Chunghwa Mobile ID Applet on

Taisys Technologies JUISE-S2

Firmware Versions: 32 53; Applet: Chunghwa Mobile ID Applet v1.0

Hardware Version 46 43

FIPS 140-2 Cryptographic Module

Non-Proprietary Security Policy

Version 1.0

September 11, 2019

References

Reference	Full Specification Name
[ISO 7816]	ISO/IEC 7816-1: 2011 Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics ISO/IEC 7816-2:2007 Identification cards - Integrated circuit cards - Part 2: Cards with contacts - Dimensions and location of the contacts ISO/IEC 7816-3:2006 Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols ISO/IEC 7816-4:2013 Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange ISO/IEC 7816-8:2004 Identification cards - Integrated circuit cards - Part 8: Commands for security operations
[JavaCard]	Java Card 3.0.4 Classic - Runtime Environment (JCRE) Specifications Java Card 3.0.4Classic - Virtual Machine (JCVM) Specifications Java Card 3.0.4 Classic - Application Programming Interface (API) Published by ORACLE , September 2011
[GlobalPlatform]	GlobalPlatform Card Specification 2.2.1 - January 2011, GlobalPlatform Card Specification – Amendment E – Security Upgrade for card content management – Public Release November 2011 v1.0 GlobalPlatform Card Basic ID Configuration - Version 1.0 - December 2011 GlobalPlatform Card Technology Card Specification – ISO Framework Version 0.9.0.18 Public Review July 2013 GlobalPlatform Consortium: http://www.globalplatform.org
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002
[ANS X9.31]	American Bankers Association, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998 - Appendix A.2.4.
[FIPS140-2]	NIST, Security Requirements for Cryptographic Modules, May 25, 2001
[IG]	NIST, Implementation Guidance for FIPS PUB 140 - 2 and the Cryptographic Module Validation Program, last updated 07 August 2017.
[FIPS113]	NIST, Computer Data Authentication, FIPS Publication 113, 30 May 1985.
[FIPS197]	NIST, Advanced Encryption Standard (AES), FIPS Publication 197, November 26, 2001.
[FIPS 186-4]	NIST, Digital Signature Standard (DSS), FIPS Publication 186-4, July, 2013
[FIPS 180-4]	NIST, Secure Hash Standard, FIPS Publication 180-4, March 2012
[SP800-38F]	NIST, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012
[SP 800-56A]	NIST Special Publication 800-56A, Recommendation for Pair - Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007
[SP 800-67]	NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, version 1.2, July 2011
[SP800-108]	NIST, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011

Table 1 – References

Acronyms and definitions

Acronym	Definition
AIS 31	A German acronym referring to standard for functionality and evaluation of random number generation
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CHT	Chungwa Telecom
CHV	Card Holder Verification
CM	Card Manager, see [GlobalPlatform]
COS Library	Common OS Library
CRT	Chinese Remainder Theorem
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	Global Platform
GSM	Global System for Mobile communications
HE	Home Environment
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
NESlib	Next Step Library, provides access to cryptographic hardware
NVM	Non-Volatile Memory (e.g. EEPROM, Flash)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SIMoME™	An ultra-slim SIM card designed to work together with a second SIM sized card into the existing SIM slot of the mobile device.
STD	Standard, as in Standard (non-CRT) RSA
SPA	Simple Power Analysis
UICC	universal integrated circuit card

Table 2 – Acronyms and Definitions

1. Introduction

This document defines the Security Policy for the Chunghwa Telecom Co., Ltd. Chunghwa Mobile ID Applet on Taisys Technologies JUISE-S2 v1.0 contact/contactless cryptographic module. The module, is a single chip secure controller module validated to FIPS 140-2 Overall Security Level 3, is the combination of the Chunghwa Mobile ID Applet (denoted **Mobile ID Applet** below) running on and bound to the Taisys Technologies JUISE-S2 platform, Cert. #3441 module (denoted **platform** below).

The Module is bound to the Cert. # xxxx Taisys JUISE-S2 module, which provides a Global Platform Java Card operational environment. The platform provides an operational environment for the **Mobile ID Applet**: all cryptographic algorithm implementations and associated self-tests, random number and key generation, card lifecycle management, and key storage and protection are provided by platform. Unusable functionality is not discussed further in this document.

The **Mobile ID Applet** is a Javacard applet that provides security for stored user data and credentials for Mobile ID services (e.g. for strong authentication, encryption and digital signatures).

The FIPS 140-2 security levels for the module are as follows:

Security Requirement	*Security Level*
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State 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

Table 3 – Security Level of Requirements

1.1 Versions, Configurations and Modes of operation

Hardware: 46 43.
Firmware: 32 53
Applets: CHT Mobile ID Applet V1.0

The module will be embedded into three kinds of form:

- Smart Card
- SIMoME Card
- ECoffer chip

There is only one firmware version. An operator can send the following command for the **platform** 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 4 – Get Firmware information Command

The **Mobile ID Applet** uses the standard Javacard APIs work on the Taisys JUISE-S2 module FIPS approved mode. The associated FIPS 140-2 Level 3 Taisys JUISE-S2 module is configured at factory to operate exclusively in Approved mode when providing access to FIPS Approved algorithms and services for the Chunghwa Mobile ID Applet. The explicit indicator of the Approved mode of operation is obtained by using the ***Context*** service to select the **Mobile ID Applet** and using the ***Mobile ID Applet Info(Unauthenticated)*** service (GET DATA APDU, tag '0105'), which is expected to return '03030601'.

1.2 Hardware and Physical Cryptographic Boundary

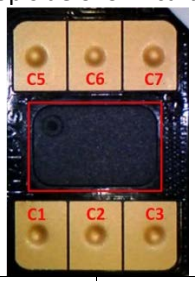
The cryptographic module boundary is realized as the external surface of the ST33G1M2 single chip microprocessor and does not include smart card contact plate in contact, the antenna for contactless, the fixation glue. The boundary contains all of the relevant module components (processors performing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

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:

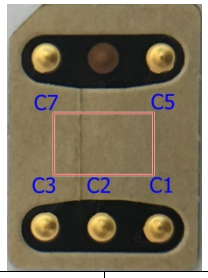
Smart Card and SIMoME Card form:

Up side of SIM card



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

SIMoME Card

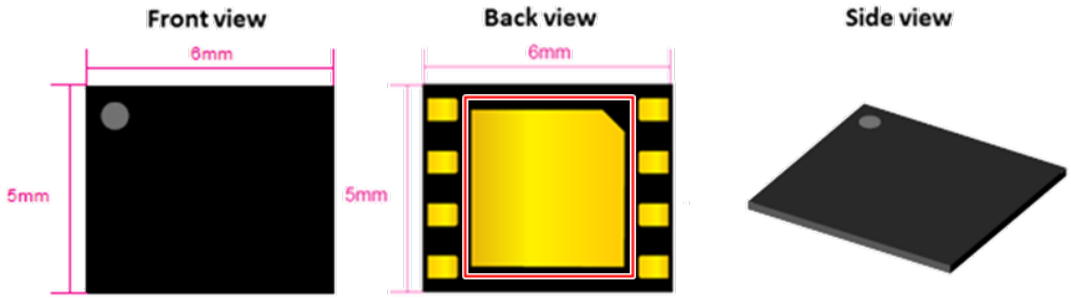


C1	VCC	C5	GND
C2	Q-RST		
C3	CLK	C7	Q-SIO

(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.

1.3 Firmware and Logical Cryptographic Boundary

Figure 1 depicts the module architecture. The red outline depicts the logical cryptographic boundary.

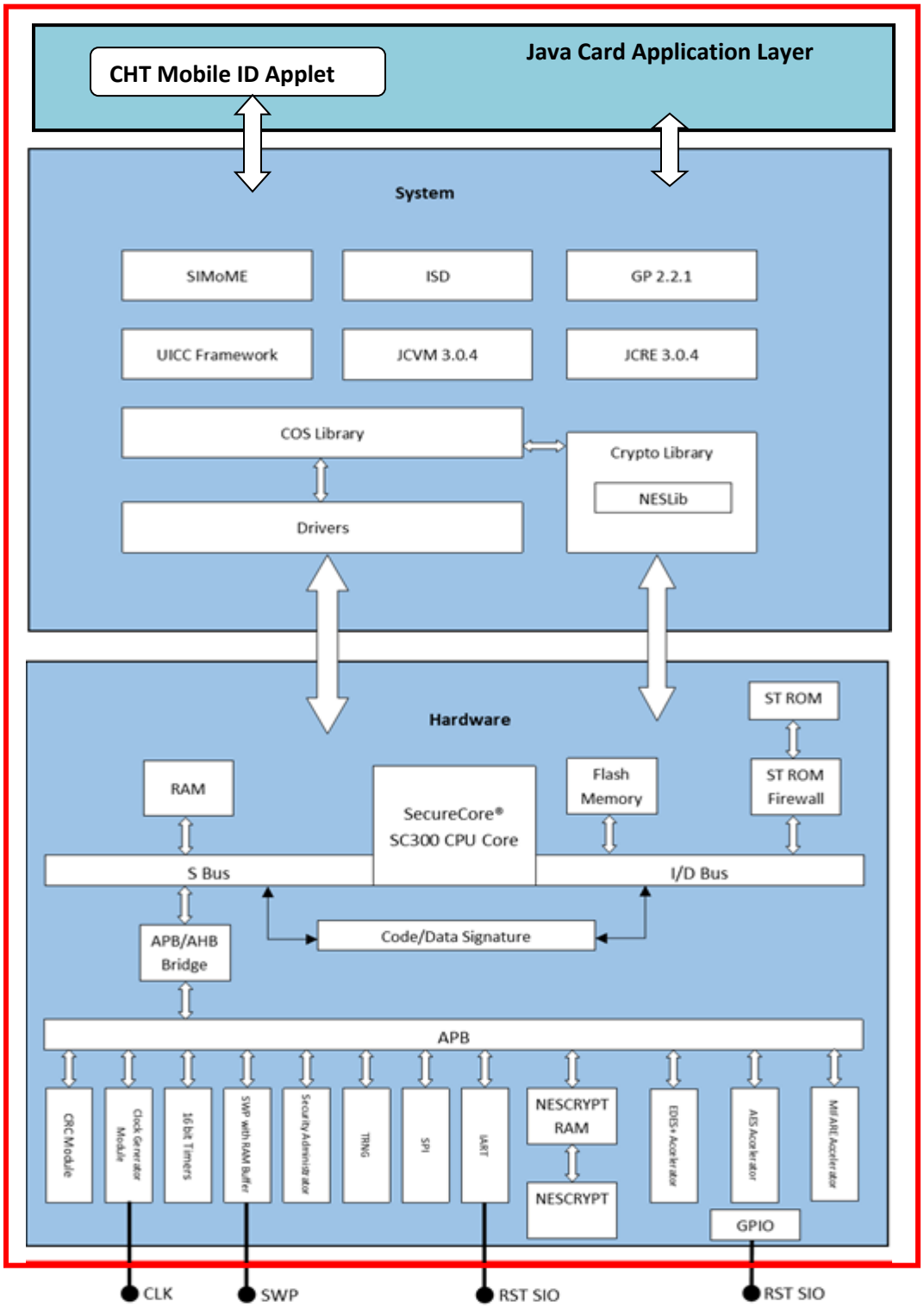


Figure 1 - Module Block Diagram
(Cryptographic Boundary Outlined in Red)

Section 4 describes applet functionality in greater detail. The Java Card and Global Platform APIs are internal interfaces available only to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

2. 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
Q-RST PIN	ISO 7816 : Reset of Reader	Control input interface
Q-SIO PIN	ISO 7816 : Input / output of Reader	Data input interface Data output interface

Table 5 – Mapping Physical and Logical Interfaces

3. Cryptographic Functionality

The module implements the Approved and Non-Approved but Allowed cryptographic functions implemented by Cert. #3441 module and listed in Table 6 and Table 7 below:

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 and 3072 bits keys; RSA signature verification for PKCS1_V1.5, PKCS1_PSS and X9.31 on 1024, 2048, and 3072 bits keys; RSA signature supports SHA1, SHA224, SHA256 and SHA512.	#2933
DRBG, [SP 800-90A] HASH_DRBG SHA 256.	#2134
ECDSA, [FIPS 186-4] Elliptic Curve Digital Signature Algorithm. ECDSA Key Generation supports P-256, P-384, P-521 Signature generation supports P-256, P-384, P-521 on SHA1, SHA224, SHA256, SHA384 and SHA512. Signature verify supports P-256, P-384, P-521 on SHA1, SHA224, SHA256, SHA384 and SHA512.	#1459
CVL (EC-CDH Primitive [SP 800-56A] supports FIPS P-256, P-384 and P-521)	#1910
CVL (ECC Sig Gen, [FIPS 186-4] Supports 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
KTS (AES) key establishment methodology provides between 128 and 256 bits of encryption strength).	#5461
CKG (NIST SP 800-133) Note-1	Vendor Affirmed

Table 6 – FIPS Approved Algorithms

Note-1: The CAVP certificates associated with Cert. #3441 module include other algorithms, modes, and curves or key sizes that have been CAVP validated but are not available in this module. Only the algorithms, modes, and curves or key sizes shown in Table 6 are available in this module.

Note-2: "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 - 256-bits of seed data is obtained before generated 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 Cryptographic Functions

NOTE-1: The module only uses Triple DES to obfuscate Keys and CSPs, and each Key/CSP has their own Triple DES key, the obfuscation operation will be done only once, when storing to memory.

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 Security Function

3.1 Critical Security Parameters

All CSPs used by the module are described in this section.

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.

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.

In the tables below, the **PKI** prefix denotes a Mobile ID Application CSP.

CSP	Type	Length(bits) Or Curve	Description / Usage
DRBG-SEED		256	256-bit entropy input from H/W TRNG (NDRNG) to seed the SHA-256 based Hash_DRBG. Stored in RAM.
DRBG-STATE		440	The current DRBG state include 440-bits V, 440-bits C and other state information used by DRBG. Stored in RAM.
SCP03-MKEY-SET	AES	128,192,256	AES Keys, SCP03 Secure Channel Authentication, input in stage of issuer personalization in the factory. Stored in NVM. **SD-KENC**, Master key for SD-SENC generation

			SD-KMAC, Master key for SD-SMAC generation **SD-KDEK**, Sensitive data decryption
SCP03-SKEY-*	AES	128,192,256	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 **SD-SENC**, Session encryption key to encrypt / decrypt secure channel data. **SD-SMAC**, Session MAC key to verify inbound secure channel data integrity.
SCP03-CM-SYM	AES	128,192,256	AES Keys, SCP03 Card Management Security Keys, input in stage of issuer personalization in the factory. Stored in NVM.
SD-CM-ASYM	RSA	2048, 3072	Card Management Security RSA Keys, 2048 and 3072 bits, initialized in issuer personalization stage. Stored in NVM.

Table 9 – Platform Critical Security Parameters

CSP	Type	Length(bits) Or Curve	Description / Usage
PKI-KXAUTH	AES,	128, 192, 256	Mobile ID applet External Authentication key.
PKI-KRSA-PRI	RSA	2048	Mobile ID applet signature generation private keys.
PKI-KECC-PRI	ECC	P-256, P-384, P-521	EC Curves private keys used for signature generation.
PKI-AUTH	Secret	10 bytes	Two instances: Card holder PIN verification; PIN unblocking.

Table 10 – Mobile ID Applet Critical Security Parameters

The Taisys JUISE-S2 module provides all of the tested algorithms, the CSP tables only lists the algorithms and sizes supported by the Mobile ID App.

3.2 Public Keys

CSP	Type	Length(bits) Or Curve	Description / Usage
DAP-Pub	RSA	2048	Firmware load test signature verification key.
PKI-KRSA-PUB	RSA	2048	Public keys held in the module for retrieval by external users through the Mobile ID applet.
PKI-KECC-PUB	ECC	P-256, P-384, P-521	Public keys held in the module for retrieval by external users through the Mobile ID applet.

Table 11 – Public Keys

All algorithms are implemented by the bound module, the Chunghwa applet does not provide any additional algorithms beyond what is available in the Taisys module

4. Roles, Authentication and Services

The module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.

- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

Authentication of each operator and their access to roles and services is as described below. Only one operator at a time is permitted on a channel. Applet de-selection (including ISD/Card Manager), card reset or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services. Authentication data is encrypted during entry (by SD-KDEK), and is only accessible by authenticated services.

Table 11 lists all operator roles supported by the module.

Role ID	Role Description
CO	Cryptographic Officer - role that manages module configuration, including issuance and management of module data via the ISD. Authenticated as described in GP Secure Channel Protocol Authentication below.
AA	Application Administrator - a role that manages Mobile ID application-related content and configuration. Authenticated using the GP Secure Channel Protocol Authentication method or Mobile ID Applet Symmetric Key Authentication method.
User	Card Holder – The human user of the module, authenticated by Mobile ID Applet Secret Value authentication with Mobile ID applet selected

Table 12 – Roles Supported by the Module

4.1 GP Secure Channel Protocol Authentication Method

The GP Secure Channel Protocol provides confidentiality, integrity and mutual authentication. The module supports this mechanism in two services: the ***GP Secure Channel*** service and the ***Mobile ID Applet Secure channel*** service. These services each invoke the same underlying library calls, but from the Card Manager and PKI Applet, respectively.

The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The SD-SENC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the module in the CO role).

The probability that a random attempt will succeed using this authentication method is:

 1/(2^128) = 2.9E-39 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

The module enforces a maximum of 80 failed SCP authentication attempts. The probability that a

random attempt will succeed over a one minute interval is:

 80/(2^128) = 2.4E-37 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

4.2 Mobile ID Applet Symmetric Key Authentication Method

The external entity obtains a 16-byte challenge from Mobile ID applet, encrypts the challenge and sends the cryptogram to Mobile ID applet, along with a key ID. PKI applet decrypts the cryptogram, and the external entity is authenticated if the decrypted value matches the challenge.
The strength of authentication using this method is dependent on the key size used, the minimum is 128 bits:
The probability that a random attempt will succeed using this authentication method is:

 1/(2^128)= 3.4E-38

Based on the module's maximum communication rate and the sizes of command and response APDU, the maximum number of authentication attempts is 1.2E5 attempts per minute. The probability that a random

attempt will succeed over a one minute interval is:
1.2E5/(2^128) = 3.5E-34

4.3 Mobile ID Applet Secret Value Authentication Method

The external entity submits an identifier and corresponding secret value. The module enforces a minimum length of 6 characters, with the character space of all printable characters (95 possible characters).

The probability that a random attempt will succeed using this authentication method is:

 1/(95^6) = 1.4E-12

Based on the module's maximum communication rate and the sizes of command and response APDU, the maximum number of authentication attempts is 3.6E-5 attempts per minute. The probability that a random attempt will succeed over a one minute interval is:

 3.6E5/(95^6) = 4.9E-7

4.4 Services

All services implemented by the module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Service	Description
Context	Select an application or manage logical channels.
Module Reset	Power cycle or reset the module. Includes Power-On Self-Test.
Module Info	Get module production information
UICC Service	Perform telecom UICC functions
SIMoME Service	Perform film card functions
Mobile ID Applet Info	Read unprivileged Mobile ID applet data objects.

Table 13 – 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	AA	User
Platform				
Lifecycle	Manage card and applet life cycle. NOTE 1.	X		
Card Manager	Load. Install and Delete card content including package, applet, key and data. NOTE 1, 2.	X		
GP Secure Channel	Create Secured Channel and keep secured communication. NOTE 1	X		
Mobile ID Applet				
Mobile ID Applet Info	Read unprivileged Mobile ID applet data objects.		X	X
Mobile ID Applet Secure channel	Establish and use Mobile ID Applet secure communications channel.		X	X
Mobile ID Applet preparation	Manage Mobile ID applet authentication data and PKI Applet lifecycle		X	
Generate asymmetric key pair	Generate an RSA or EC key pair and set key identifiers associated with User.		X	
Entity authentication with symmetric key	Authentication of AA role to the module.		X	
Unblock PIN	Mechanism to reset the retry counter when the PIN / authentication Key are blocked after too many failed verifies attempts.		X	
Key Management	Update Mobile ID applet keys.		X	
Entity authentication with password	Authenticate User role to the module (PIN verification).			X
Change PIN	It is used to change the PIN			X
Digital Signature	Sign provided data with the specified key			X
Generate shared secret	Generate the shared secret by using the specified private key and the external participant's public key.			X
Get public key	Retrieve the specified public key			X
Applet Content Manage	Read or update binary data (non-sensitivity data) stored in the Mobile ID applet		X	X

Table 14 – 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. Card Manger only manage keys that used by card management, keys and algorithms are defined in Globalplatform Specifications.

The below table shows the services available to each role and the keys and CSP's associated with each Role, it is organized to correspond to the set of unauthenticated services, then authenticated services.

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP (read access to the CSP by an outside entity).
- E = Execute: The module executes using the CSP.
- W = Write: The CSP is imported into the module.
- Z = Zeroize: The module zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure)
- - - = Not accessed by the service.

Service	***C S Ps and public keys***															
	Platfrom CSPs	DRBG-SEED	DRBG-STATE	SCP03-MKEY-SET	SCP03-SKEY-*	SCP03-CM-SYM	SD-CM-ASYM	TDES-KEK	***Mobile ID Applet CSPs***	PKI-KXAUTH	PKI-KRSA-PRI	PKI-KECC-PRI	PKI-AUTH	***Public Keys***	DAP-Pub	PKI-KRSA-PUB	PKI-KECC-PUB
Unauthenticated Services																	
Context		--	--	--	Z	--	--			--	--	--	--		--	--	--
Module Reset		GEZ	GE WZ	--	Z	--	--	Z		--	--	--	--		--	--	--
Module Info		--	--	--	--	--	--	--		--	--	--	--		--	--	--
UICC Service		--	--	--	--	--	--	--		--	--	--	--		--	--	--
SIMoMe Service		--	--	--	--	--	--	--		--	--	--	--		--	--	--
Platform Services																	
Life Cycle		--	Z	Z	E	Z	Z	--		Z	Z	Z	Z		Z	Z	Z
Card Manager		--	--	W	E	W	W	GEZ		--	--	--	--		WE	--	--
Secure Channel			EW	E	GE	E	E	GEZ		--	--	--	--		--	--	--
Mobile ID Applet Services																	
Mobile ID Applet Info		--	--	--	--	--	--	--		--	--	--	--		--	--	--
Mobile ID Applet Secure channel		--	EW	--	GE	--	--	--		--	--	--	--		--	--	--
Mobile ID Applet preparation		--	--	--	E	--	--	--		W	--	--	W		--	--	--
Entity authentication with symmetric key		--	--	--	E	--	--	--		E	--	--	--		--	--	--
Entity authentication with		--	--	--	E	--	--	--		--	--	--	E		--	--	--

password																	
Change PIN		--	--	--	E	--	--	--		--	--	--	W		--	--	--
Unblock PIN		--	--	--	E	--	--	--		--	--	--	W		--	--	--
Generate asymmetric key pair		--	--	--	E	--	G	--		--	G	G	--		--	--	--
Digital Signature		--	--	--	E	--	--	--		--	E	E	--		--	--	--
Generate shared secret		--	--	--	E	--	--	--		--	--	E	--		--	--	--
Get public key		--	--	--	E	--	--	--		--	--	--	--		--	R	R
Key Management		--	--	--	E	--	--	--		W	W	--	--		--	W	W
Applet Content Manage		--	--	--	E	--	--	--		--	--	--	--		--	--	--

Table 15 – Access to CSPs by Service

Below are brief descriptions to help readers understand Table 15 Explanations are provided in groups of services and/or keys (as best suited to explain the pattern of access), describing first those aspects that have commonality across services or keys/CSPs.

Lifecycle: must be used with Secure Channel active (hence SD Session keys are 'E'); zeroizes all keys except session keys when *Lifecycle* is used for card termination.

OS-DRBG CSPs: OS-DRBG-SEED is the NDRNG entropy input to the DRBG instantiation *block_cipher_df* at power-on (*Module Reset*), zeroized after use. OS-DRBG-STATE is generated at startup (*Module Reset*), zeroized at shutdown as part of *Module Reset*, or by *LifeCycle* card termination. Each 'EW' in the OS-DRBG-STATE column indicates the use of the DRBG to generate keys, as the value is used and the state is updated.

Secure Channel Master Keys (SCP03-MKEY-SET): 'E' when a secure channel is initialized (*GP Secure Channel*, Mobile ID *Applet Secure Channel channel*). May be updated ('W') using the *Card Manage* service; zeroized by *Lifecycle* card termination

Secure Channel Session Keys (SCP03-SKEY-*): 'E' for any service that can be used with secure channel active. 'GE' on *GP Secure Channel*, Mobile ID *Applet Secure Channel* as a consequence of secure channel initialization and usage; 'Z' on *Module Reset* as a consequence of RAM clearing/garbage collection.

Entity authentication services: PKI-KXAUTH, PKI-AUTH enters the module via Mobile ID *Applet preparation.* PKI-AUTH is used ('E') by *Entity Authentication with Password* and may be updated by *Change PIN* or *Unblock PIN* ('W'). Entity authentication with symmetric key uses PKI-KXAUTH for external authentication.

Digital Signature: uses PKI-KRSA-PRI/PKI-KRSA-PUB or PKI-KECC-PRI/PKI-KECC-PUB for digital signature ('E').

Generate shared secret: uses PKI-KECC-PRI for Generate the shared secret ('E').

5. Self – tests

The module performs power-up self-tests and conditional self-tests. Power-up Self-Test will be performed automatically after the first command comes into the card, if pass power-up self-tests, the command will be processed normally, if power-up self-tests fail, the module will get into shut down mode and no any response comes out, the connection with reader will be broken.

5.1 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 the module or power off the module and on again to perform Firmware Integrity Test. And then enter FIPS mode to perform self-tests.

5.2 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: Test:

A package integrity test is performed during load sequence of package. By following the Global platform 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

6. Physical Security Policy

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 a plastic smartcard, a slim card 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.

7. Operational Environment

The module is designated as a limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

8. Mitigation of Other Attacks Policy

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 have 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 provide SBOX mechanism to protect security calculation against DEMA attacks.

9. Security Rules and Guidance

The module implementation also enforces the following security rules:

- No additional interface or service is implemented by the module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- DRBG Seed, State and SCP03-SKEY_SET, will be zeroized when card reset. When 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 does not support manual key entry, output plaintext CSPs or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.