gemalto
security to be free

MultiApp V4.0 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 2.2.1,* January 2011, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1* Amendment E V1.0.1, July 2014 *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1* Amendment D V1.1.1, July 2014 *GlobalPlatform Consortium:ID Config 1.0 December 2011* *GlobalPlatform Consortium:Common Config 1.0 February 2014* *GlobalPlatform Consortium:Global Platform card API org.globalplatform specifications 1.6*
[ISO 7816]	ISO/IEC 7816-1:2011 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2013 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange* ISO/IEC 7816-4/AC1:2014 *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 14443-1:2016 Part 1*: Physical characteristics* ISO/IEC 14443-2:2016 Part 2: *Radio frequency power and signal interface* ISO/IEC 14443-3:2016 Part 3: *Initialization and anticollision* ISO/IEC 14443-4:2016 Part 4: *Transmission protocol*
[JavaCard]	*Java Card 3.0.4 Runtime Environment (JCRE) Specification* *Java Card 3.0.4 Virtual Machine (JCVM) Specification* *Java Card 3.0.4 Application Programming Interface* *Java Card 3.0.5 Application Programming Interface [only for algos ECDSA PLAIN, CIPHER_RSA_OAEP]* Published by Sun Microsystems,
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 1, November 2015
[SP 800-90A]	NIST Special Publication 800-90A, *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 (TDES) 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

Acronym	Full Specification Name
[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
[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 29 June 2012.

Table 1 – References

Acronyms and Definitions

Acronym	Definition
API	Application Programming Interface
BPU	Bound Protection Unit
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	Global Platform
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
LSB	Least Significant Bit
MSB	Most Significant Bit
OBKG	On Board Key Generation
PCT	Pairwise Consistency Test
PDM	Product Data Management
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 MultiApp V4.0 cryptographic module, herein denoted the *Module*. The *Module*, validated to FIPS 140-2 overall Level 3, is a single-chip “contact-only”, “contactless-only” or “dual” module implementing the Global Platform operational environment, with Card Manager and a Demonstration Applet.

The module is available in the following six part numbers:

1) SLE78CFX4000PH (contact-only, 400k memory)
2) SLE78CFX3000PH (contact-only, 300k memory)
3) SLE78CLFX400VPH (dual mode or contactless-only, 400k memory, increased baud rate)
4) SLE78CLFX300VPH (dual mode or contactless-only, 300k memory, increased baud rate)
5) SLE78CLFX4000PH (dual mode or contactless-only, 400k memory)
6) SLE78CLFX3000PH (dual mode or contactless-only, 300k memory)

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

1.1.1 Hardware and Physical Cryptographic Boundary

The *Module* is designed to be generally embedded into a plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna. The cryptographic boundary is defined as the surfaces and edges of the packages as shown in Figures 1,3 and 4. The *Module* relies on [ISO 7816] and/or [ISO 14443] card readers as input/output devices.

1.1.2 Physical Port - Contact mode

1.1.2.1 PIN assignments and Contact Dimensions:

The *Module* follows the standards [ISO 7816] part 1 and part 2.

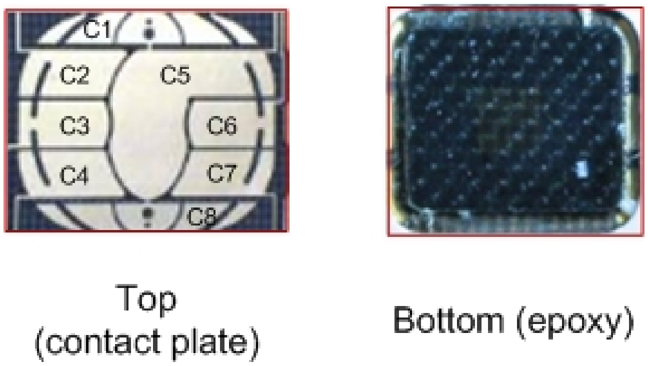


Figure 1 – Contact plate example – Contact physical interface

Contact No.	Description	Logical interface type
C1	VCC (supply voltage)	Power
C2	RST (Reset signal)	Control in
C3	CLK (Clock signal)	Control in
C4	Not connected	N/A
C5	GND (Ground)	N/A
C6	Not connected	N/A
C7	I/O	Data in, data out, control in, status out
C8	Not connected	N/A

Table 4 – Contact plate pin list – Contact mode

1.1.2.2 Conditions of Use

The electrical signals and transmission protocols follow the [ISO 7816] part 3. The conditions of use are the following:

Conditions	Range
Voltage	1.8 V, 3 V and 5.5 V
Frequency	1MHz to 10MHz

Table 5 – Voltage and frequency ranges

1.1.3 Physical Port – Contactless mode

1.1.3.1 Contacts Assignments

In the contactless mode the *Module* follows the standard [ISO 14443] part 1 and only uses two connections that are physically different and distinct from the connections used in the contact mode. Those electrical connections, LA and LB, are placed on the module backside and are used to connect an external **antenna loop that is not within the cryptographic boundaries of the module**.

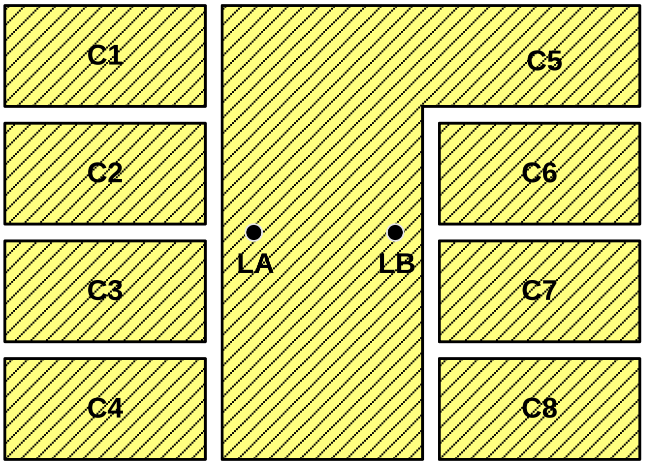


Figure 2 - Contact plate example - Contactless antenna contacts

Contact No.	Description	Logical interface type
LA	LA (Antenna coil connection)	Power In, Data in, Data out, Control IN, Status out ‘FIPS' interfaces
LB	LB (Antenna coil connection)	Power In, Data in, Data out, Control IN, Status out ‘FIPS' interfaces

Table 6 – Contact plate pin list – Contactless mode

1.1.3.2 Condition of uses

The radio frequencies and transmission protocols follow the [ISO 14443] parts 2, 3 and 4. The conditions of use are the following:

Conditions	Range
Type	ISO 14443 Type A and Type B
Supported bit rate	106 Kbits/s, 212 Kbits/s, 424 Kbits/s, 848 Kbits/s, 1.7 Mbit/s for RX and TX 3.4 and 6.8 Mbit/s for TX
Operating field	Between 1.5 A/m and 7.5 A/m rms
Frequency	13.56 MHz +- 7kHz

Table 7 – Voltage and frequency ranges

1.1.3.3 Pictures - Dual Mode and Contactless Mode only

In Dual mode the properties of both Contact mode and Contactless mode apply. The dual mode module has contact points for both types of signals. In Contactless Mode only, the top of the module does not have a contact plate.

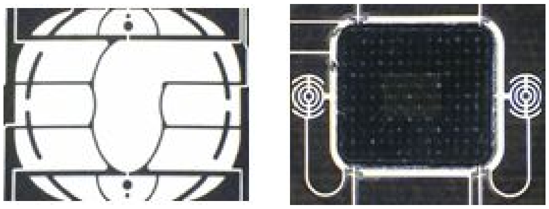
World Combi Thermal black resin process, contact and contactless technology

Module design and thermal black resin technology

Figure 3 – Dual mode example – World Combi module

Figure 4 – Contactless only example – Top of World Combi module

1.2 Firmware and Logical Cryptographic Boundary

Figure 5 depicts the Module operational environment and applets.

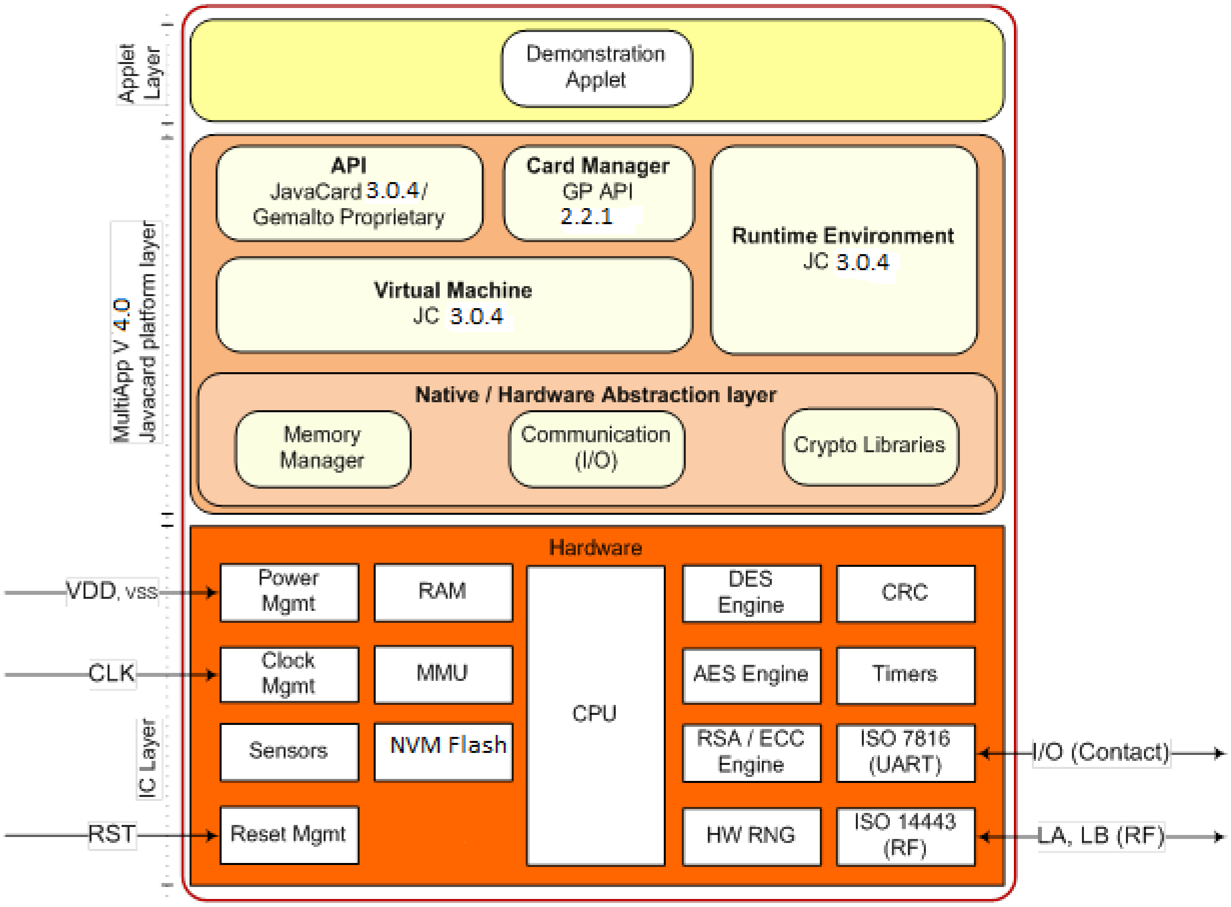


Figure 5 – Module Block Diagram

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:

- SLE78CFX4000PH
- SLE78CFX3000PH
- SLE78CLFX400VPH
- SLE78CLFX300VPH
- SLE78CLFX4000PH
- SLE78CLFX3000PH

Firmware: MultiApp V4.0, Demonstration Applet version V9.1

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 and tag 9F7F). The *Module* responds with a multi-byte data set; refer to Tables 8 and 9 below for additional information. Refer to Table 10 below for optional cryptographic algorithm settings; if an option is called without first being enabled, a status word of 0x9103 will be output by the Module.

Note that “X” entries in Tables 8 and 10 indicate the value can vary and does not have significant meaning.

Name	Length	Description	Value
Gemalto Family Name	1	Java Card	B0h
Gemalto OS name	1	MultiApp	85h
Gemalto Mask Number	1	MultiappV4	55h
Gemalto Product Name	1	MultiappV4	52h
Flow id Version	1	V0.1	01h
Filter set	1	No filter	00h
Chip Manufacturer	2	Infineon	4090h
Chip Identifier	2	Identifier	7897(SLE78CLFX400VPHM)
BPU	2	BPU configuration	7901 (SLE78CLFX400VPH) 7902 (SLE78CLFX300VPH) 7818 (SLE78CLFX4000PH) 7819 (SLE78CLFX3000PH) 7881 (SLE78CFX4000PH) 7874 (SLE78CFX3000PH)
PDM Technical Product Identifier	3	--	XXXXXX
PDM Customer Item Identifier	3	--	XXXXXX
Feature FLag – Crypto Config	2	--	XXXX
Feature Flag – Feature Config	1	--	XX
Feature Flag – Following features	1	--	XX
Platform Certificates	1	--	Bit 8 :FIPS Configuration
APPLI CERTIFICATES byte 1	1	--	XX
APPLI CERTIFICATES byte 2	1	--	00h

Table 8 – GET DATA command with Tag 0103

Name	Length	Description	Value
IC Fabricator	2	Chip fabricator	4090
IC Type	2	Chip model number	7897 (SLE78CLFX400VPHM)
Operating system identifier	2	OS developer	1291 (Gemalto)
Operating system release date	2	Date of OS release	6153 (2016/05/19)
Operating system release level	2	OS release version	0400 (4.0)

Table 9 – First 10 bytes of GET DATA command with Tag 9F7F

Description	b8	b7	b6	b5	b4	b3	b2	b1
Crypto flags value (MSB)								
ECC enabled (ECDSA and ECDH)								1
Features	b8	b7	b6	b5	b4	b3	b2	b1
Crypto flags value (LSB)								
RSA Key/Cipher/Signature enabled up to RSA 2k for public, private standard and private CRT								1
RSA OBKG enabled				1				
RSA 4k enabled (only applicable if RSA enabled), the extension is only available for public and private CRT keys		1						

Table 10 – Optional Settings

Cryptographic functionality

The Module operating system implements the *FIPS Approved and Non-Approved but Allowed* cryptographic function listed in Tables 11 and 12 below:

Algorithm	Description	Cert. #
AES	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128-, 192- and 256-bit key lengths with ECB and CBC modes.	4457
AES CMAC	[SP 800-38D] The Module supports 128-, 192- and 256-bit key lengths.	4457
CKG	[SP800-133] The Module uses unmodified SP 800-90A DRBG output for symmetric key and asymmetric seed generation.	Vendor Affirmed
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.	1165

CVL (RSADP)	[SP 800-56B] RSA key decryption primitive using 2048-bit keys.	1171
CVL (RSACRTDP)	[SP 800-56B] RSA CRT key decryption primitive using 2048-bit keys.	1172
CVL (RSASP1)	[FIPS 186-4] [PKCS#1 v2.1] RSA signature generation primitive using 2048-bit keys.	1166
CVL (RSACRTSP1)	[FIPS 186-4] [PKCS#1 v2.1] RSA CRT signature generation primitive using 2048-bit keys.	1167
DRBG	[SP 800-90A] Deterministic Random Bits Generator (CTR-DRBG based on AES)	1444
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). *Note: ECDSA P-192 signature verification is allowed for legacy-use only	1086
KBKDF	[SP 800-108] The Module supports 128-, 192- and 256-bit key lengths	128
KTS	[SP 800-38F] Use of approved AES and AES CMAC for key wrapping, in accordance with SP 800-38F §3.1 ¶3.	4457
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) *Note: RSA 1024 signature verification is allowed for legacy-use only	2435
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). *Note: RSA CRT 1024 signature verification is allowed for legacy-use only	2436
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. *Note: Use of SHA-1 in a signature verification algorithm is allowed for legacy-use only	3670
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. The module restricts the maximum number of same-key Triple-DES encryptions to 2,000,000.	2394
Triple-DES MAC	[FIPS 113] Triple DES Message Authentication Code. Vendor affirmed, based on validated Triple DES.	2394

Table 11 – FIPS Approved Cryptographic Functions

Algorithm	Description
AES Key Unwrap	AES key unwrapping, allowed per IG D.9. Key establishment methodology provides 128 bits of encryption strength.
NDRNG	True Random Number Generator.

Table 12 – FIPS Non-Approved but Allowed Cryptographic Functions

1.4 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.

Key	Description / Usage
OS-DRBG-EI	256 bits of full entropy used to instantiate the SP 800-90A DRBG.
OS-DRBG-STATE	16-byte AES state V and 16-byte AES key used in the [SP800-90A] CTR DRBG implementation.
OS-GLOBALPIN	4 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.
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.
DM-TOKEN-SYM	AES-128/192/256 (SCP03) Delegate Management Token Symmetric key
DM-RECEIPT-SYM	AES-128/192/256 (SCP03) Delegate Management Receipt Symmetric key

Table 13 – Platform Critical Security Parameters

Key	Description / Usage
DEM-EDK	AES-128/192/256 or 3-Key Triple-DES encryption / decryption key used by the Demonstration Applet *Symmetric Cipher* service.
DEM-AUTH	AES-128 CMAC key used by the Demonstration Applet *to authenticate* wrapped keys.
DEM-KAP-PRI	P-224, P-256, P-384, P-521 ECDSA private key used by the Demonstration Applet *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 Asymmetric Key Pair* service.
DEM-MAC	AES-128/192/256 CMAC or 3-Key Triple-DES MAC key used by Demonstration Applet *Message Authentication* service.
DEM-MK	AES-128 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 Asymmetric Signature service.

Table 14 – Demo Applet Critical Security Parameters

The provided demonstration applet enforces the restrictions of algorithms, modes, and key sizes per NIST SP 800-131A Revision 1.

1.5 Public Keys

Key	Description / Usage
DAP-ASYM	2048-bit RSA Data Authentication Pattern Asymmetric key, used to verify package loading process.
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.
DM-TOKEN-ASYM	2048-bit RSA Delegate Management Token Asymmetric key

Table 15 – Public Keys

2. 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 15 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 16 – Roles supported by the Module

2.1 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)

2.2 Demonstration applet Authentication Method

This authentication method compares a PIN value sent to the Module over an encrypted channel to the stored OS-GLOBALPIN value; 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 4 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 1/256^4.
- 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 15/256^4.

2.3 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 17 – 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 and ECDSA digital signature generation and verification.	-	X
Generate Key Pair	Demonstrate RSA and ECDSA key generation	-	X
Key Agreement	Demonstrate Approved IFC and EC Diffie-Hellman key agreement primitives.	-	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
Verify PIN	Demonstration applet authentication method	-	X

Table 18 – Authenticated Services

The provided demonstration applet enforces the restrictions of algorithms, modes, and key sizes per NIST SP 800-131A Revision 1.

	Keys and CSPs																						
Service	OS-DRBG-EI	OS-DRBG-STATE	OS-GLOBALPIN	OS-MKDK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	DAP-SYM	DAP-ASYM	DM-TOKEN-SYM	DM-RECEIPT-SYM	DEM-EDK	DEM-MAC	DEM-SGV-PRI	DEM-KGS-PRI	DEM-KAP-PRI	DEM-MK	DEM-KAP-PUB	DEM-KGS-PUB	DEM-SGV-PUB	DM-TOKEN-ASYM
Module Reset	E W	Z E G W	--	--	--	--	--	Z	Z	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Module Info (Unauth)	--	--	--	--	--	--	--	E[1]	E[1]	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Context	--	--	--	--	--	--	--	Z	Z	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure Channel	--	E W	--	--	E	E	E	G E[1]	G E[1]	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Manage Content	--	--	W	--	W	W	W	E[1]	E[1]	E W	EW	E W	E W	--	--	--	--	--	--	--	--	--	E W
Lifecycle	Z	Z	Z	Z	Z	Z	Z	--	--	Z	Z	Z	Z	Z	--	Z	Z	Z	Z	Z	Z	Z	Z
Module Info (Auth)	--	--	--	--	--	--	--	E[1]	E[1]	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Symmetric Cipher	--	--	E	--	--	--	--	--	--	--	--	--	--	E R W Z	--	--	--	--	E	--	--	--	--
Message Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E W Z	--	--	--	--	--	--	--	--
Digital Signature	--	E W	E	--	--	--	--	--	--	--	--	--	--	--	--	E R W Z	--	--	E	--	--	E R W Z	--

[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.

	Keys and CSPs																						
Service	**OS-DRBG-EI**	**OS-DRBG-STATE**	**OS-GLOBALPIN**	**OS-MKDK**	**SD-KENC**	**SD-KMAC**	**SD-KDEK**	**SD-SENC**	**SD-SMAC**	**DAP-SYM**	**DAP-ASYM**	**DM-TOKEN-SYM**	**DM-RECEIPT-SYM**	**DEM-EDK**	**DEM-MAC**	**DEM-SGV-PRI**	**DEM-KGS-PRI**	**DEM-KAP-PRI**	**DEM-MK**	**DEM-KAP-PUB**	**DEM-KGS-PUB**	**DEM-SGV-PUB**	**DM-TOKEN-ASYM**
Generate Key Pair	--	E W	E	--	--	--	--	--	--	--	--	--	--	--	--	--	G E R W Z	--	E	- -	G E R W Z	- -	--
Key Agreement Primitives	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E R W Z	E	E R W Z	--	--	--
Verify PIN	--	--	R	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Table 19 – Key and 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.

3. Self-test

3.1 Power-on Self-test

On power on or reset, the *Module* performs self-tests described in Table 20. 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 NVM (Flash memory)..
DRBG	Performs SP800-90A Health tests (Instantiate and Generate) [2].
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.

Test Target	Description
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 20 – Power-On Self-Test

3.2 Conditional Self-tests

- On every call to the [SP800-90A] CTR DBRG [2], 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-SMAC key. Optionally, the Module may also:

  - verify a MAC or signature [3] of the new firmware (applet) using the DAP-SYM or DAP_ASYM key respectively. The signature or MAC block in this scenario is generated by an external entity using the key corresponding to the asymmetric key DAP-ASYM or the secret key DAP-SYM.

[2] Note that the DRBG reseed function is not implemented in this module; the DRBG is seeded only once from the NDRNG each power cycle. A reseed Health test is not applicable, and per IG 9.8 a CRNGT is not required to be implemented on the output of the NDRNG.

[3] Note that RSA and RSA CRT share the same implementation of signature verification, and therefore both Certs. #2435 and #2436 are used any time signature verification is performed.

4. 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 7 below.

5. 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.

6. 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.

7. 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

8. 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