NXP Semiconductors

JCOP 3 SecID P60 OSA

FIPS 140-2 Cryptographic Module

Non-Proprietary Security Policy

Version: 1.2
Date: 11/14/2017

Table of Contents

List of Tables

List of Figures

References

Acronym	Full Specification Name
Approved Algorithm References	
[108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions*, October 2009.
[180]	NIST, *Secure Hash Standard (SHS)*, FIPS Publication 180-4, August 2015.
[186]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013.
[197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[38A]	NIST, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.
[38B]	NIST, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.
[38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012.
[56A]	NIST, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, Revision 2, May 2013.
[67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[90A]	NIST, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Revision 1, June 2015.
Other References	
[Annex_A]	NIST, *Approved Security Functions*, September 2015.
[Annex_C]	NIST, *Approved Random Number Generators*, February 2012.
[Annex_D]	NIST, Approved Key Establishment Techniques, October, 2014.
[DTR]	NIST, *Derived Test Requirements [DTR] for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, January 2011.
[FIPS140]	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
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, December 28 2015.
[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
[PKCS#1]	PKCS #1 (IETF RFC3447): *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*, February 2003.
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, November 2015.

Table 1: References

Acronyms and definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CRNGT	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	Global Platform
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
JCOP	JavaCard Open Platform
KAT	Known Answer Test
NDRNG	Non-deterministic random number generator
NVM	Non-Volatile Memory (e.g. EEPROM, Flash)
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]

Table 2: Acronyms and Definitions

1 Introduction

This document defines the Security Policy for the NXP Semiconductors JCOP 3 SecID P60 (OSA) 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 the Card Manager.

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

The Module is available in four configurations:

Product Identifier	EEPROM	Interface	HW Version	FW Version
J2H082000586400	80 kByte	Contact	P6022y VB	0503.8211
J2H145000586400	80 kByte	Dual		
J3H082000586400	144 kByte	Contact		
J3H145000586400	144 kByte	Dual		

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.

To verify the version of the firmware, use the context service to select the card Manager and the *Info* service (GET DATA APDU, tag '9F7F') to verify the fields shown next.

Data Element	Length	Value	Associated Version
IC fabricator	2	0x4790	NXP P6022y VB
IC type	2	0x0503	Firmware Version Part 1
Operating system identifier	2	0x8211	Firmware Version Part 2
Operating system release date	2	0x6057	Firmware release date
Operating system release level	2	0x0002	Firmware release level (the first byte is the patch level)

Table 4: Product version indicator

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 5 below

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

Table 5: FIPS mode indicator

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 surfaces and edges of the integrated circuit die and the associated bond pads. The cross-hatching indicates the presence of active 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 compliant card readers as input/output devices.

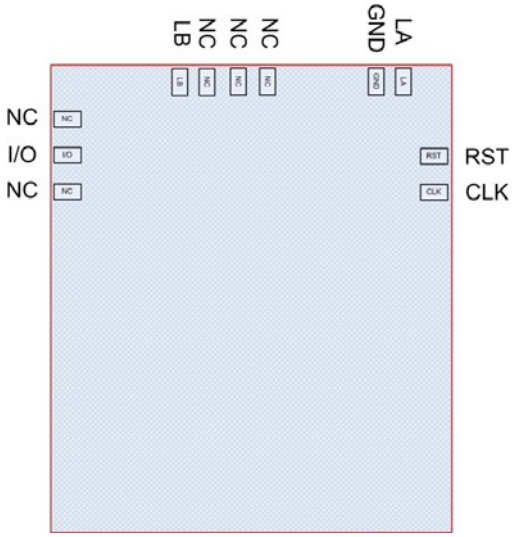

Figure 1: NXP Semiconductors P6022y VB

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 6: 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.

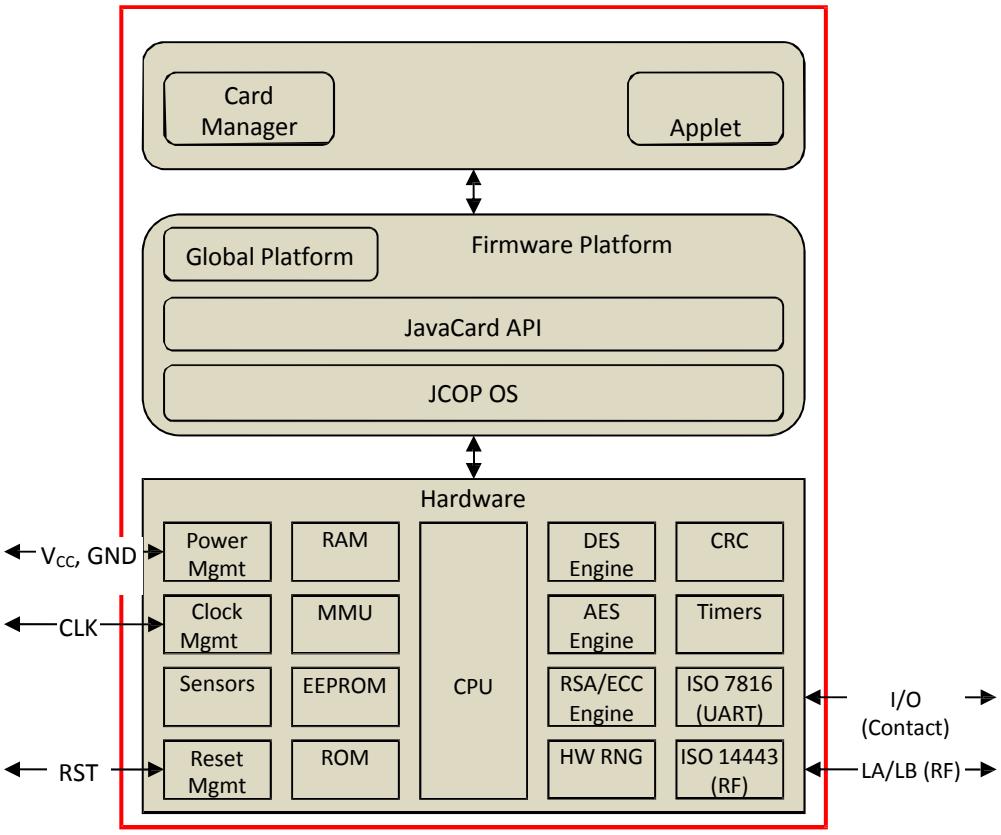

Figure 2: Module Block Diagram

2 Cryptographic Functionality

The Module implements the Approved and Non-Approved but Allowed cryptographic functions listed in Table 7 and Table 8 below.

CAVP	Algorithm	Mode/Method	Strength[1]	Usage
3997	AES [197], [38A] [38B]	CBC, ECB CMAC	128, 192, 256	Data encryption and decryption CMAC generation and verification
3997	KTS [38F]	AES/AES-CMAC	(128, 192, 256)	Meets the SP 800-38F §3.1 ¶3 requirements for symmetric key wrapping, using Cert. #3397 AES and AES CMAC.
824	ECC CDH [56A]	P-224, P-256, P-384, P-521		Shared secret generation
1187	DRBG [90A]	Hash_DRBG	256	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-521: (SHA-512)		Digital signature generation
		P-192: (SHA-1) P-224: (SHA-224) P-256: (SHA-256) P-521: (SHA-512)		Digital signature verification
91	KBKDF [108]	CTR	128, 192, 256	Key derivation
2086	RSA [186]		n=2048, {n=3072}	Key generation
2053	RSA [186]	n=2048 SHA(224,256,384,512)		Digital signature generation
		n=2048 SHA(1,224,256,384,512) {n=1024 SHA(1,224,256,384) }		Digital signature verification
3299	SHS [180]	SHA-1, SHA-2 (224, 256, 384, 512)		Message digest generation
2195	Triple-DES [67]	TCBC, TECB	3-Key (112)	Data encryption, decryption
VA[2]	Triple-DES MAC [113]		3-Key (112)	MAC generation, verification.

Table 7: Approved algorithms

References to standards are given in square bracket [ ]; see the References table.
Items in curly brackets { } are CAVP tested but not used by the module.

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 8: Non-Approved but Allowed Cryptographic Functions

[1] "Strength" indicates DRBG Strength, Key Lengths, Curves or Moduli
[2] Vendor Affirmed, using Cert. #2195 primitives

2.1 Critical Security Parameters and Public Keys

All CSPs used by the Module are described in this section. All usages 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 APP prefix denotes an Applet CSP.

Name	Description and usage
Card Manager CSPs	
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 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 generate SD-SENC.
SD-KMAC	AES (128-bit, 192-bit, 256-bit) Master key used to generate 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.
API CSPs	
APP-DES	3-Key Triple-DES key used by *Symmetric cipher* and *Authentication* (Triple-DES MAC).
APP-AES	AES (128, 192 or 256) key used by *Symmetric cipher* and *Authentication* (AES CMAC).
APP-RSA	RSA (n=2048) private key, potentially generated by the *Asymmetric key generation* service, used by *Digital signature* service.
APP-ECDSA	ECDSA (P-224, P-256, P-384, P-521) private key, generated by the *Asymmetric key generation* service, used by *Digital signature* service.
APP-ECSSG	ECDH private key for testing ECC CDH shared secret generation

Table 9: Critical Security Parameters

Public Keys	
Name	Description and usage
DAP-PUB	RSA-2048 -or ECDSA P-256 new firmware signature verification key.
APP-RSAPUB	RSA public key of size 2048, 3072 or 4096 for testing RSA key generation and RSA encryption
APP-ECDSAPUB	ECDSA public key for testing ECDSA signatures
APP-ECDHPUB	ECDSA public key for testing ECC CDH shared secret generation

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 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 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	The Applet Developer User - Considered an internal, privileged user of the platform. Entities in this role create and deploy smart card applets that utilize JavaCard APIs as the only means of communicating with OS internals. The Applet Developer User is in charge of installing and managing their own applications in their respective Application Provider Security Domain (APSD) on the card. Authenticated as described in *Secure Channel Protocol 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)

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 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	CO	User
Card Reset	Power cycle or reset the Module. Includes Power-On Self-Test.	Not authenticated	
Context	Select an applet or manage logical channels.		
Framework	API: Math, string, command parsing and utilities		
Info	Read unprivileged data objects, e.g. module configuration or status information.		
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	
Secure Channel	Establish and use a secure communications channel.	X	X
API Services			
Asymmetric key generation	API for generation of RSA and ECDSA keys.		X
Authentication	API for AES CMAC and Triple-DES MAC generation and verification.		X
Digital signature	API for ECDSA and RSA signature generation and verification.		X
Random bit generation	API for [SP 800-90A] conformant random number generation.		X
Secure hash	API for [FIPS 180-4] compliant hash algorithms.		X
Shared secret generation	API for [SP 800-56A] §5.7.1.2 conformant ECC CDH.		X
Symmetric cipher	API for AES and Triple-DES encryption and decryption.		X
Symmetric key generation	API for generation of AES and Triple-DES keys.		X

Table 12: Services

Table 13 below describes the access to CSPs by service with brief descriptions next 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 first 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, PKI Applet Secure Channel, TWNID Applet GP Secure Channel). May be updated ('W') using the Manage Content service; zeroized by Lifecycle card termination. SD-KDEK is used to decrypt CSPs entered into the module.

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, PKI Applet Secure Channel and TWNID Applet GP Secure Channel as a consequence of secure channel initialization and usage; however, while the SD-RMAC key is generated by default, the PKI Applet Secure Channel and TWNID Applet GP Secure Channel services do not use it). '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 API services may potentially be 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 Authentication service provides AES CMAC or Triple-DES MAC generation and verification, with access to the corresponding secret key. 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 local private key and the external participant's public key to generate the shared secret. The Symmetric cipher service provides AES and Triple-DES encryption and decryption. The symmetric key generation service provides generation of AES or Triple-DES keys.

Service	CSPs														Public Keys			
	OS-DRBG-EI	OS-DRBG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	APP-DES	APP-AES	APP-RSA	APP-ECDSA	APP-ECSSG	DAP-PUB	APP-RSAPUB	APP-ECDSAPUB	APP-ECDHPUB
Unauthenticated Services																		
Card Reset	GE Z	GE WZ	--	--	--	--	Z	Z	Z	--	--	--	--	--	--	--	--	--
Context	--	--	--	--	--	--	EZ	EZ	EZ	--	--	--	--	--	--	--	--	--
Framework	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Info																		
ISD Services																		
Lifecycle	Z	Z	Z	Z	Z	Z	E	E	E	--	--	--	--	--	--	--	--	--
Manage Content	Z	Z	Z	WZ	WZ	WZ	E	E	E	Z	Z	Z	Z	Z	EZ	Z	Z	Z
Privileged Info	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--
Secure Channel	--	--	--	--	--	--	GE	GE	GE	--	--	--	--	--	--	--	--	--
API Services																		
Asymmetric key generation	--	EW	E	--	--	--	E	E	E	--	--	G	G	G	--	GR	GR	--
Authentication	--	--	E	--	--	--	E	E	E	E	E	--	--	--	--	--	--	--
Digital signature	--	EW	E	--	--	--	E	E	E	--	--	E	E	--	--	--	--	--
Random bit generation	--	EW	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--
Secure hash	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--
Shared secret generation	--	--	E	--	--	--	E	E	E	--	--	--	--	E	--	--	--	WE
Symmetric cipher	--	--	E	--	--	--	E	E	E	E	E	--	--	--	--	--	--	--
Symmetric key generation	--	EW	E	--	--	--	E	E	E	G	G	--	--	--	--	--	--	--

Table 13: Service Access to CSPs

- 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 (overwrite of 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 14 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	Cert. #	Description
AES	3997	Performs separate encrypt and decrypt KATs using an AES-128 key in CBC mode.
AES CMAC	3997	Performs AES CMAC generate and verify KATs using an AES-128 key.
DRBG	1187	Performs a fixed input KAT and all SP 800-90A health test monitoring functions.
ECC CDH	CVL 824	Performs an ECC CDH KAT using the ECC P-256 curve.
ECDSA	890	Performs separate ECDSA signature and verify KATs using the P-256 curve.
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.
KBKDF	91	Performs a fixed input KAT on SP 800-108 AES CMAC based KBKDF
RSA	2053	Performs separate RSA signature and verify KATs using an RSA 2048-bit key.
SHA-1	3299	Performs a fixed input KAT.
SHA-256	3299	Performs a fixed input KAT (inclusive of SHA-224, per IG 9.4)
SHA-512	3299	Performs a fixed input KAT (inclusive of SHA-384, per IG 9.4).
Triple-DES	2195	Performs encrypt and decrypt KATs using 3-Key Triple-DES in CBC mode.

Table 14: Power-On Self-Tests

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 15: 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.

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

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 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[3], 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.

8 Security Rules and Guidance

The Module implementation 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.

[3] FIPS 140-2 defines EFP in Level 4; in this submission, the platform vendor declined to perform additional testing beyond Level 3 and what was already performed for Common Criteria validation.