NXP Semiconductors
JCOP 3 SecID P60 CS (OSB)

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Document Version: 1.2
Date: 3/29/2018

Table of Contents

List of Tables

List of Figures

References

Table 1: References

Acronym	Full Specification Name
References used in Approved Algorithms Table	
[38A]	NIST, Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December, 2001
[38B]	NIST, Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May, 2005
[38F]	NIST, Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December, 2012
[56A]	NIST, Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March, 2007
[67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July, 2011
[90A]	NIST, Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January, 2012
[108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, FIPS Publication 108, October, 2009
[113]	NIST, *Computer Data Authentication*, FIPS Publication, May, 1985
[133]	NIST Special Publication SP800-133, *Recommendation for Cryptographic Key Generation*, December 2012
[180]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March, 2012
[186]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001

Other References	
[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 -- Confidential Card Content Management -- Card Specification 2.2 -- Amendment A*, January 2011 *GlobalPlatform Consortium: GlobalPlatform Card Technology -- Contactless Services -- Card Specification v2.2 -- Amendment C*, July 2014 GlobalPlatform Consortium: GlobalPlatform Card Technology -- Secure Channel Protocol '03' – Card Specification v2.2 – Amendment D, May 2009
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated May 10, 2017
[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*

Other References	
	ISO/IEC 7816-4:2013 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange* ISO/IEC 7816-6:2016 *Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange* ISO/IEC 7816-8:2016 *Identification cards -- Integrated circuit cards – Part 8: Commands and mechanisms for security operations* ISO/IEC 7816-12:2005 *Identification cards -- Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures* ISO/IEC 7816-15:2016 *Identification cards – Integrated circuit cards – Part 15: Cryptographic Information application*
[ISO 14443]	ISO/IEC 14443-3:2016 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision* ISO/IEC 14443-4:2016 *Identification cards -- Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol*
[JavaCard]	*Java Card 3.0.5 Runtime Environment (JCRE) Specification*, *May 2015* *Java Card 3.0.5 Virtual Machine (JCVM) Specification*, *May 2015* *Java Card 3.0.5 Application Programming Interface* Published by Oracle
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, November 2015
[DTR]	NIST, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, January 2011

Acronyms and Definitions

Table 2: Acronyms and Definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CNRNGT	Continuous random Number Generator Test, see [DTR] AS09.42
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	GlobalPlatform
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 GlobalPlatform)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis
TPDU	Transaction Protocol Data Unit, see [ISO 7816]

1 Overview

This document defines the Security Policy for the NXP Semiconductors JCOP 3 SecID P60 CS (OSB) cryptographic module, hereafter denoted *the Module*. The Module, validated to FIPS 140-2 overall Level 3, is a single chip module implementing the Global Platform operational environment, with a Card Manager and an application, the FIPS_Applet v1.0.

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 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:

Table 3: Security Level of Security Requirements

Security Requirement	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

1.1 Versions, Configurations and Modes of Operation

The JCOP3 OSB component can be identified by using the IDENTIFY APDU command. This command returns the card identification data, which includes a Platform ID, a Patch ID and other information that allows the identification of the content in ROM, EEPROM and loaded patches (if any). The Platform ID is a data string that allows the identification of the JCOP3 OSB component.

The Module is available in two configurations:

Product Identifier	EEPROM	Interface	Hardware Version	Firmware Version
J2H145C0019790400	80 kByte	Contact	P6022y VB	19790400
J3H145C0019790400	144 kByte	Dual		

Table 4: Module Configurations and versions

The variations in EEPROM size and interface support are achieved by enabling or disabling the features on a common die design, permanently set at the factory during a fabrication step.

The “identify” command is formatted as follow:

Code	Value	Parameter settings
CLA	‘80’	GlobalPlatform
INS	‘CA’	GET DATA (IDENTIFY) - ISD
P1	‘00’	High order tag value
P2	‘FE’	Low order tag value - proprietary data
Lc	‘02’	Length of data field
Data	‘DF28’	Module identification data
Le	‘00’	Length of response data

Table 5: APDU command

The command answers the content of the DF28 file. The firmware version is located at the tag ‘03’, the value is 4AXX48YYYYYY30303139373930343030 (JxHyyy0019790400 in ASCII, where x and yyy identify the configuration and “19790400” the firmware version).

To verify that the Module runs in the Approved mode of operation, use the context service to select the card Manager and the *Info* service (GET DATA APDU, tag ‘88’) to verify the field shown in Table 6 below:

Data Element	Length	Value
FIPS Compliance	2	‘xxxx’ (where ‘A5F0’ or ‘3BC4’ is FIPS DISABLED. Any other value is FIPS ENABLED)

Table 6: FIPS mode indicator

The FIPS_Applet always runs in an Approved mode of operation.

The personalized product shall have the applet identification:

- Package ID: A00000000001H
- Applet ID: A0000000000101H
- Instance ID: A0000000000101H

The certified configuration of the product identified here has exactly one applet instance: the FIPS_Applet applet instance. No other applet instance is allowed. The presence of another applet instance put the product outside of the certified configuration.

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 [ISO 7816] and [ISO 14443] card readers as input/output devices.

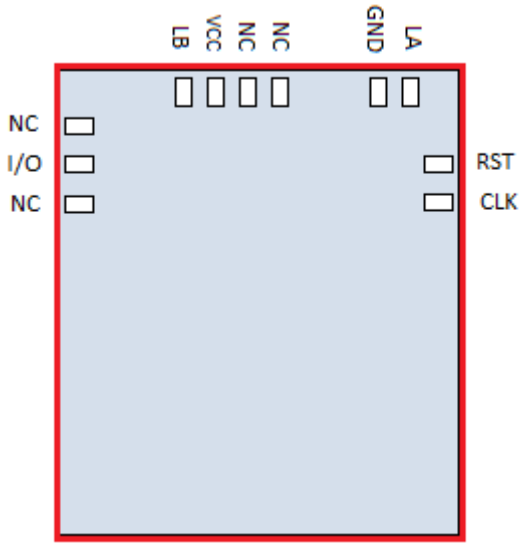

Figure 1: NXP Semiconductors JCOP 3 SecID P60 CS (OSB): Physical Form

Table 7: Ports and Interfaces

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

Table 8: Ports and Interfaces

In the table above, an “X” in the C column indicates the port is active in the Contact mode; an “X” in the D column indicates the port is active in the Dual interface (Contact and contactless) mode.

1.3 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

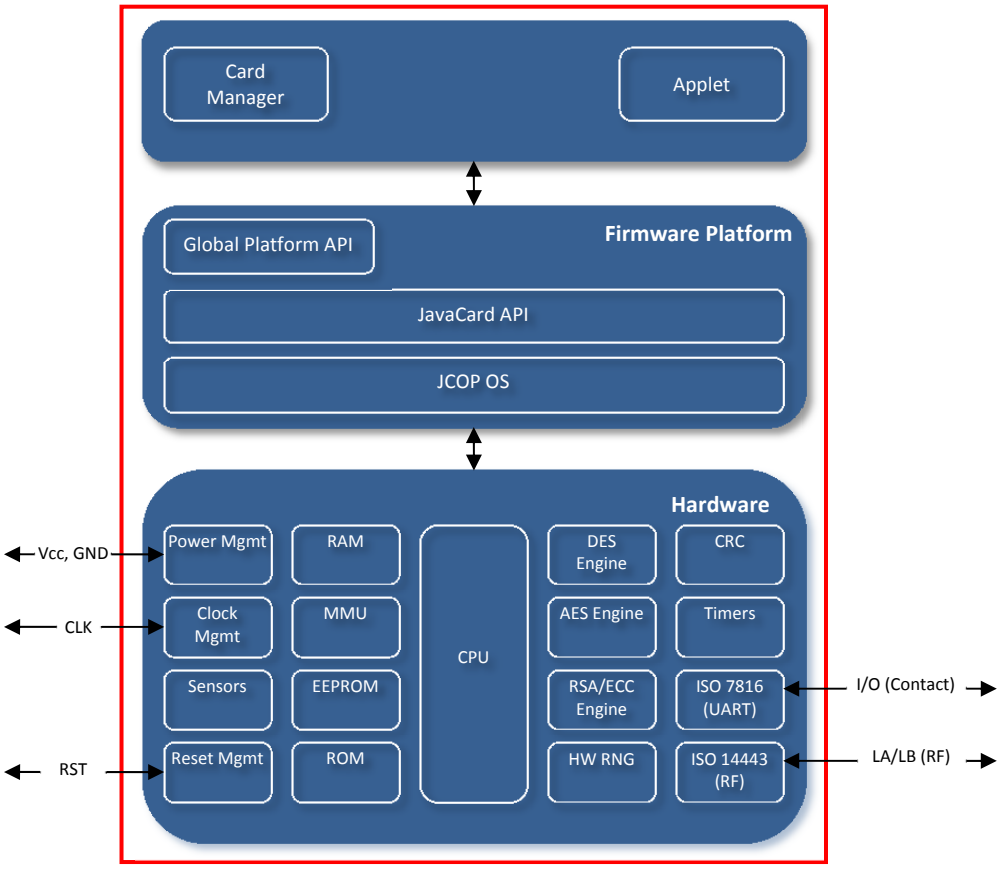

Figure 2: Module Block Diagram

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).
The product is delivered personalized with a defined PIN and Secure Messaging Key. Those are set during wafer test operation before product's delivery to customer.

2 Cryptographic Functionality

The module implements the Approved and Allowed cryptographic functions listed below.

CAVP Cert	List	Standard	Mode/ Method	Strength[1]	Use
4812	AES	[197], [38A]	CBC, ECB	128, 192, 256	Data Encryption/ Decryption
4812	AES CMAC	[197], [38B]	CMAC	128, 192, 256	Message Authentication; SP 800-108 KDF
Vendor Affirmed	CKG	[133]	N/A	128, 192, 256	Vendor Affirmed, Key Generation based on unmodified output of the DRBG cert. # 1187
824	CVL	[56A]	ECC CDH Primitive	P-224, P-256, P-384, P-521	Shared Secret Computation
1187	DRBG	[90A]	Hash_DRBG	256	Deterministic Random Bit Generation
890	ECDSA	[186]	P-224, P-256, P-384, P-521		ECC Key Generation
			P-224: (SHA-224), P-256: (SHA-256), P-384: (SHA-384), P-521: (SHA-512)		Digital Signature Generation
			P-192: (SHA-1)[2], P-224: (SHA-224), P-256: (SHA-256), P-384: (SHA-384), P-521: (SHA-512)		Digital Signature Verification
91	KBKDF	[108]	CTR	128, 192, 256	Deriving keys from existing keys
4812	KTS	[38F]	AES/CMAC	128, 192, 256	Meets the SP 800-38F §3.1 ¶3 requirements for symmetric key wrapping, using Cert. #4812 AES and AES CMAC. Key establishment methodology provides between 128 and 256 bits of encryption strength.
2086	RSA	[186]	n=2048, 3072		RSA key generation
2053	RSA	[186]	n=2048, 3072, SHA-(224, 256, 384, 512)		Digital signature generation and verification
			n=1024[2], 2048, 3072 SHA-(1[2], 224, 256, 384, 512[3])		Digital signature verification
3299	SHS	[180]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest generation
2547	Triple-DES[4]	[67]	CBC, ECB	3-Key (112)	Data encryption, decryption

Table 9: Approved Algorithms

Note that CKG requirement is met for direct output from DRBG used for symmetric keys.

[1] Strength indicates DRBG Strength, Key Lengths, Curves or Moduli
[2] This algorithms is Approved for legacy use
[3] The SHA-512 is not available for 1024-bit RSA signature verification
[4] The same Triple-DES key shall not be used to encrypt or decrypt more than 2^{16} 64-bit blocs per IG A.13.

Algorithm	Description
NDRNG	Hardware NDRNG; used as entropy input (384 bits) to the FIPS approved (Cert. #1187) DRBG. The non-deterministic hardware RNG outputs 8 bits per access, buffered by the device driver, which performs the continuous RNG test when a 32-bit value is available.

Table 10: Non-Approved but Allowed Cryptographic Functions

2.1 Critical Security Parameters and Public Keys

All CSPs used by the Module are described in this section. All usage of these CSPs is described in the services detailed in Section 3.3. In the tables below, the following prefixes are used:

- OS prefix denotes operating system.
- SD prefix denotes a GlobalPlatform Security Domain.
- DAP prefix denotes the GlobalPlatform Data Authentication Protocol.
- APP prefix denotes an Applet CSP or a Public Key.

CSP	Description/Usage
	Card Manager
OS-DRBG-EI	384-bit NDRNG entropy input to Hash_DRBG.
OS-DRBG-STATE	880-bit value; the current DRBG state.
OS-MKEK	AES-128/192/256 key used to encrypt all secret and private key data stored in NVM.
SD-KENC	AES (128-bit, 192-bit, 256-bit) Master key used to derive SD-SENC.
SD-KMAC	AES (128-bit, 192-bit, 256-bit) Master key used to derive SD-SMAC.
SD-KDEK	AES (128-bit, 192-bit, 256-bit) Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES (128-bit, 192-bit, 256-bit) Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to verify inbound secure channel data integrity.
SD-RMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to generate response secure channel data MAC.
	Applet
APP-SC-KENC	AES (256-bit) encryption key used to encrypt / decrypt secure channel data.
APP-SC-KMAC	AES (256-bit) MAC key used to verify inbound secure channel data integrity.
APP-DES	3-Key Triple-DES key used by Symmetric cipher
APP-AES	AES (128, 192 or 256) key used by Symmetric cipher.
APP-RSA	RSA (n=2048, n=3072) private key used by Digital signature service.
APP-ECDSA	ECDSA (P-224, P-256, P-384, P-521) private key used by Digital signature service.
APP-ECSSG	ECC CDH (P-224, P-256, P-384, P-521) private key used for testing the shared secret generation
APP-PIN	Application PIN for user authentication

Table 11: Critical Security Parameters

Public Key	Description/Usage
	Card Manager
DAP-PUB	RSA (2048-bit) new firmware signature verification key.
	Applet
APP-RSAPUB	RSA public key of size 1024, 2048, or 3072 for testing RSA key generation and RSA encryption
APP-ECDSAPUB	ECDSA (P-192, P-224, P-256, P-384, P-521) public key for testing ECDSA signatures
APP-ECDHPUB	ECC CDH (P-224, P-256, P-384, P-521) public key, used to generate a shared secret

Table 12: 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-KDEK), is stored in plaintext and is only accessible by authenticated services.

Table 13 lists all operator roles supported by the Module.

Role ID	Role Description
CO	Cryptographic Officer – 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	The Card Holder (applet user) – performs FIPS approved cryptographic operations. Authenticated as described in *PIN authentication method*.

Table 13: 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)

This authentication method includes a counter of failed authentication called “velocity checking” by GlobalPlatform. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication.

The Module enforces a maximum of 80 failed SCP authentication attempts before blocking the card. The probability that a random attempt will succeed over a one minute interval is:

- 80/2^128 = 2.4E-37 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

3.2 PIN authentication method

The PIN verification method is used to authenticate a user at the applet level. The user must enter his PIN and call the VERIFY_PIN command.
The PIN value is set during pre-personalization of the product, before product delivery.
The probability that a random attempt will succeed using this authentication method is:

- 1/2^48 = 3.5E-15 (for any of 48-bits PIN)

The Module enforces a maximum of three (3) failed PIN based authentication attempts. The probability that a random attempt will succeed over a one-minute interval is:

- 3/2^48 = 1.1E-14 (for any of 48-bits PIN)

If the user fails to authenticate, the card state is set to “Terminated” (card is blocked and not useable) and all cryptographic objects are zeroized.

3.3 Services

All services implemented by the Module are listed in the tables below. The *ISD Services* are provided by the module or Card Manager and are available to off card entities. Such services are related to card content management (e.g., applet loading, installation, deletion, card data access or storage) accessed via communication protocols like ISO7816. The *API Services* are available to on card entities, i.e., Java Card applets. These services are typically cryptographic services available via the Java Card API.

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

Table 14: Unauthenticated Services

Service	Description	CO	User
	ISD (OS/Card Manager) Services		
Lifecycle	Modify the card or applet life cycle status.	X	
Manage Content	Load and install application packages and associated keys and data.	X	
Privileged Info	Read module data (privileged data objects, but no CSPs).	X	

Service	Description	CO	User
	ISD (OS/Card Manager) Services		
Secure Channel	Establish and use a secure communications channel.	X	
	Applet Services		
Asymmetric key generation	Trigger OS API for generation of RSA and ECDSA keys.		X
Digital signature	Trigger OS API for ECDSA and RSA signature generation and verification.		X
Secure hash	Trigger OS API for [FIPS 180-4] compliant hash algorithms.		X
Shared secret generation	Trigger OS API for [SP 800-56A] §5.7.1.2 conformant ECC CDH. The Shared Secret Generation service is an EC CDH function demonstrator service. If the shared secret is output, the shared secret is not a CSP and shall not be used to derivate keys.		X
Symmetric cipher	Trigger OS API for AES and Triple-DES encryption and decryption.		X
Verify PIN	Verify the user's PIN (authenticate the user) through the OS OwnerPIN object and associated methods.		X
Open secure messaging	Initialize the OS secure messaging functions and establish a secure messaging channel for communicating with the applet.		X
Import key	Initialize the OS key object with a key value that will be required for Triple-DES, AES, RSA, and/or ECC cryptographic operations.		X
Import domain parameters	Import parameters (initialize the OS Key Object) that will be required and used by further cryptographic commands related to Elliptic Curve.[5]		X

Table 15: Authenticated Services

Table 16 below describes the access to CSPs by service with brief descriptions, which are intended to help readers understand the patterns of access. Explanations are provided in groups of services and/or keys (as best suited to explain the pattern of access), describing those aspects that have commonality across services or keys/CSPs.

Lifecycle: must be used with Secure Channel active (hence SD Session keys are 'E'); zeroizes all keys except session keys when Lifecycle is used for card termination.

OS-MKEK: generated on first power-up of the Module in a manufacturing setting; used whenever any private or secret key is accessed; zeroized on Lifecycle card termination.

OS-DRBG CSPs: OS-DRBG-EI is the NDRNG entropy input to the DRBG instantiation at power-on (Module Reset), zeroized after use. OS-DRBG-STATE is generated at startup (Module Reset), zeroized at shutdown as part of Module Reset, or by LifeCycle card termination. Each 'EW' in the OS-DRBG-STATE column indicates the use of the DRBG to generate keys (or nonces), as the value is used and the state is updated.

Secure Channel Master Keys (SD-KENC, SD-KMAC): 'E' when a secure channel is initialized (GP Secure Channel). May be updated ('W') using the Manage Content service; zeroized by Lifecycle card termination.

[5] It is the operator's responsibility to either use a NIST-Approved parameter as specified in FIPS 186-4 Appendix D or generate the parameter according to FIPS 186-4 Section 6.1.1

SD-KDEK: is used to decrypt CSPs entered into the module during the applet personalization.

Secure Channel Session Keys (SD-SENC, SD-SMAC, SD-RMAC): 'E' for any service that can be used with secure channel active. 'GE' on GP Secure Channel as a consequence of secure channel initialization and usage; however, while the SD-RMAC key is generated by default. 'Z' on Module Reset is a consequence of RAM clearing/garbage collection.

DAP-PUB: is imported into the module at the factory, but may be updated using the Manage Content service. It is used by the Manage Content for signature verification of patch or applet code.

All applet services, with the exception of importation of public domain parameters service, are used with an active secure channel. The Asymmetric key generation service is used for ECC or RSA key generation; public keys are typically output in the service response. The Digital signature service provides ECDSA or RSA signature generation and verification; ECDSA signature generation utilizes a random value. The Shared secret generation provides the SP 800-56A §5.7.1.2 ECC CDH function, using the card private key and the external participant's public key to generate the shared secret. The shared secret is not used by the Module and it can be output from the Module; this service is available for demonstration purpose only. The Symmetric cipher service provides AES and Triple-DES encryption and decryption. The applet keys can be imported with the dedicated service.

Services	**CSPs**																**Public Keys**			
	OS-DRBG-EI	OS-DRBG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	APP-SC-KENC	APP-SC-KMAC	APP-DES	APP-AES	APP-RSA	APP-ECDSA	APP-ECSSG	APP-PIN	DAP-PUB	APP-RSAPUB	APP-ECDSAPUB	APP-ECDHPUB
Unauthenticated Role	*Card Manager*									*Applet*								*CM*	*Applet*		
Card Reset	GEZ	GEWZ	--	--	--	--	Z	Z	Z	--	--	--	--	--	--	Z	--	--	--	--	Z
Context	--	--	--	--	--	--	EZ	EZ	EZ	--	--	--	--	--	--	--	--	--	--	--	--
Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
ISD Role	*Card Manager*									*Applet*								*CM*	*Applet*		
Lifecycle	Z	Z	Z	Z	Z	Z	E	E	E	--	--	--	--	--	--	--	Z	--	--	--	--
Manage Content	Z	Z	Z	WZ	WZ	WZE	E	E	E	WZ	WZ	Z	Z	Z	Z	--	WZ	EZ	Z	Z	--
Privileged Info	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--
Secure Channel	--	--	--	--	--	--	GE	GE	GE	--	--	--	--	--	--	--	--	--	--	--	--
API Role	*Card Manager*									*Applet*								*CM*	*Applet*		
Asymmetric key generation	--	EW	--	--	--	--	--	--	--	E	E	--	--	GW	GW	--	--	--	GWR	GWR	--
Digital signature	--	EW	--	--	--	--	--	--	--	E	E	--	--	E	E	--	--	--	E	E	--
Secure hash	--	--	--	--	--	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--

Services	CSPs																	Public Keys			
	OS-DRBG-EI	OS-DRBG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	APP-SC-KENC	APP-SC-KMAC	APP-DES	APP-AES	APP-RSA	APP-ECDSA	APP-ECSSG	APP-PIN	DAP-PUB	APP-RSAPUB	APP-ECDSAPUB	APP-ECDHPUB
Shared secret generation	--	EW	--	--	--	--	--	--	--	E	E	--	--	--	--	GE	--	--	--	--	GER
Symmetric cipher	--	--	--	--	--	--	--	--	--	E	E	E	E	--	--	--	--	--	--	--	--
PIN Verify	--	--	E	--	--	--	--	--	--	E	E	--	--	--	--	--	R	--	--	--	--
Open secure messaging	--	--	E	--	--	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--
Import key	--	--	--	--	--	--	--	--	--	E	E	W	W	W	W	--	--	--	W	W	--
Import domain parameters	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Table 16: CSPs and Public Keys Access within Services

- 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.

4 Self-test

4.1 Power-On Self-tests

On power-on or reset, the Module performs self-tests as described in Table 17 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
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.
DRBG	Performs a fixed input KAT and all SP 800-90A health test monitoring functions.
ECC CDH	Performs separate ECDSA signature and verify KATs using the P-256 curve.
ECDSA	Performs ECDSA signature and verify KATs using the P-256 curve; this self-test is inclusive of the ECC CDH self-test.
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.
KBKDF	Performs a fixed input KAT on SP 800-108 AES-CMAC based KBKDF.
RSA	Performs separate RSA signature and verify KATs using an RSA 2048-bit key.
SHA-1	Performs a fixed input KAT.
SHA-256	Performs a fixed input KAT (inclusive of SHA-224, per IG 9.4)
SHA-512	Performs a fixed input KAT (inclusive of SHA-384, per IG 9.4).
Triple-DES	Performs encrypt and decrypt KATs using 3-Key Triple-DES in CBC mode.

Table 17: Power-On Self-Test

4.2 Conditional Self-Tests

Test Target	Description
DRBG CRNGT	On every call to the DRBG, the Module performs the AS09.42 continuous RNG test to assure that the output is different than the previous value.
FW Load	When new firmware is loaded into the Module using the LOAD command, the Module verifies the integrity of the new firmware (applet) using RSA Signature Verification with the DAP-PUB public key; the new firmware in this scenario is signed by an external entity using the private key corresponding to DAP-PUB.
Generate PCT	Pairwise consistency test performed when an asymmetric key pair is generated for RSA or ECC.
NDRNG CRNGT	AS09.42 continuous RNG test performed on each 32 bits access from the NDRNG (buffered by the driver) to assure that the output is different than the previous value.
Signature PCT	Pairwise consistency test performed when a signature is generated for RSA or ECDSA.

Table 18: Conditional Self-Tests

5 Physical Security Policy

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques and is protected by 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 *Tamper is detected* error state.

Hardness Testing was conducted at three (3) different temperatures; at nominal temperature (20^{o} C, 68^{o} F), at high temperature (120^{o} C, 248^{o} F), and at low temperature (-40^{o} C, -40^{o} F).

The Module is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging.

6 Mitigation of Other Attacks Policy

The module is protected against SPA, DPA, Timing Analysis and Fault Induction using a combination of firmware and hardware counter-measures. Protection features include detection of out-of-range supply voltages, frequencies or temperatures, and detection of illegal address or instruction. All cryptographic computations and sensitive operations such as PIN comparison provided by the module are designed to be resistant to timing and power analysis. Sensitive operations are performed in constant time, regardless of the execution context (parameters, keys, etc.), owing to a combination of hardware and firmware features.

7 Security Rules and Guidance

The Module implementation also enforces the following security rules:

- The Module does not output CSPs (plaintext or encrypted).
- The Module does not support manual key entry.
- The Module does not output intermediate key values.
- 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 CSPs are zeroized by the zeroization service.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.