FTDN-080008

FEITIAN
WE BUILD SECURITY

FT-JCOS (Feitian Java Card Platform)
FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Version: 1.0.7

Revision Date: Sep. 9, 2015

Feitian Technologies Co., Ltd

CHANGE RECORD

Revision	Date	Author	Description of Change
1.0.0	Dec. 30, 2012	Jeff Zhang	Initial Draft
1.0.1	Jan. 8, 2013	Jeff Zhang	Modify description of CSPs and Services
1.0.2	Apr. 24, 2013	ZhanQiang Gao	Add description of the Demonstation Applet
1.0.3	Apr. 17, 2014	ZhanQiang Gao	Modify description about self-test,authentication and Demonstration services
1.0.4	Aug. 5, 2014	ZhanQiang Gao	Use RSA 2048-bit key for the KAT
1.0.5	Nov. 25, 2014	ZhanQiang Gao	Change module name
1.0.6	Apr. 9, 2015	ZhanQiang Gao	Changes per CMVP comments
1.0.7	Sep. 9, 2015	ZhanQiang Gao	Remove description about AES MAC

Contents

1 Introduction **6**
1.1 Hardware and Physical Cryptographic Boundary . . . 7
1.2 Firmware and Logical Cryptographic Boundary . . . 8
1.3 Versions and Mode of Operation . . . 10

2 Cryptographic Functionality **11**
2.1 Cryptographic functions . . . 11
2.2 Critical Security Parameters and Public Keys . . . 13

3 Roles, Authentication and Services **15**
3.1 Assumption of Roles . . . 15
3.2 Secure Channel Protocol (SCP) Authentication . . . 15
3.3 Services . . . 16

4 self-test **19**
4.1 Power Up Self-tests . . . 19
4.2 Conditional Self-tests . . . 20

5 Physical Security Policy **21**

6 Operational Environment **21**

7 Electromagnetic interference and compatibility (EMI/EMC) **21**

8 Mitigation of Other Attacks Policy **21**

9 Security Rules and Guidance **22**

10 References **23**

11 Acronyms and Definitions **24**

List of Tables

1 Security Level of Security Requirements . . . 6
2 Ports and Interfaces . . . 8
3 Module information . . . 10
4 Differences among the Three HW Part Numbers . . . 10
5 Indication command of Approved Mode . . . 11
6 Approved Cryptographic Functions . . . 13
7 Non-Approved But Allowed Cryptographic Functions . . . 13
8 Critical Security Parameters . . . 14
9 Public Keys (FipsDemoApplet) . . . 14
10 Roles Description . . . 15
11 Authenticated Services . . . 18
12 Unauthenticated Services . . . 19
13 Power Up Self-tests . . . 20
14 Conditional Self-tests . . . 20
15 References . . . 24
16 Acronyms and Definitions . . . 24

List of Figures

1 Physical Form and Cryptographic Boundary . . . 7
2 Contact plate example - Contact physical interface . . . 7
3 Contact plate example - Contact-less antenna contacts . . . 8
4 Module Logical Block Diagram and Boundary . . . 9

1 Introduction

This document defines the Security Policy for the Feitian Technologies Co., Ltd. (“Feitian”) FT-JCOS (Feitian Java Card Platform) cryptographic module, hereafter denoted the Module. The Module, validated to FIPS 140-2 overall Level 3, is a single chip smartcard module implementing the JavaCard and Global Platform operational environment, with Card Manager that also considered as Issuer Security Domain(ISD), a demonstration Applet with name FipsDemoApplet and a supplementary security domain that also considered as Applet Provider Security Domain (APSD).The demonstration applet, whose secure channel service provided by APSD, is only used to demonstrate the cryptographic functions of the module and is not for general use.

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated smartcard such as bank, health and etc. 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 1: Security Level of Security Requirements

The Module implementation is compliant with:

- ISO 7816
- ISO 14443
- JavaCard version 2.2.2
- GlobalPlatform 2.2.1 and GlobalPlatform 2.2 Amendment D

1.1 Hardware and Physical Cryptographic Boundary

The Module is designed to be embedded into plastic card bodies or SIMs, with a contact plate and contactless antenna connections. The physical form of the Module is depicted in Figure 1 (to scale); the red outline depicts the physical cryptographic boundary. In production use, the module is wire-bonded to a frame connected to a contact plate, enclosed in epoxy and mounted in a card body. The contactless ports of the module are electrically connected to an antenna embedded in the card body. The Module relies on [ISO7816] and [ISO14443] card readers as input/output devices. Figure 2 shows the contact physical interface of the Module, and Figure 3 shows the contact-less antenna contacts of the Module.

Figure 1: Physical Form and Cryptographic Boundary

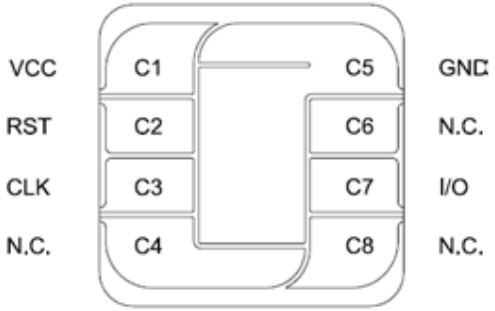

Figure 2: Contact plate example - Contact physical interface

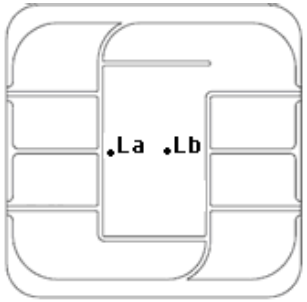

Figure 3: Contact plate example - Contact-less antenna contacts

Port	Description	Logical Interface Type
VCC	ISO 7816: Supply voltage, 1.62V~5.5V	Power
GND	ISO 7816: Ground	Power
RST	ISO 7816: Control input (Reset signal)	Control in
CLK	ISO 7816: Clock input, 1~10MHz	Control in
I/O	ISO 7816: Bidirectional data line (open drain)	Data in, data out, control in, status out
La, Lb	ISO 14443: Antenna	Power, Data in, data out, control in, status out
N.C.	Not connected	Not used

Table 2: Ports and Interfaces

1.2 Firmware and Logical Cryptographic Boundary

Figure 4 depicts the Module operational environment. The red outline depicts the logical cryptographic boundary.

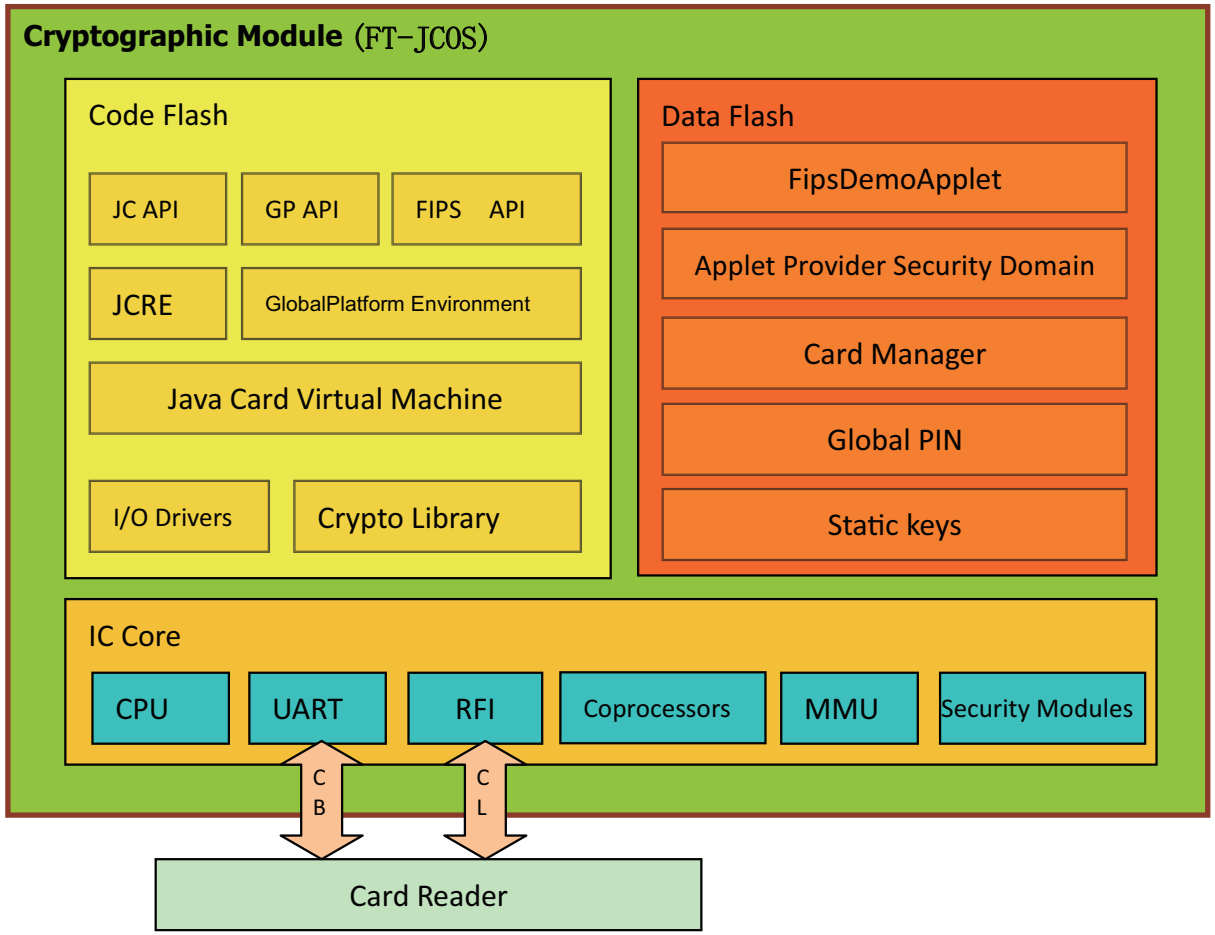

Figure 4: Module Logical Block Diagram and Boundary

- The ISO 7816-3 UART supports the T=0 and T=1 communication protocol variations.
- The RFI module is compliant with ISO14443-2 communication protocol.
- 404KB Flash (Code Flash and Data Flash): It includes the program code and user data.
- 8KB RAM: It is used to store the temporary data, global variables, session keys, etc.

- The Card Manager is the module adminstrator with the highest privilege and responsible for card content management, creating and authorizing other officers and users.
- The FipsDemoApplet is intended for cryptographic functions demonstration.
- The APSD, just a supplementary security domain without any privilege, is used to provide the FipsDemoApplet with secure channel with different static key set from ISD to demonstrate the identity-based authentication difference between CO and user.
- The global PIN and static keys are described in section 2.2.

1.3 Versions and Mode of Operation

Module	HW P/N	FW Version	OE (if applicable)
FT-JCOS(Feitian JavaCard Platform)	SLE78CLFX4000PM	1.0.0	N/A
FT-JCOS(Feitian JavaCard Platform)	SLE77CLFX2400PM	1.0.1	N/A
FT-JCOS(Feitian JavaCard Platform)	SLE78CLUFX5000PHM	1.0.2	N/A

Table 3: Module information

The firmware differences (FW Versions 1.0.0, 1.0.1 and 1.0.2) are only to support the different chips. The functionality is the same for all three versions. The differences among the hardware part numbers are listed in Table 4, where they have different memory size.

HW P/N	Flash Size	RAM Size
SLE78CLFX4000PM	400KB	8KB
SLE77CLFX2400PM	240KB	6KB
SLE78CLUFX5000PHM	500KB	16KB

Table 4: Differences among the Three HW Part Numbers

The module only provides a FIPS Approved mode. To verify that a module is in the Approved mode of operation, an operator can send SELECT Card Manager and the command shown below. The Module responds with the following information:

Command and associated elements	Expected Response
GET DATA with tag=9F80	9F 80 0A F8 F8 vv vv xx xx yy yy 00 00 90 00

Table 5: Indication command of Approved Mode

The data in response is explained as following:

- 9F80h Private Tag for module information
- 0Ah The following information length
- F8h Product Family-Feitian JavaCard Platform
- F8h Product Firmware Identifier-FT-JCOS
- vvvv Firmware Version 0100h, 0101h or 0102
- xxxx Chip Type-Infineon Security Controller 7892h (M7892), 7794h (M7794) or 7893(M7893)
- yyyy Feitian Private Chip Identifier 0010h for SLE78CLFX4000PM, 0011h for SLE77CLFX2400PM and 0012 for SLE78CLUFX5000PHM
- 0000h Reserve For future Use
- 9000h APDU status word,indicates the command has performed successfully.

To get the FipsDemoApplet and its associated APSD information, operator can send the GET STATUS (P1P2 with values 40h 00h) command after authenticated by the Card Manager,and get the Application Identifier(AID) values D1560001320A64656D6F01 for the FipsDemoApplet and D156000132080801 for APSD.

2 Cryptographic Functionality

2.1 Cryptographic functions

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Table 6 and Table 7 below.

Algorithm	Description	Cert#
AES	[FIPS 197, SP 800-38A]	2357
	Functions: Encryption, Decryption	3182
	Modes: ECB, CBC	3183
	Key sizes: 128, 192, 256 bits	
	CMAC[SP 800-38B]	2358
	Functions: Generation, Verification	3184
	Key sizes: AES with 128, 192, 256 bits	3185
DRBG	[SP 800-90A]	300
	Functions: CTR DRBG	664
	Option: AES-128 use df	665
	Security Strengths: 128	
	DRBG (key generation methodology provides 128 bits of security strength)	
RSA	[FIPS 186-4, and PKCS #1 v2.1 (PKCS1.5)]	1216
	Functions: Key Pair Generation, Signature Generation, Signature Verification	1617
	Key type: standard NDE, CRT	1623
	Key size: 1024 bits (Signature Verification only), 2048 bits	
SHA	[FIPS 180-4]	2030
	Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications	
	SHA sizes: SHA-1 (not used for Digital Signature Generation), SHA-256, SHA-512	
Triple-DES (TDES)	[SP 800-20]	1474
	Functions: Encryption, Decryption	1814
	Modes: TECB, TCBC	1815
	Key sizes: 2-key [1], 3-key	
Triple-DES MAC	[FIPS PUB 113]	1474,1814
	3-Key Triple-DES Message Authentication Code.Vendor affirmed based on Triple-DES Certs.	1815
KBKDF, using Pseudorandom	[SP 800-108]	9
	Functions: CMAC-based KDF using AES	42

[1]Per NIST SP 800-131A: Through December 31, 2015, the use of 2-key Triple DES for encryption is restricted: the total number of blocks of data encrypted with the same cryptographic key shall not be greater than 2^{20}. After December 31, 2015, 2-key Triple DES shall not be used for encryption. Decryption using 2-key Triple DES is allowed for legacy-use

Algorithm	Description	Cert#
Functions	Mode:Counter Key sizes:128,192,256	43

Table 6: Approved Cryptographic Functions

Algorithm	Description
NDRNG(TRNG)	[Annex C] Hardware Non-Deterministic RNG; minimum of 16 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG.
AES Key Wrap	[IG G.13] AES Certs.#2357,#3182 and #3183; (256-bit); key establishment methodology provides 256 bits of encryption strength

Table 7: Non-Approved But Allowed Cryptographic Functions

2.2 Critical Security Parameters and Public Keys

All CSPs and public keys used by the Module are described in Table 8 and Table 9. All usage of these keys by the Module (including all CSPs lifecycle states) is described in the services detailed in Section 3.3.

CSP	Description / Usage
RNG_STATE	CTR_DRBG (AES 128): V (128bits) and Key (128bits) are the critical values of the internal state upon which the security of this DRBG mechanism depends (i.e., V and Key are the "secret values" of the internal state). Note: The entropy,nonce for DRBG instantiation, generated by HW TRNG, are cleared after DRBG internal state has been instantiated once the module is reset.
Global PIN	64~256 bits，the Global PIN (Personal Identification Number) is one CVM (Cardholder Verification Method) standardized by GlobalPlatform, which may be used by all Applications on the card.
Kpin	168-bit Triple-DES KEY used to encrypt the Global PIN
Kpinmac	128-bit AES key of CMAC used to verify the integrity of the encrypted Global PIN (CMAC)
Kenc	256-bit AES base key used by the Security Domain to derive Ksenc

CSP	Description / Usage
Kcmac	256-bit AES base key used by the Security Domain to derive Kscmac
Kdek	256-bit AES sensitive data decryption key used by the Module to decrypt CSPs (the keys in the secure channel data – APDU command)
Ksenc	256-bit AES session encryption key used by the Module to encrypt/decrypt secure channel data.
Kscmac	256-bit AES session CMAC key used by the Module to verify inbound secure channel data integrity.
Kenckey	256-bit AES key only used to encrypt and decrypt the static keys (Kenc, Kcmac or Kdek) stored internally in flash, and every static key has its own Kenckey.
Kmackey	128-bit AES key of CMAC used to verify the integrity of encrypted static key, and every static key has its own Kmackey.
FipsDemoApplet	
Kfda-aesenc	128-bit AES key used to encrypt all keys stored as persistent objects in Flash.
Kfda-tdea	168-bit Triple-DES KEY used to demonstrate 3 key Triple-DES Cipher and Triple-DES MAC generation and verification
Kfda-rsapriv	2048-bit RSA private key used to demonstrate Signature generation
Kfda-rsacrt	2048-bit RSA CRT private key used to demonstrate Signature generation
Kfda-rsapriv-gen	2048-bit RSA private key generated by RSA key pair genenration demonstration
Kfda-rsacrt-gen	2048-bit RSA CRT private key generated by RSA CRT key pair genenration demonstration
Kfda-aescmac	128,192,256-bit AES keys used to demonstrate AES cipher, KDF,CMAC generation

Table 8: Critical Security Parameters

Public Key	Description / Usage
Kfda-rsapub	2048-bit RSA public key used to demonstrate Signature verification
Kfda-rsapub-gen	2048-bit RSA public key generated by RSA key pair generation demonstration

Table 9: Public Keys (FipsDemoApplet)

All module CSPs may be zeroized by use of the SET STATUS command to set the GP card lifecycle to TERMINATED, or by the module when some fatal errors occur. For Ksenc and Kscmac stored in RAM, are cleared when a new role is assumed or the module is reset.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles using the authentication scheme: One authentication is allowed per module reset. Re-authentication is enforced when changing roles.

Table 10 lists all operator roles supported by the module. The Module does not support a maintenance role.

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer: This role is responsible for managing the security configuration of the Module, including issuance and management of Module data via the ISD. The CO role is authenticated using Ksenc and Kscmac of ISD	Identity-based	Kenc and Kcmac and their Key Set Version Number of the ISD
User	User: This role is allowed to use services of the FipsDemoApplet and APSD. The User role is authenticated using Ksenc and Kscmac of APSD	Identity-based	Kenc and Kcmac and their Key Set Version Number of the APSD

Table 10: Roles Description

3.2 Secure Channel Protocol (SCP) Authentication

The Global Platform Secure Channel Protocol 03 authentication method is performed when the EXTERNAL AUTHENTICATE service is invoked after successful execution of the INITIALIZE UPDATE command. These two commands operate as described next. In the description below, the process is identical regardless of domain, e.g. Issuer Security Domain (ISD) or Applet Provider Security Domain (APSD). The Kenc and Kcmac keys are used along with other information to derive the Ksenc and Kscmac keys, respectively. The Ksenc 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 and user role). The EXTERNAL AUTHENTICATE process also checks the expected MAC value using the Kscmac. Based on the length of Ksenc and Kscmac (AES-256), the Module' s authentication security strength is determined to be 256 bits:

- The probability that a random attempt at authentication will succeed is $\frac{1}{2^{256}}$,less than one in 1,000,000 as required for FIPS 140-2.
- Based on the maximum retry count value(32) of the authentication, the probability that a random attempt will succeed over a one minute period is

$\frac{32}{2^{256}}$, less than 1 in 100,000 as required by FIPS 140-2.

3.3 Services

All services implemented by the Module are listed in Table 11 and Table 12 below. Each service description also describes all usage of CSPs by the service, where X indicates that the service is available to the entity, blank indicates the service is not available to that entity.

Service	Description	CO	U
DELETE	Delete an applet instance or package from the card and reclaim the flash occupied by them. CSP usage: Ksenc,Ksmac of ISD. All CSPs associated with the deleted applet or package are cleared.	X	
GET STATUS	Retrieve information about the card. CSP Usage: Ksenc,Ksmac of ISD.	X	
INSTALL	Perform Card Content management. CSP Usage: Ksenc,Ksmac of ISD.	X	
LOAD	Load a Executable Load File (CAP) into the module(e.g. package with or without applet). CSP Usage: Ksenc, Kscmac of ISD.	X	
PUT KEY	Replace existing key(s) or add new key(s). CSP Usage : Ksenc,Kscmac and Kdek of ISD or APSD	X	X
SET STATUS	Modify the card or applet life cycle status. CSP Usage: Ksenc and Kscmac of ISD.	X	
STORE DATA	Transfer data to the ISD for configuring issuer Data. CSP Usage: Ksenc, Kscmac of ISD.	X	
INITIALIZE UPDATE	Initialize the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. CSP Usage: Executes using Kenc, Kcmac of ISD or APSD.Writes Ksenc, Kscmac of ISD or APSD	X	X
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel.Must be preceded by a successful INITIALIZE UPDATE. CSP Usage: Ksenc, Kscmac of ISD or APSD	X	X

Service	Description	CO	U
TDES Cipher Demonstration	Perform encryption or decryption on provided values in ECB or CBC mode. CSP Usage: Kfda-tdea,Ksmac,Ksenc and Kdek of APSD		X
TDES MAC Demonstration	Perform TDES MAC generation and verification on provided values. CSP Usage: Kfda-tdea,Ksmac,Ksenc and Kdek of APSD		X
AES Cipher Demonstration	Perform encryption or decryption on provided values in ECB or CBC mode. CSP Usage: Kfda-aescmac,Ksmac,Ksenc and Kdek of APSD		X
CVM Operation Demonstration	Perform CVM (global PIN) verification,reconfiguration. CSP Usage: Global PIN, Kpin,Kpinmac,Ksmac and Ksenc of APSD		X
RSA Signature Demonstration	Perform PKCS#1V1.5 signature on provided values . CSP Usage: Kfda-rsapriv, Kfda-rsacrt, Ksmac, Ksenc and Kdek of APSD		X
RSA Signature Verification Demonstration	Perform PKCS#1V1.5 signature verification on provided values. CSP Usage: Kfda-rsapub,Ksmac and Ksenc of APSD		X
RSA Key pair Generation Demonstration	Perform RSA key pair generation using provided public exponent. CSP Usage: Kfda-rsapriv-gen,Kfda-rsacrt-gen,Kfda-rsapub-gen,Ksmac and Ksenc of APSD		X
CMAC Demonstration	Generate/Verify CMAC using provided messages/CMAC values. CSP Usage: Kfda-aescmac,Ksmac,Ksenc and Kdek of APSD		X
KDF Demonstration	Generate KDF result using provided messages CSP Usage: Kfda-aescmac,Ksmac,Ksenc of APSD		X

Service	Description	CO	U
DRBG Demonstration	Generate DRBG with 128-bit block size using provided parameters CSP Usage: RNG_STATE, Ksmac and Ksenc of APSD		X
Hash Demonstration	Generate SHA1,SHA256 and SHA512 digest using provided message CSP Usage: Ksmac and Ksenc of APSD		X
SET_DES_KEY	Load DES key for TDES Cipher and TDES MAC Demonstration CSP Usage: Kfda-tdea,Ksmac,Ksenc and Kdek of APSD		X
SET_AES_KEY	Load AES key for AES Cipher,KDF,DRBG Demonstration CSP Usage: Ksmac,Ksenc and Kdek of APSD		X
SET_RSA_PRIKEY	Load RSA private key for RSA Signature Demonstration CSP Usage: Ksmac,Ksenc and Kdek of APSD		X
SET_RSA_PUBKEY	Load RSA public key for RSA Signature Verification Demonstration CSP Usage: Ksmac,Ksenc and Kdek of APSD		X

Table 11: Authenticated Services

Service	Description
GET DATA	Retrieve a single data object using specified Tag.
MANAGE CHANNEL	Opens and closes supplementary logical channels.
SELECT	Select an applet in order to change role
SELF-TEST (RESET)	The module can be reset via both contact and contactless interface. For contact interface, the reader can enable RST pin or eject and re-insert card into reader; For contactless interface, the card is removed from and moved back to reader RF field or reader switches off and on the RF field. After the module is reset, the power up self-tests is performed.

Service	Description

Table 12: Unauthenticated Services

All services listed above are all available on contact and contactless interface. Since the FipsDemoApplet may import keys from external entity(card reader), all input APDU data must be encrypted and appended with CMAC to ensure the integrity and confidentiality of the command, which leads to the authentication security level mandatorily using C-DECRYPTION and C-MAC specified in [GP]. Moreover, the keys presented in APDU data field must be encrypted using Kdek of APSD; therefore,most services for demonstration use Ksmac,Ksenc and optionally Kdek of APSD as CSPs.

4 self-test

4.1 Power Up Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self tests described in Table 13 below after the first APDU command received. All KATs must be completed successfully prior to any other use of cryptography by the Module. If all KATs have performed successfully, the response will be returned; otherwise, the module will be muted and enter into an error state.

Test Target	Description
Firmware Integrity	16-bit CRC performed over all code in Flash.
AES	KATs: Encryption, Decryption Modes: ECB,CBC Key size: 256 bits
CMAC	KATs: Generation, Verification Key size: AES with 256 bits
DRBG	KATs: CTR DRBG Security Strengths: 128 bits
RSA	KATs: PKCS#1 v1.5 Signature Generation, Signature Verification Key size: 2048 bits
SHA	KATs: SHA-1, SHA-256, SHA-512
Triple-DES	KATs: Encryption, Decryption Modes: TECB,TCBC Keying option: 3-key
KBKDF, using Pseudorandom Functions	KATs: The Validation Test for KDF Mode: Counter

Table 13: Power Up Self-tests

4.2 Conditional Self-tests

Test Target	Description
NDRNG (TRNG)	Module performs a continuous stuck fault test to assure that the output is different than the previous value.
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation.
Firmware Load Test	When new firmware is loaded into the module using the LOAD command, the module verifies the integrity of the new firmware using a CMAC process.

Table 14: Conditional Self-tests

5 Physical Security Policy

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques and is protected by passive shielding (metal layer coverings opaque to the circuitry below) and active shielding (a grid of top metal layer wires with tamper response - not tested).

The Module is intended to be mounted in a plastic smartcard or other package as described in Section 1; physical inspection of the module boundary is not practical after mounting. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process.

NOTE: Module hardness testing was performed at ambient temperature only. No assurance is provided for Level 3 hardness conformance at any other temperature.

6 Operational Environment

This section does not apply to the Module. No code modifying the behavior of the cryptographic module operating system can be added after its manufacturing process.

Only FIPS 140-2 validated applets can be loaded and instantiated at post-issuance under control of the Cryptographic Officer. Their execution is controlled by the cryptographic module operating system following its security policy rules. (Note: This validation encompasses the tested platform and demonstration applet. Any other applets/firmware loaded onto the module are out of the scope of this validation and require a separate FIPS 140-2 validation.)

7 Electromagnetic interference and compatibility (EMI/EMC)

The Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

8 Mitigation of Other Attacks Policy

The Module implements defenses against:

- Light attacks
- Invasive fault attacks

- Side-channel attacks (SPA/DPA)
- Timing analysis
- Differential fault analysis (DFA)

9 Security Rules and Guidance

The Module design corresponds to the Module 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.

1. No additional interface or service is implemented by the Module which would provide access to CSPs.
2. Data output is inhibited during key generation, self-tests, zeroization, and error states.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
4. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
5. The module does not enter or output plaintext CSPs.
6. The module does not output intermediate key values.

10 References

Reference	Full Specification Name
[FIPS140-2]	Security Requirements for Cryptographic Modules, May 25, 2001
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011
[ISO 7816-3]	*ISO/IEC 7816-3:2006 Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols*
[ISO 14443]	*ISO/IEC 14443-1:2008 Identification cards – Contactless integrated circuit cards –Proximity cards – Part 1: Physical characteristics* *ISO/IEC 14443-2:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface* *ISO/IEC 14443-3:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards –Part 3: Initialization and anticollision* *ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit cards –Proximity cards – Part 4: Transmission protocol*
[JavaCard]	*Java Card™ Platform, Version 2.2.2 March 2006* Java Card 2.2.2 Runtime Environment (JCRE) Specification Java Card 2.2.2 Virtual Machine (JCVM) Specification Java Card 2.2.2 Application Programming Interface
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1, January 2011, http://www.globalplatform.org* *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2 Amendment D, September 2009*
[FIPS 140-2 IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, June 2012*
[FIPS 113]	Computer Data Authentication, 30 May 1985
[FIPS 197]	Advanced Encryption Standard (AES), November 26, 2001
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation Methods and Techniques, December 2001
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

Reference	Full Specification Name
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012
[FIPS 186-4]	Digital Signature Standard (DSS),July 2013
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard, June 14, 2002
[FIPS 180-3]	Secure Hash Standard, October 2008
[SP 800-20]	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS):Requirements and Procedures,March 2012
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions, October 2009

Table 15: References

11 Acronyms and Definitions

Acronym	Definition
APDU	Application Protocol Data Unit
GP	Global Platform
KAT	Known Answer Test
MMU	Memory Management Unit
UART	Universal Asynchronous Receiver/Transmitter
CB	contact-based
CL	contactless
RFI	Radio Frequency Interface

Table 16: Acronyms and Definitions