TOPDLv2.1 Platform

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Table of Contents

Table of Tables

Table 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 *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2* Amendment D, Sept 2009
[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]	*Identification cards – Contactless integrated circuit cards – Proximity cards* ISO/IEC 14443-1:2008 Part 1*: Physical characteristics* ISO/IEC 14443-2:2010 Part 2: *Radio frequency power and signal interface* ISO/IEC 14443-3:2011 Part 3: *Initialization and anticollision* ISO/IEC 14443-4:2008 Part 4: *Transmission protocol*
[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* *Java Card 3.0.1 Application Programming Interface [only for algos ECDSA, SHA2]* Published by Sun Microsystems, March 2006
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP 800-90A]	NIST Special Publication 800-90, *Recommendation for the Random Number Generation Using Deterministic Random Bit Generators (Revised)*, March 2007
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (Triple-DES) 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 186-4]	NIST, Digital Signature Standard (DSS), FIPS Publication 186-4, July, 2013
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015

Acronym	Full Specification Name
[AESKeyWrap]	NIST, *AES Key Wrap Specification*, 16 November 2001. This document defines symmetric key wrapping, Use of 2-Key Triple-DES in lieu 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 1 August 2016.

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
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 Gemalto TOPDLv2.1 Platform cryptographic module, herein denoted the *Module*. The *Module*, validated to FIPS 140-2 overall Level 3, is a single-chip "dual" module (P60D144) 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	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 Security Requirements

1.1 Cryptographic Module Ports and Interfaces

The *Module* is designed to be embedded into plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna. 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 the hard opaque outer layer shielding. In production use, the *Module* is wire-bonded to a frame connected to a contact plate (pads CLK, RST, VDD, I/O and VSS) and/or to an RF antenna (pads LA and LB), enclosed in epoxy and mounted in a card body. The *Module* relies on [ISO 7816] and/or [ISO 14443] card readers as input/output devices.

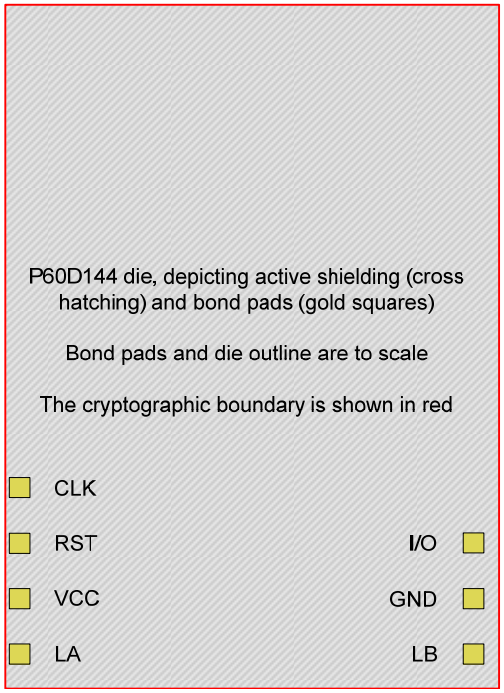

Figure 1 - Physical form and Cryptographic Boundary (P60D144)

Contact No.	Description	Logical interface type
VCC	Supply voltage	Power
RST	Reset signal	Control in
CLK	Clock signal	Control in
GND	Ground	Power
I/O	Input/output	Data in, data out, control in, status out
LA	LA (Antenna coil connection)	Power, Data in, Data out, Control in, Status out
LB	LB (Antenna coil connection)	Power, Data in, Data out, Control in, Status out

Table 4 – Module Physical Ports and Corresponding Logical Interfaces

For contact interface operation, the *Module* conforms to [ISO 7816] part 1 and part 2. The electrical signals and transmission protocols follow the [ISO 7816] part 3. The conditions of use are the following:

Conditions	Range
Voltage	3 V and 5.5 V
Frequency	1MHz to 10MHz

Table 5 - Voltage and Frequency Ranges

For contactless interface operation, the *Module* conforms to [ISO 14443] part 1 for physical connections, and to [ISO 14443] parts 2, 3 and 4 for radio frequencies and transmission protocols. The external antenna loop required for contactless operation is outside the module cryptographic boundary.

The conditions of use are the following:

Conditions	Range
Supported bit rate	106 Kbits/s, 212 Kbits/s, 424 Kbits/s, 848 Kbits/s
Operating field	Between 1.5 A/m and 7.5 A/m rms
Frequency	13.56 MHz +- 7kHz

Table 6 – Contactless voltage and Frequency Ranges

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment and applets.

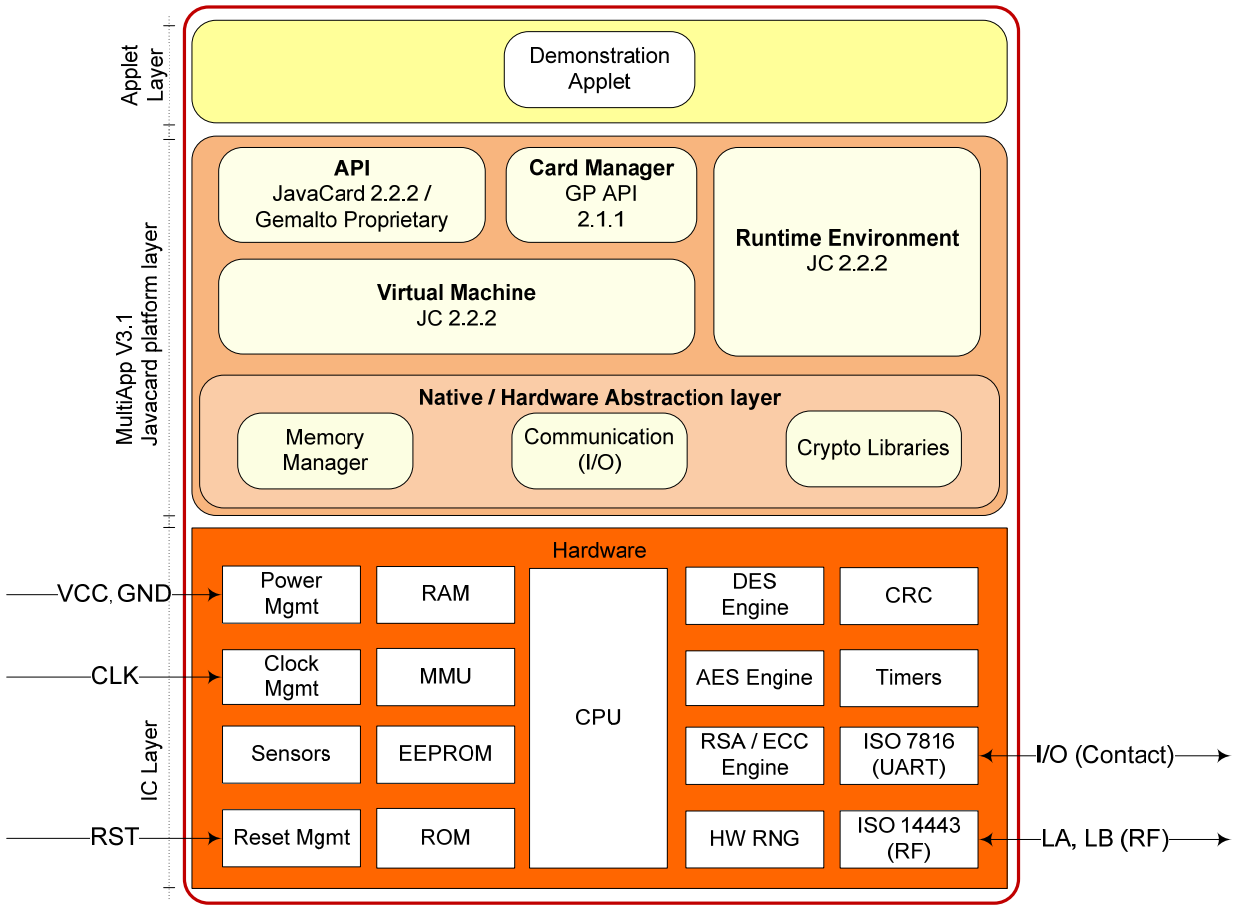

Figure 2 - Module Block Diagram

The *JavaCard API* is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary). The *Cryptography Libraries* implement the algorithms listed in Section 2. The *Javacard Runtime Environment* implements the dispatcher, registry, loader, and logical channel functionalities. The *Virtual Machine* implements the byte code interpreter, firewall, exception management and byte code optimizer functionalities.

The *Card Manager* is the card administration entity, allowing authorized users to manage the card content, keys, and life cycle states. The Card Manager behaves similarly to an applet, but is properly represented as a constituent of the platform. The *Memory Manager* implements functions such as memory access, allocation, deletion and garbage collection.

The *Communication* handler implements the ISO 7816 and ISO 14443 communications protocols in contactless mode and dual mode.

Section 3 describes applet functionality in greater detail.

1.3 Versions and Mode of Operation

Hardware:

NXP P60D144P VA (MPH149)

Firmware: TOPDLV2.1 (Filter04), Demonstration Applet version V1.3

The Module implements only an Approved mode of operation, as delivered from the manufacturing environment. The explicit indicator of FIPS mode is available using the *Module Information* service (specifically, the GET DATA command with tag 0103). The *Module* responds with a multi-byte data set; the most significant bit of the 5th byte set to 1 is the explicit indicator of the FIPS approved mode.

Specifically, the first five bytes will be:

FOR MPH149

B0 84 49 53 **81** (represented in hexadecimal with the 5th byte shown in bold red font)

Where the 5th byte is 1000 0001 (represented in binary, with FIPS Approved mode indicator in bold red font).

2. Cryptographic functionality

The Module implements the *FIPS Approved* cryptographic functions listed in Table 7 below:

Algorithm	Description	Cert #
DRBG	[SP 800-90A] Deterministic Random Bits Generator (CTR-DRBG based on AES)	900
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The Module supports the 3-Key options; CBC and ECB modes. Note that the Module does not support a mechanism that would allow collection of plaintext / ciphertext pairs aside from authentication, limited in use by a counter.	1984
Triple-DES MAC	[FIPS 113] Triple DES Message Authentication Code. Vendor affirmed, based on validated Triple DES.	1984
Triple-DES Key Wrap	[SP 800-38F] Use of approved 3 key Triple-DES for key wrapping, in accordance with SP 800-38F §3.1 ¶3.; provides 112 bits of security	1984
AES	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128-, 192- and 256-bit key lengths with ECB and CBC modes.	3543
AES CMAC	[SP 800-38D] The Module supports 128-, 192- and 256-bit key lengths.	3543
AES Key Wrap	[SP 800-38F] Use of approved AES and AES CMAC for key wrapping, in accordance with SP 800-38F §3.1 ¶3.	3543
KDF AES CMAC	[SP 800-108] The Module supports 128-, 192- and 256-bit key lengths	85
RSA	[FIPS 186-2] [PKCS#1 v1.5 and PSS] RSA algorithms. – Signature verification using 4096-bit key (any SHA size). [FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA algorithms – Key pair generation using 2048-bit keys – Signature generation using 2048-bit keys using with SHA-2 – Signature verification using 1024, 2048-bit and 3072-bit keys (any SHA size)	1822
RSA CRT	[FIPS 186-2] [PKCS#1 v1.5 and PSS] RSA CRT algorithm. – Signature verification using 4096-bit key with SHA-2. [FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA CRT algorithm. – Key pair generation using 2048-bit keys; – Signature generation using 2048-and 3072-bit keys with SHA-2; – Signature verification using 1024-, 2048-and 3072-bit keys (any SHA size).	1823
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm using the NIST defined curves – Key pair generation: P-224, P-256, P-384 and P-521 curves – Signature generation: P-224, P-256, P-384 and P-521 curves with SHA-2 – Signature verification: P-192, P-224, P-256, P-384 and P-521 curves (any SHA size).	721
CVL (ECC CDH)	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive using the NIST defined curves: P-224, P-256, P-384 and P-521.	597
SHA-1 SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms. The Module supports the SHA-1 (160 bits), SHA-2 (224- bit, 256-bit, 384-bit, 512-bit) variants.	2921
CVL (RSASP1)	[FIPS 186-4] [PKCS#1 v2.1] RSA signature generation primitive using 2048-bit keys.	815
CVL (RSADP)	[SP 800-56B] RSA key decryption primitive using 2048-bit keys.	834

Table 7 – FIPS Approved Cryptographic Functions

The Module also implements the *FIPS Non Approved but Allowed* cryptographic functions listed in Table 8 below:

Algorithm	Description
NDRNG	True Random Number Generator. Provides at least 128 bits of entropy.

Table 8 – FIPS Non-Approved but Allowed 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 3. 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.

Key	Description / Usage
OS-DRBG-EI-KEY	AES-128 random key generated by the card during startup is used as a entropy input for the [SP800-90A] DRBG implementation.
OS-DRBG-STATE	16-byte AES state V and 16-byte AES key used in the [SP800-90A] CTR DRBG implementation.
OS-GLOBALPIN	6 to 16 byte Global PIN value. Character space is not restricted by the module.
OS-MKDK	AES-128/192/256 (SCP03) key used to encrypt OS-GLOBALPIN value
SD-KENC	AES-128/192/256 (SCP03) encryption master key used to derive SD-SENC
SD-KMAC	AES-128/192/256 (SCP03) Security Domain MAC master key, used derive SD-SMAC
SD-KDEK	AES-128/192/256 (SCP03) Security Domain Sensitive data decryption key.
SD-SENC	AES-128/192/256 (SCP03) Security Domain Session decryption key used to decrypt secure channel messages.
SD-SMAC	AES-128/192/256 (SCP03) Security Domain Session MAC key, used to verify secure channel message integrity.
SD-SDEK	AES-128/192/256 (SCP03) Session DEK key used by the CO role to decrypt CSPs.
DAP-SYM	AES-128/192/256 (SCP03) key optionally loaded in the field and used to verify the MAC of packages loaded into the Module.
DEM-EDK	AES-128/192/256 or 3-Key Triple-DES encryption / decryption key used by the Demonstration Applet *Symmetric Cipher* service.
DEM-KAP-PRI	P-224, P-256, P-384, P-521 ECDSA private key used by the Demonstration Applet *Generate Key Pair* and *Key Agreement Primitives* service.
DEM-KGS-PRI	2048-bit RSA or P-224, P-256, P-384, P-521 ECDSA private key used by Demonstration Applet *Generate Key Pair and RSADP Primitive* services.
DEM-MAC	AES-128/192/256 CMAC or 3-Key Triple-DES key used by Demonstration Applet *Message Authentication* service.
DEM-MK	3-Key Triple-DES master key used to encrypt or decrypt Demonstration Applet CSPs exported out of or imported into the Module.
DEM-SGV-PRI	2048-, 3072-, 4096-bit RSA or P-224, P-256, P-384, P-521 ECDSA private key used by Demonstration Applet *Digital Signature* service.

Table 9 -Critical Security Parameters

2.2 Public Keys

Key	Description / Usage
DEM-KAP-PUB	P-224, P-256, P-384, P-521 ECDSA public key used by the Demonstration Applet *Key Agreement Primitives* service.
DEM-KGS-PUB	2048-bit RSA or P-224, P-256, P-384, P-521 ECDSA public key used by Demonstration Applet *Generate Asymmetric Key Pair* service.
DEM-SGV-PUB	1024-, 2048-, 3072-, 4096-bit RSA or P-192, P-224, P-256, P-384, P-521 ECDSA public key used by Demonstration Applet Asymmetric Signature service.

Table 10 –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 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.

Authentication data is encrypted during entry (by SD-SDEK), is stored in plaintext 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 content and configuration , including issuance and management of Module data via the ISD authenticated as described in *Secure Channel Protocol Authentication* below.
User	User - The user role for FIPS 140-2 validation purposes, authenticated as described in *Demonstration Applet Authentication* below..

Table 11 - 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:

- 1/2^128 = 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:

- 255/2^128 = 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

This authentication method compares a PIN value sent to the Module over an encrypted channel to be stored OS-GLOBALPIN values; if the two values are equal, the operator is authenticated. This method is used in the Demonstration Applet services to authenticate to the User role.

The module enforces OS-GLOBALPIN string length of 6 bytes minimum (16 bytes maximum), allowing all characters, so the strength of this authentication method is as follows:

- The probability that a random attempt at authentication will succeed is 1/256^6.
- Based on a maximum count of 15 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is 15/256^6.

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 (Unauth)	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 12 - 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 (Auth)	Read module configuration or status information (privileged data objects)	X	
Secure Channel	Establish and use a secure communications channel.	X	
Digital Signature	Demonstrate RSA (inclusive of RSASP1) and ECDSA digital signature generation and verification.		X
Generate Key Pair	Demonstrate RSA and ECDSA key generation		X
ECC CDH Primitive	Demonstrate EC Diffie-Hellman primitive.		X
RSADP Primitive	Demonstrate RSADP primitive.		X
Message Authentication	Demonstrate Triple-DES Mac and AES CMAC.		X
Symmetric Cipher	Demonstrate use of Triple-DES and AES for encryption and decryption.		X

Table 13 – Authenticated Services

CSPs																	
Service	**OS-FRBG-EI-KEY**	**OS-DRBG-STATE**	**OS-GLOBALPIN**	**OS-MKDK**	**SD-KENC**	**SD-KMAC**	**SD-KDEK**	**SD-SENC**	**SD-SMAC**	**SD-SDEK**	**DAP-SYM**	**DEM-EDK**	**DEM-MAC**	**DEM-SGV-PRI**	**DEM-KGS-PRI**	**DEM-KAP-PRI**	**DEM-MK**
Module Reset	ZE W	ZE GW	--	--	--	--	--	Z	Z	Z	--	--	--	--	--	--	--
Module Info (Unauth)	--	--		--	--	--	--	E[1]	E[1]	E[1]	--	--	--	--	--	--	--
Context	--	--		--	--	--	--	Z	Z	Z	--	--	--	--	--	--	--
Secure Channel	--	EW		E	E	E	E	GE[1]	GE[1]	GE[1]	--	--	--	--	--	--	--
Manage Content	--	--	W	E	W	W	W	E[1]	E[1]	E[1]	EW	--	--	--	--	--	--
Lifecycle	Z	Z	Z	Z	Z	Z	Z	--	--	--	Z	Z	--	Z	Z	Z	Z
Module Info (Auth)	--	--	--	--	--	--	--	E[1]	E[1]	E[1]							
Symmetric Cipher	--	--	E	E	--	--	--	--	--	--	--	ER WZ	--	--	--	--	E
Message Authentication	--	--	--	E	--	--	--	--	--	--	--	--	EW Z	--	--	--	--
Digital Signature	--	EW	E	E	--	--	--	--	--	--	--	--	--	ER WZ	--	--	E
Generate Key Pair	--	EW	E	E	--	--	--	--	--	--	--	--	--	--	GER WZ	GER WZ	E
ECC CDH Primitive	--	EW	E	E	--	--	--	--	--	--	--	--	--	--	--	GER WZ	E
RSADP Primitive	--	EW	E	E	--	--	--	--	--	--	--	--	--	--	GER WZ	--	E

Table 14 – CSP Access by Service

- 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.

[1] "E" for Secure Channel keys is included for situations where a Secure Channel has been established and all traffic is received encrypted. The Secure Channel establishment includes authentication to the module.

4. Self-test

4.1 Power-on Self-test

On power on or reset, the *Module* performs self-tests described in Table 15. All KATs must be completed successfully prior to any other use of cryptography by the *Module*. If one of the KATs fails, the *Module* enters the *Card Is Mute* error state.

Test Target	Description
FW 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.
DRBG	Performs SP800-90A Health tests with fixed inputs, inclusive of KAT
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key TDEA in ECB mode.
AES	Performs decrypt KAT using an AES 128 key in ECB mode. AES encrypt is self-tested as an embedded algorithm of AES-CMAC.
AES-CMAC	Performs an AES-CMAC Generate KAT using an AES 128 key. Note that AES-CMAC Verify is identical to a Generate KAT (perform Generate then compare to the input) hence a single KAT verifies both functions.
RSA	Performs separate RSA PKCS#1 signature and verification KATs using an RSA 2048 bit key.
RSA CRT	Performs RSA PKCS#1 signature KAT using an RSA 2048 bit key. RSA CRT signature verification is tested as part of the RSA signature verification KAT as described above.
ECDSA	Performs separate ECDSA signature and verification KATs using P-224.
ECC CDH	Performs a KAT for ECC CDH using P-224 keys constituents.
SHA-1, SHA-2	Performs separate KATs for SHA-1, SHA-256 and SHA-512.

Table 15 – Power-On Self-Test

4.2 Conditional Self-tests

On every call to the [SP800-90A] CTR DBRG, the *Module* performs a stuck fault test to assure that the output is different than the previous value.

When 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 with the SD-MAC key. Optionally, the Module may also verify a signature of the new firmware (applet) using the DAP-SYM key; the signature block in this scenario is generated by an external entity using the private key corresponding to the symmetric key 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.

The *Module* is designed to be mounted in a plastic smartcard or similar package; physical inspection of the epoxy side of the Module is not practical after mounting. The *Module* also provides a key to protect the *Module* from tamper during transport and the additional physical protections listed in Section 8 below.

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:

- Fault attacks
- Side channel analysis (Timing Analysis, SPA/DPA, Simple/Differential Electromagnetic Analysis)
- Probing attacks
- Card tearing

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 Mo*d*ule.

END OF DOCUMENT