NXP JCOP 2.4.2 R3
FIPS 140-2 Cryptographic Module Security Policy

Version: 0.6
Date: 31 July 2014

Table of Contents

List of Tables

List of Figures

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[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
[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*
[JavaCard]	*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* Published by Sun Microsystems, March 2006
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[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.
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS 197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[FIPS 186-2]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-2, January, 2000 with Change Notice 1. (DSA, RSA and ECDSA)
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[FIPS 180-3]	NIST, *Secure Hash Standard*, FIPS Publication 180-3, October 2008
[AESKeyWrap]	NIST, *AES Key Wrap Specification*, 16 November 2001. This document defines symmetric key wrapping, Use of 2-Key Triple-DES 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 2 May 2012.

Table 1 – References

Acronyms and definitions

Acronym	Definition
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	Global Platform
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
NVM	Non-Volatile Memory (e.g. EEPROM, Flash)
OP	Open Platform (predecessor to Global Platform)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis

Table 2 – Acronyms and Definitions

1 Introduction

This document defines the Security Policy for the NXP JCOP 2.4.2 R3 cryptographic module, hereafter denoted *the Module*. The Module, validated to FIPS 140-2 overall Level 3, is a single chip smartcard 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 term *platform* herein is used to describe the chip and operational environment, not inclusive of the Demonstration Applet.

The Module is a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load function 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.

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 3 – Security Level of Security Requirements

1.1 Versions, Configurations and Modes of operation

Hardware: P/Ns P5CC081 V1A, P5CD081 V1A, P5CD081 V1D, P5CC145 V0B, P5CD145 V0B
Firmware: JCOP 2.4.2 R3 Mask ID 64 and patchID 1, Demonstration Applet v1.1

In the FIPS 140-2 approved mode, the module will respond to the Module Information (Unauthenticated) service IDENTIFY command with the value “01” (hex) in the 19th byte. In the non-FIPS 140-2 mode, the Module responds with an error.

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-FIPS 140-2 mode (either MIFARE or DESFire) or into the FIPS 140-2 Approved mode (JCOP 2.4.2 R3). 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.

1.2 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.

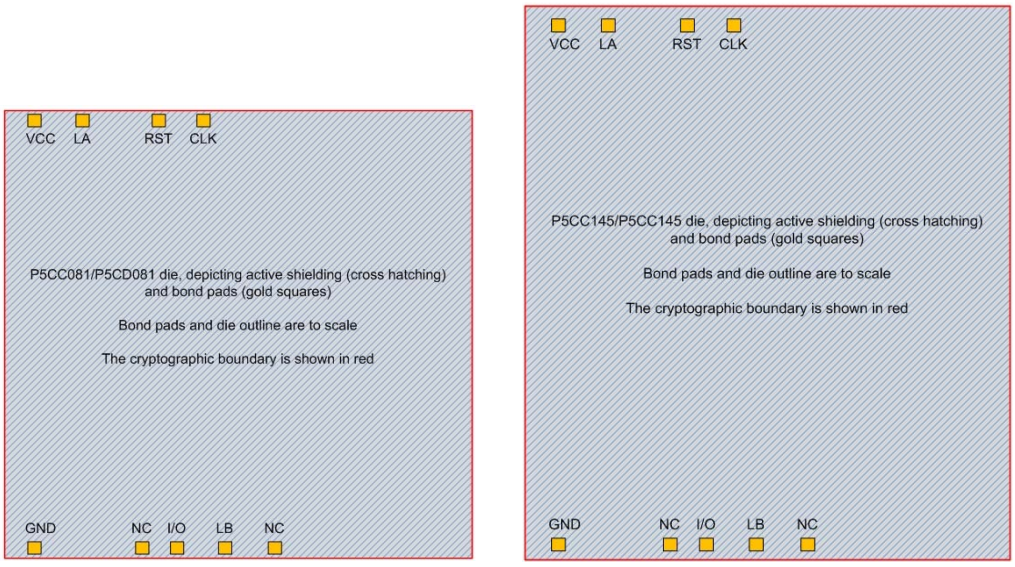

Figure 1 – NXP JCOP 2.4.2 R3: Physical Form (P5CC081/P5CD081 left; P5CC145/P5CD145 right)

Port	Description	Logical Interface Type
$V_{CC,}$ GND	ISO 7816: Supply voltage	Power
RST	ISO 7816: Reset	Control in
CLK	ISO 7816: Clock	Control in
I/O	ISO 7816: Input/Output	Control in, Data in, Data out, Status out
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out
NC	Not connected	Not connected

Table 4 – Ports and Interfaces

1.3 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

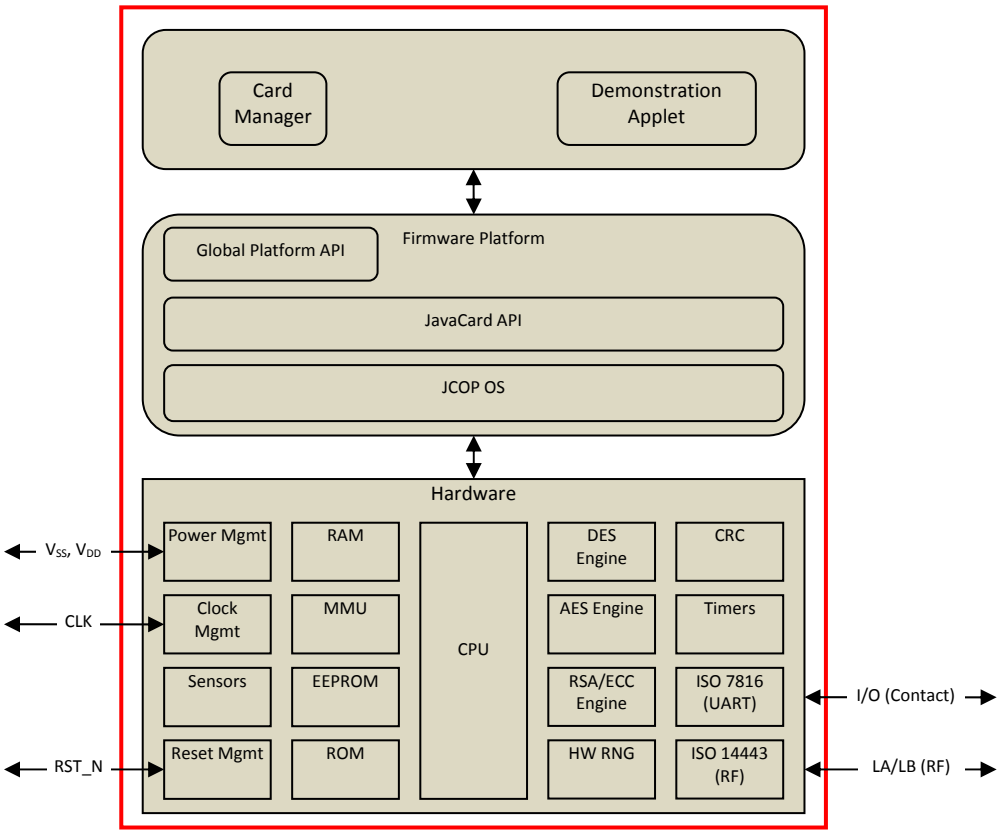

Figure 2 - Module Block Diagram

- 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. 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).

2 Cryptographic Functionality

The Module implements the Approved and Non-Approved but Allowed cryptographic functions listed in Table 5 and Table 6 below.

Algorithm	Description	Cert #
RNG	[ANSI X9.31] 3-Key Triple-DES RNG.	1229
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports the 2-Key[1] and 3-Key options; CBC and ECB modes.	1552
Triple-DES MAC	[FIPS 113] Triple-DES MAC, vendor affirmed based on Cert. #1552.	[1552]
Triple-DES CMAC	[SP 800-38B] 3-Key Triple-DES CMAC.	1553
AES_X	[FIPS 197] Advanced Encryption Standard algorithm. The module supports 128-, 192- and 256-bit key lengths and ECB and CBC modes.	2596
AES_X CMAC	[SP 800-38B] AES-128 or AES-256 CMAC (192-bit keys are not used)	2597
AES_FAST	[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.	2561
AES_FAST CMAC	[SP 800-38B] AES-128 or AES-256 CMAC (192-bit keys are not used). This is a faster implementation of the AES CMAC algorithm for this module.	2564
SHA-1, SHA-2	[FIPS 180-2] Secure Hash Standard compliant one-way (hash) algorithms; SHA-1, SHA-224, SHA-256.	1553
RSA	[FIPS 186-2] RSA 1024 and 2048-bit keys (1536-bit keys are not used). – Signature generation: 2048-bit RSA keys; SHA-256 – Signature verification: 1024 and 2048-bit RSA keys; SHA-1 and SHA-256	1090
RSA CRT	[FIPS 186-2] RSA 1024 and 2048-bit keys (1536-bit keys are not used). – Signature generation: 2048-bit RSA keys; SHA-256 – Signature verification: 1024 and 2048-bit RSA keys; SHA-1 and SHA-256	1091
ECDSA	[FIPS 186-2] Elliptic Curve Digital Signature Algorithm using NIST defined curves. – Key pair generation: P-224 and P-256 curves – Signature verification: P-192, P-224 and P-256 curves; SHA-1	317
CVL	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive only using NIST defined curves. – P-224 and P-256 curves	26

Table 5 –Approved Cryptographic Functions

[SP 800-131A] Section A.1 provides the NIST rationale for 2-Key Triple-DES security strength. 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 Triple-DES 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.

[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
HW RNG	Hardware RNG; minimum of 8 bits per access. The HW RNG output used to seed the FIPS approved RNG.
Symmetric Key Wrap	Symmetric key wrapping as allowed by [FIPS 140 IG] D2. Using 2-Key Triple-DES (Cert. #1552), provides 112 bits of security strength. Using AES-128 (Cert. #2561 or #2596), provides 128 bits of security strength.

Table 6 – Non-Approved but Allowed Cryptographic Functions

The module implements algorithms, modes and key sizes that are Disallowed as of January 1, 2014 per the NIST SP 800-131A transitions. Algorithms providing less than 112 bits of security strength (Disallowed per NIST SP 800-131A) are not allowed in the FIPS Approved mode of operation for use by Federal agencies. The Disallowed algorithms, modes and key sizes are listed in Table 7 below.

Algorithm	Description	Cert #
RSA	[FIPS 186-2] RSA 1024 and 2048-bit keys (1536-bit keys are not used). – Signature generation: 1024-bit RSA keys using SHA-1 or SHA-256; 2048-bit RSA keys using SHA-1	1090
RSA CRT	[FIPS 186-2] RSA 1024 and 2048-bit keys (1536-bit keys are not used). – Signature generation: 1024-bit RSA keys using SHA-1 or SHA-256; 2048-bit RSA keys using SHA-1	1091
ECDSA	[FIPS 186-2] Elliptic Curve Digital Signature Algorithm. – Key pair generation: P-192 curve – Signature generation: P-192, P-224 and P-256 curves; SHA-1	317
CVL	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive only. – P-192 curve	26
RSA Key Gen	RSA 1024 and 2048-bit key pair generation (untested, non-compliant).	N/A

Table 7 – Disallowed Cryptographic Functions

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module are described in the services detailed in Section 4. In the tables below, the OS prefix denotes operating system, the SD prefix denotes the Global Platform Security Domain, the DAP prefix denotes the Global Platform Data Authentication Protocol, and the DEM prefix denotes a Demonstration Applet CSP.

CSP	Description / Usage
OS-RNG-SEED-KEY	3-key Triple-DES key generated by HW RNG, used for the RNG seed key.
OS-RNG-STATE	320 bit value; the current RNG state.
OS-MKEK	2-Key Triple-DES Master key used to encrypt all keys stored in NVM. Generated outside the module, loaded during manufacturing.
SD-KENC	AES-128 or 2-Key Triple-DES Master key used to generate SD-SENC.
SD-KMAC	AES-128 or 2-Key Triple-DES Master key used to generate SD-SMAC.
SD-KDEK	AES-128 or 2-Key Triple-DES Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES-128 or 2-Key Triple-DES Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES-128 or 2-Key Triple-DES Session MAC key used to verify inbound secure channel data integrity.
SD-SDEK	AES-128/192/256 (SCP03) or 2-Key Triple-DES (SCP01) DES Session data decryption key used to decrypt sensitive data.
DAP-SYM	AES-128 or 2-Key Triple-DES authentication key used by the *Manage Content* service.
DEM-AUTH	A fixed 16 byte value and AES-128 key used by the *Authenticate* service.
DEM-KAP-PRI*	EC P-192, P-224 or P-256 private key used to demonstrate the ECC CDH shared secret generation. The *Key Agreement Primitive* service allows any of the valid EC curves to be used.
DEM-MAC	3-Key Triple-DES MAC or AES-128 bit CMAC key used by the *Message Authentication* service.
DEM-SGV-PRIV*	1024 or 2048 bit RSA or EC P-192, P-224, or P-256 private key used by the *Key Generation* and *Digital Signature* services.

Table 8 –Critical Security Parameters

* CSPs impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Table 7).

2.2 Public Keys

Key	Description / Usage
DAP-PUB	RSA 1024 new firmware signature verification key.
DEM-KAP-PUB	P-192, P-224, P-256 ECDSA public key used by the *Key Agreement Primitives* service.
DEM-SGV-PUB	P-192, P-224, P-256 ECDSA or RSA 1024-, 2048-bit public key used by the *Digital Signature* service.

Table 9 – Public Keys

3 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, independent of logical channel usage. Only one operator at a time is permitted on a channel. Applet de-selection (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. Authentication data is encrypted during entry (by SD-SDEK), is stored in plaintext and is only accessible by authenticated services.

Table 9 lists all operator roles supported by the Module.

Role ID	Role Description
CO	Cryptographic Officer – role that manages Module content and configuration, including issuance and management of Module data via the ISD. Authenticated as described in *Secure Channel Protocol Authentication* below.
User	User - authenticated as described in *Demonstration Applet Authentication* below.

Table 10 - Roles Supported by the Module

3.1 Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method is provided by the *Secure Channel* service. 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:

- 1/2^64 = 5.4E-20 (for 2-Key Triple-DES SD-KENC/SD-SENC)
- 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 255 failed SCP authentication attempts. The probability that a random attempt will succeed over a one minute interval is:

- 255/2^64 = 1.30E-18 (for 2-Key Triple-DES SD-KENC/SD-SENC)
- 255/2^128 = 7.5E-37 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

3.2 Demonstration Applet Authentication Method

The Demonstration Applet uses a predetermined datum and an AES-128 key (DEM-AUTH) 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 60x10^6 = 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.

3.3 Services

All services implemented by the Module are listed in the tables below.

Service	Description
Context	Select an applet or manage logical channels.
Module Info (Unauthenticated)	Read unprivileged data objects, e.g. module configuration or status information.
Module Reset	Power cycle or reset the Module. Includes Power-On Self-Test.

Table 11 - Unauthenticated Services

Service	Description	CO	User
Lifecycle	Modify the card or applet life cycle status.	X	
Manage Content	Load and install application packages and associated keys and data.	X	
Module Info (Authenticated)	Read module configuration or status information (privileged data objects)	X	
Secure Channel	Establish and use a secure communications channel.	X	
Authenticate	Demonstration Applet authentication service.		X
Digital Signature*	Demonstrate RSA and ECDSA digital signature generation and verification.		X
Key Agreement Primitive*	Demonstrate Approved ECC CDH primitive (SP 800-56A Section 5.7.1.2).		X
Message Authentication	Demonstrate Triple-DES MAC and AES CMAC.		X
Destroy Demo Applet CSPs	Destroys all Demonstration Applet CSPs.		X

Table 12 –Authenticated Services

* Services impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Table 7).

CSPs														
Service	OS-RNG-SEED-KEY	OS-RNG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-SDEK	DAP-SYM	DEM-AUTH	DEM-KAP-PRI*	DEM-MAC	DEM-SGV-PRIV*
Module Reset	GE WZ	GE WZ	Z[2]--	--	--	--	Z	Z	Z	--	--	--	--	--
Module Info (Unauthenticated)	--	--	--	--	--	--	E	E	E	--	--	--	--	--
Context	--	--	--	--	--	--	Z	Z	Z	--	--	--	--	--
Secure Channel	--	EW	--	E	E	E	GE	GE	GE	--	--	--	--	--
Manage Content	--	--	EW	W	W	W	E	E	E	EW	--	--	--	--
Lifecycle	Z	Z	Z	Z	Z	Z	E	E	E	Z	Z	Z	Z	Z
Module Info (Authenticated)	--	--	--	--	--	--	E	E	E	--	--	--	--	--
Authenticate	--	--	--	--	--	--	--	--	--	--	EW Z	--	--	--
Message Authentication	--	--	--	--	--	--	--	--	--	--	--	--	EW Z	--
Digital Signature*	--	EW	--	--	--	--	--	--	--	--	--	--	--	GE WZ
Key Agreement Primitive*	--	--	--	--	--	--	--	--	--	--	--	GE WZ	--	--
Destroy Demo Applet CSPs	--	--	--	--	--	--	--	--	--	--	Z	Z	Z	Z

Table 13 – CSP Access within Services

* Services and CSPs impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Table 7).

- 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 Module writes the CSP. The write access is typically performed after a CSP is imported into the Module or when the module overwrites an existing CSP.
- 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.

[2] RAM copy is destroyed on power-cycle or reset.

4 Self-test

4.1 Power-On Self-tests

On power-on or reset, the Module performs self-tests as described in Table 13 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 NVM. This integrity test is not required or performed for code stored in masked ROM code memory.
ANSI X9.31 RNG	Performs a fixed input KAT.
Triple-DES	Performs encrypt and decrypt KATs using 3-Key Triple-DES in CBC mode.
Triple-DES CMAC	Performs Triple-DES CMAC generate and verify KATs using a 3-Key Triple-DES key.
AES	Performs separate encrypt and decrypt KATs using an AES-128 key in CBC mode. Both the standard and fast implementations of AES encrypt and decrypt are separately tested.
AES CMAC	Performs AES CMAC generate and verify KATs using an AES-128 key. Both implementations of AES CMAC are tested.
RSA	Performs RSA signature and verify KATs using an RSA 2048-bit key; this self-test is inclusive of the SHA-1 self-test.
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 and the SHA-256 self-test.

Table 14 – 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 AS09.42 continuous RNG test to assure that the output is different than the previous value.

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

When new firmware is loaded into the Module using the *Manage Content* service, the Module verifies the integrity of the new firmware (applet) using MAC verification (Triple DES MAC or AES CMAC) with the SD-SMAC key. Optionally, the Module may also verify a signature of the new firmware (applet) using the DAP-SV-PUB public key or the DAP-SYM key; the signature block in this scenario is generated by an external entity using the private key corresponding to DAP-SV-PUB or the symmetric DAP-SYM.

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.

Module hardness testing was performed at the following temperatures:

- Nominal temperature: 20°C
- Low temperature: -40°C
- High temperature: 120°C

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 induction

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.

