NXP Semiconductors
FIPS SE051

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Document Version: 1.2
Date: June 10, 2021

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
[38A]	NIST, Special Publication 800-38A Addendum, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, October, 2010
[38B]	NIST, Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May, 2005
[38C]	NIST, Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, May, 2004
[38D]	NIST, Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, November, 2007
[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 (Revised)*, March, 2007
[56Arev3]	NIST, Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, Revision 3, April, 2018
[56B]	NIST, Special Publication 800-56B*, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*, Revision 1, September 2014
[56Brev2]	NIST, Special Publication 800-56B*, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*, Revision 2, March 2019
[56Crev1]	NIST, Special Publication 800-56C*, Recommendation for Key-Derivation Methods in Key-Establishment Schemes*, Revision 1, April 2018
[67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Revision 2, July, 2017
[90A]	NIST, Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Revision 1, June, 2015
[90B]	NIST, Special Publication 800-90B, *Recommendation for Entropy Sources Used for Random Bit Generation*, January, 2018
[108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, FIPS Publication 108*,* October, 2009
[132]	NIST, *Recommendation for Password-Based Key Derivation, Part 1: Storage Applications*, FIPS Publication 132*,* December, 2010
[133]	NIST Special Publication SP800-133, *Recommendation for Cryptographic Key Generation*, Revision 2 June 2020
[180]	NIST, *Secure Hash Standard*, 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
[198]	NIST, *The Keyed-Hash Message Authentication Code (HMAC)*, FIPS Publication 198-1, July 2008

Other References	
[APDUSpec]	*AN12543, SE051 IoT applet APDU Specification,* NXP Semiconductors, Rev 1.12, 15 July 2020.
[DTR]	NIST, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, January 2011
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Card Specification 2.3, GlobalPlatform Inc., December 2015* *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 Technology Secure Element Management Service Card Specification v2.3 – Amendment I,* Version 1.0
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated August 12, 2020
[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 7816-6:2016 *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
[NXP I2C]	NXP UM10204, I2C-bus specification and user manual, Rev. 6, April 4, 2014.
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[RFC5639]	Request for Comments: 5639, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*, March 2010
[SCP03]	*GlobalPlatform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 – Amendment D,* Global Platform, Version 1.1.1

Other References	
[SEC2]	*SEC 2: Recommended Elliptic Curve Domain Parameters,* Certicom Research, January 27, 2010 Version 2.0
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 2, March 2019

Acronyms and Definitions

Table 2: Acronyms and Definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
BCD	Binary-Coded Digit
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	GlobalPlatform
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain
I^2C or I2C	Inter-Integrated Circuit, see [NXP I2C]
ISD	Issuer Security Domain, see [GlobalPlatform]
JCOP	Java Card Open Platform
KAT	Known Answer Test
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
SEMS	Secure Element Management Service, see [GlobalPlatform]
OP	Open Platform (predecessor to GlobalPlatform)
PCR	Platform Configuration Register
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SSD	Supplementary Security Domain, 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 FIPS SE051 cryptographic module, hereafter denoted *the Module* or *Secure Element*. The Module, validated to FIPS 140-2 overall Level 3, is a single chip module named, "FIPS SE051," implementing the GlobalPlatform operational environment (Card Manager (ISD/SSD)) and the applications:

- NXP IoT applet v6.0.0
- NXP SEMS Lite applet v1.4.0.11

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 FIPS SE051 module is composed of a GlobalPlatform operational environment and Java Card applets running on the SE050 chip. The FIPS SE051 GlobalPlatform operational environment is identified with the ROM ID, the Platform ID, the Patch ID, and other information (see Section 1.1.1), describing the content in ROM, NVM and loaded patches. The Platform ID is a data string that allows the identification of the FIPS SE051 Card Manager component.

Part Number	Interface	Hardware Version	Platform ID	ROM ID	Patch ID
FIPS SE051 Full	Dual + I2C	SE050 (N7121 B1)	4A335233353130323942343131130304C0954E73E773C6E	2E5AD88409C9BADB	1
FIPS SE051 Reduced	Dual + I2C	SE050 (N7121 B1)	4A335233353130323942343131130301A08FA5067B5F256	2E5AD88409C9BADB	1

Table 4: Operating System Identification

The FIPS SE051 GlobalPlatform operational environment is provided in two OS versions (base mask configurations): FIPS SE051 Full and FIPS SE051 Reduced. The GlobalPlatform operational environment of FIPS SE051 Reduced version is a subset of the FIPS SE051 Full base mask configuration, the FIPS SE051 Reduced does not include the ISO/IEC 7816 Contact interface with T=0 and T=1 protocol.

Both FIPS SE051 Full and Reduced are loaded with the NXP SEMS Lite applet instance. In addition, the FIPS SE051 Reduced configuration is loaded with the NXP IoT applet instance by default. The FIPS SE051 Full can support or not support the NXP IoT applet instance.

The NXP IoT applet instance and related content can be disabled and removed in order to gain additional memory without impacting the validation.

The FIPS SE051 module supports one Approved mode of operation only.

1.1.1 FIPS Indicator

To verify that the GlobalPlatform operational environment runs in the Approved mode of operation, the operator will call the IDENTIFY APDU command (*Info* service) 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 platform version is located at the tag ‘03’, the value is 4A335233353130323942343131313030304C0954E73E773C6E in case of FIPS SE051 Full and 4A33523335313032394234313131303031A08FA5067B5F256 in case of FIPS SE051 Reduced.

Both versions have the same patch version and ROM ID:
Tag 02 identifies the patch version: 0000000000000001.
Tag 08 identified the ROM ID: 2E5AD88409C9BADB.

The DF28 file tag ‘05’ contains the status of the FIPS compliancy, where ‘00’ identified FIPS mode not active and ‘01’ - FIPS mode active.

The FIPS SE051 product will support:

- NXP IoT applet v6.0.0 identification (FIPS SE051 reduced only):
  - Package ID: A000000396545300000001030**0**00200H
  - Applet ID: A000000396545300000001030**0**0000000H
  - Instance ID: A000000396545300000001030**0**0000000H
- NXP SEMS Lite appletv1.4.0.11 identification:
  - Package ID: A00000039654530000000103**3**00000H
  - Applet ID: A00000039654530000000103**3**0000000H
  - Instance ID: A00000039654530000000103**3**0000000H

If present, the operator can verify that NXP IoT applet v6.0.0 is in an Approved mode of operation by sending the following two (2) commands to the Module:

1. The SELECT APDU command (*Context* service) will be called with the following parameters: CLA = 00, INS = A4, P1 = 04, P2 = 00, Lc = 10, Incoming Data = A0000003965453000000010300000000, and Le = 00. The Module shall answer 06000027F2FFFF followed by status code 9000. The

response includes the BCD encoded applet version (060000) and the supported applet feature bitmap (27F2). It is not possible to modify the applet version or the supported features bitmap after the device leaves the factory.

2. The GetVersion APDU command (*IoT Applet Management* service) shall be called to get the extended feature bitmap. This command is 80040021 and shall return 27F20000011F81C1E101000000000010000000000000000000000000000000000 to be in FIPS approved mode of operation.

The operator can verify that NXP SEMS Lite applet v1.4.0.11 is in Approved mode of operation by sending the following three (3) commands to the Module:

1. The SELECT APDU command (*SEMS Lite General* service) shall be called with the following parameters: CLA = 00, INS = A4, P1 = 04, P2 = 00, Lc = 10, Incoming Data = A0000003965453000000010330000000, and Le = 00.
2. The GET DATA APDU command (*SEMS Lite General* service) shall be called with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = DE, and Le = 00.
   The command shall return DE04010400119000 with 01040011 indicating the NXP SEMS Lite applet version.
3. The GET DATA APDU command (*SEMS Lite General* service) shall be called with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = C6, and Le = 00.
   The command shall return C601019000 with C60101 indicating the NXP SEMS Lite applet is configured in FIPS approved mode of operation.

1.2 Hardware and Physical Cryptographic Boundary

The Module is designed to be used as a part of an IoT system. It works as an auxiliary security device attached to a host controller. 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.

In production use, the Module is delivered to either vendors or end user customers in a HX2QFN20 (SOT1969-1) package, which is excluded from the FIPS140-2 security testing. The package dimensions are 3 mm x 3 mm x 0.32 mm with a 0.4 mm pitch.

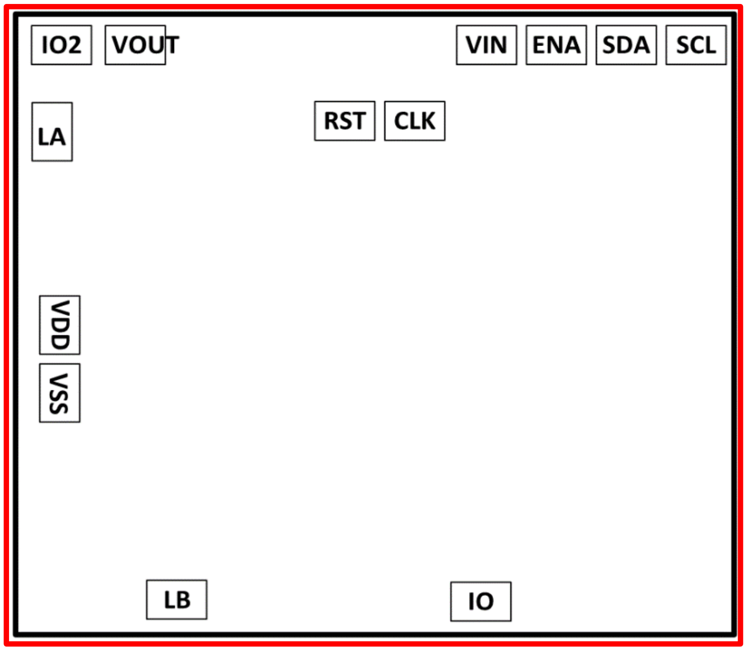

Figure 1: NXP Semiconductors FIPS SE051 Physical Form

The Module can be operated with different communication modes: Contact ([ISO 7816]), Contactless ([ISO 14443]), and I2C ([NXP I2C]). Depending on the communication mode, Module interfaces are enabled or not.

Port	Description	Logical Interface Type	Full	Reduced
VSS, VDD	ISO 7816: Supply voltage	Power	X	
VIN, VOUT	ISO 7816 / ISO 14443 / T1I2C: Supply voltage and logic supply in case deep power-down mode is used.	Power	X	X
ENA	Deep power-down mode enabled	Control in	X	X
RST	ISO 7816: Reset	Control in	X	
CLK	ISO 7816: Clock	Control in	X	
IO	ISO 7816: Input/Output or T1I2C: Master SDA	Control in, Data in, Data out, Status out	X	X
IO2	ISO 7816: Input/Output 2 or T1I2C: Master SCL	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	X
SDA	I2C: Slave data	Control in, Data in, Data out, Status out	X	X
SCL	I2C: clock	Control in	X	X

Table 6: Ports and Interfaces

In the table above, an "X" in the column indicates the ports/interfaces which are enabled in the FIPS SE051 Full and Reduced configurations.

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, or a [NXP I2C] connection to a host controller.

1.3 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

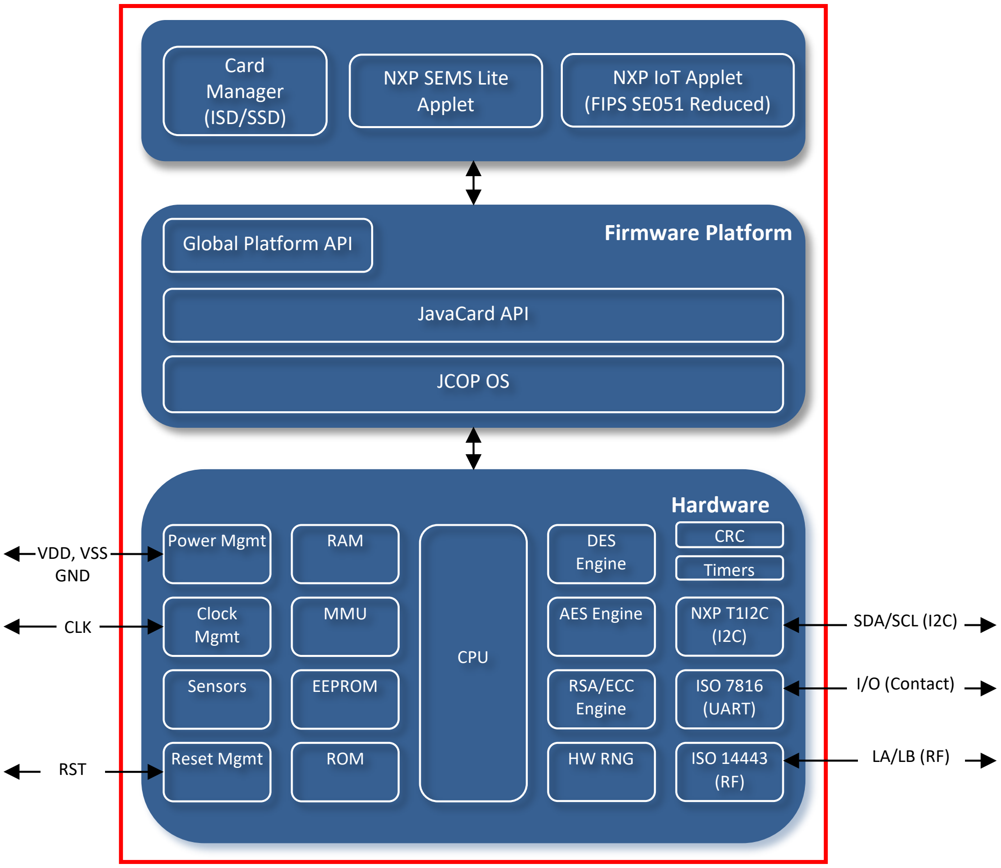

Figure 2: Module Block Diagram

The JavaCard and Global Platform APIs are internal interfaces available to applets. Only NXP applets and Card Manager (ISD/SSD) services are available at the card edge (the interfaces that cross the cryptographic boundary).

The product is delivered with:

- NXP IoT applet installed and configured before product's delivery to customer. The end-user can personalize the Module with its objects but cannot modify the configuration of the Module, the Module always operates in an Approved mode of operation.
- NXP SEMS Lite Applet installed and configured before product's delivery to customer. The end-user cannot modify the configuration of the Module. The Module always operates in an Approved mode of operation. Only the CO role can authenticate to the SEMS Lite Applet to load and install new applet signed by NXP. Thus, the end-user cannot bring unauthorized changes to the FIPS module.

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.

2 Cryptographic Functionality

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

CAVP Cert. #	Algorithm	Standard	Mode/ Method	Description	Use
C880	AES	[197], [38A]	CBC, ECB, CTR	AES-128, AES-192, AES-256	Data Encryption/ Decryption
Vendor Affirmed	AES CBC CS	[197], [38A]	CBC-CS3	AES-128	Data protection
C880	AES CMAC	[197], [38C]	CMAC	AES-128, AES-192, AES-256	Message Authentication; generation and verification SP 800-108 KDF
C1819	AES CCM	[38C]	CCM	AES-128, AES-192, AES-256	Authentication Encryption with AES CTR mode and CBC-MAC
C1822	**AES GCM/GMAC** (*)	[38D]	GCM/GMAC	AES-128, AES-192, AES-256	Authentication Encryption with Associated Data MAC calculation, MAC verification
C1820	CVL	[56A]	ECC CDH Primitive	P-256 Not used: P-224, P-384, P-521	Shared Secret Computation
C1825	CVL	[56B]	RSADP	n=2048, 3072, 4096	RSA decryption primitive. 3072 and 4096-bit are approved per IG A.14.
C838	CVL	[56B]	RSADP	n=2048, 3072, 4096	RSA decryption primitive based on RSA CRT. 3072 and 4096-bit are approved per IG A.14.
C1825	CVL	[186]	RSASP1	n=2048, 3072, 4096	RSA Signature primitive; 3072 and 4096-bit are approved per IG A.14.
C838	CVL	[186]	RSASP1	n=2048, 3072, 4096	RSA Signature primitive based on RSA CRT; 3072 and 4096-bit are approved per IG A.14.
C1823	**CVL**	[135r1]	TLS version 1.2 Key Derivation	HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	TLS KDF
C886	DRBG	[90A]	CTR_DRBG	AES-128, AES-256	Deterministic Random Bit Generation AES-128: RSA key generation AES-256: ECDSA key generation

	ENT(P)	[90B]	Hardware RNG; used as entropy input to the FIPS approved (Cert. #C886) DRBG. The non-deterministic RNG provides a minimum entropy of 128 bits for AES-128 CTR_DRBG and 256 bits for AES-256 CTR_DRBG.		Entropy Generation
C1820	ECDSA	[186]	P-224, P-256, P-384, P-521		ECC Key Generation
			P-224: (SHA-224, SHA-256, SHA-384, SHA-512), P-256: (SHA-256, SHA-384, SHA-512), P-384: (SHA-384, SHA-512), P-521: (SHA-512)		Digital Signature Generation
			P-224: (SHA-224, SHA-256, SHA-384, SHA-512), P-256: (SHA-256, SHA-384, SHA-512), P-384: (SHA-384, SHA-512), P-521: (SHA-512)		Digital Signature Verification
C1818	HMAC	[198]	SHA-1, SHA-256, SHA-384, SHA-512		Message Authentication, key strength > 112 bits
Vendor Affirmed	**KAS-SSC**	[56Arev3]	OnePass EC Diffie-Hellman	P-256	ECKey session shared secret computation
Vendor Affirmed	KAS-SSC	[56Arev3]	OnePass EC Diffie-Hellman	P-256	SEMS Lite shared secret computation (also used with non-approved but allowed curves in Table 9)
C1824	KBKDF	[108]	Counter	AES-128, AES-192, AES-256	Deriving keys from existing keys
C1818	KBKDF	[108]	KDF In Feedback Mode	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	HKDF Operations - expand only
Vendor Affirmed	**KDA**	[56Crev1]	Two-step key derivation function	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	IoT applet HKDF Operations – extract-then-expand
Vendor Affirmed	**KDA**	[56Crev1]	One-step key-derivation function option 1	SHA-256	IoT applet ECKey session key derivation

Vendor Affirmed	KDA	[56Crev1]	One-step key-derivation function option 1	SHA-256	SEMS Lite shared master key derivation
C880	KTS	[38F]	AES CBC / AES CMAC	AES-128, AES-192, AES-256	Meets the SP 800-38F §3.1 ¶3 requirements for symmetric key wrapping, using Cert. #C880 AES and AES CMAC. Key establishment methodology provides 128 bits of encryption strength.
Vendor Affirmed	**PBKDF**	[132]	PBKDF2	HMAC-SHA-1	Password-based Key Derivation. This algorithm is provided as a service for module hosting the Module.
C1821	RSA	[186]	n=2048, 3072		Key Generation
C1825	RSA	[186]	n=2048, 3072, 4096 with PKCS v1.5 and PKCSPSS and SHA-(224, 256, 384, 512)		Digital Signature Generation; 4096-bit RSA Signature Generation is allowed per IG A.14
			n=2048, 3072, 4096 with PKCS v1.5 and PKCSPSS and SHA-(1[1], 224, 256, 384, 512)		Digital Signature Verification; 4096-bit RSA Signature Verification is approved per IG A.14
C838	RSA	[186]	n=2048, 3072, 4096 with PKCS v1.5 and PKCSPSS and SHA-(224, 256, 384, 512)		Digital Signature Generation; 4096-bit RSA Signature Generation was tested against FIPS 186-2, allowed per IG G.18
			n=2048, 3072, 4096 with PKCS v1.5 and PKCSPSS and SHA-(1[2], 224, 256, 384, 512)		Digital Signature Verification; 4096-bit RSA Signature Verification is approved per IG A.14
C837	SHS	[180]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest Generation, SEMS Lite command integrity
C1816	SHS	[180]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest Generation for internal usage
C880	Triple-DES[3]	[67]	CBC, ECB	3-Key	Data Encryption and Decryption

Table 7: Approved Algorithms

(*) AES GCM IV: the module enforces the use of an approved DRBG in accordance with IG A.5 scenario 2; the internal Approved CTR_DRBG, which has a security strength of 256 bits, is used to generate the 96-bit IV.

[1] This algorithm is Approved for legacy use

[2] This algorithm is Approved for legacy use

[3] The same Triple-DES key is not used more than either 2^{16} per IG A.13. When the block limit is reached the key value is cleared and the key is set to un-initialized automatically.

Cryptographic algorithm names in **bold** in Table 7 and Table 8 indicate that the cryptographic algorithm implementations are available when the NXP IoT applet is installed only.

Algorithm	Description
AES Key Unwrapping method 1	AES Key Unwrapping according to RFC3394, as allowed per IG D.9. AES (Cert. #C880, key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)
AES Key Unwrapping method 2	AES Key Unwrapping according to [GP] Amendment-I, as allowed per IG D.9. AES (Cert. #C880, key unwrapping; key establishment methodology provides 128 bits of encryption strength).
EC Diffie-Hellman	(shared secret computation) used by the SEMS Lite applet with the non-approved but allowed Brainpool256r1 curve.

Table 8: Non-Approved but Allowed Cryptographic Functions

EC	Standard	Strength	Singular	Field	Co-Factor
Brainpool224r1	[RFC5639]	112	No	IF_p	1
Brainpool256r1	[RFC5639]	128	No	IF_p	1
Brainpool320r1	[RFC5639]	128	No	IF_p	1
Brainpool384r1	[RFC5639]	192	No	IF_p	1
Brainpool512r1	[RFC5639]	256	No	IF_p	1
Secp224k1	[SEC2]	112	No	IF_p	1
Secp256k1	[SEC2]	128	No	IF_p	1

Table 9: Non-Approved but Allowed Elliptic Curves used with ECDSA

The SEMS Lite applet can support NIST P-256 curve or vendor approved Brainpool256r1 elliptic curve to perform the ECDSA or KAS-SSC operations. In the approved mode of operation, the SEMS Lite applet supports Brainpool256r1 elliptic curve. The CO role may use SEMS Lite Module Management service to load NIST P-256 curve parameters.

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 3.4. 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 (ISD/SSD)
OS-DRBG-EI	NDRNG entropy input to CTR_DRBG.
OS-DRBG-STATE	880-bit value; the current DRBG state.
OS-SKEK	128-bit key stored in NVM, used to derive OS-MKEK

CSP	Description/Usage
OS-MKEK	AES 128-bit key used to encrypt all secret and private key data stored in NVM.
SD-KENC	AES (128, 192 or 256 bit) Master key used to derive SD-SENC.
SD-KMAC	AES (128, 192 or 256 bit) Master key used to derive SD-SMAC and SD-RMAC.
SD-KDEK	AES (128, 192 or 256 bit) Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES (128, 192 or 256 bit) Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES (128, 192 or 256 bit) Session MAC key used to verify inbound secure channel data integrity.
SD-RMAC	AES (128, 192 or 256 bit) Session MAC key used to generate response secure channel data MAC.
	IoT Applet (if present in the FIPS SE051 configuration)
APP-TRANSPORT-CIPHER	256-bit AES-CBC encryption key used to either export or import keys or data.
APP-TRANSPORT-MAC	128-bit AES-CMAC authentication key used to either export or import another key.
APP-KAS-SSC-EC-PRIV-KEY	P-256 KAS Shared Secret computation private key.
APP-KAS-IOT-SS	32 Byte KAS Shared Secret CSP.
APP-AES-KEY-AUTH	128-bit AES key used in AESKey session or ECKey session authentication methods.
APP-SENC	AES 128-bit AESKey or ECKey session encryption key used to encrypt / decrypt secure channel data.
APP-SMAC	AES 128-bit AESKey or ECKey session MAC key used to verify inbound secure channel data integrity.
APP-RMAC	AES 128-bit AESKey or ECKey session MAC key used to generate response secure channel data MAC.
APP-USERID-FILE	4 to 16-byte UserID authentication data.
APP-EC-PRIV-KEY	Elliptic curve private key that allows to perform ECDSA cryptographic operations, using NIST P-224, P-256, P-384 or P-521, Brainpool 224, 256, 320, 384 or 512-bit curves, secp224k1 or secp256k1 curve.
APP-RSA-PRIV-KEY	2048-bit, 3072-bit or 4096-bit RSA private key that allows to perform RSA cryptographic operations.
APP-AES-KEY	AES (128, 192 or 256 bits) key used to perform AES cipher mode operations.
APP-DES-KEY	3-key Triple-DES key used to perform Triple-DES cipher mode operations.
APP-HMAC-KEY	(112-bit and above) HMAC keys used to perform KDF or HMAC operations.

CSP	Description/Usage
SEMS Lite Applet	
APP-ECC-RT-PRIV-KA	Private static key used in key establishment (KAS) operations (Brainpool256r1 or P-256)
APP-KAS-SEMS-SS	32 Byte KAS Shared Secret CSP.
APP-AES-RAM-K0-Key	128-bit AES key used to unwrap the SEMS Lite Authentication data.
APP-AES-RAM-Kn-Key	128-bit AES key used to unwrap the SEMS Lite script.

Table 10: Critical Security Parameters

Public Key	Description/Usage
Card Manager (ISD/SSD)	
DAP-DAPK	256-bit ECC public key used for Mandated DAP.
IoT Applet (if present in the FIPS SE051 configuration)	
APP-KAS-SSC-EC-PUB-KEY	256-bit KAS Shared Secret computation public key.
APP-EC-PUB-KEY-CO	256-bit ECDSA public key used to authenticate the CO.
APP-EC-PUB-KEY-USER	256-bit ECDSA public key used to authenticate as user.
APP-EC-PUB-KEY	Elliptic curve public key that allows to execute ECDSA cryptographic operations (keys can be inserted by users) using NIST P-224, P-256, P-384 or P-521, Brainpool 224, 256, 320, 384 or 512-bit curves, secp224k1 or secp256k1 curve.
APP-RSA-PUB-KEY	2048-bit, 3072-bit or 4096-bit RSA public key that allows to execute RSA cryptographic operations (keys can be inserted by users).
SEMS Lite Applet	
APP-ECC-PUB-eKA	256-bit ephemeral EC public key used in key establishment (KAS) operation.
APP-ECC-RT-PUB-AUT	256-bit static EC public key used to verify the certificate signature of APP-CERT-AUT or APP-CERT-KR-AUT.
APP-ECC-PUB-AUT	256-bit static EC public key used to verify the SEMS script signature.
APP-CERT-AUT	ECC Certificate with 256-bit EC public key providing authorization and authenticity to SEMS Lite applet.
APP-CERT-KR-AUT	ECC Certificate with 256-bit EC public key providing authorization and authenticity to SEMS Lite applet for SEMS Lite Root Key Update service by CO.

Table 11: Public Keys

3 Roles, Authentication and Services

The Module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports concurrent operators

Table 12 lists all operator roles supported by the Module.

Role ID	Role Description
CO	Cryptographic Officer – manages Module content and configuration, including management of Module data via the SSD. Authenticated as described in *Platform authentication, IoT applet authentication (ECKey session), and SEMS Lite applet authentication* in sub-section below.
User	The device Holder (applet user) – performs FIPS approved cryptographic operations. Authenticated as described in *Platform authentication*, *IoT applet authentication, and SEMS Lite Applet authentication* in sub-section below.

Table 12: Roles Supported by the Module

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.
- CO authentication method does not exchange plaintext CSP.
- User authentication data is encrypted and authenticated during entry with GlobalPlatform SCP03, is stored encrypted with OS-MKEK and is only accessible by authenticated services.

3.1 Platform Authentication (Secure Channel Protocol 03 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, SD-SMAC, and SD-RMAC session keys. These sessions keys are used with AES-CBC and AES-CMAC to provide an end-to-end confidential and authenticated protected channel (Approved KTS) between the external entity (User) and the Module.
The external entity participating in the mutual authentication sends a 64-bit challenge to the Secure Element. The Secure Element generates its own challenge and computes a 64-bit cryptogram with SD-SMAC key and both challenges. The Secure Element cryptogram and challenge are sent to the external entity which checks the Secure Element cryptogram and creates its own 64-bit cryptogram with both challenges. A 64-bit message authentication code (MAC) is also computed on the command containing the external entity cryptogram with AES-CMAC and SD-SMAC key. The MAC is concatenated to the command, and the command is sent to the Secure Element. The Secure Element checks the message authentication code and compares the received cryptogram to the calculated cryptogram. If all of this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module).

The probability that a random attempt will succeed using this authentication method is:

- 1/(2^128) = 2.9E-39 (MAC||cryptogram, using a 128-bit block for authentication)

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 60 failed Global Platform SCP03 authentication attempts before blocking permanently the card. The probability that a random attempt will succeed over a one-minute interval is:

- 60/(2^128) = 1.7E-37 (MAC||cryptogram, using a 128-bit block for authentication)

3.2 IoT applet Authentication (if present in the FIPS SE051 module configuration)

The applet allows creating an authenticated session using an Authentication Object which can be either UserID session, AESKey session, or ECKey session.

An authenticated session allows users to protect and safeguard their credentials against third party use as only the authenticated user has proper rights on the credentials. This is ensured by applying correct policies to the credentials. A policy binds functional access to an Authentication Object where an Authentication Object represents a user. See Sections 3.2.3 and 3.7 of [APDUSpec] for more details.

The different authentication methods are described in the sub-sections below.

3.2.1 UserID Session

An UserID session authentication method is provided by the *Session management* service.
During a UserID session, the session user identifier (UserID) is verified in order to allow setting up a session. If the UserID is correct, the session establishment will succeed; otherwise, the session will not be opened.

An UserID can be configured from a minimum of four (4) bytes up to a maximum of 16 bytes (128 bits). In the worst-case scenario, a 4-byte UserID is used, the probability that a random attempt will succeed using this authentication method is:

- 1/(2^32) = 4.3E-9

The number of authentication attempts is configurable. It can be an infinite attempt number, or it can be limited by a counter comprised between 1 and 255 attempts. A maximum of 4700 authentications can be performed in one minute. In the worst-case scenario, the probability that a random attempt will succeed over a one-minute period is:

- 4700/(2^32) = 1.0E-6

3.2.2 AESKey Session

The AESKey session authentication method is provided by the *Session management* service. The APP-AES-KEY-AUTH key is used to derive the APP-SENC, APP-SMAC keys, and APP-RMAC. These sessions keys are used with AES-CBC and AES-CMAC to provide an end-to-end confidential and authenticated protected channel (Approved KTS) between the external entity (User) and the Module.
The external entity participating in the mutual authentication sends a 64-bit challenge to the Secure Element. The Secure Element generates its own challenge and computes a 64-bit cryptogram with APP-SMAC key and both challenges. The Secure Element cryptogram and challenge are sent to the external entity which checks the Secure Element cryptogram and creates its own 64-bit cryptogram with both challenges. A 64-bit message authentication code (MAC) is also computed on the command containing the external entity cryptogram with AES-CMAC and APP-SMAC key. The MAC is concatenated to the command, and the command is sent to the Secure Element. The Secure Element checks the message authentication code and compares the received cryptogram to the calculated cryptogram. If all of 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 (MAC||cryptogram, using a 128-bit block for authentication)

The number of authentication attempts is configurable. It can be an infinite attempt numbers or it can be limited by a counter comprised between 1 and 32767. A maximum of 4700 authentications can be performed in one minute. In the worst-case scenario, the probability that a random attempt will succeed over a one-minute period is:

- 4700/(2^128) = 1.3E-35 (MAC||cryptogram, using a 128-bit block for authentication).

3.2.3 ECKey Session

An ECKey session authentication method is provided by the *Session management* service.
The ECKey session authentication method consists in verifying a P-256 ECDSA signature. The P-256 EC public key is either initially imported by the User (APP-EC-PUBLIC-KEY-USER) or provisioned during the manufacturing (APP-EC-PUBLIC-KEY-CO). The user will own the corresponding ECDSA private key.
In addition to User's authentication, ECKey session is used to establish APP-KAS-IOT-SS with the Approved KAS algorithm. The shared secret is used to derive the AES-128 APP-AES-KEY-AUTH which is itself used to derive the APP-SENC, APP-SMAC and APP-RMAC session keys. These sessions keys are used with AES-CBC and AES-CMAC to provide an end-to-end confidential and authenticated protected channel (Approved KTS) between the external entity (User) and the Module.

First, the user requests the Module public key, APP-KAS-SSC-EC-PUB-KEY; this key is signed with the private key APP-KAS-SSC-EC-PRIV-KEY by the Module. Then, the User sends the ephemeral KAS public key signed with User's ECDSA private key. Finally, the Module verifies the ECDSA signature of the ephemeral key with either APP-EC-PUBLIC-KEY-USER or APP-EC-PUBLIC-KEY-CO before initiating the KAS shared secret computation.

The probability that a random attempt will succeed using this authentication method is:

- 1/(2^128) = 2.9E-39 (using a 256-bit EC key for authentication)

The number of authentication attempts is configurable. It can be an infinite attempt numbers or it can be limited by a counter comprised between 1 and 32767. A maximum of 4700 authentications can be performed in one minute. In the worst-case scenario, the probability that a random attempt will succeed over a one-minute period is:

- 4700/(2^128) = 1.4E-35 (using a 256-bit EC key for authentication)

3.3 SEMS Lite Applet Authentication

The SEMS Lite applet is provided by the *SEMS Lite Authentication* service. The service provides authentication, confidentiality, and integrity of each authenticated service. The SEMS Lite Applet authentication consists in verifying a Brainpool256r1 ECDSA signature computed on a 113-byte data generated off the module and the CO public key APP-ECC-RT-PUB-AUT, see section 5.1.4 of [GP] Amendment-I.

The probability that a random attempt will succeed using this authentication method is:

- 1/(2^128) = 2.9E-39 (using a 256-bit EC key for authentication)

To keep the SEMS Lite Applet from blocking, an infinite number of attempts is allowed. A maximum of 4700 authentications can be performed in one minute. In the worst-case scenario, the probability that a random attempt will succeed over a one-minute period is:

- 4700/(2^128) = 1.4E-35 (using a 256-bit EC key for authentication)

3.4 Services

All services implemented by the Module are listed in the tables below. The ISD / SSD Services are provided by the Card Manager. Such services can be accessed directly with a selection of Security Domain or through the NXP IoT applet for the SSD. The Applet Services are provided by the NXP IoT applet or SEMS Lite applet.

Service	Description
	ISD / SSD Services
Card Reset	Power cycle or reset the Module.
Context	Select an applet or manage logical channels.
Info	Read unprivileged data objects, e.g., Module configuration or status information (Show Status). This service includes the Power-On Self-Test on-demand.
	SEMS Lite Applet Services
SEMS Lite General	This service provides generic operations which are not required to be protected by applying security. It includes selecting the SEMS Lite applet, reading version of the SEMS Lite applet, or APP-ECC-RT-PUB-AUT public key of SEMS Lite Applet

Table 13: Unauthenticated Services

Service	Description	CO	User
	ISD / SSD Services		
Lifecycle	Modify the card or applet life cycle status.	X	
Manage Content	Load 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	
	IoT Applet Services (if present in the FIPS SE051 configuration)		
Module Management	This service manages the FIPS SE051 applet configuration.	X	
Session Management	This service manages the applet sessions. Users can decide to open a session or not. Opening a session requires authentication to the applet using either an UserID, an AES-128 key or an EC key depending on the session type.	X	X
Secure Object Write Functionality	This service manages the generation (either an RSA or EC key pair) or transport (EC keys, RSA keys, symmetric keys, binary files, UserIDs, monotonic counters, PCRs) of Secure Objects.	X	X
Secure Object Read Functionality	This service manages the reading of Secure Objects or its attributes. Asymmetric private keys or symmetric keys can never be read in plaintext.	X	X

Service	Description	CO	User
Secure Object Management	This service manages the reading of Secure Object attributes.	X	X
EC Curve Management	This service manages the EC curves that can be used during EC cryptographic operations.	X	X
Crypto Object Management	This service manages the Crypto Objects that can be used. Crypto Objects allow to do operations in multiple steps (init/update/final). Supported Crypto Objects allow to use a digest, cipher or MAC algorithm to be used.	X	X
EC Crypto Operations	This service triggers OS API for ECDSA signature generation and verification, and for EC DH shared secret calculation according to [56Arev3] §5.7.1.2.	X	X
RSA Crypto Operations	This service triggers OS API for RSA signature generation and verification, and for RSA encryption and decryption (components only).	X	X
Symmetric Cipher Crypto Operations	This service triggers OS API for AES and Triple-DES encryption and decryption.	X	X
Authenticated Encryption Crypto Operations	This service provides execution of the AEAD function using OS API primitives for AES GCM encryption and decryption, and DRBG for internal IV generation.	X	X
MAC Calculation Crypto Operations	This service triggers OS API for MAC Calculation.	X	X
HKDF operations	This service triggers OS API for HKDF operations (either Two Step Key Derivation using HMAC or the Key Derivation Function using Pseudorandom functions).	X	X
PBKDF Operation	This service provides execution of the Password-Based Key Derivation Function. The derived key is returned to the operator and not used by the module.	X	X
TLS KDF Functions	This service provides support for TLS v1.2 calculations. The module does not implement the TLS v1.2 protocol.	X	X
Secure Hash Crypto Operations	This service triggers OS API for [FIPS 180-4] compliant hash algorithms.	X	X
	SEMS Lite Applet Services		
SEMS Lite Authentication	This service authenticates the CO or User and initiates the SEMS Lite unwrapping mechanism used by the SEMS Lite Manage Content service, SEMS Lite Root Key Update service.	X	X
SEMS Lite Manage Content	The service manages the loading, installation, personalization and delete of applets on the module.	X	X
SEMS Lite Root Key Update	This service is used to update APP-ECC-RT-PRIV-KA and APP-ECC-RT-PUB-AUT keys.	X	

Table 14: Authenticated Services

Table 15 and Table 16 below describe the access to CSPs and Public Keys 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-SKEK: loaded on first power-up of the Module in a manufacturing setting; used to derive OS-MKEK; zeroized on Lifecycle card termination.

OS-MKEK: derived from OS-SKEK; 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 'E' 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 ('I') using the Manage Content service; zeroized by Lifecycle card termination.

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 are used with secure channel active. 'GE' on GP Secure Channel as a consequence of secure channel initialization and usage. 'Z' on Module Reset is a consequence of RAM clearing/garbage collection.

SD-CLFDBK: loaded during first power-up of the Module in a manufacturing setting; is used to load ciphered packages

DAP-DAPK: loaded during first power-up of the Module in a manufacturing setting; is used to verify loading of DAP enabled packages

Applet CSPs (APP-): Applet CSPs and public keys are separated between cryptographic operations services and management services.

CSPs APP-EC-PRIV-KEY, APP-RSA-PRIV-KEY, APP-AES-KEY, APP-DES-KEY, APP-HMAC-KEY are called by the cryptographic operation services.

All other keys are either used to protect confidentiality and to authenticate the data exchanged between an external entity and the Module, to authenticate the users, or to establish CSPs and public keys.

The transport mechanism allows exporting transient CSP keys stored on the module ('O' of *Secure Object Read Functionality* service for CSPs) and importing these exported keys only. The keys are protected during the transport with **APP-TRANSPORT-CIPHER** and **APP-TRANSPORT-MAC** over the Secure Channel.

The public key can also be output 'O' in plaintext with the *Secure Object Read Functionality* service.

APP-KAS-SSC-PRIV-KEY and **APP-KAS-SSC-PUB-KEY** are used to compute the KAS shared secret **APP-KAS-IOT-SS**.

APP-AES-KEY-AUTH is the (master) key type for AESKey session authentication or establish with the ECKey session KAS.

APP-SENC, **APP-SMAC** and **APP-RMAC** are the session keys used by the secure messaging in AESKey or ECKey sessions.

ECKey session authentication used either **APP-EC-PUBLIC-KEY-CO** or **APP-EC-PUBLIC-KEY-USER**.

Secure Object Management service can zeroize 'Z' all persistent object of the Module.

Secure Object Write Functionality service is used to either import CSPs and Public keys or to generate the asymmetric keys.

APP-ECC-RT-PUB-AUT, **APP-CERT-KR-AUT**, **APP-ECC-PUB-AUT**, and **APP-CERT-AUT** are used to authenticate the CO and the User and can be updated by the CO using *SEMS Lite Module Management* or *SEMS Lite Root Key Update* services.

APP-ECC-RT-PRIV-KA and **APP-ECC-PUB-eKA** are used to establish the are used to compute the KAS shared secret **APP-KAS-SEMS-SS** with Key establishment (KAS-SSC). **APP-ECC-RT-PRIV-KA** can be updated by CO using *SEMS Lite Module Management* or *SEMS Lite Root Key Update* service.
APP-APP-AES-RAM-K0-Key and **APP-AES-RAM-Kn-Key** are used to unwrap the script commands.

The modes of access shown in the tables below are defined as:

- G = Generate: The service generates or derives the CSP/Public Key.
- I = Input: The service inputs the CSP/Public Key.
- E = Execute: The Module executes using the CSP/Public Key.
- E' = Execute: The Module executes using the CSP/Public Key if present.
- O = Output: The service outputs the CSP/Public Key. CSP are always protected with the approved KTS.
- Z = Zeroize: The Module zeroizes the CSP/Public Key. For the Context service, SD session keys are destroyed on applet deselect (channel closure).
- -- = Not accessed by the service.

Services	CSPs													
	OS-DRBG-EI	OS-DRBG-STATE	OS-SKEK	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	APP-ECC-RT-PRIV-KA	APP-KAS-SEMS--SS	APP-AES-RAM-K0-KEY	APP-AES-RAM-Kn-Key
Unauthenticated Role	*Card Manager*										*SEMS Lite Applet*			
Card Reset	GZ	GEZ	E	G	--	--	--	Z	Z	Z	--	Z	Z	Z
Context	--	--	--	--	--	--	--	EZ	EZ	EZ	--	--	Z	Z
Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SEMS Lite General	--	--	--	--	--	--	--	--	--	--	--	--	--	--
CO Role	*Card Manager*										*SEMS Lite Applet*			
Lifecycle	Z	Z	Z	Z	Z	Z	Z	EZ	EZ	EZ	Z	Z	Z	Z
Manage Content	Z	Z	IZ	E	IE	IE	IE	E	E	E	--	--	--	--
Privileged Info	--	--	--	E	E	E	--	E	E	E	--	--	--	--
Secure Channel	GZ	GEZ	--	E	E	E	--	GE	GE	GE	--	--	--	--
SEMS Lite Root Key Update	--	--	--	E	--	--	--	--	--	--	I	--	--	E
CO / User Role	*Card Manager*										*SEMS Lite Applet*			
Module Management	--	--	--	--	--	--	--	E	E	E	E	--	GE	IE
Session Management	GZ	GEZ	--	E	E	E	--	GE	GE	GE	--	--	--	--
Secure Object Write Functionality	GZ	GEZ	--	E	--	--	--	E	E	E	--	--	--	--

Services	CSPs													
	OS-DRBG-EI	OS-DRBG-STATE	OS-SKEK	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	APP-ECC-RT-PRIV-KA	APP-KAS-SEMS--SS	APP-AES-RAM-K0-KEY	APP-AES-RAM-Kn-Key
Secure Object Read Functionality	--	--	--	E	--	--	--	E	E	E	--	--	--	--
Secure Object Management	--	--	--	E	--	--	--	E	E	E	--	--	--	--
EC Curve Management	--	--	--	--	--	--	--	E	E	E	--	--	--	--
Crypto Object Management	--	--	--	--	--	--	--	E	E	E	--	--	--	--
EC Crypto Operations	GZ	GEZ	--	E	--	--	--	E	E	E	--	--	--	--
RSA Crypto Operations	GZ	GEZ	--	E	--	--	--	E	E	E	--	--	--	--
Symmetric Cipher Crypto Operations	--	--	--	E	--	--	--	E	E	E	--	--	--	--
Authenticated Encryption Crypto Operations	--	--	--	--	--	--	--	E	E	E	--	--	--	--
MAC Calculation	--	--	--	E	--	--	--	E	E	E	--	--	--	--
HKDF Operations	--	--	--	--	--	--	--	E	E	E	--	--	--	--
PBKDF Operations	--	--	--	--	--	--	--	E	E	E	--	--	--	--
TLS KDF Functions	--	--	--	--	--	--	--	E	E	E	--	--	--	--
Secure Hash Crypto Operations	--	--	--	--	--	--	--	E	E	E	--	--	--	--
SEMS Lite Authentication	--	--	--	E	--	--	--	--	--	--	E	GEZ	GEZ	--
SEMS Lite Manage Content	--	--	--	E	--	--	--	--	--	--	--	--	--	IEZ

Table 15: Card Manager and SEMS Lite Applet CSPs Access within Services

Services	**CSPs**													
	APP-TRANSPORT-CIPHER	APP-TRANSPORT-MAC	APP-KAS-SSC-EC-PRIV-KEY	APP-KAS-IOT--SS	APP-AES-KEY-AUTH	APP-SENC	APP-SMAC	APP-RMAC	APP-USERID-FILE	APP-EC-PRIV-KEY	APP-RSA-PRIV-KEY	APP-AES-KEY	APP-DES-KEY	APP-HMAC-KEY
Unauthenticated Role	*IoT Applet*													
Card Reset	--	--	--	Z	--	Z	Z	Z	--	--	--	--	--	--
Context	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SEMS Lite General	--	--	--	--	--	--	--	--	--	--	--	--	--	--
CO	*IoT Applet*													
Lifecycle	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Manage Content	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Privileged Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure Channel	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SEMS Lite Root Key Update	--	--	--	--	--	--	--	--	--	--	--	--	--	--
CO / User	*IoT Applet*													
Module Management	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Session Management	--	--	E	GEZ	E	GEZ	GEZ	GEZ	E	E	--	E	--	--
Secure Object Write Functionality	E	E	--	--	I	--	--	--	I	GI	GI	I	I	I
Secure Object Read Functionality	E	E	--	--		--	--	--	--	O	O	O	O	O
Secure Object Management	--	--	--	--	Z	--	--	--	Z	Z	Z	Z	Z	Z
EC Curve Management	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Crypto Object Management	--	--	--	--	--	--	--	--	--	--	--	E	E	E
EC Crypto Operations	--	--	--	--	--	--	--	--	--	E	--	--	--	--
RSA Crypto Operations	--	--	--	--	--	--	--	--	--	--	E	--	--	--
Symmetric Cipher Crypto Operations	--	--	--	--	--	--	--	--	--	--	--	E	E	--
Authenticated Encryption Crypto Operations	--	--	--	--	--	--	--	--	--	--	--	E	--	--

Services	CSPs													
	APP-TRANSPORT-CIPHER	APP-TRANSPORT-MAC	APP-KAS-SSC-EC-PRIV-KEY	APP-KAS-IOT--SS	APP-AES-KEY-AUTH	APP-SENC	APP-SMAC	APP-RMAC	APP-USERID-FILE	APP-EC-PRIV-KEY	APP-RSA-PRIV-KEY	APP-AES-KEY	APP-DES-KEY	APP-HMAC-KEY
MAC Calculation	--	--	--	--	--	--	--	--	--	--	--	--	--	E
HKDF Operations	--	--	--	--	--	--	--	--	--	--	--	--	--	E
PBKDF Operations	--	--	--	--	--	--	--	--	--	--	--	--	--	E
TLS KDF Functions	--	--	--	--	--	--	--	--	--	E	E	E	E	E
Secure Hash Crypto Operations	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SEMS Lite Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SEMS Lite Manage Content	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Table 16: IoT applet CSPs Access within Services (if present in FIPS SE051 configuration)

Services	Public Keys										
	DAP-DAPK	APP- KAS-SSC-EC-PUB-KEY	APP-EC-PUB-KEY-CO	APP-EC-PUB-KEY-USER	APP-EC-PUB -KEY	APP-RSA-PUB-KEY	APP-ECC-PUB-eKA	APP-ECC-RT-PUB-AUT	APP-ECC-PUB-AUT	APP-CERT-KR-AUT	APP-CERT-AUT
Unauthenticated Role	*CM*	*IoT Applet*					*SEMS Lite applet*				
Card Reset	--	--	--	--	--	--	--	--	--	--	--
Context	--	--	--	--	--	--	--	--	--	--	--
Info	--	--	--	--	--	--	--	--	--	--	--
SEMS Lite General	--	--	--	--	--	--	--	O	--	--	--
CO	*CM*	*IoT Applet*					*SEMS Lite applet*				
Lifecycle	Z	Z	Z	Z	Z	Z	Z	Z	Z	--	--
Manage Content	--	--	--	--	--	--	--	--	--	--	--
Privileged Info	--	--	--	--	--	--	--	--	--	--	--
Secure Channel	--	--	--	--	--	--	--	--	--	--	--
SEMS Lite Root Key Update	--	--	--	--	--	--	IE	EI	IE	I	I

Services	Public Keys										
	DAP-DAPK	APP- KAS-SSC-EC-PUB-KEY	APP-EC-PUB-KEY-CO	APP-EC-PUB-KEY-USER	APP-EC-PUB -KEY	APP-RSA-PUB-KEY	APP-ECC-PUB-eKA	APP-ECC-RT-PUB-AUT	APP-ECC-PUB-AUT	APP-CERT-KR-AUT	APP-CERT-AUT
CO / User	*CM*	*IoT Applet*					*SEMS Lite applet*				
Module Management	--	--	IE	IE	--	--	IE	E	IE	--	--
Session Management	--	E	E	E	--	--	--	--	--	--	--
Secure Object Write Functionality	--	--	I	I	I	I	--	--	--	--	--
Secure Object Read Functionality	--	O	O	O	O	O	--	--	--	--	--
Secure Object Management	--	--	--	Z	Z	Z	--	--	--	--	--
EC Curve Management	--	--	--	--	--	--	--	--	--	--	--
Crypto Object Management	--	--	--	--	--	--	--	--	--	--	--
EC Crypto Operations	--	--	--	--	E	--	--	--	--	--	--
RSA Crypto Operations	--	--	--	--	--	E	--	--	--	--	--
Symmetric Cipher Crypto Operations	--	--	--	--	--	--	--	--	--	--	--
Authenticated Encryption Crypto Operations	--	--	--	--	--	--	--	--	--	--	--
MAC Calculation	--	--	--	--	--	--	--	--	--	--	--
HKDF Operations	--	--	--	--	--	--	--	--	--	--	--
PBKDF Operations	--	--	--	--	--	--	--	--	--	--	--
TLS KDF Functions	--	--	--	--	--	--	--	--	--	--	--
Secure Hash Crypto Operations	--	--	--	--	--	--	--	--	--	--	--
SEMS Lite Authentication	--	--	--	--	--	--	E	E	E	--	--
SEMS Lite Manage Content	E	--	--	--	--	--	--	I	I	I	I

Table 17: Public Keys Access within Services

4 Self-Test

4.1 Power-On Self-Tests

The module complies with IG 9.11; on the first power-on or on demand, the Module performs self-tests described in Table 18 below. All self-tests must be completed successfully prior to any other use of cryptography by the Module. If one of the self-tests fails, the system is halted and will start again after a reset.

For successive power-on, the Firmware Integrity (Flash and ROM) check is performed on every reset.

Test Target	Description
AES	Performs separate encrypt and decrypt KATs using an AES-128 key (Cert. #C880) in CBC mode.
CMAC	Performs an AES-CMAC (Cert. #C880)KAT with AES-128
DRBG	Performs a fixed input DRBG (Cert. #C1820) KAT all of SP 800-90A health test monitoring functions.
ECDSA	Performs ECDSA (Cert. #C1820) signature generation and verification KATs using the P-521 curve and SHA-256 (Cert. #C837); this self-test is inclusive of the CVL ECC CDH self-test.
Firmware Integrity	32-bit CRC performed over all code located in Flash and ROM.
HMAC	Performs a HMAC (Cert. #C1818) KAT with SHA-256 (Cert. #C1816).
KBKDF	Performs a KBKDF (Cert. #C1824) KAT with AES-128 CMAC.
KBKDF	Performs a KBKDF (Cert. #C1818) in Feedback Mode with HMAC-SHA1
RSA	Performs separate RSA (Cert. #C1825) and RSA CRT (Cert. #C838) signature generation and verification KATs using an RSA 2048-bit key and SHA-256 (Cert. #C837).
SHA-1	Performs a fixed input KAT for both Cert. #C837 and #C1816.
SHA-256	Performs a fixed input KAT for both Cert. #C837 and #C1816 (inclusive of SHA-224, per IG 9.4)
SHA-512	Performs a fixed input KAT for both Cert. #C837 and #C1816 (inclusive of SHA-384, per IG 9.4).
Triple-DES	Performs encrypt and decrypt KATs using 3-Key Triple-DES (Cert. #C880) in CBC mode.

Table 18: Power-On Self-Test

All the Power-On Self-Tests can be performed on-demand with the GET DATA APDU command (*Info* service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00. The expected result is FE04DF4B0120.

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.
Generate PCT	Pairwise consistency test (Sign/Verify) performed when an asymmetric key pair is generated for RSA or ECC. The conditional test is implemented at the applet level.
NDRNG CRNGT	CRNGT is implemented following IG 9.8 by performing RCT on raw data.
Signature PCT	Pairwise consistency test performed when a signature is generated for RSA or ECDSA.
Firmware Load Test	DAP signature verification based on ECDSA P-256 with SHA-256

Table 19: 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* error state. The Module includes also Environmental Failure Protection features (see Section 6 below).

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 countermeasures. Protection features include detection of out-of-range supply voltages, frequencies or temperatures, and detection of illegal addresses or instructions. All cryptographic computations and sensitive operations such as critical data 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:

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
2. The Module does not support a maintenance interface or role.
3. The Module provides identity-based authentication.
4. The Module clears previous authentications on power cycle.
5. Power up self-tests do not require any operator action.
6. The Module allows the operator to initiate self-tests on-demand.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. The Module does not enter or output plaintext CSPs.
10. There are no restrictions on which CSPs are zeroized by the zeroization services, see Table 15.
11. The Module does not support manual key entry.
12. The Module does not output intermediate key values.
13. The module does not provide bypass services or ports/interfaces.
14. No additional interface or service is implemented by the Module which would provide access to CSPs.

In addition, the following guidance shall be followed:

15. The default SSD SD-KENC, SD-KMAC, and SD-KDEK CSPs shall be changed at the reception of the Module.
16. For PBKDF, the input parameters shall follow these requirements:
    a. Salt length is 16 up to 64 bytes
    b. Iteration count is 1 up to 32767 bytes. The iteration count shall be selected as large as possible, as long as the time required to generate the key using the entered password is acceptable for the users. A minimum of 1,000 iteration count is recommended in [132]

c. Output length is 112 up to 512 bytes.

The use of the derived master key to protect data will be defined by the module host, see Section 5.4 of [SP800-132] for the possible options.

17. Output of the PBKDF shall only be used in storage applications.
18. A policy that restricts the use of the keys to one specific algorithm shall be applied to EC Keys used to perform Elliptic Curve operations, the policy shall ensure that no key can be used for multiple cryptographic operations.
19. For a static key pair used in key agreement a trusted third party (TTP) (trusted by the owner and any recipient of the public key) shall generate the key pair as specified in Section 5.6.1 of SP800-56Arev.3 and provide it to the owner. It is assumed that the TTP is trusted by both the owner and any public-key recipient to generate the key pair as specified in Section 5.6.1 and not to use the owner's private key to masquerade as the owner.