NXP JCOP 2.4.2 R2
FIPS 140-2 Cryptographic Module Security Policy

Version: 0.6
Date: 10 April 2013

Table of Contents

Table of Tables

Table of Figures

1 Introduction

This document defines the Security Policy for the NXP JCOP 2.4.2 R2 cryptographic 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, with Card Manager and a Demonstration Applet. The Demonstration Applet is available only to demonstrate the complete cryptographic capabilities of the Module for FIPS 140-2 validation, and is not intended for general use.

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.

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	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 1 – Security Level of Security Requirements

The Module implementation is compliant with:

- [ISO 7816] Parts 1-4
- [ISO 14443] Parts 1-4
- [JavaCard]
- [GlobalPlatform]

1.1 Hardware and Physical Cryptographic Boundary

The Module is designed to be embedded into plastic card bodies, 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, representing the surface of the chip and the bond pads. The cross-hatching indicates the presence of active and passive tamper shields. In production use, the Module is delivered to either vendors or end user customers in various forms:

- As bare die in wafer form for direct chip assembly by wire bonding or flip chip assembly
- Wire bonded and encapsulated by epoxy with additional packaging e.g. Dual Interface Modules; Contact only Modules; Contactless Modules; SMD packages

The contactless ports of the module require connection to an antenna. The Module relies on [ISO7816] and [ISO14443] card readers as input/output devices.

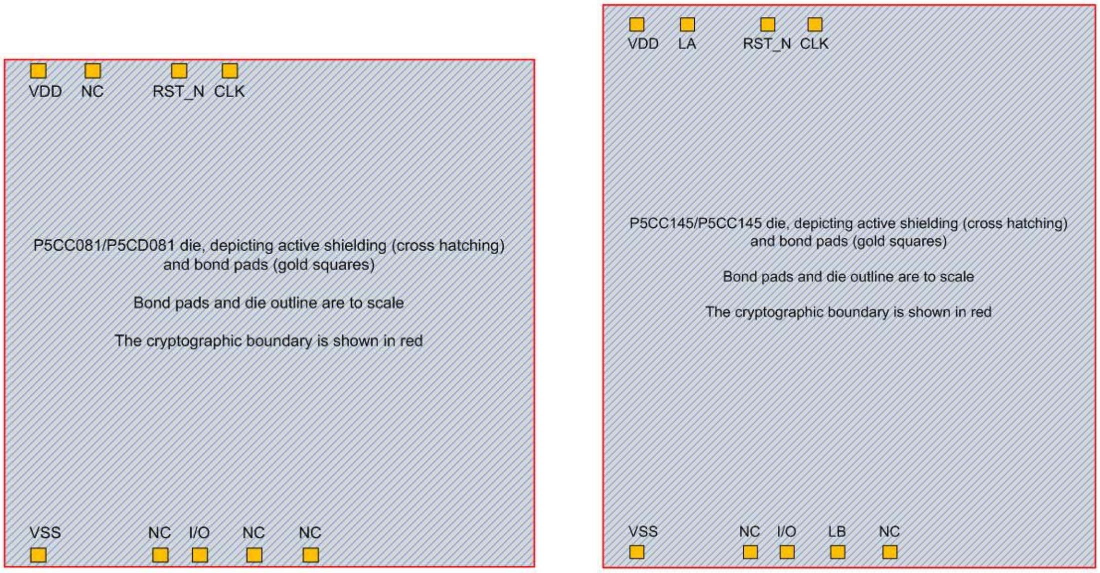
VDD
NC
RST_N
CLK
P5CC081/P5CD081 die, depicting active shielding (cross hatching) and bond pads (gold squares)
Bond pads and die outline are to scale
The cryptographic boundary is shown in red
VSS
NC
I/O
NC
NC
VDD
LA
RST_N
CLK
P5CC145/P5CC145 die, depicting active shielding (cross hatching) and bond pads (gold squares)
Bond pads and die outline are to scale
The cryptographic boundary is shown in red
VSS
NC
I/O
LB
NC

Figure 1 – NXP JCOP 2.4.2 R2: Physical Form (P5CC081/P5CD081 left; P5CC145/P5CD145 right)

The module is available in five configurations:

- P5CC081 V1A – 80 KB memory, Contact only
- P5CD081 V1A – 80 KB memory, Contact and Contactless, includes a non-FIPS mode (MIFARE)
- P5CD081 V1D – 80 KB memory, Contact and Contactless, includes a non-FIPS mode (DESFire)
- P5CC145 V0B - 144 KB memory, Contact only
- P5CD145 V0B – 144 KB memory, Contact and Contactless, includes a non-FIPS mode (MIFARE)

The five configurations are produced from a single hardware design with two memory configurations, with the communications interface and mode options determined during the fabrication process.

The contactless interfaces are permanently disabled for the P5CC081 and P5CC145 configurations.

The P5CD081 V1A, P5CD081 V1D and P5CD145 V0B include a mechanism which permits the Module to power on into a non-Approved mode (either MIFARE or DESFire) or into the FIPS 140-2 Approved mode (JCOP 2.4.2 R2). These modes use separate, non-shared memory partitions managed by the on-chip memory manager, with no possibility of shared critical security parameters between modes. The non-approved modes apply only to contactless operation, selected at power on by detection of communications type in the initial frames sent to the Module. The mode can be changed only by power cycling the Module.

The MIFARE mode of operation provides READ, WRITE, DECREMENT, INCREMENT, TRANSFER and RESTORE operations, operating in a small memory space. No security functions are provided in this mode, and the Memory Management Unit (MMU) firewall prevents access between MIFARE and JCOP.

The DESFire mode of operation provides services to manage ISO 7816 file system nodes on the card; authenticate; and change password. In the DESFire non-approved mode, the module allows DESFire data to be loaded into the DESFire memory space, but does not permit any executable firmware to be loaded. The module contains a memory management unit (MMU) that prevents all access by the DESFire mode into JCOP memory space, and similarly, prevents all JCOP access into the DESFire memory space.

Pad	Description	Logical interface type
VSS, VDD	ISO 7816: Power, ground	Power
CLK	ISO 7816: Clock	Control in
RST_N	ISO 7816: Reset	Control in
IO	ISO 7816: Serial interface	Data in, data out, control in, status out
LA, LB	ISO 14443: Antenna	Data in, data out, control in, status out (Disabled on P5CC081, P5CC145)
NC	No connect	Not used

Table 2 – Ports and Interfaces

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

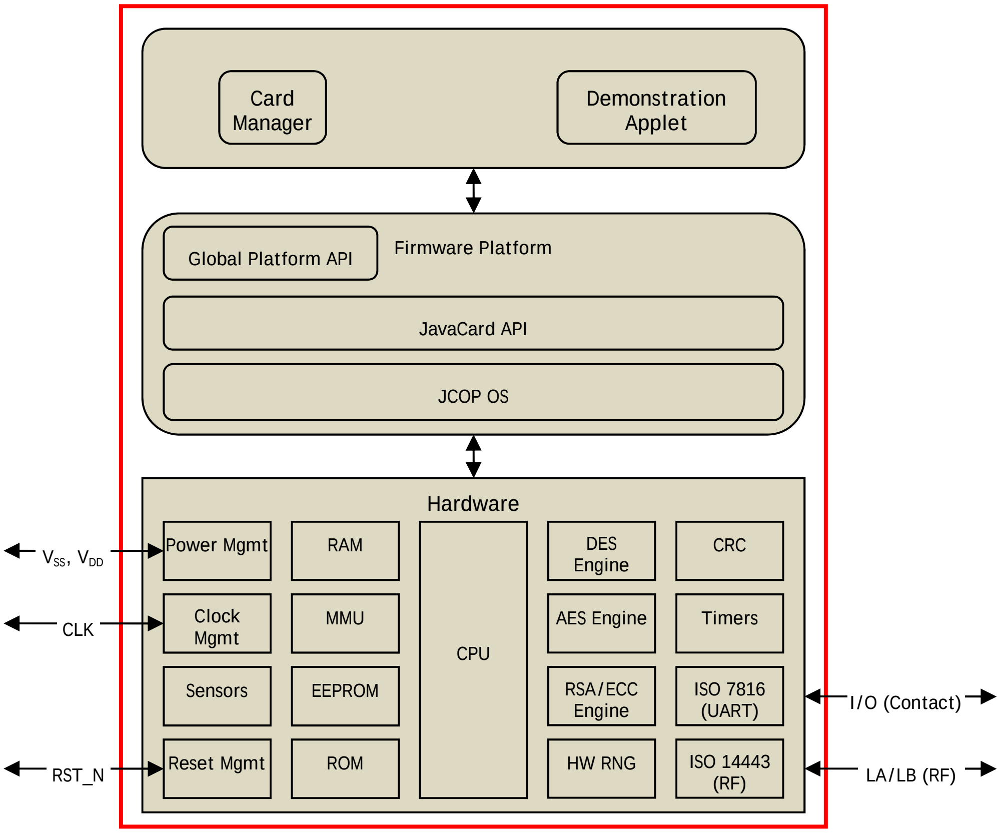

Figure 2 - Module Block Diagram

- The ISO 7816 UART supports the T=0 and T=1 communications protocol variants
- The ISO 14443 communications block supports 13.56 MHz Type A signaling (106 kbps; 212 kbps; 424 kbps and the T=CL protocol)
- 80 KB EEPROM; 264 KB ROM; 7.5 KB RAM [P5CC081 V1A, P5CD081 V1A, P5CD081 V1D]
- 144 KB EEPROM; 264 KB ROM; 7.5 KB RAM [P5CC145 V0B, P5CD145 V0B]

Section 3 describes applet functionality in greater detail. The JavaCard and Global Platform APIs are internal interfaces available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

1.3 Versions and Mode of Operation

Hardware: P/N P5CC081 V1A, P5CD081 V1A, P5CD081 V1D, P5CC145 V0B, P5CD145 V0B
Firmware: JCOP 2.4.2 R2 Mask ID 59 and patchID 3, Demonstration Applet v1.0

To verify that a module is in the approved mode of operation, an operator sends the IDENTIFY command. If the Module is in the FIPS 140-2 approved mode, it responds with the value "01" (hex) in the 19th byte. In the non-FIPS 140-2 mode, the Module responds with an error.

2 Cryptographic functionality

The Module operating system implements the FIPS Approved and Non-FIPS Approved but Allowed cryptographic functions listed in Table 3 and Table 4 below.

Algorithm	Description	Cert #
RNG	[ANSI X9.31] 2-Key TDES RNG.	942
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm (TDES). The module supports the 2-Key and 3-Key options; CBC and ECB modes.	1144
TDES MAC	[FIPS113] TDES MAC, vendor affirmed based on Cert. #1144.	1144
TDES CMAC	[SP800-38B] 3-Key TDES CMAC	1145
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports 128-, 192- and 256-bit key lengths and ECB and CBC modes.	2151
AES CMAC	[SP800-38B] AES-256 CMAC	2152
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports 128-, 192- and 256-bit key lengths and ECB and CBC modes. This is a faster implementation of the AES algorithm for this module.	2120
AES CMAC	[SP800-38B] AES-256 CMAC. This is a faster implementation of the AES algorithm for this module.	2121
SHA-1, SHA-2	[FIPS 180-2] Secure Hash Standard compliant one-way (hash) algorithms; SHA-1, SHA-224, SHA-256.	1553
RSA	[PKCS#1] RSA signature generation and verification. The module supports 1024 and 2048-bit RSA keys.	1090
RSA CRT	[PKCS#1] RSA signature generation. The module supports 1024 and 2048-bit RSA keys.	1091
ECDSA	[FIPS 186-2] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-192, P-224 and P-256 curves for key pair generation, signature and signature verification.	317
CVL	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive only. The module supports the NIST defined P-192, P-224 and P-256 curves.	26

Table 3 – FIPS Approved Cryptographic Functions

Algorithm	Description
HW RNG	Hardware RNG; minimum of 8 bits per access. The HW RNG output used to seed the FIPS approved DRNG.
Symmetric Key Wrap	Key wrapping as described in [AES Key Wrap]. Using 2-Key TDES as allowed by [FIPS 140 IG] D2; provides 112 bits of security strength. Using AES-128, provides 128 bits of security strength.
RSA Key Gen	RSA 1024- and 2048-bit key pair generation (as permitted per IG 7.12).

Table 4 – Non-FIPS Approved But Allowed Cryptographic Functions

[SP 800-131A] Section A.1 provides the NIST rationale for 2-Key TDES security strength. 2-Key TDES is used for GlobalPlatform Secure Channel operations, in which the module derives session keys from the master keys and a handshake process, performs mutual authentication, and decrypts data for internal use only. The Module encrypts a total of one block (the mutual authentication cryptogram) over the life of the session encryption key; no decrypted data is output by the module. The Module claims 112-bit security strength for its 2-Key TDES operations, as the meet-in-the-middle attack rationale described in [SP 800-131A] does not apply unless the attacker has access to encrypt/decrypt pairs.

2-Key TDES key establishment provides 112 bits of security strength. The Module uses the SD-KDEK key to decrypt critical security parameters, and does not perform encryption with this key or output data decrypted with this key.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module, including all CSP lifecycle states, is described in the services detailed in Section 3.

The following critical security parameters are always present:

Key	Description / Usage
OS-SEED	64 bit random value; Seed from Fast RNG used for ANSI X9.31 DRNG seed.
OS-SEED-KEY	192 bit seed key; Seed key used for ANSI X9.31 DRNG
OS-RNG-STATE	320 bit value; Current RNG state
OS-MKEK	2-Key TDES Master key used to encrypt all CSP data stored in the EEPROM.
SD-KENC	AES-128 or 2-Key TDES Master key used by the CO role to generate SD-SENC
SD-KMAC	AES-128 or 2-Key TDES Master key used by the CO role to generate SD-SMAC.
SD-KDEK	AES-128 or 2-Key TDES Sensitive data decryption key used by the CO role to decrypt CSPs.
SD-SENC	AES-128 or 2-Key TDES Session encryption key used by the CO role to encrypt / decrypt secure channel data.
SD-SMAC	AES-128 or 2-Key TDES Session MAC key used by the CO role to verify inbound secure channel data integrity.
SD-SDEK	AES-128 or 2-Key TDES Session data decryption key used by the CO role to decrypt sensitive data.
DEMO-AUTH	A fixed 16 byte value used by the Demo Authenticate service.
DEMO-AUTH-KEY	AES-128 key used by the Demo Authenticate service.
DEMO-AES-CMAC	AES-128 key used by the Demo AES_CMAC service.
DEMO-TDEA-CMAC	3-Key TDES key used by the Demo TDEA_CMAC service.
DEMO-RSA	RSA 1024- or 2048- private key used to demonstrate RSA signature generation. The *Demo RSA* service allows either an RSA or RSA CRT key pair to be used. SHA-1 is used with RSA 1024, SHA-2 (256) is used with RSA 2048.
DEMO-ECDSA	EC P-192, P-224, or P-256 private key used to demonstrate ECDSA key pair generation and signature generation. The *Demo ECDSA* service allows any of the valid EC curves to be used, and uses SHA-2. SHA-2 (224) is used with P-192, SHA-2 (256) is used with P-256.
DEMO-ECC-CDH	EC P-192, P-224 or P-256 private key used to demonstrate ECC CDH shared secret generation. The *Demo ECC CDH* service allows any of the valid EC curves to be used.

Table 5 - Module Critical Security Parameters

2.2 Public keys

Key	Description / Usage
DAP-PUB	RSA 1024-bit public key used for new firmware signature verification.
DEMO-RSA-PUB	RSA 1024-bit or 2048-bit public key used by the *Demo RSA* service.
DEMO-ECDSA-PUB	ECDSA P-192, P-224 or P-256 public key used by the *Demo ECDSA* service
DEMO-ECC-CDH-PUB	EC P-192, P-224 or P-256 public key used by the *Demo ECC CDH* service.

Table 6 - Public Keys

3 Roles, authentication and services

3.1 Roles

Table 7 lists all operator roles supported by the module. This Module does not support a maintenance role. The Module clears previous authentications on power cycle. The Module supports GP logical channels, allowing multiple concurrent operators. Authentication of each operator and their access to roles and services is as described in this section, independent of logical channel usage. Only one operator at a time is permitted on a channel. Applet deselection (including 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. A velocity check on the Global Platform authentication procedure is performed. Maximum PIN try limit is implemented: During CVM verification, if the CVM verification fails and the Retry Limit has been reached, the CVM state shall transition to BLOCKED.

Role ID	Role Description
CO	Cryptographic Officer This role is responsible for card issuance and management of card data via the Card Manager applet. Authenticated using the SCP authentication method with SD-SENC.
USR	The role used in the demonstration applet, the User role for FIPS 140-2 purposes. Authenticated using symmetric AES mechanism with DEMO-AUTH and DEMO-AUTH-KEY.

Table 7 - Roles description

3.2 Secure Channel Protocol (SCP) Authentication

The GlobalPlatform Secure Channel Protocol 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.

The SD-KENC and SD-KMAC keys are used along with other information 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 SD- keys may be 2-Key TDES (SCP01/02) or AES-128 (SCP03). Note that the only use of the any of the SD- keys for encryption is for a total of 1 block over the life of the associated SD-SENC session key. The Module's designed encryption limitation using SD-SENC prevents the meet-in-the-middle attack described in [SP800-131A]. In accordance with [SP800-131A], the Module's 2-Key TDES security strength is 112 bits. Based on this strength (expressed in scientific notation format in parentheses):

- The probability that a random attempt at authentication will succeed is 1/2^64 (5.42E-20) for SCP01/02; 1/2^128 for SCP03 (2.94E-39).
- Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^64 (1.38E-17) for SCP01/02; 255/2^128 for SCP03 (7.49E-37).

3.3 Demonstration Applet Symmetric Authentication

The Demonstration Applet uses a predetermined datum (DEMO-AUTH) and an AES-128 key (DEMO-AUTH-KEY) to authenticate the USR operator. The probability that a random attempt at authentication will succeed is determined by the message size (16 bytes), chosen to correspond to the AES block size. Therefore:

- The probability that a random attempt at authentication will succeed is 1/2^128 (2.94E-39).
- A conservative lower bound for processing a single message is 1 µs, and so the corresponding conservative upper bound for the number of authentication attempts in a one minute period is 6x10^7. Therefore, the probability that a random attempt at authentication will succeed in a one minute period is (6x10^7)/(2^128), (1.76E-31).

3.4 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. The columns to the right of the description indicate which roles are allowed access to the service. The SD-SENC and SD-SMAC keys are used by every Card Manager service when a secure channel has been established, for decryption and MAC verification (packet integrity and authenticity), respectively. This is noted below as “Optionally uses SD-SENC, SD-SMAC (SCP)”. Unauthenticated commands listed below function whether or not a secure channel has been established.

Service	Description
Card Reset (Self-test)	This service is activated by power cycling the Module. On the contact interface, this is done by removing and reinserting the Module into the contact reader slot, or by reader assertion of the RST signal. On the contactless interface, this is done by removing and re-inserting the Module into the contactless reader’s field or by transmitting an ISO 14443 DESELECT then activating the Module. The *Card Reset* service will invoke the power on self-tests described in Section 4.1, and On the first instance of card reset, the Module generates OS-MKEK. On any card reset, the Module overwrites OS-SEED, OS-SEED-KEY and OS-RNG-STATE. On any card reset, the card overwrites all volatile memory with zeros.
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. Uses SD-SENC and SD-SMAC.
INITIALIZE UPDATE	Initialize the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. Uses the SD-KENC, SD-KMAC and SD-KDEK master keys to generate the SD-SENC, SD-SMAC and SD-SDEK session keys, respectively.
GET DATA	Retrieve a single data object. Optionally uses SD-SENC, SD-SMAC (SCP).
MANAGE CHANNEL	Open and close supplementary logical channels. Optionally uses SD-SENC, SD-SMAC (SCP).
SELECT	Select the Card Manager or Demonstration Applet. Optionally uses SD-SENC, SD-SMAC (SCP).
IDENTIFY	Retrieve card identification data. Optionally uses SD-SENC, SD-SMAC (SCP).

Table 8 - Unauthenticated Operating System and Card Manager Services and CSP Usage

Service	Description	CO
DELETE	Delete an applet from EEPROM. Optionally uses SD-SENC, SD-SMAC (SCP)	X
GET STATUS	Retrieve information about the card. Optionally uses SD-SENC, SD-SMAC (SCP)	X
INSTALL	Perform Card Content management. Optionally uses SD-SENC, SD-SMAC (SCP)	X
LOAD	Load a load file (e.g. an applet). Uses SD-SMAC for firmware load integrity, or alternatively, may use DAP-PUB for new firmware signature verification.	X
PUT KEY	Load Card Manager keys. Writes any of SD-KENC, SD-KMAC, SD-KDEK. Uses SD-KDEK to decrypt new key values.	X
SET STATUS	Modify the card or applet life cycle status. Optionally uses SD-SENC, SD-SMAC (SCP)	X
STORE DATA	Transfer data to an application during command processing. Optionally uses SD-SENC, SD-SMAC (SCP)	X

Table 9 – *Card Manager* Services and CSP Usage

Service	Description	USR
Demo Authenticate	Decrypts an authentication value (DEMO-AUTH) with an AES 128 authentication key (DEMO-AUTH-KEY). Responds with status word.	X
Demo AES_CMAC	Generates and verifies an input value with the DEMO-AES-CMAC key. Responds with CMAC output and status word.	X
Demo TDEA_CMAC	Generates and verifies an input value with the DEMO-TDEA-CMAC key. Responds with CMAC output and status word.	X
Demo RSA	Generates a signature using the provided input message and a static private key (DEMO-RSA), and verifies the signature using the provided message and corresponding public key (DEMO-RSA-PUB). Responds with the message signature and status word. This service can use either RSA or RSA CRT, and can use any valid RSA modulus size.	X
Demo ECDSA	Generates an ECDSA key pair (DEMO-ECDSA, DEMO-ECDSA-PUB), generates a signature using the provided input message and the generated private key (DEMO-ECDSA), and verifies the signature using the provided message and generated public key (DEMO-ECDSA-PUB). Responds with the message signature, public key and status word.	X
Demo ECCCDH	Generates a ECDSA key pair (DEMO-ECC-CDH, DEMO-ECC-CDH-PUB) and, using the provided public key, computes Z value generated per SP 800-56A Section 5.7.1.2 , responds with the generated public key, and the status word.	X
Destroy Demo	Destroys all Demonstration Applet CSPs.	X

Table 10 – *Demonstration Applet* Services and CSP Usage

4 Self-test

The Module does not define critical self-tests. The power-on and conditional self-tests performed by the Module are listed below.

4.1 Power-on self-test

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

On power on or reset, the Module performs the self-tests described in Table 11 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the system is halted and will start again after a reset.

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code located in EEPROM. This integrity test is not required or performed for code stored in masked ROM code memory.
ANSI X9.31	Performs a fixed input KAT.
TDES	Performs encrypt and decrypt KATs using 3-Key TDES in CBC mode.
AES	Performs encrypt and decrypt KATs using an AES-128 key in CBC mode. Both implementations of AES encrypt and decrypt are tested.
AES CMAC	Performs AES CMAC generate and verify KATs using an AES-128 key. Both implementations of AES CMAC are tested.
TDES CMAC	Performs TDES CMAC generate and verify KATs using a 3-Key TDES key.
RSA	Performs RSA signature and verify KATs using an RSA 2048-bit key.
RSA CRT	Performs RSA CRT signature and verify KATs using an RSA 2048-bit key.
ECDSA	Performs ECDSA signature and verify KAT using the P-256 curve; this self-test is inclusive of the ECC CDH self-test.
SHA-256	Performs a fixed input KAT.

Table 11 – Power-On Self-Test

4.2 Conditional self-tests

On every call to the HW RNG or ANSI X9.31 RNG, the Module performs the FIPS 140-2 Continuous RNG test as described in AS09.42 to assure that the output is different than the previous value.

When any RSA or ECDSA key pair is generated the Module performs a pairwise consistency test.

When new firmware is loaded into the module using the LOAD command, the module verifies the integrity and authenticity of the new firmware using a TDES MAC process and the SD-SMAC key. Optionally, the new firmware can be integrity tested by verifying the signature provided by the host, using the DAP-PUB key.

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). A tamper event detected by the active shield places the Module permanently into the SYSTEM HALTED error state.

The Module is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process.

6 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 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 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.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- 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.

10 References

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001 CHANGE NOTICES (12-03-2002)
[FIPS201-1]	*Personal Identity Verification (PIV) Of Federal Employees and Contractors*, March 2006
[ISO 7816]	ISO/IEC 7816-1: 1998 *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 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[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]	Sun Microsystems: Java Card 3.0.1 http://java.sun.com/products/javacard
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1,* March 2003, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[AESKeyWrap]	NIST, *AES Key Wrap Specification*, 16 November 2001. This document defines symmetric key wrapping, Use of 2-Key TDES in lieue of AES is described in [IG] D.2.
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 29 June 2012.

Table 12 – References

11 Acronyms and definitions

Acronym	Definition
APDU	Application Protocol Data Unit
SCP	Secure Channel Protocol

Table 13 – Acronyms and Definitions