Mxtran Payeeton Solution Security Policy

Version	:	v1.2
Effective Date	:	July 11, 2011
Classification	:	Public

EDITOR

Author	Title
CW Pang	Department Manager

Revision History

Version	Description	Date	By
0.1	Initial Version	2010/09/15	CW Pang
0.2	Response for comments	2010/10/01	CW Pang
0.3	Update	2010/10/22	CW Pang
1.0	Final Version	2010/10/29	CW Pang
1.1	Response for CMVP comments	2011/03/30	CW Pang
1.2	Response for CMVP comments	2011/07/11	CW Pang

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary security policy for the Mxtran Payeeton Solution (MPS, hereafter referred to as the module) of Mxtran Inc. This Security Policy describes how the cryptographic module meets the requirements for a FIPS 140-2 level 3 validation as specified in the FIPS 140-2 standard. This Security Policy is part of the evidence documentation package to be submitted to the validation lab.

FIPS 140-2 specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard, please visit http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

1.2 Scope

This Security Policy specifies the security rules under which the cryptographic module operates its major properties. It does not describe the requirements for the entire system, which makes use of the cryptographic module.

1.3 Security Level

The module meets the overall requirements applicable to FIPS140-2 Security Level 3. In the individual requirement sections of FIPS 140-2 the following Security Level ratings are achieved:

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3

Section	Section Title	Level
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	3

Table 1 – Security Level per FIPS 140-2 Section

2 Cryptographic Module Specification

The cryptographic module acts as a flexible platform for diversified mobile commerce services, allowing Mxtran clients to support both proximity payment and mobile payment via SMS for prepaid, online paid and post-paid services including e-ticketing, e-coupons, access control, membership management and more. Mxtran leverages extensive integrated circuit expertise to deliver highly customizable, portable applications and payment services in a single handset.

The module is a single-chip module that contains a CPU, ROM, EEPROM, and RAM based on MX11E25664E controller by Mxtran. The MX11E25664E is a dual interface smart card controller that being designed for multiple applications. This device is a microcontroller combining contactless smart card technology based on the [14443] standard and contact smart card technology on a single chip. It is organized with OTPROM and EEPROM. The CPU accesses OTPROM and EEPROM via the MPU to implement data encryption.

2.1 Cryptographic Module Boundary

The cryptographic module boundary is the edge of the controller globe-topped with opaque epoxy resin. The module will be embedded into a plastic film body and connected to two [7816] compliant contact plates and/or to an [14443] compliant external antenna loop. The boundary separates the module from the plastic film body, contact plates, and external antenna loop.

The module is a single-chip implementation of a cryptographic module. During the manufacturing process, the epoxy-covered controller is wire-bonded into plastic film body with contact plates on both sides and/or an external antenna loop. The perimeter of the module forms the cryptographic boundary of this FIPS140-2 Security Level 3 compliant single-chip cryptographic module.

The module block diagram and logical boundary are shown as following.

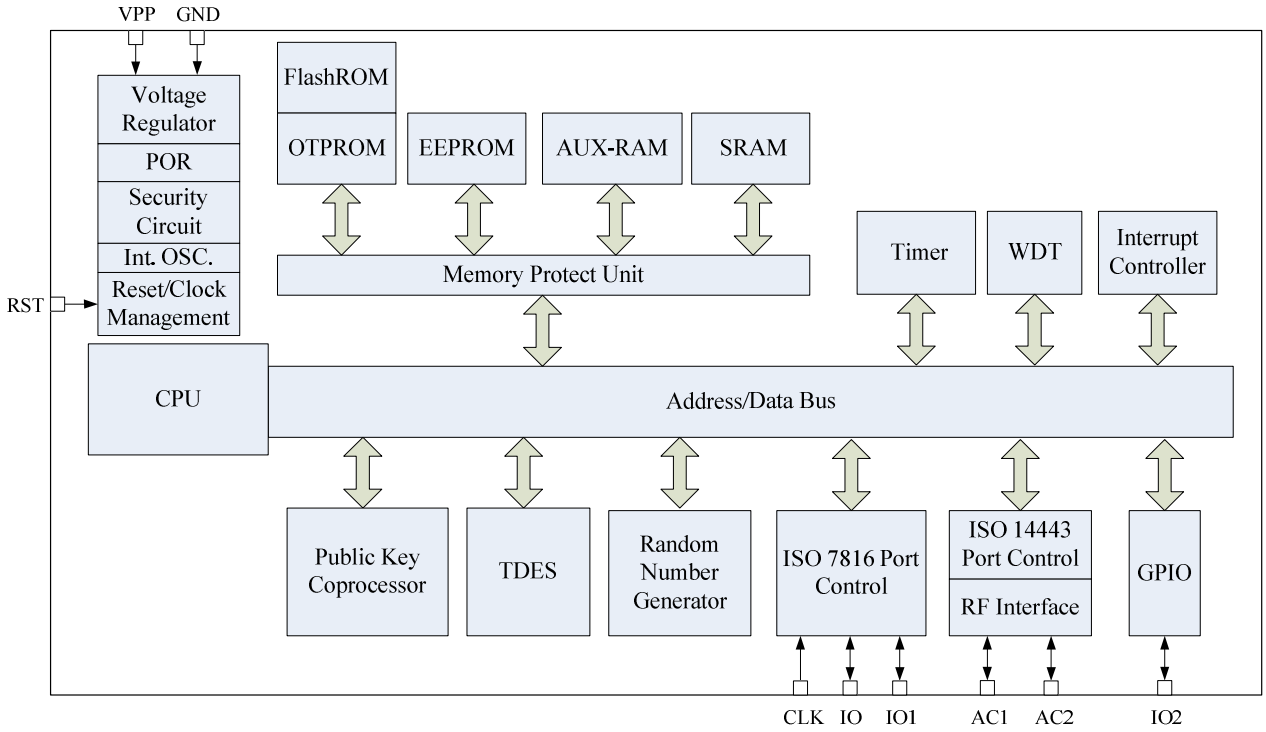

Figure 1 – Cryptographic Module Block Diagram

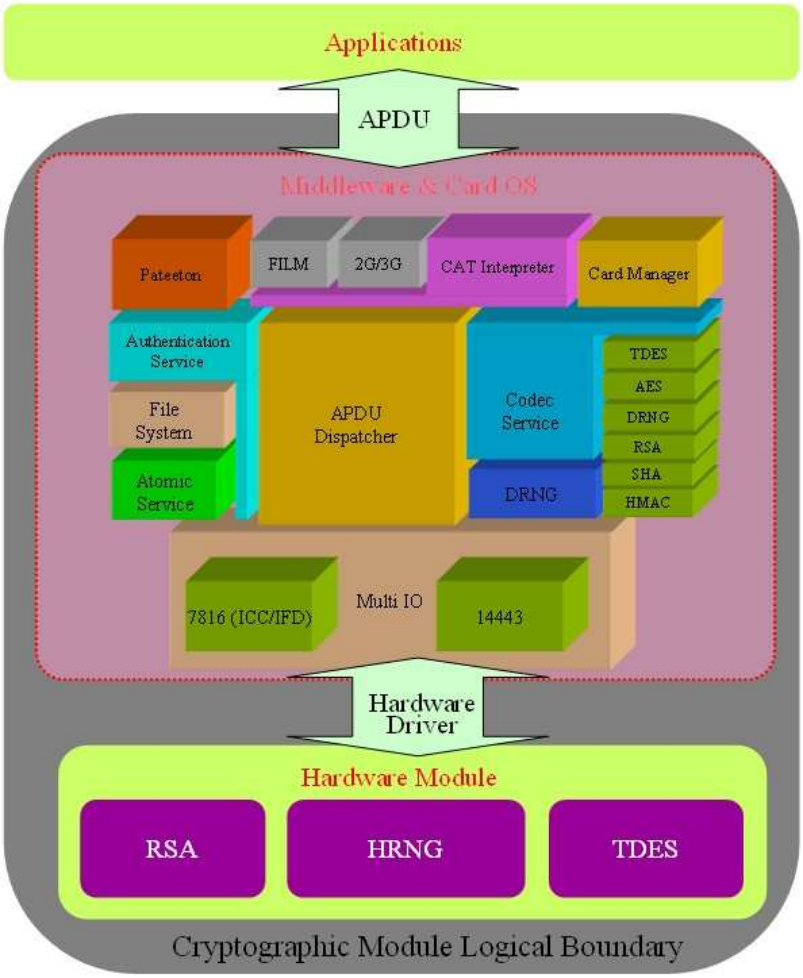

Figure 2 – Cryptographic Module Logical Boundary

2.2 Hardware

The module is a single-chip module that contains a CPU, ROM, EEPROM, and RAM. The boundary of the single-chip module is the edges and surfaces of the integrated circuit die. No components are excluded from the cryptographic boundary.

The module is designed to be encased into different form factors such as a plastic SIM card, a SIM card with antenna, or any other support to produce the MX11E25664E controller, on which FIPS

140-2 Level 3 validated applications may be loaded and instantiated at post issuance.

The following figures show two various form factors available from the module. Red perimeter indicates the cryptographic module boundary.

Figure 3 – Contact Mode
(Top view and bottom view)

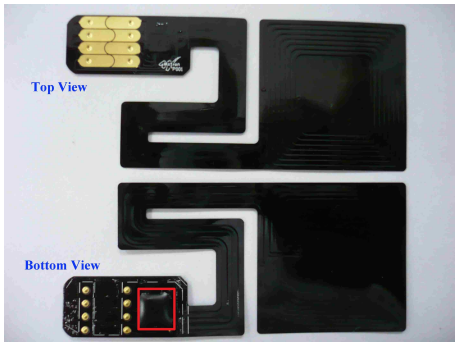

Figure 4 – Contactless Mode
(Top view and bottom view)

The cryptographic module is based on the MX11E25664E controller. This module comprises the following components:

- CPU core
- OTPROM as program memory
- Flash ROM as data/program memory
- EEPROM as data/program memory
- EEPROM as secure data memory
- Internal SRAM
- Auxiliary SRAM (including RSA dedicated SRAM)
- Dual data pointer
- Interrupt controller
- Four 16-bit Timers with ETU clock sources
- Watch Dog Timer with two clock sources (CLK and internal clock/16)
- Random number generator (DRNG)
- Triple-DES accelerator
- RSA coprocessors with DMA function

- Two [7816] compliant electrical interfaces and response T=0 and T=1 protocol
- Contactless RF interface according to [14443]
- 13.56 MHz operating frequency
- 847 kHz subcarrier for load modulation
- CRC engine compliant to ISO/IEC 13239

2.3 Firmware

The module contains platform firmware that resides in ROM of MX11E22664E controller, with key storage and future application storage functionality in the EEPROM. This firmware is implemented using high level language (C Language). It is loaded onto the module during manufacturing and does not allow for modification. An Error Detection Code (EDC) is calculated over the firmware during this installation and is checked at each power up.

After completion of the manufacturing process (including pre-personalization), only trusted FIPS 140-2 validated applications shall be loaded or installed onto the module. Furthermore, at the time of loading, these applications must be identified as part of the cryptographic module. The module uses HMAC to authenticate prior validated applications and avoid the loading of any unauthorized applications. Applications are isolated from each other due to the fact that the platform firmware does not contain any constructs that allow cross-application communication directly; any such communication must go by way of systems software mechanisms, which allow for implementation of strict security measures. Applications can only perform callable Approved security functions. The platform firmware restricts direct access to CSP through APDU ([7816] communication interface) and other hardware resources for a single user application.

The FIPS 140-2 validation testing targeted this specific configuration. Changes to that configuration (for example, loading another application), would constitute a new module, and the new configuration would need to undergo 140-2 testing for FIPS 140-2 compliance. There is no assurance of operation unless the modified module has been validated to FIPS 140-2, per CMVP requirements.

The firmware version supported by the module described in this security policy is: Simker 2.30.

The firmware comprises the following components:

- Authentication (AuthtnServ): FileSystem, Atomic
- Crypto (CodeServ): AES, RSA, SHA, TDES, HMAC, DRNG
- Multiple IO (Multi_IO): ISO7816, ISO14443
- APDU (Dispatcher): APDU bypass, Logical channel, multi-selectable applet management
- Interpreter(Interpreter): CAT applet interpreter

2.4 FIPS Approved Mode of Operation

The module shall not contain a non-FIPS Approved mode of operation. Hence, as configured during production process, the module only operates in a FIPS Approved mode of operation, comprising all services described in section below. The module does not implement bypass or maintenance modes. The module will enter FIPS Approved mode following on a successful response to the initial authentication sequence handshake command. Successful transition to the FIPS Approved mode is indicated by an ATR and a Success response to the initial authentication sequence handshake command. The ATR value returned by the module during power-up serves as an Approved mode indicator. The ATR returned by the module is: ATR: 3B 97 94 80 1F C3 80 31 A0 73 BE 21 13 B1

2.5 FIPS Approved Security Functions

The following table gives the list of FIPS Approved security functions that are provided by the module.

Security Function	Details	CAVP Cert. #
TDES	TECB(e/d; KO 1,2); TCBC(e/d; KO 1,2)	#1007

Security Function	Details	CAVP Cert. #
AES	ECB (e/d; 128 , 192 , 256); CBC (e/d; 128 , 192 , 256);	#1511
SHS	SHA-1 (BYTE-only) SHA-256 (BYTE-only)	#1354
RNG	ANSI X9.31 [TDES-2Key TDES-3Key AES-128Key AES-192Key AES-256Key]	#820
RSA	ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 1024 , 1536 , 2048 , SHS: SHA-1(Cert. #1354) , SHA-256(Cert. #1354)	#739
HMAC	HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) SHS (Cert. #1354) HMAC-SHA256 (Key Size Ranges Tested: KS<BS) SHS (Cert. #1354)	#886

Table 2 –FIPS Approved Security Functions

3 Cryptographic Module Ports and Interfaces

The module supports two modes of operations: Contact mode and Contactless mode.

Contact communication is achieved through a physical connection to a smart card contact plate. Contactless communication is achieved through a physical connection to a loop antenna. Neither the contact plate nor the antenna is within the cryptographic boundaries of the module. The mode of operation is determined at power-up, depending on the interface (contact or contactless) that powers the module. It cannot be changed until the module is reset.

3.1 Physical Ports

This module supports two types of distinct and non-concurrent physical ports which are contact and contactless. It is not intended that the contact interface will be connected.

3.1.1 Contact mode

This module provides a contact port with contacts that is fully compliant with [7816].

Contact (Top Side)	Contact (Bottom Side)	Contact Assignments	I/O	Description
C1	C1’	VCC	Power	Voltage range: 2.25V to 5.5V
C2		RST	Input	Reset: Active low
C3	C3’	CLK	Input	Clock: ISO clock input
C4		AC1	Analog	Antenna port
C5	C5’	GND	Power	Ground
C6	C6’	N.C.		Not Connected
C7		IO	Input/Output	Serial data input/output port
C8		AC2	Analog	Antenna port
	C2’	IO2	Input/Output	GPIO: General purpose IO
	C4’	N.C.		Not Connected
	C7’	IO1	Input/Output	Serial data input/output port
	C8’	N.C.		Not Connected

Table 3 – Physical Ports

This module supports two transmission half-duplex oriented protocols: T=0 and T=1.

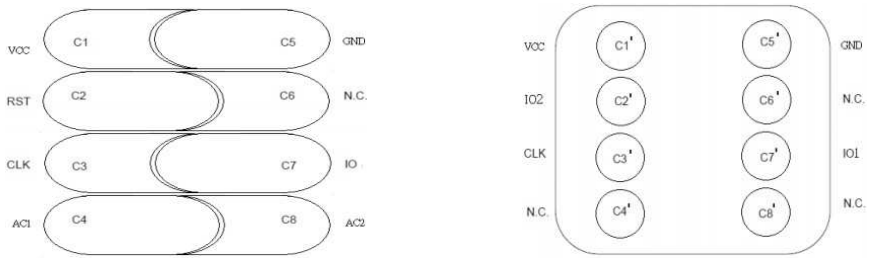

Figure 5 – Contact Mode Physical Ports

3.1.2 Contactless mode

This module provides a contactless port with antenna that is fully compliant with [14443].

The contactless reader produces an energizing RF field that transfers power to the module by coupling. The module operates independently of the external clock applied on the interfaces.

It uses two electrical connections AC1 and AC2 that link the antenna and the cryptographic boundaries of the module. RF contactless interface operating at 13.56 MHz are powered by and communicate with the Proximity Coupling Device via inductive coupling of the antenna to the Proximity Integrated Circuit Card antenna. When an out-of-range frequency is detected, module is reset.

Data input, control input, data output, status output are transmitted through the antenna using signal modulation as specified in [14443].

3.2 Logical Interfaces

The cryptographic module functions as a slave controller to process and respond to the reader commands. The I/O ports of the platform provide the following logical interfaces:

Logical Interface	Contact Mode ([7816])	Contactless Mode ([14443])
Data Input	IO, IO1, IO2	AC1 and AC2 (RF Modulation)
Data Output	IO, IO1, IO2	AC1 and AC2 (RF Modulation)
Control Input	IO, IO1, IO2, RST, CLK	AC1 and AC2 (RF Modulation)
Status Output	IO, IO1, IO2	AC1 and AC2 (RF Modulation)
Power	VCC, GND	AC1 and AC2 (RF Modulation)

Table 4 – Logical Interfaces

The logical interfaces are kept logically separate when sharing a physical port by the protocols used.

Information flows for the data input, data output, control input, and status output interfaces are encapsulated into APDU commands. They do not use the same physical port at the same time. Basically all commands are initiated from the terminal to inform the module what to do. The terminal will always act as master and the module as a slave. The direction of the transmission is assumed to be known to both the module and the terminal. This clause defines the transmission protocols used to exchange data between the terminal and the module in asynchronous half duplex transmission protocols.

4 Roles, Services and Authentication

The module supports two roles, Crypto Officer (CO) and User, and enforces the separation of these roles by restricting the services available to each one. The cryptographic module enforces the separation of roles using identity-based operator authentication. One authentication is allowed per module reset, i.e., an operator must re-authenticate after a power down or reset. Re-authentication is enforced when changing roles.

4.1 Roles

- **Crypto Officer Role**

The CO role is responsible for initializing the module and managing the security configuration of the cryptographic module with its loaded applications. Before issuing a module to an end user, the CO initializes the module with keying material and private information. The cryptographic module validates the CO identity using PIN verification before accepting any initialization commands. This role is also authorized to import keys, exchange keys or load application into this module.

- **User Role**

The User role is available after the cryptographic module has been loaded with a user personality.

This role is authorized to read user data and use cryptographic services. User role is not authorized to import keys into the module. The module allows only one operator to assume the User role, and the corresponding “User PIN” shall be known by one operator (i.e., the User) only.

Upon power-up or reset of the module an operator first assumes this role, until being successfully authenticated (and thus assuming CO or User role). The cryptographic module offers multiple logical data in/out interface to external operators. The module validates the User identity before access is granted. However, only one communication session can be open per authenticated role.

The module does not implement any maintenance interface, thus there is no maintenance role defined.

4.2 Identification and Authentication

The module implements identity-based authentication which is accomplished by PIN entry by the operator. Each PIN phrase is 8 ASCII printable characters in length.

The hardware security components (ICC with COS) are initialized at the factory with a default CO PIN. The CO must change the default value during logon to make the module ready for initialization. During initialization the module allows the execution of only the commands required to complete the initialization process.

Before a user can access or operate the module, the CO must initialize it with the User PIN. The CO is authorized to log on to the module any time after initialization to change parameters.

On invocation by the user, the module waits for authentication of the User or CO role by entry of a PIN phrase. In this module, there are only two PINs which are “User PIN” and “CO PIN”. Multiple User and CO accounts are not permitted. Only if an operator presents the correct PIN value to the module, he will be authenticated as CO or User, respectively. Once a valid PIN phrase has been accepted the module cryptographic services may be accessed. Due to the fact that the module allows only one operator to assume the CO role and only one operator to assume the User role, this way an

identity-based authentication of the operator is realized.

Besides from that, the authentication meets the following rules:

- Power-on or reset of the module puts it into not authenticated state.
- An unsuccessful PIN verification attempt puts the module into not authenticated state, regardless of the authentication state prior to the PIN verification attempt.
- A successful PIN verification puts the module into CO authenticated state or User authenticated state, respectively, regardless of the authentication state prior to PIN verification. I.e., it is impossible that CO and User are authenticated at the same time.
- Feedback of authentication data to an operator is obscured during authentication (e.g., no visible display of characters result when entering a password). The PIN value is input to the "Verify PIN" command as a parameter by the calling application. No return code or pointer to a return value that contains the PIN is provided.
- Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism. The only feedback provided by the "Verify PIN" command is a return code denoting success or failure of the operation. This information in no way affects the probability of success or failure in either single or multiple attacks.

For CO PIN and User PIN separate retry counters are managed by the module, which are limited the default maximum number of consecutive unsuccessful PIN verification attempts to eight, meeting the following rules:

- If the retry counter has reached eight, all further attempts to verify the corresponding PIN are rejected (the PIN is locked), i.e., no more CO or User authentication, respectively, is possible. The module goes Error state.
- Each unsuccessful PIN verification attempt increases the corresponding retry counter by one.
- A successful PIN verification resets the corresponding retry counter to zero.

The strength of the authentication mechanism conforms to the following specifications.

- Single PIN-entry attempt / False Acceptance Rate

  The probability that a random PIN-entry (using 94 printable characters) attempt will succeed or a false acceptance will occur is $1/94^8=1.64\times10^{-16}$. The requirement for a single–attempt / false acceptance rate of no more than 1 in 1,000,000 (i.e., less than a probability of 10^{-6}) is therefore met.

- Multiple PIN-entry attempt in one minute

  With the module, the CO or User PIN authentication takes about 0.2 second. The maximum number of tries in one minute is 60/0.2 = 300. There is also a maximum bound of 8 successive failed authentication attempts before system halt occurs. The probability of a successful attack of multiple attempts in a one minute period is no more than 1.31×10^{-15} due to the maximum of 8 attempts. This is less than one in 100,000 (i.e., 10^{-5}), as required.

4.3 Services

The services provided by the module to each role in terms of commands are specified in the table below (for a brief description of the services see table “Services Description” hereinafter).

Role	Authorized Services (Commands)		
Crypto Officer	Activate File	Erase EEPROM	Search Record
	Append Record	External Authenticate	Select
	CAT Decipher	Fetch	Set data
	CAT DRNG	Get Challenge	Show Status
	CAT Encipher	Get Chip ID	Terminal Response
	CAT Hash	Get Version	Unblock Key
	CAT Sign Signature	Increase	Update Binary
	CAT Verify Signature	Internal Authenticate	Update Record
	Change Key	Load Content	Verify PIN

Role	Authorized Services (Commands)		
	Deactivate File Disable Key Enable Key Envelope	Load Key Read Binary Read Record Retrieve Data	Verifying CAT Applet Terminal Profile
User	Activate File Append Record CAT Decipher CAT DRNG CAT Encipher CAT Hash CAT Sign Signature CAT Verify Signature Change Key Deactivate File	Enable Key Envelope External Authenticate Fetch Get Challenge Get Chip ID Increase Read Binary Read Record Retrieve Data	Search Record Select Set data Show Status Terminal Response Update Binary Update Record Verify PIN Terminal Profile

Table 5 – Roles and Authorized Services

Details of Services are given in the following table as well as the CSPs access when performing the services.

No.	Service (Command)	Service Description	CSPs /Keys	Type of Access
1.	Activate File	To active a specified EF/DF		
2.	Append Record	Append a new record		
3.	CAT Decipher	Decrypts data via approved security function TDES or AES	User Keys	Use
4.	CAT DRNG	Generates a random number via approved security DRNG function	ANSI X9.31 DRNG Seed and Seed Key	Use
5.	CAT Encipher	Encrypts data via approved security function TDES or AES	User Keys	Use

No.	Service (Command)	Service Description	CSPs /Keys	Type of Access
6.	CAT Hash	Calculates a message digest via approved hash function (SHS or HMAC)	User Keys	Use
7.	CAT Sign Signature	Generates a RSA digital signature with a previously loaded private key	RSA private key	Use
8.	CAT Verify Signature	Verifies a RSA digital signature with a previously loaded public key	RSA public key	Use
9.	Change Key	Change User keys/PIN	User Keys/PIN RSA Keys Session key	Write
10.	Deactivate File	To de-active a specified EF/DF		
11.	Disable Key	Disable user verification mechanism	User Keys PIN	Use
12.	Enable Key	Enable user verification mechanism	User Keys PIN	Use
13.	Envelope	Trigger a register CAT applet	User Keys PIN	Use
14.	Erase EEPROM	Erase the content of EEPROM	User Keys	Zeroize
15.	External Authenticate	Perform a external authentication procedure	User Keys	Use
16.	Fetch	Get the proactive command	User Keys PIN	Use
17.	Get Challenge	Get a random value for external authentication	ANSI X9.31 DRNG Seed and Seed Key	Use
18.	Get Chip ID	Get Chip unique ID		
19.	Get Version	Get the COS version		
20.	Increase	Increases the content of a record in the currently selected Cyclic EF.		

No.	Service (Command)	Service Description	CSPs /Keys	Type of Access
21.	Internal Authenticate	Perform a internal authentication procedure	User Keys	Use
22.	Load Content	Loading file content to specific file		
23.	Load Key	Loading a new key/PIN content through secure channel	User Keys/PIN RSA Keys Session key	Write
24.	Read Binary	Read binary data from selected EF		
25.	Read Record	Read data from selected EF		
26.	Retrieve Data	Get TLV data object on selected EF		
27.	Search Record	Search a data pattern on selected EF		
28.	Select	Select an applet/file		
29.	Set data	Append a new TLV data object on selected EF		
30.	Show status	This service provides the current status of the cryptographic module.		
31.	Terminal Response	To inform the result of proactive command	User Keys PIN	Use
32.	Unblock Key	Unlock User key/PIN while locked.	User Keys PIN	Write
33.	Update Binary	Update binary data from selected EF		
34.	Update Record	Update data from selected EF		
35.	Verify CAT Applet	Verifying a CAT Applet	User Key	Use
36.	Verify PIN	Verifies User PIN	PIN	Use

No.	Service (Command)	Service Description	CSPs /Keys	Type of Access
37.	Terminal Profile	To inform the capacity of handset		

Table 6 – Services

5 Physical Security

The module is a production grade, single-chip cryptographic module as defined by FIPS 140-2 and is designed to meet level 3 physical security requirements. The chip die is mounted on a substrate and covered by a protective coating that provides evidence of attempts to tamper with the module. The module finally will be embedded between two opaque plastic films and be connected to copper trace providing two [7816] compliant contact plates and/or to an [14443] compliant external antenna loop. And on the top side of module there is a hard opaque epoxy resin cover. It employs physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module. All hardware and firmware within the cryptographic boundary are protected.

5.1 Physical Security mechanisms as required by FIPS 140-2

The cryptographic module is covered with a hard opaque coating that provides evidence of attempts to tamper with the module. The thermal black resin technology consists in an epoxy resin that is also applied on top of the chip at the back side of the embedded module after the connection (bonding) of the chip to the two sides of the contact plates have been completed. This resin is characterized by its black color and opacity that makes observation of the silicon chip impossible when the embedded module is finished. The substrate side of the chip is covered by the opaque coating and plastic film.

The hardness of the coating and of the epoxy resin provides efficient mechanical protection and

tamper evidence for the module. Tamper attempts will result in visible damage of the coating body, and when trying to access the surface of the chip inside the card, again the module has to be opened. A continued attempt of tampering, trying to get access to the chip's surface, will result in a non-functioning module by breaking of either silicon chip and/or bond wires with high likelihood.

No maintenance access interface is available. No special procedures are required to maintain physical security of the module while delivering to operators.

5.2 Additional Hardware Security Mechanisms

The cryptographic module includes the following additional physical protections which were not tested as part of this FIPS validation:

- High/low voltage detector
- High/low frequency detector
- High/low temperature detector
- Security reset detection
- Light sensors
- Active shield against physical probing

6 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements do not apply to the module in this validation because the module does not contain a modifiable operational environment.

7 Cryptographic Key Management

7.1 Critical Security Parameters and Public Keys

The cryptographic module includes system keys and PINs for card administration purposes. The following table provides a list and description of all CSPs and public keys managed by the module.

CSP/ Public Key	Type	Generate/ Input	Output	Storage	Use
ANSI X9.31 DRNG Seed	8-byte random number/ 16-byte random number	Generated by the HRNG of module	None	RAM	Used to seed the ANSI X9.31 DRNG.
ANSI X9.31 DRNG Seed Key	168-bit TDES keys/ 256-bit AES key	Generated by the HRNG of module	None	RAM	Used to seed the ANSI X9.31 DRNG.
PIN	8 ASCII printable characters in length	Load in encrypted form with “Load Key” command	None	EEPROM	Used for User/CO authentication.
RSA private key	PKCS#1 V1.5 1024-bit RSA key	Load in encrypted form with “Load Key” command	None	EEPROM	Used to generate signature during RSA generation.
RSA public key	PKCS#1 V1.5 1024-bit RSA key	Load in encrypted form with “Load Key” command	None	EEPROM	Used to verify signature during RSA verification.
Secure Channel Session Key	168-bit TDES keys	Diversified by User keys with random numbers using TDES	None	RAM	Used to encrypt and decrypt PIN/keys data transmitted to the module.
User keys (TDES)	168-bit TDES keys	Load in encrypted form with “Load Key” command	None	EEPROM	Encryption / Decryption
User keys (AES)	256-bit AES keys	Load in encrypted form with “Load Key” command	None	EEPROM	Encryption / Decryption
User keys (HMAC)	FIPS 198 Key	Load in encrypted form with “Load Key” command	None	EEPROM	Used to generate HMAC message authentication code

Table 7 – Critical Security Parameters and Public Keys

7.2 Key Generation and Diversification

The module does not provide key generation functionality.

Through mutual authentication between the CO and the card terminal a secure channel will be established to execute services in a secure manner so that access to security-critical information and services can be granted. The module uses the ephemeral “Secure Channel Session Key” to encrypt / decrypt all communication sent / received via the secure channel. “Secure Channel Session Key” is derived from three random numbers which are generated by DRNG and encrypted using TDES with User keys (TDES).

7.3 Key Entry and Output

Keys shall always be input in encrypted format, using the “Load Key” or “Change Key” command within a secure channel. During this process, the keys are encrypted in TDES using the cryptographic key “Secure Channel Session Key”.

The secure channel session used must be such that the cryptographic strength of the encryption key is at least equal to the cryptographic strength of the key being loaded.
Keys can never be output by the module through any service.

7.4 Key Storage

“Secure Channel Session Key” as well as RNG seed values are stored in RAM for temporarily usage. Other keys and CSPs are stored in a dedicated space of the EEPROM. Before CSPs stored into memory, they are manipulated by hardware data scramble function.

7.5 Key Zeroization

Cryptographic keys stored in non volatile memory can be zeroized by reloading another randomized value using the “Load Key” or “Chang Key” command. The module also has the ability to destroy all keys and CSPs by an “Erase EEPROM” command. The contents of EEPROM including all keys and CSPs being deleted are erased and over written. Should a power-down occur during the execution of the “Erase EEPROM”, the action of zeroization will resume on a subsequent power-on event, ensuring that access to zeroized information is prevented.

Session cryptographic keys are stored in volatile memory and are zeroized upon termination of the session, i.e., when the secure channel is closed or when the module is powered off.

7.6 RNG Seed Values

During power up initialization, the module use HRNG to compute new DRNG Seed and DRNG Seed Key values. Any old seed values (which were randomized) are then overwritten with the new computed values. These seed values are temporarily exists in volatile memory and are zeroized by power cycling the module. These values are not accessible to any user.

8 Electromagnetic Interference/Compatibility (EMI/EMC)

The cryptographic module has been successfully tested by Sporton International Inc. with the certificate No.: FV0NC002 to meet the EMI/EMC requirements according to FCC 47 CFR part 15, subpart B, class B (Home Use), and received the corresponding certificate of conformity.

9 Self-Tests

The module performs both power-on and conditional self-tests. These tests are conducted

automatically as part of the normal functions of the cryptographic module. They do not require any additional operator intervention. All data output via the output interface is inhibited while any power-up and conditional self-test is running.

Self-Tests failure resulting in the module goes into an Error (“mute”) state. In the error mode, the module no longer responds to further commands, and output any data. One technique to remove the module from the mute mode is to perform a ”hard reset“ on the module (i.e., remove the module from terminal) and start over. However, with implementations, if such a reset is used to reset the module's CPU, the enumeration, configuration, etc. of the module on the bus is lost.

9.1 Power-up Self-Tests

Each time this cryptographic module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged.
When the module is inserted into a terminal, a “Reset” signal is sent from the reader to the module. The module responds (as specified by [7816]) with an ATR packet of information. After a reset of the module, power-up self-tests are executed. The cryptographic module start-up process has been designed in such a way that it cannot be bypassed. This enforces the execution of self-tests before allowing any use of the module, thus guaranteeing a secure execution of the module’s cryptographic services. Resetting the cryptographic module provides a means by which the operator can perform the power-up self-tests on demand.

These tests include:

- Cryptographic algorithm testing

  Known Answer Tests (KATs) are conducted for each cryptographic algorithm in one mode of operation. Known input data and answers are stored in EEPROM. KATs include following:

  - Triple-DES
  - AES
  - SHA

- RSA
- HMAC
- ANSI X9.31 DRNG

KATs function by encrypting/decrypting, hashing or signing a string for which the calculated output is known and stored within the cryptographic module. An encryption, hashing or signature test passes when the calculated output matches the expected (stored in OTPROM) value. The test fails when the calculated output does not match the expected value.

KATs for DRNG function by seeding the DRNG with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The module also performs Continuous RNG tests for HRNG and DRNG described below.

- Firmware integrity testing

An EDC using standard 16-bit checksum is stored in EEPROM and is used to verify that the firmware present in EEPROM has not been modified. OTPROM code is excluded from firmware integrity verification.

If and only if all power-up self-tests are passed successfully, the cryptographic module performs the command procedure according to the first APDU (received before or after power-up self-tests started) and returns the corresponding response and status word via the data output interface and status output interface (and then further incoming APDU commands are processed).

9.2 Conditional Self-Tests

- Continuous RNG Tests:

A continuous RNG test is performed during each use of both DRNG and HRNG to verify that it is not generating the same value. The HRNG is used to generate ANSI X9.31 DRNG seed and seed keys. They are tested by repetition of serial output 1 block (8 bytes) random number to compare the saved 1st block on initial phase. If the comparison is equal then the module discards the random number to get a new one. If the situation occurs continuously, the module does not

provide any service.

- Software Load Test:

  A “Verify CAT applet” service is triggered to perform Software Load Test whenever an application is loaded onto the cryptographic module. The module uses HMAC to authenticate prior validated applications and avoid the loading of any unauthorized applications. The module enters an error state if the Software Load Test fails.

10 Design Assurance

10.1 Configuration Management

The module was designed and developed using a configuration management system “Subversion” that is clearly ruled and operated.

The definition methods, mechanisms and tools that allow identifying and placing under control all the data and information are specified in the configuration management document.

10.2 Delivery and Operation

The “Secure Delivery and Installation/Generation/Start” documentation and the administration/user guidance documentation define and describe the steps necessary to deliver and operate the module securely.

10.3 Guidance Documents

The administration and user document was designed to allow a secure operation of the module by its users as defined in the “Roles, Services and Authentication” chapter and in the scope of the Security Policy boundaries.

11 Mitigation of Other Attacks

This Cryptographic Module is protected against SPA, DPA, Timing Analysis and Fault Induction by combining State of the Art firmware and hardware counter-measures.

- Power Analysis (SPA/DPA)

  The module includes protections against SPA and DPA attacks for all embedded cryptographic algorithms involving secret elements. The cryptographic module mitigates SPA and DPA attacks using a combination of hardware and software design that makes differentiation of key values impractical by equalizing or scrambling current consumption of the card during algorithm cryptographic computation. Based on the algorithm used, the defense mechanisms vary, as the internal hardware implementations of these algorithms do not use the same underlying hardware.

- Timing Analysis

  All cryptographic algorithms offered by the chip are designed to be protected against Timing Analysis. This is done by enforcing the fact that any sensitive operation is achieved in a constant time regardless of the value of keys or data involved.

- Fault Induction

  The cryptographic module includes a combination of software and hardware protections in order for the chip not to operate in extreme conditions that may cause processing errors that could lead to revealing the values of cryptographic keys or secret elements. Extreme Conditions refer to abnormal temperature, external power supply and external clock supply. The Cryptographic Module does not operate in abnormal conditions such as extreme temperature, power and external clock, increasing its protection against fault induction.

12 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

12.1 General Security Rules

- The module only implements Approved mode.
- The module does not support a bypass capability.
- The module does not support a platform firmware loading service for update. However, FIPS 140-2 Level 3 validated applications may be loaded and instantiated at post issuance.
- No hardware, software, or firmware components of the cryptographic module are excluded from the security requirements of FIPS 140-2.
- The 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.
- The module logically disconnects the output data path from the circuitry and processes when performing self-tests, key generation, manual key entry, key zeroization, or error states.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- The secret cryptographic keys shall be entered in encrypted form over a physically separate port.
- The module implements all software using a high-level language, except the limited use of low-level languages to enhance performance.

12.2 Identification and Authentication Security Rules

- The module enforces Identity-Based authentication.

- The module provides two distinct operator roles: User role, and the Crypto Officer role.
- Authenticated operators are authorized to assume either supported role. The module does not allow the operator to change roles.
- The module does not support multiple concurrent operators.
- The module does not support a maintenance interface or role.
- When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
- The module contains the authentication data required to authenticate the operator for the first time.
- The module re-authenticates an operator when it is powered-up after being powered-off.
- The cryptographic module clears previous authentications on power cycle.
- The module's authentication mechanism does not supply any feedback information to the operator.
- A limit of 8 failed authentication attempts is imposed; 8 consecutive failed authentication attempts causes system halted.

12.3 Access Control Security Rules

- While processing a transaction, prior to returning a response, the module will ignore all other inputs to the module. No output is performed until the transaction is completed, and the only output is the transaction response.
- The module does not enter plaintext CSPs. Authentication data (e.g. PINs) are entered in encrypted form. Authentication data is not output during entry.
- The module protects secret keys, private keys and public keys from unauthorized disclosure, modification, and substitution.

- The module generates all keys having at least 80-bits of strength.
- The module establishes all keys being at least as strong as the key being established.
- The module does not support manual key entry.
- The module does not have any external input/output devices used for entry/output of data.
- The module does not perform any cryptographic functions while key loading or in an error state.
- The module does not output of plaintext cryptographic keys, encrypted cryptographic keys, intermediate key values, CSPs, or sensitive data.
- The module provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the module.
- Once a module has been zeroized, it must be returned to the factory for firmware loading and configuring prior to being usable by a customer.
- Seed keys are not entered into the module during the key generation process, they are gathered internally.
- The module ensures that the seed and seed key inputs to the approved RNG are not equal.
- The operator commands the module to perform the power-up self-test by cycling power or resetting the module (pulse the RST pin low).
- Power-up self test is automatically triggered.
- Recovery from “soft” error states is possible via power-cycling. Recovery from “hard” error states is not possible.
- When the Power up Self-Tests fail the module would be in non operative (“mute”) state.
- The module enters an error state if the Cryptographic Algorithm Test, Continuous Random Number Generator Test, or Integrity Test fails. This error state may be exited by powering the module off then on.

12.4 Physical Security Rules

- The opaque coating of module deters direct observation within the visible spectrum.
- The hard tamper-evident coating provides evidence of tampering, with high probability of causing serious damage to the chip while attempting to probe it or remove it from the module.
- The operator shall check of epoxy coating and contact plate, whether the module is physically intact.
- The operator shall check of film body, in particular opposite to the contact plate, whether the module is physically intact.
- The security provided from the hardness of the module's epoxy encapsulate is claimed at ambient temperature (20 to 25 degrees Celsius or 68 to 77 degrees Fahrenheit) only. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range.

12.5 Mitigation of Other Attacks Security Rules

This Cryptographic Module is protected against SPA, DPA, Timing Analysis and Fault Induction, which is outside of the scope of FIPS 140-2.

13 Security Policy Check List Tables

13.1 Roles and required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	PIN verification	User PIN

Role	Type of Authentication	Authentication Data
Crypto officer	PIN verification	Crypto Officer PIN

Table 8 - Roles and Required Identification and Authentication

13.2 Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
PIN verification	The module prevents brute-force attacks on its PIN by using an 8-character PIN. And a limit of 8 failed authentication attempts is imposed; 8 consecutive failed authentication attempts causes system halted. According the calculation in Section 4.2. ▪ Single PIN-entry attempt / False Acceptance Rate The probability that a random 8-character PIN-entry attempt will succeed or a false acceptance will occur is 1.64×10^{-16}. ▪ Multiple PIN-entry attempt in one minute The probability of a successful attack of multiple attempts in a one minute period is no more than 1.31×10^{-15}.

Table 9 - Strength of Authentication Mechanisms

13.3 Services Authorized for Roles

Role	Authorized Services

Role	Authorized Services
User	Section.4.3 lists authorized services for this role
Crypto Officer	Section.4.3 lists authorized services for this role

Table 10 - Services Authorized for Roles

13.4 Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A
Timing Analysis	Counter Measures against Timing Analysis	N/A
Fault Induction	Counter Measures against Fault Induction	N/A

Table 11 - Mitigation of Other Attacks

14 References

[FIPS140-2] Security Requirements for Cryptographic modules, May 25, 2001

[IG] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

[14443] ISO/IEC 14443-1, First edition 2008-06-04, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical characteristics

ISO/IEC 14443-2, First edition 2010-08-19, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface

ISO/IEC 14443-3, First edition 2001-02-01, Identification cards - Contactless

integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anti-collision

ISO/IEC 14443-4, First edition 2008-07-07, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol

[7816] ISO/IEC 7816-1, First edition 1998-10-15, Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics

ISO/IEC 7816-2, First edition 2007-10-11, Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts

ISO/IEC 7816-3, Third edition 2006-11-01, Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols

ISO/IEC 7816-4, Second edition 2005-01-15, Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange

15 Acronyms

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
ATR	Answer To Reset
CAT	Card Application Toolkit
CBC	Cipher Block Chaining
CLK	Clock
CMVP	Cryptographic Module Validation Program
COS	Card Operating System
CSP	Critical Security Parameter
DES	Data Encryption Standard
DF	Dedicated File
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator

ECR	EEPROM Control Register
EDC	Error Detection Code
EEROM	Electrically Erasable, Programmable Read Only Memory
EF	Elementary File
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FMU	Firewall Management Unit
GND	Ground pin
HMAC	Keyed-Hash Message Authentication Code
HRNG	Hardware Random Number Generator (Non-Deterministic Random Number Generator)
ICC	Integrated Circuit Chip
KAT	Known Answer Test
MPS	Mxtran Payeeton Solution
MPU	Memory Protection Unit
OTPROM	One Time Programmable Read Only Memory
RAM	Random Access Memory
RF	Radio Frequency
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir and Adleman Public Key Algorithm
RST	Reset pin
SFR	Special Function Registers
SHA	Secure Hash Algorithm
SMS	Short Message Service
SPA	Simple Power Analysis

SRDI	Security Related Data Item
SVN	Subversion
TDES	Triple DES (see DES)
VCC	IC power supply pin
WDT	Watchdog Timer