Taisys Technologies Co., Ltd.

TAISYS JUISE-S2

Firmware Version: 32 53

Hardware Version: 46 43

FIPS 140-2 Non-Proprietary

Security Policy

Level 3 Validation

April, 2019

Table of Contents

Document History

Authors	Date	Version	Comment
Brad Proffitt	March 30, 2017	0.1	First Draft
Brad Proffitt	June, 2018	0.2 to 1.0	Incorporate Lab comments
Brad Proffitt	April 2019	1.1 to 1.3	Address CMVP comments

1. INTRODUCTION

This is a non-proprietary FIPS 140-2 Security Policy for the Taisys Technologies JUISE-S2 v1.0 contact/contactless module hereafter denoted **the Module**. The Module, validated to FIPS 140-2 overall Level 3, is a single chip secure controller module implementing the Global Platform operational environment, Taisys Card Manager This Policy forms a part of the submission package to the validating lab.

The Module is a smart card platform, intended for use only as a platform for vendors to develop applets, ultimately for use by US Federal agencies. The loading of non-validated firmware within the validated cryptographic module invalidates the module's validation.

FIPS 140-2 (Federal Information Processing Standards Publication 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 visit www.nist.gov/cmvp

The product meets the overall requirements applicable to Level 3 security for FIPS 140 2.

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles and Services and Authentication	3
Finite State Machine Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3
Overall Level of Certification	3

Table 1 - Module Compliance Levels

The Module implementation is compliant with:

- [ISO 7816] Parts 1-4
- ETSI 102 613 UICC – Contactless Front-end (CLF)
- ETSI 102 622 UICC – Host Control Interface (HCI)
- [JavaCard] API 3.0.4
- [JavaCard] RE 3.0.4
- [JavaCard] VM 3.0.4
- [GlobalPlatform] Card Spec 2.2.1

2. PRODUCT DESCRIPTION

The TAISYS JUISE-S2 is a contact/contactless module that provides security services targeted at mobile devices in a single Integrated Circuit Chip specifically designed for the security of data. Once inside the phone the module becomes an independent secure element to deploy to customers, as government and enterprise, and may download the applications in the card for identification, health or banking markets.

Java technology is the leading multiple applications operating system for smart cards. It offers developers a convenient platform on which to develop and implement smart card applets. The TAISYS JUISE-S2 has been designed to offer a modular and open solution based on reliable and standardized technologies.

To that end, the TAISYS JUISE-S2 Open module contains an implementation of the Sun Java Card ™ 3.0.4 Classic Edition [JCS] specifications. It allows implementing multiple applications associated with a high security level to execute the applications by providing context independence between each of them. The TAISYS JUISE-S2 Open module is also compliant with the GlobalPlatform Card Specification - Version 2.2.1 [GP] with SCP03 as defined in the Amendment D [GP_AMD_D], where it secures the application management and manages the card life cycle.

2.1. Cryptographic Boundary

The cryptographic module boundary is realized as the external surface of the ST33G1M2 single chip microprocessor and does not include smart card contact plate in contact, the antenna for contactless, the fixation glue. The boundary contains all of the relevant module components (processors performing cryptography, etc.) consistent with [FIPS 140-2]. The module is a single chip hardware module.

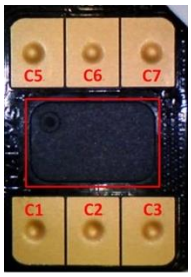
Module boundary

The module relies on a hard-opaque plastic package to meet FIPS 140-2 level 3 physical requirements. TAISYS ships the module in three form factors, Smart Card, SIMoME and ECoffer chip. The module does not rely on the form factors to meet the FIPS 140-2 physical security requirements. The modules interfaces (chip pin outs) are not modified by any of these form factors.

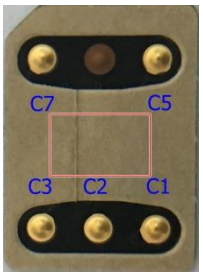
Details on the form factors are below:

Smart Card and SIMoME Card form:

Up side of SIM card SIMoME Card



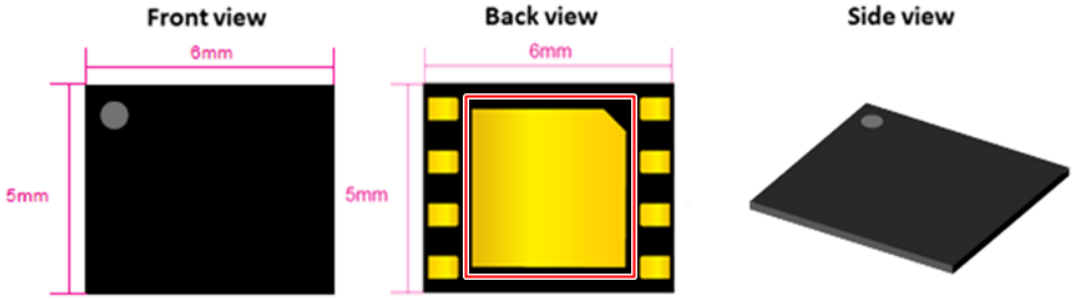
C1	VCC	C5	GND
C2	RST	C6	SWP
C3	CLK	C7	SIO



C1	VCC	C5	GND
C2	Q-RST		
C3	CLK	C7	Q-SIO

(The red rectangle indicates hardware cryptographic boundary)

The ECoffer chip form:



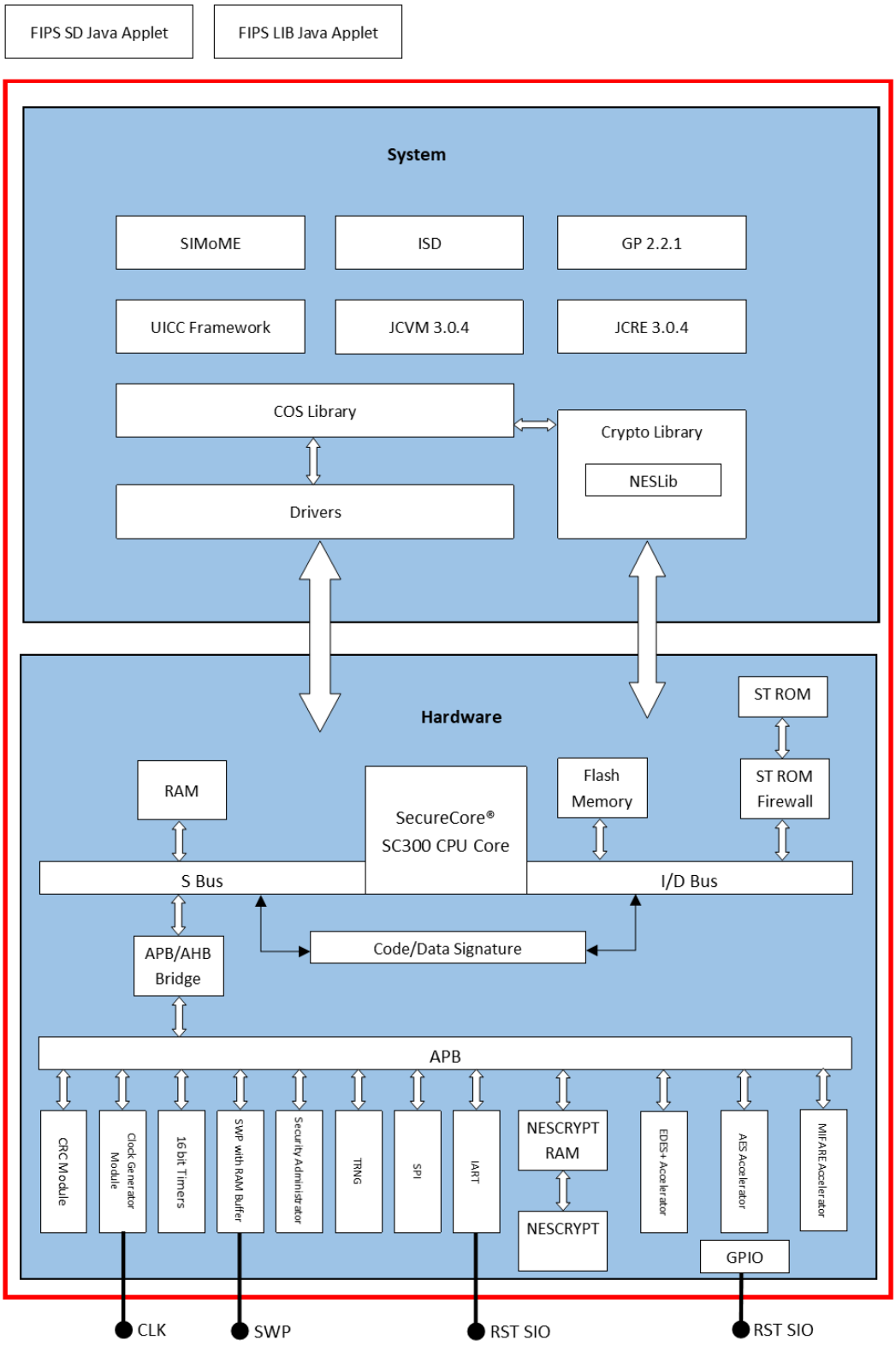
VCC	GND
Q-SIO	SWP
Q-RST	SIO
RST	CLK

(The red rectangle indicates hardware cryptographic boundary)

The ECoffer form is an IC package form. It will be embedded into smart phones. It communicates with main chip of smart phones via ISO7816 communication channel.

2.2. Firmware and Logical Cryptographic Boundary

The diagram depicts the module architecture. The red outline depicts the logical cryptographic boundary.



The JavaCard API and GP API are internal interfaces available only to applets. Only applet services are available at the card edge.

FIPS LIB provides FIPS Services API and FSM Implementations. Base on FIPS Service API, service provider can

program their applications more convenient and needs not their own FSM. Service provide can also program their application by standard JavaCard API and their own application level FSM and manage their own application level roles. Platform level FSM will manage states of low-level functions, include power-up self-tests, conditional self-tests, algorithm security checks, role of Crypto-Officer is controlled by platform level FSM. Application level FSM manages roles other than Crypto-Officer. All code is executed from FLASH.

2.3. Firmware version and hardware

There is only one firmware version. An operator can send the following command for the firmware version when the system is powered on or after reset:

Command	Expected Response
GET CARD INFO	H1 H2 V1 V2 Where H1 H2 is product ID, For the module, H 1 H2 is 46 43. Product ID internally maps to the hardware model and firmware version. V1 V2 is the version number. For the module V1 V2 is 32 53

Table 2 - Get Firmware Information Command

2.4. FIPS Approved Mode of Operation

The module provides two API's for entering FIPS mode, `FIPSSystem.getAdminService()` and `FIPSSystem.getUserService()`. When an applet calls one of two API's with correct PIN ADM or USR code, the API returns a Java Object and enters FIPS mode.

The module provides standard Javacard APIs to support FIPS validated applets that work in a FIPS approved mode. Before a FIPS validated applet is activated (Selected), the module successfully completes self-tests during the power-up procedure. Java Applets access services through the FSM platform, by calling `FIPSSystem.getAdminService()` or `FIPSSystem.getUserService()`.

The module also provides two API for FIPS state, `FIPSSystem.get_state()` and `FIPSSystem.get_role()`. An applet should call both API's to retrieve the current FIPS state. If the module state is in error states, these two API will throw exception and interrupt the invoking procedure. Available states of returned values are listed in Table 3.

If the FIPS approved applet has its own application level FSM, it must check the platform level state after it is activated successful by using `FIPSSystem.get_state()`. The applet must validate `FIPSSystem.get_state()` returns normally without any exception and the returned state is not values `STATE_SHUTDOWN`, `STATE_INTEGRITY_BROKEN` or `STATE_SELF_TEST_FAIL`.

Command	Expected Response
FIPSSystem.get_state()	0000 = STATE_UNINITIALIZED 0013 = STATE_ADM_UNINITIALIZED 0073 = STATE_USR_UNINITIALIZED 0119 = STATE_UNAUTHORIZED 37AB = STATE_AUTHORIZED Error States: 819E = STATE_SHUTDOWN 89A5 = STATE_INTEGRITY_BROKEN 99B3 = STATE_SELF_TEST_FAIL
FIPSSystem.get_role()	0000 = none 6000 = Crypto Officer 0300 = ADM 000E = USR

Table 3 - State and Role Defines

2.5. Unauthenticated mode of Operation

The module will stay in an unauthenticated mode after power up or reset. The module can enter an Approved Mode using two methods as described in 2.4. In an unauthenticated mode, FIPS services and FIPS Approved Security functions are not available. A list of services available in the unauthenticated mode can be found in Table 13.

2.6. unauthenticated mode Identification of Approved Mode

Before the operator is authorized by passing authentication of Crypto-Officer, ADMIN or USER, the module is in unauthenticated mode. FIPS API provide `FIPSSystem.get_state()` function to find if current mode is Non-Approved or Approved, if returned value is not `FIPSSystem.STATE_AUTHORIZED`, the current mode will be Unauthenticated mode. The operator can also call `FIPSSystem.get_role()` to check which role is currently activated, if returned value is `FIPSSystem.ROLE_NONE`, the mode is not in FIPS Approved mode.

As description in 2.4, FIPS CSPs and Keys can be referred via Admin Service and User Service, these 2 services can only obtained by input correct Admin password or User PIN. Any unauthorized operator cannot get the service and has no way to access or refer CSP and Key directly or indirectly.

2.7. Security Limitation of Approved and Unauthenticated modes

In an unauthenticated state, the module does not provide access to FIPS services and Keys/CSPs.

The module supports applet download functions, new applets to be downloaded into the module must be validated through the FIPS 140-2 CMVP. Any other applet loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

3. MODULE PORTS AND INTERFACES

The module is considered to be a single chip standalone module designed to meet FIPS 140-2 Level 3 requirements. The module has the following interfaces:

Data Input interface: Data input parameters of API function calls are defined as the data input interface through which data is input to the module.

Data Output Interface: Data output parameters of API function calls are defined as the data output interface through which data is output from the module.

Control input interface: Control input parameters of API function calls that command the module that are input that are used to configure or control the operation of the module.

Status output interface: Status output parameters of API function calls that show the status of the module are status output interfaces.

Power Interface: Describe the power interface.

The below table describes the relationship between the logical and physical interfaces.

Physical Interface	Logical Interface	Applied FIPS 140-2 Interface
VCC PIN	ISO 7816 : Power supply	Power interface (5V/3V/1.8V)
GND PIN	ISO 7816 : Power supply	Power interface (5V/3V/1.8V)
RST PIN	ISO 7816 : Reset	Control input interface
CLK PIN	ISO 7816 : Clock	Control input interface
SIO PIN	ISO 7816 : Input / output	Control input interface Data input interface Data output interface Status output interface
SWP PIN	ETSI 102 613 SWP	Control input interface Data input interface Data output interface Status output interface
O-RST PIN	ISO 7816 : Reset of Reader	Control input reference
O-SIO PIN	ISO 7816 : Input / output of Reader	Data input interface Data output interface

Table 4 – Mapping Physical and Logical Interfaces

4. CRYPTOGRAPHIC KEY MANAGEMENT

Cryptographic key management is a summary of the supported keys within the module and its various characteristics.

4.1. Key Establishment and Entropy

The module provides asymmetric key pair generation methods to generate key. The generated public key can be output in plain text format via FIPS Service API. The module also provides SP 800-108 KDF and a Triple-DES key is generated internally for the TDES-KEK.

Key generation and the seed for asymmetric key generation uses the HASH DRBG. The min-entropy of SP800-90B Entropy Estimation Test is 5.75367per 8-bits which provides 184 bits of strength.

Note: The module generates cryptographic keys whose strengths are modified by available entropy

4.2. Cryptographic Keys and CSPs

The following table summarizes the module's keys and CSP's:

Key/CSP	Description/Usage	Output	Generation /Input
DRBG-SEED	256-bit entropy input from H/W TRNG (NDRNG) to seed the SHA-256 based Hash_DRBG. Stored in RAM.	NO	Internal generated
DRBG-STATE	The current DRBG state include 440-bits V, 440-bits C and other state information used by DRBG. Stored in RAM.	NO	Internal generated
SCP03-MKEY-SET	AES Keys, SCP03 Secure Channel Authentication, input in stage of issuer personalization in the factory. Stored in NVM.	NO	By CO
SCP03-SKEY-*	AES Keys, SCP03 Session Keys. Derived from SCP03-MKEY-SET and session data defined by SCP03, Specification of Globalplatform. Stored in RAM. Session Key Derivation algorithm is NIST SP 800-108	NO	Internal generated
SCP03-CM-SYM	AES Keys, SCP03 Card Management Security Keys, input in stage of issuer personalization in the factory. Stored in NVM.	NO	By CO
SD-CM-ASYM	Card Management Security RSA Keys, 2048 and 3072-bits, initialized in issuer personalization	NO	By CO

	stage. Stored in NVM.		
FIPS-ADM-PIN	Password for ADM verification, initialized by Crypto Officer, in stage of issuer personalization. Stored in NVM.	NO	NOTE1 Initial Value is generated by CO Updated by ADM
ECDH Primitives	The module implements only the ECDH primitive which can be utilized by a Java applet. Subsequent keys are stored and managed by the calling Java applet.	NO	Initial Value is generated by CO/ADM/USER.
FIPS-USER-PIN1	PIN for USER verification, will be initialized by ADM, in stage of personalization of Service Provider. Stored in NVM.	NO	NOTE1 Initial Value is generated by ADM Updated by USER
FIPS-SVC-KEY-SET1	FIPS Service created HMAC keys on demand by USER or ADM, initialized by user or Service Provider. Stored in RAM or NVM according to memory type argument when create the HMAC key.	NO	NOTE1 Initial Value is generated by CO/ADM/USER.
FIPS-KEYPAIRs	ADM and USER generated key pairs, include RSA and ECDSA keys	Public Key	Initial Value is generated by CO/ADM/USER.

NOTE1: As a platform product, the module allows Service Providers to download their applet and work on ADM role or USER role, after the module is issued. The FIPS Services will manage all keys created by USER or ADM. Applet of Service Provider should be validated by FIPS CMVP. Initial value or input of those ADM/USER created keys will be defined and secured by the Service Provider. Service Provider should use FIPS Approved algorithms to keep security of ADM password, USER PIN and KEY input on their user interface devices such as PIN-Pad, PC or Cell-phone.

Table 5 – Cryptographic Module Keys and CSP's in Approved Services

All Keys and CSPs are stored in Triple-DES obfuscated format using the TDES-KEK; however the key derivation scheme used for this purpose is non-compliant (derived by sensitive data storage header and chip serial number). All keys obfuscated by the TDES-KEK are effectively considered to be plaintext under FIPS 140-2, but are obfuscated within the secure confines of the tamper responsive physical boundary. The module's zeroization method destroys all keys in the module when invoked.

Keys and CSPs listed in Table 6 are created and used by FIPS Approved Services. Other FIPS approved Keys such as ECDSA keys will be created by service providers after the module is released to them.

4.3. Key Destruction / Zeroization

DRBG Seed, State and SCP03-SKEY_SET, will be zeroized when the card is powered up or warm-reset. When the secure channel is closed or broken, SCP03-SKEY_SET will be zeroized. When FIPS secure domain is deleted, all Keys, PINs, DRBG data will be destroyed.

The module provides authorized operators on-demand key zeroization methods.

In FIPS Service API, provided API to allow authorized role to destroy or zeroize any Keys of FIPS Service.

```
void clear_key(short key_id, boolean destroy) throws FIPSException
```

```
void clear_keypair(short keypair_id, boolean destroy) throws FIPSException
```

In Crypto Office Guidance, the last command is to destroy all CSPs of FIPS by sending DESTROY FIPS-SD command. Zeroization process clears both key storage area and key state area to zero.

4.4. Key Entry / Output

Except public key of FIPS Service generated key pair, all CSPs and Keys generated or used by FIPS Services, have no API or method to export their values, and cannot output from the module. For key input and output features, please refer to Table 5. All Issuer/CO generated Keys should be personalized in Security Environment of Issuer, such as factory or personalization-bureau. Issuer/CO should personalize their keys in secured form and follow standard of Globalplatform SCP03.

ADM Password/USER PIN updates, key creation and crypto functions used by ADM/USER are functions of Service Provider Applet. Service Provider should keep security between their User Interface Device and the security module. The key-entering security mechanism of Service Provider is out of boundary of the module.

4.5. Approved or Allowed Security Functions

The module keys map to the following algorithms certificates:

Approved or Allowed Security Functions	Certificate
AES, [FIPS 197] Advanced Encryption Standard algorithm. The module supports AES-128, AES-192, AES-256 key, ECB, CBC, CMAC modes.	#5461
AES CMAC [NIST SP 800-38B]. The module supports AES-128, AES-192 and AES-256 key.	#5461
SHA, [FIPS 180-4] Secure Hash Standard compliant one-way algorithms. SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512.	#4369
RSA, [FIPS 186-4] RSA key pair generation for 2048 and 3072 bits keys; RSA signature generation for PKCS1_V1.5, PKCS1_PSS and X9.31 on 2048, 3072 and 4096 bits keys; RSA signature verification for PKCS1_V1.5, PKCS1_PSS and X9.31 on 1024, 2048, 3072 and 4096 bits keys; RSA signature supports SHA1, SHA224, SHA256 and SHA512.	#2933
DRBG, [SP 800-90A] HASH_DRBG SHA 256.	#2134
HMAC, [FIPS 198-1] (w/SHA-1, w/SHA224, w/SHA256, w/SHA384, w/SHA512)	#3619
ECDSA, [FIPS 186-4] Elliptic Curve Digital Signature Algorithm.	#1459

Approved or Allowed Security Functions	Certificate
Signature generation supports P-224, P-256, P-384, P-521 on SHA1, SHA224, SHA256, SHA384 and SHA512. Signature verify supports P192 (Only for Legacy use), P-224, P-256, P-384, P-521 on SHA1, SHA224, SHA256, SHA384 and SHA512. ECDSA Key Generation supports P-224, P-256, P-384, P-521	
CVL (EC-CDH Primitive [SP 800-56A] supports FIPS P-224, P-256, P-384 and P-521)	#1910
CVL (ECC Sig Gen, [FIPS 186-4] Supports P-224, P-256, P-384, P-521)	#1911
CVL (RSADP, [SP800-56B] RSA decryption primitive. Supports 2048 bits key)	#1912
CVL (RSASP1, [FIPS 186-4] [PKCS#1 v2.1] RSA signature generation primitive using 2048-bit keys.)	#1931
AES CMAC based Key Derivation Function [NIST SP 800-108]. Counter mode. The module supports AES-128, AES-192 and AES-256 key.	#223
CKG (NIST SP 800-133)[Note-1]	Vendor Affirmed

Table 6 - FIPS Approved Algorithms

KTS (AES Cert. #5461; key establishment methodology provides between 128 and 256 bits of encryption strength)

Note-1 "In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG."

Non-Approved but allowed Security Function
NDRNG - A minimum of 256-bits of entropy is obtained before generating keys.
Triple DES, (non-compliant, no security claimed) [SP 800-67] Triple Data Encryption Algorithm. The module support 3-key, CBC and ECB mode.

Table 7 – Non-Approved but allowed Algorithms

NOTE-1: The module only uses Triple DES to obfuscate storage of Key and CSPs, and each Key/CSP has their own obfuscation Triple DES key, the obfuscation operation will be done only once, when storing to memory. This is far lower than A.13 requested time limit 2^{28}.

Non-Approved and Non-Allowed Security Function
DES - Industrial standard of GSM defined telecom to protect OTA security SMS. Used by UICC Service.
COMP 128 - Industrial standard of GSM defined telecom authentication algorithm. Used by UICC Service.
MILENAGE - Industrial standard of ETSI defined telecom authentication algorithm. Used by UICC Service.

Table 8 – Non-Approved and Non-Allowed Algorithms Table

5. ROLES, SERVICES AND AUTHENTICATION

The module supports a Crypto Officer, an ADM role and a User role which assumed by authenticated entity. The module implements identity based authentication using a combination of unique user id and password or unique keys. Initial authentication to the module is controlled by a factory set password which the CO uses to authenticate to the module and to configure it.

The module doesn't support a maintenance role.

The module doesn't support multiple concurrent operations for FIPS service.

5.1. FIPS Roles

Crypto Officer	Cryptographic Officer, a role that can manage module configuration and data, include 1. Installing the Demo Applet. 2. Re-installing and removing the Demo Applet. 3. Initial default ADM PIN. 4. Key management and algorithm calculation
ADM	An administrator, a user who can manage application-related content include 1. Change ADM PIN. 2. Initial / re-initial USER PIN. 3. Initial / re-initial USER data. 4. Key management and algorithm calculation
USER	The card holder, a user who can 1. Change USER PIN. 2. Access USER data. 3. Key management and algorithm calculation

Table 9 – FIPS API defines Roles

5.2. Identification and Authentication

The module supports Identity Based authentication.

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity Based	128-256 bits AES Key
ADM	Identity Based	8-16 characters password
USER	Identity Based	8-16 characters password

Table 10 - Authentication Type Table

5.3. Strength of Authentication

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

Role	Authentication Data	Strength of Mechanism
Crypto Officer	128-256 bits AES Keys	Crypto-Officers must authenticate using 2 AES 128 keys via SCP03 Secure Channel initialization defined in GlobalPlatform Specification. An attacker would have a 1 in 2^{128} chance of randomly obtaining the key, which is much stronger than the one (1) in 1,000,000 chance required by FIPS 140-2. 48 times of authentication failures is limited to avoid guessing of a Key. The probability of a success with multiple consecutive attempts in a one-minute period is $48/(2^{128})$, which is less than 1/100,000.
ADM and USER	8-16 Character alpha/numeric password	Users must authenticate using a password that is at least 8 characters and at most 16 characters in length. The characters used in the password must be from the ASCII character set of alphanumeric and special (shift number) characters. the probability of randomly guessing the correct sequence is one (1) in 6,095,689,385,410,816. This is calculated by performing 94^8. The possibility of correctly guessing a password is greater than 1 in 1,000,000. . In order to successfully guess the sequence in one minute would require the ability to make over 101,594,823,090,180 guesses per second, which far exceeds the operational capabilities of the module.

Table 11 - Authentication Type Table

5.4. Roles and Services

The module supports the services listed in the following table.

Service	Description
Context	Select an applet or manage channel
Module Reset	Power cycle, reset the module, including Power-On-Self-Test
Module Info	Get module production information
UICC Service	Perform telecom UICC functions
SIMoME Service	Perform film card functions
FIPS System Get State	This function is used to find if current mode is Non-Approved or Approved, if returned value is not FIPSSystem.STATE_AUTHORIZED, the current mode will be Unauthenticated mode.
FIPS System Get Role	The function is used to check which role is currently activated, if returned value is `FIPSSystem.ROLE_NONE`, the mode is not in FIPS Approved mode.

Table 12 - Unauthenticated Services

Context Service

Following the Javacard Specification, Context Service accept two input APDU commands from the communication port, SELECT and MANAGE CHANEL, according to these two command, switch context and setup related status of Javacard VM and Javacard Runtime Environment. Context service does not access FIPS Service data or function.

Module Reset Service

Module Reset Service is a low level system service. Following Javacard Specification, when the card if powered on or RESET signal is received, the chip hardware triggers a reset interrupt and Module Reset Service is activated. The service is in charge of clear RAM to zero, abort incomplete transactions, setup initial value of the card system and call power-on self-test.

Module Info Service

Module Info Service accept one input APDU command, GET CARD INFO, the service output card production information, such as product ID, manufactory ID, version information, ISO-14443 UID. The service does not access FIPS Service data or functions.

UICC Service

Following GSM and ETSI specifications, UICC Service accept all APDU commands from the mobile phone, and in charge of UICC file access, CHV management, GSM/USIM authentication with mobile base station, trigger STK Menu and Events, perform remote file management and remote application management. UICC Service does not access FIPS Service data or functions.

SIMoME Service

SIMoME Service is an application level service, it provides multiple SIM function, allow the module work on different SIM mode King or Queen. SIMoME Service is active by the Phone Menu Selection event triggered by UICC Service and send proactive commands to the phone, the phone show next level function menu, and send the menu item selection information back to UICC Service by another APDU command. UICC Service send selected item id to SIMoME Service, and SIMoME Service switch the mode according to the item id. SIMoME Service does not access FIPS Service data or function.

Service	Description	CO	ADM	USER
Life Cycle	Manage card and applet life cycle. NOTE 1.	Y		
Card Manager	Load. Install and Delete card content including package, applet, key and data. NOTE 1, 3.	Y		
Secure Channel	Create Secured Channel and keep secured communication. NOTE 1	Y		
FIPS CO Service	Create ADM role and password, destroy FIPS CSP and data, key management and algorithm calculation. NOTE 2.	Y		
FIPS ADM Service	Create USER role, key management and algorithm calculation. NOTE 2.		Y	
FIPS USER Service	Key management and algorithm calculation. NOTE 2.			Y

Table 13 - Authenticated Services

NOTE 1. Services are available only when CO role is authenticated, services are function groups defined in Globalplatform Specifications. Globalplatform SCP03 defined authentication methods are used as CO authentication.

NOTE 2. FIPS Service only manage keys that used by FIPS Services themselves.

NOTE 3. Card Manger only manage keys that used by card management, keys and algorithms are defined in Globalplatform Specifications.

The table groups the authorized services by the operator roles and identifies the Cryptographic Keys and CSPs associated with the services. The modes of access are also identified per the explanation.

- **G** - The item is **Generate** CSP by the service.
- **Z** - The item is **Zeroize** or referenced by the service.
- **W** - The item is **written** or updated by the service.
- **R** - The item is **public key and read** by the service.
- **E** - The item is **executed** by the service. (The item is used as part of a cryptographic function.)
- **–** - The item is **NOT Accessed** by the service.

The below table shows the services available to each role and the keys and CSP's associated with each Role:

Service	DRBG-SEED	DRBG-STATE	SCP03-MKEY-SET	SCP03-SKEY-*	SCP03-CM-SYM	SD-CM-ASYM	FIPS-ADM-PIN	FIPS-USER-PIN	FIPS-SVC-KEY-SET	FIPS-KEYPAIRs	ECDH primitive
Context	–	–	–	Z	–	–	–	–	–	–	-
Module Reset	GEW Z	GEW	–	Z	–	–	–	–	–	–	-
Module Info	–	–	–	–	–	–	–	–	–	–	-
UICC Service	–	–	–	–	–	–	–	–	–	–	-
SIMoME Service	–	–	–	–	–	–	–	–	–	–	-
Life Cycle	–	Z	Z	E	Z	Z	Z	Z	Z	Z	Z
Card Management	–	–	W	E	W	W	–	–	–	–	–
Secure Channel	–	EW	E	GE	E	E	–	–	–	–	
FIPS CO Service	–	EW	–	–	–	–	GW	–	–	–	GEZ
FIPS ADM Service	–	EW	–	–	–	–	EW	GW	GEW	GW Z, R	GEZ
FIPS USER Service	–	EW	–	–	–	–	–	EW	GEW	GW Z, R	GEZ

Table 14 - Mapping of Cryptographic Keys and CSPs to Services

PHYSICAL SECURITY

The module is defined as a single chip standalone module. The module consists of production grade components which include standard passivation techniques.

The module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability and shock/vibrations.

The module is intended to be mounted in SIM, SIMoMe or ECoffer chip.

The chip is protected by a hard epoxy coating and active tamper envelope shield. If an attacker attempts to penetrate and the module detects, the module deactivates this chip. The module is not recoverable from this state. The module hardness testing was only performed at a single temperature and no assurance is provided for Level 3 hardness conformance at any other temperature." The hardness testing was performed at an ambient temperature of 72 degrees F.

Temperature: The normal operating temperature range of the security module is -25°C to +85°C.
Voltage: The normal operating voltage range of the security module is -0.3V to 6.5V.

6. OPERATIONAL ENVIRONMENT

Not Applicable

7. SELF-TEST

The module performs power-up self-tests and conditional self-tests. Power-up Self-Test will execute automatically upon issuance of a command to the module. If the power-up self-tests pass, the command will be processed normally, if the power-up self-tests fail, the module will shut down without completing the instruction. At this point, the connection with reader will be broken.

7.1. Power-up Self-Tests

Cryptographic Algorithm KATs:

Known Answer Tests (KATs) are run at FIPS Service start-up for:

- Triple DES (3-Key CBC mode for Encrypt/Decrypt) KAT
- AES (256-bits CBC mode for Encrypt/Decrypt) KAT
- RSA (2048-bits Decryption) KAT
- RSA (2048-bits SHA-256 PKCS-1 Sign/Verify) KAT
- ECDSA (FP-224 SHA256 Sign/Verify) KAT
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- HMAC SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 KAT
- DRBG (HASH DRBG, SHA256) KAT
- Diffie-Hellman ECCDH Primitive Z (FP-224) KAT

Firmware Integrity Tests:

The module performs Firmware Integrity Test using 32-bit CRC over all executable code in Flash. An operator can reset or power-cycle the module to perform on demand self-tests. The module performs the firmware integrity test and all self-tests prior to entering FIPS mode of operation.

7.2. Conditional Self-Tests

The module performs the following conditional self-tests:

Conditional RNG Test:

A conditional test is performed for the Approved DRBG and NDRNG implemented within the module.
If random data generated is the same as the previous one, the FIPS service will force a shutdown of the module.

Load Integrity Test:

A package integrity test is performed during load sequence of package. By following the Globalplatform specification, a RSA-2048 based Signature and a DAP of the downloaded package must be sent into the module with the package itself. Signature is RSA-2048 with SHA-256 or SHA-1 of the whole package data, DAP is SHA-1 or

SHA-256 hash of the whole package data. Both signature and DAP are verified by the module, if DAP is not same with the hash of package, or Signature verification is failed, the module will terminate the load sequence and restore the module to the condition before the download.

Pairwise Consistency Test:

Pairwise consistency tests are run when the module generates key pairs. The module performs a sign operation with the private key and verifies it with the public key. Pairwise consistency tests will be performed in both RSA and ECDSA key pair generation.

Critical Self-Test:

DRBG health tests will be performed during DRBG functions DRBG_Instantiate, DRBG_Reseed and DRBG_Generate, any error detected such as invalid state and continuous check failure, the module will get into Shut-Down mode. The module also implements a repetitive failure test and an adaptive proportion test as per SP800-90B.

8. Crypto-Officer and User Guidance

This section shall describe the configuration and administration of the cryptographic module.

8.1. Secure Setup and Initialization

This section shall describe the procedures necessary for the setup and initialization of the module to place the module in a FIPS Approved Mode of operation.

For Crypto Officer:

1. Install FIPS-SD
2. Install service provider Applet
3. Initial ADM PIN

3.1. Select FIPS-SD

3.2. Create Secure Channel for FIPS-SD

3.3. Send INIT-ADM-PIN APDU command with ADM PIN

8.2. Module Security Policy Rules

This section shall describe the rules for which the module must operate in for it to be operating in FIPS Approved Mode of operation.

- No additional interface or service is implemented by the module which would provide access to CSPs.
- Data output is inhibited during generation, self-tests, zeroization and error states.
- Status information does not contain CSPs or sensitive data if misused could lead to compromise of the module.
- The module does not support manual key entry, output plaintext CSPs, or output intermediate key values.

9. Mitigation of Other Attacks

The module implements defenses against:

- Light attacks, the module hardware has Laser Detect Sensor, if the sensor detect laser attack, module hardware will reboot.

- Invasive attacks, the module hardware has memory scrambling, bus encryption and glue logic layout mechanism to protect the chip from invasive attacks.

- Side-channel attacks (SPA/DPA), the module hardware provides desynchronization and confusing mechanism to protect security calculation against SPA and DPA attacks.

- Timing analysis, the module hardware provides data content and key independence crypto engine, to avoid timing analysis attack on the algorithm calculations.

- Differential fault analysis (DFA), the module used hardware provided SBOX mechanism and reverse calculation to validate the result for DES/AES, any fault found, the module will shut down.

- Electromagnetic attacks, the module hardware provides SBOX mechanism to protect security calculation against DEMA attacks.

Abbreviations

Term	Meaning
SIMoME™	Is an ultra-slim SIM card designed to work together with a second SIM sized card into the existing SIM slot of the mobile device.
GP	Global Platform
UICC	universal integrated circuit card
ISD	Issuer Security Domain
FIPS SD	FIPS SD is a Java Applet used for testing module functionality
FIPS LIB	FIPS LIB is a Java Applet used for testing the module
COS Library	Common OS Library
NESlib	Next Step Library, provides access to cryptographic hardware