the same set of public keys for the authentication of the Manufacturer.
- Stored protected items, such as the operator hashes and audit log entries are verified by means of an error detection code (EDC) which is checked whenever one of these items is accessed.
- An Application firmware integrity test is performed (if Application firmware is present in the module) using the SHA-256 Approved security function. If the integrity verification fails the module behaves as if there is no Application firmware present.

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 180-3: Federal Information Processing Standard Publication 180-3
National Institute of Standards and Technology (NIST), 2008
"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] FIPS PUB 197: Federal Information Processing Standards Publication 197
National Institute of Standards and Technology (NIST), 2001
"Advanced Encryption Standard (AES)"

[13] SP 800-57 NIST Special Publication 800-57
National Institute of Standards and Technology (NIST), 2007
"Recommendation for Key Management – Part 1: General (Revised)"

[14] PKCS #1 v2.1: RSA Cryptography Standard
RSA Laboratories, June 2002

[15] NIST (Unnumbered publication)
National Institute of Standards and Technology (NIST), 2005
"NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms"

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
DRNG	Deterministic Random Number Generator
ECB	Electronic Code Book (DES or TDES mode of operation)
EDC	Error Detection Code
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
HRNG	Hardware Random Number Generator (used to seed the DRNG)
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
RAM	Random Access Memory (readable and writable)
rDSA	Reversible Digital Signature Algorithm
rMAC	Retail Message Authentication Code (also known as the Enhanced DES MAC)
RNG	Random Number Generator
RS232	Recommended Standard 232, a serial communications 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
TSM500	The Incognito TSM500 cryptographic security module
UID	Unique Identifier
VDC	Voltage (Direct Current)