

FIPS 140-3 Non-Proprietary Security Policy



Document Version: 1.7

Date: 31 July 2025

Revision History:

| Version | Date | Changes |
|---------|-------------------|---------------------------------------------------------------------------------------|
| 1.0 | July 18, 2022 | Full Release, added CAVP Cert. # to Table 3 |
| 1.1 | June 14, 2023 | Update after first round NIST comments |
| 1.2 | June 23, 2023 | Update chapter 10 |
| 1.3 | August 17, 2023 | Update after CMVP comments |
| 1.4 | November 24, 2023 | Update after CMVP comments |
| 1.5 | December 24, 2023 | Update after CMVP comments |
| 1.6 | March 20, 2025 | Minor updates to Section 2 to remove vendor affirmation claims based on CMVP comments |
| 1.7 | July 31, 2025 | Rebranded from JCOP 4.5 on P71D600 to SE052F |

Contents

| | | |
|----|-----------------------------------------------|----|
| 1 | General | 5 |
| 2 | Cryptographic Module Specification | 7 |
| 3 | Cryptographic Module Interfaces..... | 21 |
| 4 | Roles, Services and Authentication | 22 |
| 5 | Software/Firmware Security..... | 42 |
| 6 | Operational Environment | 43 |
| 7 | Physical Security | 44 |
| 8 | Non-Invasive Security..... | 45 |
| 9 | Sensitive Security Parameter Management | 46 |
| 10 | Self-Tests..... | 60 |
| 11 | Life-Cycle Assurance | 62 |
| 12 | Mitigation of Other Attacks | 63 |

List of Figures

| | |
|-----------------------------------------------------------|-----------|
| Figure 1 – P71D600 | 16 |
| Figure 2 – P71D600 Physical Form (Schematic) | 17 |
| Figure 3 – Module Block Diagram | 18 |

List of Table

| | |
|-------------------------------------------------------------------------------------|-----------|
| <i>Table 1 – Security Levels</i> | <i>6</i> |
| <i>Table 2 – Cryptographic Module Tested Configuration</i> | <i>7</i> |
| <i>Table 3 – Approved Algorithms</i> | <i>15</i> |
| <i>Table 4 – Non-Approved Algorithms Allowed in Approved Mode of Operation.....</i> | <i>15</i> |
| <i>Table 5 – Ports and Interfaces</i> | <i>20</i> |
| <i>Table 6 – Roles, Service Commands, Input and Output</i> | <i>25</i> |
| <i>Table 7 – Roles and Authentication</i> | <i>26</i> |
| <i>Table 8 – Approved Services</i> | <i>39</i> |
| <i>Table 9 – Physical Security Inspection Guidelines</i> | <i>42</i> |
| <i>Table 10 – EFP/EFT</i> | <i>42</i> |

| | |
|--------------------------------------------------------------------------|----|
| <i>Table 11 – Hardness Testing Temperature Ranges</i> | 42 |
| <i>Table 12 – SSPs</i> | 59 |
| <i>Table 13 – Non-Deterministic Number Generator Specification</i> | 60 |

1 General

Introduction

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a sensitive but unclassified (SBU) environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140-3 program. The National Voluntary Laboratory Accreditation Program (NVLAP) provides accreditation to independent testing labs performing FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at: <https://csrc.nist.gov/projects/cryptographic-module-validation-program>.

About this Document

This non-proprietary Cryptographic Module Security Policy for the NXP Semiconductors SE052F provides an overview of the product and a high-level description of how it meets the overall Security Level 3 requirements of FIPS 140-3.

The SE052F may also be referred to as the “Secure Element” or “module” in this document.

The module is available under several commercial type names addressing the different market segments relevant for NXP, such as:

- JCOP 4.5 on P71D600
- JCOP ID 2 on P71D600
- SE052F
- NCJ37B0HN

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. NXP Semiconductors shall have no liability for any error or damages of any kind resulting from the use of this document.

Notices

This document may be freely reproduced and distributed in its entirety without modification.

The following table lists the level of validation for each area in FIPS 140-3:

| ISO/IEC 24759 Section 6 [Number Below] | FIPS 140-3 Section Title | Security Level |
|---------------------------------------------------|-----------------------------------------|-----------------------|
| 1 | General | 3 |
| 2 | Cryptographic Module Specification | 3 |
| 3 | Cryptographic Module Interfaces | 3 |
| 4 | Roles, Services, and Authentication | 3 |
| 5 | Software/Firmware Security | 3 |
| 6 | Operational Environment | N/A |
| 7 | Physical Security | 4 |
| 8 | Non-Invasive Security | 3 |
| 9 | Sensitive Security Parameter Management | 3 |
| 10 | Self-Tests | 3 |
| 11 | Life-Cycle Assurance | 3 |
| 12 | Mitigation of Other Attacks | 3 |

Table 1 – Security Levels

The module claims an Overall Security Level 3.

2 Cryptographic Module Specification

The module, validated to FIPS 140-3 overall Level 3, is a hardware module with single chip embodiment named SE052F implementing the GlobalPlatform operational environment (Card Manager (ISD/SSD)) and the applications:

- NXP IoT applet v7.2.22
- NXP SEMS Lite applet v2.0.2.11

The module is designed for use in smart cards, IoT and automotive applications.

| Module | Hardware [Part Number and Version] | Firmware Version | | | | Distinguishing Features |
|--------|------------------------------------|------------------|------------------|----------------------|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Platform ID | ROM ID | Patch ID | Applets | |
| SE052F | N7122 A1 | J3R6000373181200 | B3375FE9B5508BC4 | 00000000 00000000 | NXP IoT applet v7.2.22 and NXP SEMS Lite applet v2.0.2.11 | The GlobalPlatform operational environment is identified with the Platform ID, the ROM ID, the Patch ID, and other information, describing the content in ROM, NVM and loaded patches; The Platform ID is a data string that allows the identification of the P71D600 Card |

Table 2 – Cryptographic Module Tested Configuration

The module is validated at an Overall Security Level 3 with Physical Security at Level 4 and all other areas at Level 3. The Operational Environment requirements do not apply to the module given that it meets Physical Security Level 4 requirements.

Cryptographic Boundary

The module is designed to be used as a part of a larger system. It works as an auxiliary security device attached to a host controller. The physical form of the module is depicted in Figures 1 and 2 (to scale); the outline depicts the cryptographic boundary, representing the surface of the chip and the bond pads. The red outline in Figure 3 also depicts the cryptographic boundary.

In production use, the module is delivered to either vendors or end user customers either on film frame carrier (FFC) or various packages such as PDM1.1, NXD6.2, MOB6/10 or HVQFN20 package. The package is outside the cryptographic boundary and thus excluded from the FIPS 140-3/ISO/IEC 19790 security testing.

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. No components have been excluded from within the cryptographic boundary.

Approved Mode of Operation

The module only supports an Approved mode of operation. The NXP SEMS Lite applet can support the NIST P-256 curve or the vendor Approved and NIST allowed Brainpool256r1 elliptic curve to perform the ECDSA or KASECC operations. In the Approved mode of operation, the NXP SEMS Lite applet supports the Brainpool256r1 elliptic curve by default. The CO role may use SEMS Lite Module Management service to load NIST P-256 curve parameters.

The P71D600 GlobalPlatform operational environment component can be identified by using the IDENTIFY APDU command (*Info* service). 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, NVM and loaded patches. The Platform ID is a data string that allows the identification of the P71D600 Card Manager component.

The IDENTIFY APDU command is formatted as follows:

| 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

The command answers the content of the DF28 file:

- Tag 02 identifies the Patch ID (see Table 2)
 - Tag 03 identifies the Platform Build ID which is made up of the Platform ID (16 Bytes, see Table 2) and the platform build fingerprint (8 Bytes)
 - Tag 08 identified the ROM ID (see Table 2)

To verify that the GlobalPlatform operational environment runs in the Approved mode of operation, use the IDENTIFY APDU (as described above). The DF28 file tag '05' contains the status of the Approved mode compliancy, where '00' identifies Approved mode not active and '01' - Approved mode active.

Both NXP IoT applet and NXP SEMS Lite applet of the module are configured to always run in an Approved mode of operation.

The personalized product shall have:

- NXP IoT applet v7.2.22 identification:
 - Package ID: A00000039654530000000103**000200**H ◦
Applet ID: A00000039654530000000103**00000000**H ◦ Instance ID: A00000039654530000000103**00000000**H
 - NXP SEMS Lite applet v2.0.2.11 identification:
 - Package ID: A00000039654530000000103**300000**H ◦
Applet ID: A00000039654530000000103**30000000**H ◦ Instance ID: A00000039654530000000103**30000000**H

The operator can verify that NXP IoT applet v7.2.22 is in an Approved mode of operation by sending the two (2) following commands to the module:

The operator can verify that NXP SEMS Lite applet v2.0.2.11 is an Approved mode of operation by sending the three (3) following 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.
Return code shall be 90 00 (OK)
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 DE04020002119000 with 02000211 indicating the NXP SEMS Lite applet version. This encoded applet version (02000211) corresponds to the decimal version v2.0.2.11 of the IoT Applet as specified in Table 2 in this document and the module certificate.
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 Approved mode of operation.

The module does not support a degraded operation.

Cryptographic Algorithms

The module implements the following Approved cryptographic algorithms.

| CAVP Cert | Algorithm and Standard | Mode/ Method | Description/ Key Size(s)/ Key Strength(s) | Use/Function |
|-----------|--------------------------|--------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------------|
| A2713 | AES-CBC | AES-CBC | AES-128, AES-192, AES-256 with 128, 192, 256-bit key strength | Data Encryption/ Decryption |
| A2713 | AES-CCM | AES-CCM | AES-128, AES-192, AES-256 with 128, 192, 256-bit key strength | Authentication Encryption with AES CTR mode and CBC-MAC |
| A2713 | AES-CMAC | AES-CMAC | AES-128, AES-192, AES-256 with 128, 192, 256-bit key Strength | Message Authentication; generation and verification SP800-108 KDF |
| A2713 | AES-CTR | AES-CTR | AES-128, AES-192, AES-256 with 128, 192, 256-bit key Strength | Data Encryption/ Decryption |
| A2713 | AES-ECB | AES-ECB | AES-128, AES-192, AES-256 with 128, 192, 256-bit key strength | Data Encryption/ Decryption |
| A2713 | Counter DRBG | Counter DRBG | AES-256 with 256-bit security strength | Deterministic Random Bit Generation AES-256: RSA and ECDSA key generation |
| A2713 | ECDSA KeyGen (FIPS186-4) | ECDSA KeyGen (FIPS186-4) | P-224, P-256, P-384, P-521 with 112, 128, 192 and 256-bit key strength | ECC Key Generation |

| CAVP Cert | Algorithm and Standard | Mode/ Method | Description/ Key Size(s)/ Key Strength(s) | Use/Function |
|-----------|--------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| A2713 | ECDSA SigGen (FIPS186-4) | ECDSA SigGen (FIPS186-4) | P-224: (SHA2-224, SHA2-256, SHA2-384, SHA2-512), P-256: (SHA2-256, SHA2384, SHA2-512), P-384: (SHA2-384, SHA2-512), P-521: (SHA2-512) with 112, 128, 192 and 256-bit key strength | Digital Signature Generation |
| A2713 | ECDSA SigVer (FIPS186-4) | ECDSA SigVer (FIPS186-4) | P-224: (SHA2-224, SHA2-256, SHA2-384, SHA2-512), P-256: (SHA2-256, SHA2384, SHA2-512), P-384: (SHA2-384, SHA2-512), P-521: (SHA2-512) with 112, 128, 192 and 256-bit key strength | Digital Signature Verification |
| A2713 | HMAC-SHA-1 | HMAC-SHA-1 | HMAC-SHA-1 with 128-bit key strength | Message Authentication |
| A2713 | HMAC-SHA2-256 | HMAC-SHA2-256 | HMAC-SHA-256 with 256-bit key strength | Message Authentication |
| A2713 | HMAC-SHA2-384 | HMAC-SHA2-384 | HMAC-SHA-384 with 256-bit key strength | Message Authentication |
| A2713 | HMAC-SHA2-512 | HMAC-SHA2-512 | HMAC-SHA-512 with 256-bit key strength | Message Authentication |

| CAVP Cert | Algorithm and Standard | Mode/ Method | Description/ Key Size(s)/ Key Strength(s) | Use/Function |
|-----------|--------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A2713 | KAS-ECC-SSC Sp800-56Ar3 | OnePass EC Diffie-Hellman FIPS 140-3 IG D.F Scenario 2 Path 2 | P-256 with 128-bit key strength | ECKey session shared secret computation; SEMS Lite shared secret computation (with Brainpool256r1 curves); The module obtains assurances per Section 5.6.2 in NIST SP800-56Ar3 self-tests |
| A2713 | KDA HKDF Sp800-56Cr1 | Two-step key derivation function | HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 with 128 and 256-bit key strength | HKDF Operations – extract-then-expand |
| A2713 | KDF SP800-108 | Counter | AES-128, AES-192, AES-256 with 128, 192 and 256-bit key strength | Deriving keys from existing keys |
| A2713 | KDF SP800-108 | Feedback | HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 with 128 and 256-bit key strength | HKDF Operations - expand only |
| A2713 | RSA Decryption Primitive | RSA Decryption Primitive | n=2048 with 112-bit decryption strength | Decryption Primitive (standard and CRT) |
| A2713 | RSA KeyGen (FIPS186-4) | RSA KeyGen (FIPS186-4) | n=2048, 3072, 4096 with 112 and 128-bit key strength | Key Generation (standard and CRT) |
| A2713 | RSA SigGen (FIPS186-4) | RSA SigGen (FIPS186-4) | n=2048, 3072, 4096 with PKCS v1.5 and PKCSPSS and SHA2-(224, 256, 384, 512) with 112, 128 and 152 bit key strength | Signature Generation |

| CAVP Cert | Algorithm and Standard | Mode/ Method | Description/ Key Size(s)/ Key Strength(s) | Use/Function |
|-----------|-------------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| A2713 | RSA SigVer (FIPS186-4) | RSA SigVer (FIPS186-4) | n=2048, 3072, 4096 with PKCS v1.5 and PKCSPSS and SHA-1, SHA2-(224, 256, 384, 512) with 112, 128 and 152 bit key strength | Signature Verification |
| A2713 | RSA Signature Primitive | RSA Signature Primitive | n=2048 with 112-bit security strength | Signature Primitive (standard andCRT) |
| A2713 | SHA-1 | SHA-1 | SHA-1 with 128-bit security strength | Message Digest Generation, SEMS Lite command integrity |
| A2713 | SHA2-224 | SHA2-224 | SHA2-224 with 112bit or 192-bit security strength | Message Digest Generation, SEMS Lite command integrity |
| A2713 | SHA2-256 | SHA2-256 | SHA2-256 with 128 or 256-bit security strength | Message Digest Generation, SEMS Lite command integrity |
| A2713 | SHA2-384 | SHA2-384 | SHA2-384 with 192 or 256-bit security strength | Message Digest Generation, SEMS Lite command integrity |
| A2713 | SHA2-512 | SHA2-512 | SHA2-512 with 256-bit security strength | Message Digest Generation, SEMS Lite command integrity |
| A2714 | AES-GCM | AES-GCM | AES-128, AES-192, AES-256 with 128, 192, 256-bit key strength | Authentication Encryption with Associated Data MAC calculation, MAC verification |
| A2714 | AES-GMAC | AES-GMAC | AES-128, AES-192, AES-256 with 128, 192, 256-bit key strength | Authentication Encryption with Associated Data MAC calculation, MAC verification |

| CAVP Cert | Algorithm and Standard | Mode/ Method | Description/ Key Size(s)/ Key Strength(s) | Use/Function |
|------------------------------------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| A2714 | AES-KW | AES-KW | AES-128, AES-192, AES-256 with 128, 192, 256-bit key strength | Key Wrapping (Decryption) |
| A2714 | KDA OneStep Sp800-56Cr1 | KDA OneStep Sp800-56Cr1 option 1 | SHA-256 with 256-bit key strength | EcKey Session Key Derivation |
| A2714 | KDF TLS | TLS version 1.2 Key Derivation SP800-135r1 | HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 with 256-bit key strength | Key Derivation Function used in TLS 1.2 |
| A2714 | PBKDF | PBKDF2 Option 1a acc. [SP800-132r2] | HMAC-SHA-1 with 128-bit key strength | Password-based Key Derivation; This algorithm is provided as a service for module hosting the Module |
| A2715 | KDA OneStep Sp800-56Cr1 | KDA OneStep Sp800-56Cr1 option 1 | SHA-256 with 256-bit key strength | SEMS Lite shared master key derivation |
| Vendor Affirmed | CKG SP800-133r2 | Section 4: Symmetric keys and seeds used for generating the asymmetric keys are generated using methods described in Section 4 of SP800-133r2 Section 5.1: Key Pairs for Digital Signature Schemes Section 6.2.1: Symmetric Keys Generated Using Key-Agreement Schemes Section 6.2.2: Symmetric Keys Derived from a Pre-existing Key Section 6.4: Distributing the Generated Symmetric Key | | Key Generation is based on unmodified output of the DRBG cert. #A2713 |
| KAS-ECC-SSC Sp80056Ar3/A2713 KDA HKDF Sp800-56Cr1/A2713 | KAS-1 | SP 800-56Arev3 KAS-ECC per IG D.F Scenario 2 path (2) | P-256 curve providing 128 bits of encryption strength | KAS (KAS-ECC-SSC Sp 800-56Ar3 with KDA (HKDF)) |

| CAVP Cert | Algorithm and Standard | Mode/ Method | Description/ Key Size(s)/ Key Strength(s) | Use/Function |
|--------------------------------------------------------------------|------------------------|-------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------|
| KAS-ECC-SSC Sp80056Ar3/A2713 KDA OneStep Sp80056Cr1/A2714 | KAS-2 | SP 800-56Arev3 KAS-ECC per IG D.F Scenario 2 path (2) | P-256 curve providing 128 bits of encryption strength | KAS (KAS-ECC-SSC Sp 800-56Ar3 with KDA (OneStep KDF)) |
| KAS-ECC-SSC Sp80056Ar3/A2713 KDA OneStep Sp80056Cr1/A2715 | KAS-3 | SP 80056Arev3. KASECC per IG D.F Scenario 2 path (2) | P-256 curve providing 128 bits of encryption strength | KAS (KAS-ECC-SSC Sp 800-56Ar3 with KDA (OneStep KDF)) |
| AES-CBC/A2713 AES-CMAC/A2713 | KTS-1 | AES CBC / AES CMAC | AES-128, AES-192, AES-256 with 128, 192, 256-bit key strength | SP 800-38D and SP 800-38F KTS (key wrapping) per IG D.G |
| AES-KW/#A2714 | KTS-2 | KW | AES-128, AES-192, AES-256 with 128, 192, 256-bit key strength | SP 800-38F KTS (key wrapping) per IG D.G |

Table 3 – Approved Algorithms

| Algorithm | Caveat | Use/Function |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AES | Cert. #A2713, key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength Per IG D.G | Symmetric key unwrapping (according to RFC3394) |
| AES | Cert. #A2713, key unwrapping; key establishment methodology provides 128 bits of encryption strength Per IG D.G | Symmetric key unwrapping (according to GlobalPlatform Amendment-I) |
| ECDSA with non-NIST recommended curves | Provides between 112 and 256 bits of encryption strength Per IG C.A | Signature Generation/Verification using non-NIST curves [Brainpool224r1, Brainpool256r1, Brainpool320r, Brainpool384r1, Brainpool512r1, Secp224k1, Secp256k1 with strengths]112, 128, 192 and 256 bits] |

| | | |
|----------------------------------------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC Diffie-Hellman with non-NIST recommended curves | Provides between 112 and 256 bits of encryption strength Per IGs D.F and C.A | Shared secret computation using non-NIST curves [Brainpool224r1, Brainpool256r1, Brainpool320r, Brainpool384r1, Brainpool512r1, Secp224k1, Secp256k1 with strengths]112, 128, 192 and 256 bits] |
|----------------------------------------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Table 4 – Non-Approved Algorithms Allowed in Approved Mode of Operation

The following non-Approved but allowed EC curves (per IG C.A) are implemented by the module for use in ECDSA and KAS-ECC:

| EC | Standard | Strength | Singular | Field | Co-Factor |
|----------------|-----------|----------|----------|----------------|-----------|
| Brainpool224r1 | [RFC5639] | 112 | No | \mathbb{F}_p | 1 |
| EC | Standard | Strength | Singular | Field | Co-Factor |
| Brainpool256r1 | [RFC5639] | 128 | No | \mathbb{F}_p | 1 |
| Brainpool320r1 | [RFC5639] | 128 | No | \mathbb{F}_p | 1 |
| Brainpool384r1 | [RFC5639] | 192 | No | \mathbb{F}_p | 1 |
| Brainpool512r1 | [RFC5639] | 256 | No | \mathbb{F}_p | 1 |
| Secp224k1 | [SEC2] | 112 | No | \mathbb{F}_p | 1 |
| Secp256k1 | [SEC2] | 128 | No | \mathbb{F}_p | 1 |

The module does not support Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed and Non-Approved Algorithms Not Allowed in the Approved Mode of Operation.

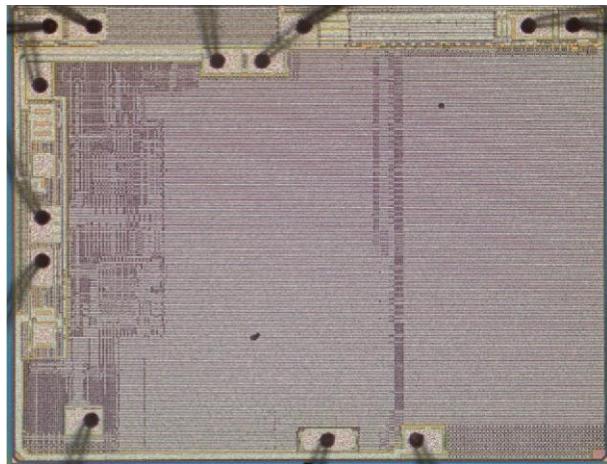


Figure 1 – P71D600

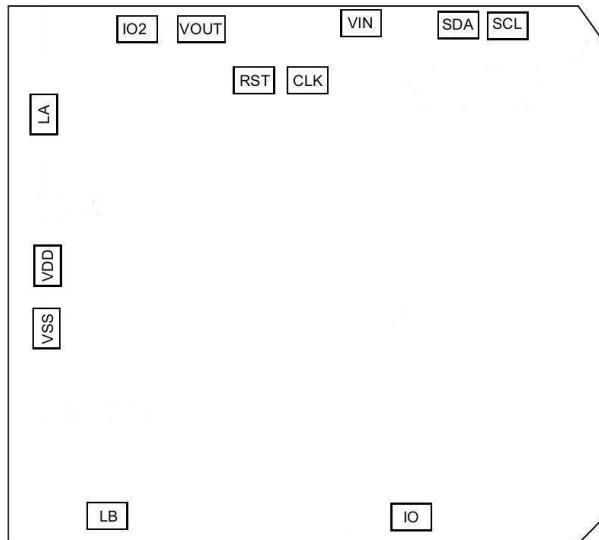
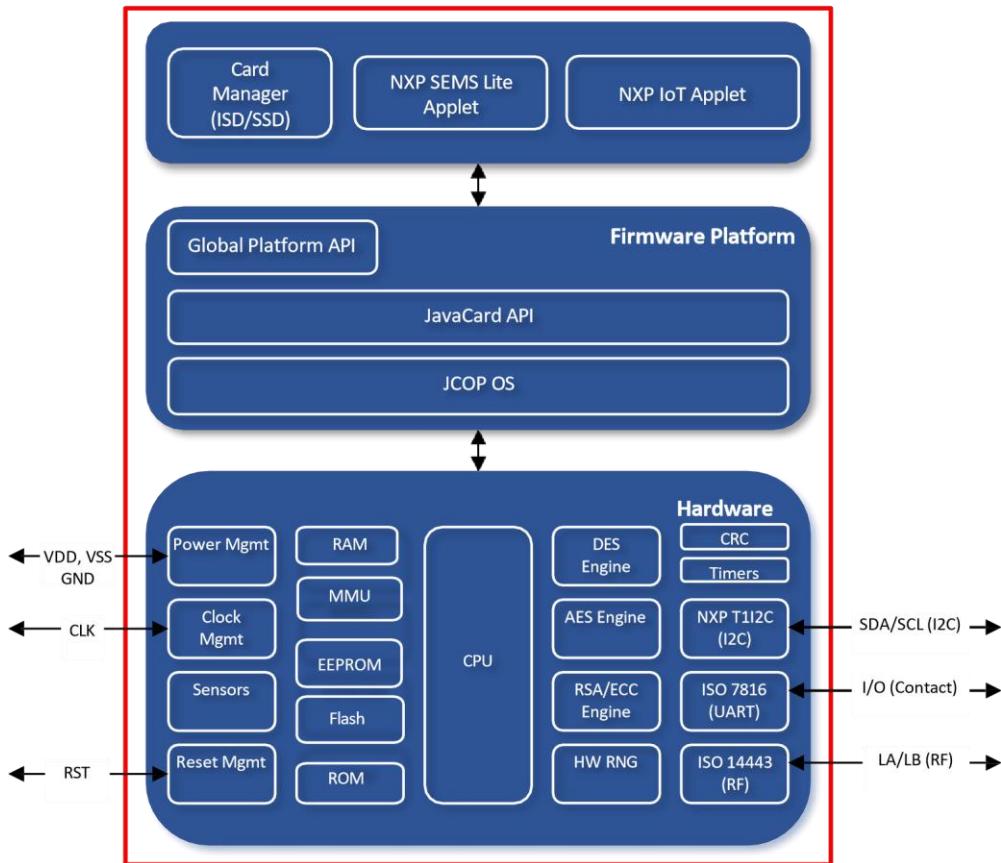


Figure 2 – P71D600 Physical Form (Schematic)

Figure 3 below depicts the module operational environment.

**Figure 3 – 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. Thus, the end-user cannot bring unauthorized changes to the Approved configuration of the module.

Overall Security Design and Rules of Operation

PBKDF Operation details • Password strength

The password is stored in an APP-HMAC-KEY object as input to the PBKDF2 function. This key requires a minimum of 112 bits. The probability that a random attempt will end up with the same output is:

- $1/(2^{112}) = 1.9E-34$ (using a minimum size for the password)

• Iteration Count and Justification

Iteration count should be at least 1000, following the recommendation in SP800-132r2.

If an application desires less iterations, the iteration count can be lower than 1000, but in any case, the iteration count shall be 2 or more.

• Storage Only Statement

Output of PBKDF Operation service shall be used in storage applications.

AES GCM IV

The module enforces the use of an Approved DRBG in accordance with IG C.H scenario 2; the internal Approved CTR_DRBG, which has a security strength of 128 bits, is used to generate the 96-bit IV.

TLS 1.2 Support

The module supports the TLS KDF Functions service. This service provides support for TLS v1.2 calculations. It does not implement the TLS v1.2 protocol. Per FIPS 140-3 IG D.C, no parts of this protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

| Physical Port | Logical Interface | Data that Passes over Port/Interface |
|---------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VSS, VDD | Power interface | These interfaces are used to supply power to the module in contact mode; The module starts when interface is powered |
| VIN, VOUT | Power interface | These interfaces are used to supply power to the module in contact, contactless and I2C mode in case deep power-down mode is used |
| RST_N | Control input interface | If a signal is sent on this interface on contact mode, the module will reboot (active low) |
| CLK | Control input interface | The interface is used by an external device (ex: smartcard reader) to provide a clock signal to the IC in contact mode; The IC will derive its own clock from this signal |
| IO1 | Control input interface, Data input interface, Data output interface, Status output interface | The interface is used to communicate with an external entity (ex: SmartCard reader) in contact mode; It also functions as I2C master SDA in I2C mode |
| IO2 | Control input interface, Data input interface, Data output interface, Status output interface | The interface is used to communicate with an external entity (ex: SmartCard reader) in contact mode; It also functions as I2C master SCL in I2C mode or as SPI interface |
| LA, LB | Power interface, Control input interface, Data input interface, Data output interface, Status output interface | The interface is used to communicate with an external entity (ex: smartcard reader) in contactless mode; This interface is also used to set the internal clock and to supply power to the module |
| SDA | Control input interface, Data input interface, Data output interface, Status output interface | The interface is used to communicate with an external entity such as a host controller |
| SCL | Control input interface | The interface is used by an external device (ex: host controller) to provide a clock signal to the I2C HW |

Table 5 – Ports and Interfaces

The module does not support control output.

4 Roles, Services and Authentication

The module supports the following roles:

- Cryptographic Officer (CO): Manages module content and configuration, including management of module data via the SSD. Authenticated as described in Table 7 below.
- User (the device Holder (applet user)): Performs Approved cryptographic operations. Authenticated as described in Table 7 below.

| Role | Service | | Input | Output |
|---------------------|-----------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------|
| ISD Services | | | | |
| CO | Manage Content | APDU(s) used: DELETE LOAD INSTALL MANAGE CHANNEL | Command parameters (data objects, SSPs) | Status Word (Response APDU 9000) |
| SSD Services | | | | |
| CO | Lifecycle (Show status and Perform zeroisation) | APDU(s) used: SET STATUS GET STATUS | Target status | Status Word (Response APDU 9000) |
| CO | Manage Content | APDU(s) used: PUT KEY STORE DATA | Command parameters (data objects, SSPs) | Status Word (Response APDU 9000) |
| CO | Privileged Info (Show module's versioning information) | APDU(s) used: GET DATA | Command parameters (privileged data objects, but no SSPs) | Requested information; Status Word (Response APDU 9000) |
| CO | Secure Channel | APDU(s) used: INITIALIZE UPDATE EXTERNAL AUTHENTICATE | Command parameters (data objects, SSPs) | Status Word (Response APDU 9000) |
| IoT Applet Services | | | | |

| CO | IoT Applet Management | APDU(s) used: SetLockState, SetPlatformSCPRequest, DeleteAll, SetAppletFeatures, ImportExternalObject | Authentication data to open an applet session | Status Word (Response APDU 9000) |
|----------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Role | Service | | Input | Output |
| User, CO | Module Usage (Perform Self-Tests and Show module's versioning information) | APDU(s) used: DisableSecureObjectCreation, SendCardManagerCommand, TriggerSelfTest, I2CM_ExecuteCommandSet, GetVersion, GetTimestamp, GetFreeMemory, GetRandom, ReadState | Command parameters (e.g. required length for GetRandom, memory type for GetFreeMemory, etc.) | Requested information; Status Word (Response APDU 9000) |
| User, CO | Session Management | APDU(s) used: CreateSession, VerifySessionUserID, SCPInitializeUpdate, SCPExternalAuthenticate, ECKeySessionInternalAuthenticate, ECKeySessionGetECKAPublicKey, ExchangeSessionData, ProcessSessionCmd, RefreshSession, CloseSession | Session creation C-APDU; authentication data to open the applet session | Status Word (Response APDU 9000) |
| User, CO | Secure Object Write Functionality | APDU(s) used: WriteECKey/WriteRSAKey, WriteSymmKey, WriteBinary, WriteUserID, WriteCounter, WritePCR, ImportObject | Object identifier; Secure Object characteristics (transient/persistent; Authentication rights or not; etc.); (optionally) Secure Object value; (optionally) Secure Object non-default policy (optionally) Secure Object version | Status Word (Response APDU 9000) |

| | | | | |
|----------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| User, CO | Secure Object Read Functionality | APDU(s) used: ReadObject, ReadAttributes, ExportObject | Object identifier | Secure Object value (if non-secret) (optionally) Secure Object attributes Status Word (Response APDU 9000) |
| User, CO | Secure Object Management | APDU(s) used: ReadType, ReadSize, ReadIDList, CheckObjectExists, DeleteSecureObject | Object identifier | Secure Object characteristics (type, size, exists, etc.) or listing of Secure Objects Status Word (Response APDU 9000) |
| User, CO | EC Curve Management (Perform approved security functions) | APDU(s) used: CreateECCurve, SetECCurveParam, GetECCurveID, ReadECCurveList, DeleteECCurve | Curve Identifier; (optionally) curve parameters Secure Object identifier (for GetECCurveID) | Status Word (Response APDU 9000) Curve set indicators (for ReadECCurveList) Curve identifier (for GetECCurveID) |
| User, CO | Crypto Object Management | APDU(s) used: CreateCryptoObject, ReadCryptoObjectList, DeleteCryptoObject | Crypto object identifier; (optionally) Crypto Object characteristics | Status Word (Response APDU 9000) List of Crypto Object identifiers (for ReadCryptoObjectList) |
| User, CO | EC Crypto Operations (Perform approved security functions) | APDU(s) used: ECDSASign, ECDSAVerify | Secure Object identifier; Input data (message/signature/exte rnal public key) | Output data (signature, result of verification, shared secret) Status Word (Response APDU 9000) |
| User, CO | RSA Crypto Operations (Perform approved security functions) | APDU(s) used: RSASign, RSAVerify, RSAEncrypt, RSADecrypt | Secure Object identifier; Input data (message/signature) | Output data (signature, result of verification, encrypted or decrypted data) Status Word (Response APDU 9000) |

| | | | | |
|----------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| User, CO | Symmetric Cipher Crypto Operations (Perform approved security functions) | APDU(s) used: CipherInit, CipherUpdate, CipherFinal, CipherOneShot | Secure Object identifier or Crypto Object identifier Input data (message) | Output data (encrypted or decrypted message) Status Word (Response APDU 9000) |
| User, CO | Authenticated Encryption Crypto Operations (Perform approved security functions) | APDU(s) used: AEADInit, AEADUpdate, AEADFinal, AEADOneShot | Secure Object identifier or Crypto Object identifier Input data (message, AAD, tag, etc.) | Output data (encrypted or decrypted message, tag or result of tag verification) Status Word (Response APDU 9000) |
| User, CO | MAC Calculation Crypto Operations (Perform approved security functions) | APDU(s) used: MACInit, MACUpdate, MACFinal, MACOneShot | Secure Object identifier or Crypto Object identifier Input data (message, MAC (for verification)) | Output data (MAC or result of MAC verification) Status Word (Response APDU 9000) |
| User, CO | HKDF operations (Perform approved security functions) | APDU(s) used: HKDFExtractAndExpand, HKDFExpandOnly | Secure Object identifier HKDF input parameters (digest type, message, requested length, salt, output object, etc.) | Output data (derived data) if not stored onchip Status Word (Response APDU 9000) |
| User, CO | PBKDF Operation (Perform approved security functions) | APDU(s) used: PBKDF2DeriveKey | Secure Object identifier PBKDF2 input data (salt, iteration count, requested length) | Output data (derived data) Status Word (Response APDU 9000) |
| User, CO | TLS KDF Functions (Perform approved security functions) | APDU(s) used: TLSGenerateRandom, TLSCalculatePremasterSecret, TLSPerformPRF | Secure Object identifier(s) TLS KDF input data (digest type, label, random, requested length) | Output data Status Word (Response APDU 9000) |

| User, CO | Secure Hash Crypto Operations (Perform approved security functions) | APDU(s) used: DigestInit, DigestUpdate, DigestFinal, DigestOneShot | Digest mode or Crypto Object identifier Input data (message) | Output data (hashed message) Status Word (Response APDU 9000) |
|-------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| SEMS Lite Applet Services | | | | |
| Role | Service | | Input | Output |
| User, CO | SEMS Lite Authentication | APDU(s) used: PROCESS, SCRIPT, COMMAND | Authentication information or SEMS Secure channel | Allow or reject SEMS Lite Manage Content service or SEMS Lite Root Key Update or Error code |
| User, CO | SEMS Lite Manage Content | APDU(s) used: SEMS_SELECT, SEMS_APDU, SEMS_BEGIN_PERSO, SEMS_END_PERSO, SEMS_INSTALL_FOR_LOAD, SEMS_LOAD, SEMS_INSTALL_FOR_INSTALL, SEMS_DELETE, SEMS_BINDING_SE, BEGIN_MANAGE_ELF_UPGRADE, END_MANAGE_ELF_UPGRADE | Content management commands wrapped in SEMS Secure channel | Implicit indication via the successful completion of service |
| CO | SEMS Lite Root Key Update | APDU(s) used: SEMS_KEY_ROTATION | Key update commands wrapped in SEMS Secure channel | Implicit indication via the successful completion of service |
| CO, User, Unauthor ised | Card Reset | APDU(s) used: N/A | Power cycle or reset the module | Status Word (Response APDU 9000) |
| CO, User, Unauthor ised | Context | APDU(s) used: SELECT. MANAGE CHANNEL | Command parameters (data objects, SSPs) | Status Word (Response APDU 9000) |

| | | | | |
|------------------------|-------------------------------------------------------------|----------------------------------------|--------------------------------------------|-------------------------------------|
| CO, User, Unauthorised | Info (Show status and Perform selftests) | APDU(s) used: GET DATA | Command parameters (data objects, SSPs) | Status Word (Response APDU 9000) |
| CO, User, Unauthorised | SEMS Lite General (Show module's versioning information) | APDU(s) used: SEMS_SELECT, GET DATA | Command parameters (data objects, SSPs) | Status Word (Response APDU 9000) |

Table 6 – Roles, Service Commands, Input and Output

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage (identity-based authentication methods implemented).

- 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. This includes user identifier (UserID) in case of UserID session method.

| Role | Authentication Method | Authentication Strength |
|---------|-----------------------|-------------------------|
| CO User | SCP03 | 128 bits |
| | UserID Session | 32 bits (minimum) |
| | AESKey Session | 128 bits |
| | ECKey Session | 128 bits |
| | SEMS Lite Applet | 128 bits |

Table 7 – Roles and Authentication

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 permanently blocking the card. The probability that a random attempt will succeed over a one-minute interval is (with the assumption here that one attempt is possible per second):

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

IoT applet Authentication

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.

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

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 worstcase 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:

- $4700/(2^{32}) = 1.0E-6$.

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 APPSMAC 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/User 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).

ECKey Session

An ECKey session authentication method is provided by the *Session management* service.

The ECKey session authentication method consists of 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-ECPUBLIC-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/APP-KAS-SEMS-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 APPKAS-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-KEYUSER 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)

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 of 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)

The module does not support bypass or self-initiated cryptographic output capabilities.

The module is a limited operational environment under the FIPS 140-3 definitions. The module includes a firmware load function to support necessary updates, but these are only limited to the vendor, NXP. 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 140-3 validation.

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|--------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|------------------------------------|----------------------------------|
| ISD Services | | | | | | |
| Manage Content | Load keys and data | N/A | OS-SKEK SD-KENC SD-KMAC SD-KDEK DAP-DAPK | CO | E, W, Z | Status Word (Response APDU 9000) |
| SSD Services | | | | | | |
| Lifecycle (Show status and Perform zeroisation) | Get or modify the card or applet life cycle status | N/A | All | CO | E, Z | Status Word (Response APDU 9000) |
| Manage Content | Load keys and data | N/A | OS-SKEK SD-KENC SD-KMAC SD-KDEK DAP-DAPK | CO | E, W, Z | Status Word (Response APDU 9000) |
| Privileged Info (Show module's versioning information) | Read Module data (privileged data objects, but no CSPs) | N/A | OS-MKEK SD-KENC SD-KMAC SD-SENC SD-SMAC SD-RMAC | CO | E | Status Word (Response APDU 9000) |
| Secure Channel | Establish and use a secure communication channel | CTR_DRBG (Cert. A2713) CKG (Vendor Affirmed) | OS-DRBG-EI OS-DRBG-SEED OS-DRBG-STATE OS-DRBG-KEY OS-DRBG-V OS-DRBG-OUTPUT OS-MKEK SD-KENC SD-KMAC SD-SENC SD-SMAC SD-RMAC | CO | E, G, Z | Status Word (Response APDU 9000) |
| IoT Applet Services | | | | | | |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|-------------------------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------|-------------------------------------|
| IoT Applet Management | This service manages the P71D600 applet | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) KDF SP800- 108 (Cert. A2713) ECDSA (Cert. A2713) P-256 SHS (Cert. A2713) KAS- ECC (Cert. A2713) P-256 SHS (Cert. A2713) CKG (Vendor Affirmed) | SD-SENC SD-SMAC SD-RMAC APP-ECC-RT-PRIV-KA APP-AES-RAM-K0-KEY APP-AES-RAM-Kn-KEY APP-EC-PUB-KEY-CO APP-EC-PUB-KEY-USER APP-ECC-RT-PUB-AUT APP-ECC-PUB-eKA APP-ECC-PUB-AUT APP-KAS-IOT-SS | CO | E, G, W | Status Word (Response APDU 9000) |
| Module Usage (Perform Self-Tests and Show module's versioning information) | Perform Self-Tests and Show module's versioning information | All | All | CO, User | E | Status Word (Response APDU 9000) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------|-------------------------------------|
| | | | | | | |
| Session Management | This service manages the applet sessions; Users can decide to open a session or not; Opening a session requires to authenticate to the applet using either an UserID, an AES128 key or an EC key depending on the session type | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) KDF SP800- 108 (Cert. A2713) ECDSA (Cert. A2713) P-256 SHS (Cert. A2713) KAS- ECC (Cert. A2713) P-256 SHS (Cert. A2713) CKG (Vendor Affirmed) | OS-DRBG-EI OS-DRBG-STATE OS-DRBG-KEY OS-DRBG-V OS-DRBG-OUTPUT OS-MKEK SD-KENC SD-KMAC SD-SENC SD-SMAC SD-RMAC 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-AES-KEY APP-KAS-SSC-EC-PUB- KEY APP-EC-PUB-KEY-CO APP-EC-PUB-KEY-USER | CO, User | E, G, Z | Status Word (Response APDU 9000) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------------------------------|----------------------------------|
| 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. | CTR_DRBG (A2713) AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) KDF SP800-108 (Cert. A2713) ECDSA (Cert. A2713) P-256 SHS (Cert. A2713) KAS-ECC (Cert. A2713) P-256 RSA (Cert. A2713) 2048, 3072, 4096 bits SHS (Cert. A2713) CKG (Vendor Affirmed) | OS-DRBG-EI OS-DRBG-STATE OS-DRBG-KEY OS-DRBG-V OS-DRBG-OUTPUT OS-MKEK SD-SENC SD-SMAC SD-RMAC APP-TRANSPORT-CIPHER APP-TRANSPORT-MAC APP-AES-KEY-AUTH APP-USERID-FILE APP-EC-PRIV-KEY APP-RSA-PRIV-KEY APP-AES-KEY APP-HMAC-KEY APP-EC-PUB-KEY-CO APP-EC-PUB-KEY-USER APP-EC-PUB-KEY APP-RSA-PUB-KEY | CO, User | E, G, R, W, Z | Status Word (Response APDU 9000) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------------------------------|----------------------------------|
| 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 | N/A | OS-MKEK SD-SENC SD-SMAC SD-RMAC APP-TRANSPORT-CIPHER APP-TRANSPORT-MAC APP-EC-PRIV-KEY APP-RSA-PRIV-KEY APP-AES-KEY APP-HMAC-KEY APP-KAS-SSC-EC-PUB-KEY APP-EC-PUB-KEY-CO APP-EC-PUB-KEY-USER APP-EC-PUB-KEY APP-RSA-PUB-KEY | CO, User | E, R | Status Word (Response APDU 9000) |
| Secure Object Management | This service manages the reading of Secure Object attributes | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) HMAC (Cert. A2713) ECDSA (Cert. A2713) P-256 SHS (Cert. A2713) RSA (Cert. A2713)2048, 3072, 4096 bits SHS (Cert. A2713) CKG (Vendor Affirmed) | OS-MKEK SD-SENC SD-SMAC SD-RMAC APP-AES-KEY-AUTH APP-USER-ID-FILE APP-RSA-PRIV-KEY APP-AES-KEY APP-HMAC-KEY APP-EC-PUB-KEY-USER APP-EC-PUB-KEY APP-RSA-PUB-KEY | CO, User | E, Z | Status Word (Response APDU 9000) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------|----------------------------------|
| EC Curve Management (Perform approved security functions) | This service manages the EC curves that can be used during EC cryptographic operations | ECDSA (Cert. A2713) P-256 SHS (Cert. A2713) | SD-SENC SD-SMAC SD-RMAC | CO, User | E | Status Word (Response APDU 9000) |
| 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 | SHS (Cert. A2713) AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) HMAC (Cert. A2713) | SD-SENC SD-SMAC SD-RMAC APP-AES-KEY APP-HMAC-KEY | CO, User | E | Status Word (Response APDU 9000) |
| EC Crypto Operations (Perform approved security functions) | This service triggers OS API for ECDSA signature generation and verification, and for EC DH shared secret calculation according to [56Ar3] Section 5.7.1.2 | ECDSA (Cert. A2713) P-256 KAS-SSC (Cert. A2713) P-256 SHS (Cert. A2713) CKG (Vendor Affirmed) | OS-DRBG-EI OS-DRBG-STATE OS-DRBG-KEY OS-DRBG-V OS-DRBG-OUTPUT OS-MKEK SD-SENC SD-SMAC SD-RMAC APP-EC-PRIV-KEY APP-EC-PUB-KEY | CO, User | E, G, Z | Status Word (Response APDU 9000) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------------------------------|----------------------------------|
| RSA Crypto Operations (Perform approved security functions) | This service triggers OS API for RSA signature generation and verification, and for RSA encryption and decryption (components only) | RSA (Cert. A2713)2048, 3072, 4096 bits SHS (Cert. A2713) CKG (Vendor Affirmed) | OS-DRBG-EI OS-DRBG-STATE OS-DRBG-KEY OS-DRBG-V OS-DRBG-OUTPUT OS-MKEK SD-SENC SD-SMAC SD-RMAC APP-RSA-PRIV-KEY APP-RSA-PUB-KEY | CO, User | E, G, Z | Status Word (Response APDU 9000) |
| Symmetric Cipher Crypto Operations (Perform approved security functions) | This service triggers OS API for AES encryption and decryption | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) | OS-MKEK SD-SENC SD-SMAC SD-RMAC APP-AES-KEY | CO, User | E | Status Word (Response APDU 9000) |
| Authenticated Encryption Crypto Operations (Perform approved security functions) | This service provides execution of the AEAD function using OS API primitives for AES GCM encryption and decryption, and DRBG for internal IV generation | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) CTR_DRBG (A2713) | SD-SENC SD-SMAC SD-RMAC | CO, User | E | Status Word (Response APDU 9000) |
| MAC Calculation Crypto Operations (Perform approved security functions) | This service triggers OS API for MAC Calculation | CMAC (Cert. A2713) HMAC (Cert. A2713) | OS-MKEK SD-SENC SD-SMAC SD-RMAC APP-HMAC-KEY | CO, User | E | Status Word (Response APDU 9000) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|----------------------------------------------------------|-------------|------------------------------------|----------------------------------|
| HKDF operations (Perform approved security functions) | This service triggers OS API for HKDF operations (either Two Step Key Derivation using HMAC or the Key Derivation Function using Pseudorandom functions) | HKDF (Certs. A2713 and A2714) | OS-MKEK SD-SENC SD-SMAC SD-RMAC APP-HMAC-KEY | CO, User | E | Status Word (Response APDU 9000) |
| PBKDF Operation (Perform approved security functions) | 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 | PBKDF2 (Cert. A2714) | OS-MKEK SD-SENC SD-SMAC SD-RMAC | CO, User | E | Status Word (Response APDU 9000) |
| TLS KDF Functions (Perform approved security functions) | This service provides support for TLS v1.2 calculations. It does not implement the TLS v1.2 protocol | KDF (Cert. A2713) | OS-MKEK SD-SENC SD-SMAC SD-RMAC | CO, User | E | Status Word (Response APDU 9000) |
| Secure Hash Crypto Operations (Perform approved security functions) | This service triggers OS API for [FIPS 180-4] compliant hash algorithms | SHA (Cert. A2713) | OS-MKEK SD-SENC SD-SMAC SD-RMAC | CO, User | E | Status Word (Response APDU 9000) |
| SEMS Lite Applet Services | | | | | | |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|--------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------|-------------------------------------|
| SEMS Lite Authentication | The service provides the authenticated secure messaging | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) ECDSA (Cert. A2713) P-256 SHS (Cert. A2713) KAS- ECC (Cert. A2713) P-256 CKG (Vendor Affirmed) | OS-MKEK APP-ECC-RT-PRIV-KA APP-AES-RAM-KO-KEY APP-AES-RAM-Kn-KEY APP-ECC-RT-PUB-AUT APP-ECC-PUB-eKA APP-ECC-PUB-AUT APP-CERT-KR-AUT APP-CERT-AUT DAP- DAPK | CO, User | E, G, W, Z | Status Word (Response APDU 9000) |
| SEMS Lite Manage Content | The service is used to load data. The data is wrapped in SEMS Lite Authentication | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) ECDSA (Cert. A2713) P-256 SHS (Cert. A2713) KAS- ECC (Cert. A2713) P-256 CKG (Vendor Affirmed) | OS-MKEK APP-ECC-RT-PRIV-KA APP-AES-RAM-KO-KEY APP-AES-RAM-Kn-KEY APP-ECC-RT-PUB-AUT APP-ECC-PUB-eKA APP-ECC-PUB-AUT APP-CERT-KR-AUT APP-CERT-AUT DAP-DAPK | CO, User | E, G, W, Z | Status Word (Response APDU 9000) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|------------------------------------|-------------------------------------|
| SEMS Lite Root Key Update | This service updates APP-ECC-RT-PRIV-KA and APP-ECC-RT-PUB-AUT keys wrapped in SEMS Lite Authentication | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/GMAC (Cert. A2714) ECDSA (Cert. A2713) P-256 SHS (Cert. A2713) KAS- ECC (Cert. A2713) P-256 CKG (Vendor Affirmed) | OS-MKEK APP-ECC-RT-PRIV-KA APP-AES-RAM-KO-KEY APP-AES-RAM-Kn-KEY APP-ECC-RT-PUB-AUT APP-ECC-PUB-eKA APP-ECC-PUB-AUT APP-CERT-KR-AUT APP-CERT-AUT | CO | E, G, W, Z | Status Word (Response APDU 9000) |
| Card Reset | Power cycle or reset the module | N/A | N/A | CO, User, Unauthorised | N/A | Status Word (Response APDU 9000) |
| Context | Select an applet or manage logical channels | N/A | N/A | CO, User, Unauthorised | N/A | Status Word (Response APDU 9000) |
| Info | Read unprivileged data objects, e.g., module configuration or status information (Show Status). This service includes the Pre-operational Self-Test on-demand | N/A | N/A | CO, User, Unauthorised | N/A | Status Word (Response APDU 9000) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/ or SSPs | Indicator |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|------------------|------------------------|------------------------------------|----------------------------------|
| 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 | N/A | N/A | CO, User, Unauthorised | N/A | Status Word (Response APDU 9000) |

Table 8 – Approved Services

The modes of access shown in the table above are defined as:

- G = Generate: The service generates or derives the CSP/Public Key.
- W = Write: The service inputs the CSP/Public Key.
- E = Execute: The Module executes using the CSP/Public Key.
- R = Read: The service outputs the CSP/Public Key. CSP are always protected with the approved KTS.
- Z = Zeroize: The Module zeroizes the CSP/Public Key after usage. A zeroised CSP is not retrievable or reusable.

5 Software/Firmware Security

The cryptographic module is considered a hardware module with firmware components. An error detection code (32-bit CRC performed over all code located in Flash) is applied to all firmware components within the module. If the integrity test fails, the module enters the hard error (MUTE) state.

An operator of the module can perform the integrity test on demand with the GET DATA APDU command. As a single-chip hardware module, the executable form of the code, i.e., firmware is binary format. The module does not support loading of firmware from an external source.

ROM endurance has been proven to be more than 10 years after manufactured date. Therefore, per FIPS 140-3 IG 5.A, no pre-operational ROM integrity self-test has been implemented. The module's end-of-life procedures must be applied prior to the degradation of the ROM by setting the module to the TERMINATE state.

All data and control inputs, and data and status outputs of the cryptographic module and services are directed through the module's defined interfaces.

6 Operational Environment

The module claims to meet Physical Security Level 4 and thus the requirements per this section do not apply.

7 Physical Security

The module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The module uses standard passivation techniques. The module includes Environmental Failure Protection features such as temperature and voltage sensors. Fault Induction mitigation techniques are light sensors and spike sensors on the supply voltage lines.

Identification of internal features such as sensitive components or interconnections is impeded by a fine mesh of metal shield lines that resides at the outermost layers of the chip.

Delivery forms of the module are QFN package, contactless chip card module, or sawn wafer. Therefore, the module does not rely on any physical security based on a package.

| Physical Security Mechanism | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|-----------------------------|------------------------------------------|----------------------------------|
| N/A | N/A | N/A |

Table 9 – Physical Security Inspection Guidelines

| | Temperature or voltage Measurement | EFP or EFT | Result (Shutdown/Zeroisation) |
|------------------|------------------------------------|------------|-------------------------------|
| Low Temperature | -40°C | EFP | Shutdown |
| High Temperature | +105°C | EFP | Shutdown |
| Low Voltage | 1.62V | EFP | Shutdown |
| High Voltage | 6.0V | EFP | Shutdown |

Table 10 – EFP/EFT

| | Hardness tested temperature measurement |
|------------------|-----------------------------------------|
| Low Temperature | -45°C |
| High Temperature | +125°C |

Table 11 – Hardness Testing Temperature Ranges

8 Non-Invasive Security

Please see Section 12 below for information regarding non-invasive security countermeasures.

9 Sensitive Security Parameter Management

| Key /SSP Name /Type | Strength | Security Function and Cert. Number | Generation | Import /Export | Establishment | Storage | Zeroisation | Use & Related Keys |
|---------------------|----------|------------------------------------|-----------------------------------------|----------------|---------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| OS-DRBG-EI CSP | 384 bits | CTR_DRBG (Cert. A2713) | Internally via ENT (P) | N/A | N/A | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | Random value from ENT (P) used to seed reciprocally and AES-256 DRBG |
| OS-DRBG-STATE CSP | 880 bits | CTR_DRBG (Cert. A2713) | Internally via SP800-90Ar1 DRBG process | N/A | N/A | Stored in NVM in plaintext; object identifier to entity association | Destroyed by termination of the module (LifeCycle/Perform Zeroisation service); overwritten with zeroes | Current DRBG state value |
| OS-DRBG-KEY CSP | 256 bits | CTR_DRBG (Cert. A2713) | Internally via SP800-90Ar1 DRBG process | N/A | N/A | Stored in NVM in plaintext; object identifier to entity association | Destroyed by termination of the Module (LifeCycle/Perform Zeroisation service); overwritten with zeroes | Current DRBG state value |
| OS-DRBG-V CSP | 256 bits | CTR_DRBG (Cert. A2713) | Internally via SP800-90Ar1 DRBG process | N/A | N/A | Stored in NVM in plaintext; object identifier to entity association | Destroyed by termination of the Module (LifeCycle/Perform Zeroisation service); | Current DRBG state value |

| | | | | | | | overwritten with zeroes | |
|--------------------|----------|-----------------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------|-----|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| OS-DRBG-OUTPUT CSP | 256 bits | CTR_DRBG (Cert. A2713) | Internally via SP800-90Ar1 DRBG process | N/A | N/A | Stored in NVM in plaintext; object identifier to entity association | Destroyed by termination of the module (LifeCycle/Perform Zeroisation service); overwritten with zeroes | Unmodified output from the DRBG used for SSP generation |
| OS-SKEK CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) | N/A | Entered during manufacturing/ personalization | N/A | Stored in NVM in plaintext; object identifier to entity association | Destroyed by termination of the module (LifeCycle/Perform Zeroisation service); overwritten with zeroes | Used to build OS-MEK |
| OS-MKEK CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) | OS-SKEK permutation (xor between OS-SKEK and a constant value) | N/A | N/A | Stored in NVM in plaintext; object identifier to entity association | Destroyed by termination of the module (LifeCycle/Perform Zeroisation service); overwritten with zeroes | Used to encrypt all secret and private key data stored in NVM |
| SD-KENC CSP | 128 bits | AES CBC, ECB, CTR, | N/A | Entered during manufacturing/ | N/A | Stored in NVM encrypted with | Destroyed because of OS-MKEK zeroisation | Used to derive SD-SENC |

| | | | | | | | | |
|--------------------|----------|-----------------------------------------------------------------------------------------------------|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------------------------------------------------|
| | | CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) | | personaliz ation Or AES-CBC (using SD- KDEK) encrypted (RFC 3394 method) and transport- ted using platform SCP03 Exported using Approved KTS | | Approved AES CBC with OS- MKEK; key version to entity association | | |
| SD- KMAC CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) | N/A | Entered during Manufacturing/personalization Or AES-CBC (using SD- KDEK) encrypted (RFC 3394 method) and transport- ted using platform SCP03 Exported using Approved KTS | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation | Used to derive SD-SMAC |
| SD- KDEK CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. | N/A | Entered during manufacturing/personalization Or Entered encrypted with the | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation | Sensitive data decryption key used to decrypt CSPs |

| | | | | | | | | |
|--------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----------------------------------------------------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------|
| | | A2713) GCM/G MAC (Cert. A2714) | | previous SD-KDEK Exported using Approved KTS | | | | |
| SD- SENC CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) KDF SP800- 108 (Cert. A2713) CKG (Vendor Affirmed) | N/A | N/A | Deri- ved with Appr - oved KDF SP 800- 108 | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | Session encryption key used to secure channel data |
| SD- SMAC CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) KDF SP800- 108 (Cert. A2713) CKG (Vendor Affirm- ed) | N/A | N/A | Deri- ved with Appr - oved KDF SP 800- 108 | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | Session MAC key used to verify inbound secure channel data integrity |

| | | | | | | | | |
|-----------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-----------------------------------------------------------------------------------------|
| SD-RMAC CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) KDF SP800- 108 (Cert. A2713) CKG (Vendor Affirm- ed) | N/A | N/A | Der- ived with Appr- oved KDF SP 800- 108 | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | Session MAC key used to verify outbound secure channel data integrity |
| APP-TRANS PORT-CIPHER CSP | 256 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) | N/A | Entered during manufac- turing/per- sonaliza- tion Output: N/A | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation | Used to encrypt either exported or imported Secure Objects or data |
| APP-TRANS PORT-MAC CSP | 128 bits | AES CMAC (Cert. A2713) | N/A | Entered during Manufac- turing/per- sonaliza- tion Output: N/A | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation | Used to authenticate either exported or imported Secure Objects |
| APP-KAS-SSC-EC-PRIV-KEY CSP | 128 bits | KAS-ECC- SSC P- 256 (Cert. A2713) KDA (Cert. | N/A | Entered during Manufac- turing/per- sonaliza- tion | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to | Destroyed because of OS-MKEK zeroisation | KAS Shared Secret computation private key |

| | | A2713) | | Output: N/A | | entity association | | |
|----------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| APP-KAS-IOT-SS CSP | 128 bits | KAS-ECC- SSC P- 256 (Cert. A2713) KDA (Cert. A2714) | N/A | N/A | Established with the SP 800- 56A- rev3 KAS- ECC | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | KAS-ECC Shared Secret |
| APP-AES-KEY-AUTH CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) or ECDSA (Cert. A2713) | N/A | Entered during Manufacturing/personalization Output: via Approved KTS | Approved KTS | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation | Used in AESKey session or ECKey session authentication methods |
| APP-SENC CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) or ECDSA (Cert. A2713) KDF SP800- 108 (Cert. A2713) CKG | N/A | N/A | Derived with Approved KDF SP 800- 108 | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | AES Key or EC Key session encryption key used to encrypt / decrypt secure channel data |

| | | (Vendor Affirm-ed) | | | | | | |
|--------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------|
| APP-SMAC CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) or ECDSA (Cert. A2713) KDF SP800-108 (Cert. A2713) CKG (Vendor Affirm-ed) | N/A | N/A | Der-ived with Appr-oved KDF SP 800-108 | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | AES Key or EC Key session MAC key used to verify inbound secure channel data integrity |
| APP-RMAC CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) or ECDSA (Cert. A2713) KDF SP800-108 (Cert. A2713) CKG | N/A | N/A | Der-ived with Appr-oved KDF SP 800-108 | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | AES Key or EC Key session MAC key used to generate response secure channel data MAC |

| | | (Vendor Affirm-ed) | | | | | | |
|-----------------------|-------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------------------------------------------------------------------------|------------------------------------------|-----------------------------------------------------------------------|
| APP-USERID - FILE CSP | N/A | N/A | N/A | Entered during Manufacturing/personalization Output: via Approved KTS | Approved KTS | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation | 4-byte up to 16-byte UserID authentication data |
| APP-EC-PRIV-KEY CSP | 112, 128, 192, 256 bits | ECDSA Key Generation P-224, P-256, P-384, P-521 (Cert. A2713) CKG (Vendor Affirm-ed) | The Approved key pair generation method is compliant with FIPS 186-4, Sections B.43.23 (RSA) or B.4.2 (ECDSA), Key Pair Generation by Testing Candidates; Generated on the module using Approved DRBG, AES-256 CTR_DRBG | Entered: N/A Output: via Approved KTS | N/A | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation | Elliptic curve key that allows to perform EC cryptographic operations |
| APP-RSA-PRIV-KEY CSP | 112, 128, 152 bits | RSA Key Generation 2048, 3072, 4096 bits (Cert. A2713) CKG (Vendor | The Approved key pair generation method is compliant with FIPS 186-4, Sections B.43.23 (RSA) or B.4.2 | Entered: N/A Output: via Approved KTS | N/A | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation | RSA key that allows to perform RSA cryptographic operations |

| | | | | | | | |
|------------------------|--------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| | | Affirmed) | (ECDSA), Key Pair Generation by Testing Candidates; Generated on the module using Approved DRBG, AES-256 CTR_DRBG | | | | |
| APP-AES-KEY CSP | 128, 192, 256 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) | N/A | Entered during Manufacturing/personalization Output: via Approved KTS | Approved KTS | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation. Used to perform AES cipher mode operations |
| APP-HMAC-KEY CSP | 128 and 256 bits | HMAC SHA-1, SHA2-256, 384, 512 (Cert. A2713) | N/A | Entered during Manufacturing/personalization Output: via Approved KTS | Approved KTS | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation Used to perform KDF or HMAC operations |
| APP-ECC-RT-PRIV-KA CSP | 256 bits | ECDSA (Cert. A2713) P-521 SHS (Cert. A2713) | N/A | Entered during Manufacturing/ Personalization or Imported in secure channel specified by GP- Amd-I Output: | N/A | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | Destroyed because of OS-MKEK zeroisation Private static key used in key establishment (KAS-SSC) operations |

| | | | | | | | | |
|------------------------|----------|-------------------------------------------------------------------------------------------------|-----|------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | N/A | | | | | |
| APP-KAS-SEMS-SS CSP | 128 bits | KAS-ECC-SSC P-256 (Cert. #A2713) KDA (Cert. A2715) | N/A | N/A | Established with the SP 800-56A rev3 KAS | Temporarily stored in RAM in plaintext (does not persist beyond a power cycle); object identifier to entity association | Power-off (temporarily stored in RAM) | KAS Shared Secret CSP |
| APP-AES-RAM-KO-Key CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) CKG (Vendor Affirmed) | N/A | N/A | Established with the SP 800-56A rev3 KAS-SCC followed by SHA2-256 as One Pass KDF | Temporarily stored in RAM (does not persist beyond a power cycle) | Power-off (temporarily stored in RAM) | Used as secret key material in the very first decryption operations as part of Authentication and Secure Messaging service of SEMS Lite applet |
| APP-AES-RAM-Kn-Key CSP | 128 bits | AES CBC, ECB, CTR, CCM, CMAC (Cert. A2713) GCM/G MAC (Cert. A2714) | N/A | Imported in secure channel specified by GP-Amd-I Output: N/A | N/A | Temporarily stored in RAM (does not persist beyond a power cycle) | Power-off (temporarily stored in RAM) | Used as secret key material in the subsequent decryption operations as part of SEMS Lite Authentication and Secure Messaging service |
| DAP-DAPK PSP | 256 bits | ECDSA P-521 (Cert. | N/A | Entered during | N/A | Stored in NVM encrypted with | N/A – Considered protected by | ECC public key used for |

| | | | | | | | | |
|---------------------------------------------------|----------|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------|
| | | A2713) | | Manufacturing/ Personalization | | Approved AES CBC with OS- MKEK; key version to entity association | ISO 19790 definition | Mandated DAP |
| APP- KAS- SSC- EC- PUB- KEY PSP | 128 bits | KAS-ECC- SSC P-256 (Cert. A2713) | N/A | Entered during Manufacturing/ Personalization Output: Approved KTS | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | N/A – Considered protected by ISO 19790 definition | KAS Shared Secret computation public key |
| APP- EC- PUB- KEY-CO PSP | 128 bits | ECDSA (Cert. A2713) P-256 SHS (Cert A2713) | N/A | Entered during Manufacturing/ Personalization Output: Approved KTS | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | N/A – Considered protected by ISO 19790 definition | ECDSA public key used to authenticate the CO |
| APP- EC- PUB- KEY- USER PSP | 128 bits | ECDSA (Cert. A2713) P-256 SHS (Cert A2713) | N/A | Entered during Manufacturing/ Personalization Output: Approved KTS | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | N/A – Considered protected by ISO 19790 definition | ECDSA public key used to authenticate as user |
| APP- EC- PUBKE Y PSP | 128 bits | ECDSA (Cert. A2713) P-256 CKG (Vendor Affirm- ed) | The Approved key pair generation method is compliant with FIPS 186-4, Sections B.43.23 (RSA) or B.4.2 (ECDSA), Key Pair | Entered: N/A Output: Approved KTS | N/A | Stored in NVM encrypted with Approved AES CBC with OS- MKEK; key version to entity association | N/A – Considered protected by ISO 19790 definition | Used to execute EC cryptographic operations |

| | | | | | | | | |
|------------------------|--------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------------|----------------------------------------------------|-------------------------------------------------------------------|
| | | | Generation by Testing Candidates; Generated on the module using Approved DRBG, AES-256 CTR_DRBG | | | | | |
| APP-RSA-PUB-KEY PSP | 112, 128, 152 bits | RSA (Cert. A2713) 2048, 3072, 4096 bits CKG (Vendor Affirmed) | The Approved key pair generation method is compliant with FIPS 186-4, Sections B.43.23 (RSA) or B.4.2 (ECDSA), Key Pair Generation by Testing Candidates; Generated on the module using Approved DRBG, AES-256 CTR_DRBG | Entered: N/A Output: Approved KTS | N/A | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | N/A – Considered protected by ISO 19790 definition | Used to execute RSA cryptographic operations |
| APP-ECC-PUB-eKA PSP | 128 bits | KAS-ECC-SSC P-256 (Cert. A2713) | N/A | Entered: Certificate is entered in plain-text Output: N/A | N/A | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | N/A – Considered protected by ISO 19790 definition | Ephemeral EC public key used in key establishment (KAS) operation |
| APP-ECC-RT-PUB-AUT PSP | 256 bits | ECDSA (Cert. A2713) P-521 SHS (Cert.) | N/A | Entered: Certificate is entered in plain text | N/A | Stored in NVM encrypted with Approved AES CBC with OS- | N/A – Considered protected by ISO 19790 definition | EC public key used in ECDSA verification operations |

| | | | | | | | | |
|---------------------|----------|---------------------------------------------------|-----|------------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| | | A2713) | | Output: In plaintext | | MKEK; key version to entity association | | |
| APP-ECC-PUB-AUT PSP | 256 bits | ECDSA (Cert. A2713) P-521 SHS (Cert. A2713) | N/A | Entered: Certificate is entered in plain-text Output: N/A | N/A | Stored in NVM encrypted with Approved AES CBC with OS-MKEK; key version to entity association | N/A – Considered protected by ISO 19790 definition | Static EC public key used in ECDSA verification operations |
| APP-CERT-AUT PSP | 256 bits | ECDSA (Cert. A2713) P-521 SHS (Cert. A2713) | N/A | Entered: Certificate is entered in plain-text Output: N/A | N/A | Stored in NVM in plaintext; object identifier to entity association | N/A – Considered protected by ISO 19790 definition | Certificate with EC public key providing authorization and authenticity to SEMS Lite applet |
| APP-CERT-KR-AUT PSP | 256-bits | ECDSA (Cert. A2713) P-521 SHS (Cert. A2713) | N/A | Entered: Certificate is entered in plain text Output: N/A | N/A | Stored in NVM in plaintext; object identifier to entity association | N/A – Considered ‘protected’ by ISO 19790 definition | Certificate with 256-bit EC public key providing authorization and authenticity to SEMS Lite applet for SEMS Lite Root Key Update service |

Table 12 – SSPs

The module implements a NIST SP800-90Ar1 Approved CTR_DRBG. The unmodified outputs of the DRBG are used for Cryptographic Key Generation (CKG) of Symmetric Keys and seeds for Asymmetric Key Generation as noted in Table 3 in this document per Section 4 in NIST SP800-133r2.

| Entropy sources | Minimum Number of bits of entropy | Details |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| NIST SP800-90B ENT (P) – Used as entropy input to the Approved DRBG | 256-bits of overall entropy for AES-256 CTR_DRBG; 0.912949 per entropy source output bit | Noise source based on hardware implementing an iterated Bernoulli Shift Map |

Table 13 – Non-Deterministic Number Generator Specification

Per FIPS 140-3 IG 9.5.A, the module supports AD/EE (Automated Distribution/Electronic Entry).

10 Self-Tests

On power-on or on demand, the module performs self-tests described below. The pre-operational self-test must be completed successfully prior to any other use of cryptography by the module. The Cryptographic Algorithm Self-Tests are either performed at boot or prior to first use. The conditional self-tests are performed when the corresponding conditions occur. If one of the self-tests fails, the system is halted and will start again after a reset.

ROM endurance has been proven to be more than 10 years after manufactured date. Therefore, no pre-operational ROM integrity self-test has been implemented. The module's end-of-life procedures must be applied prior to the degradation of the ROM by setting the module to the TERMINATE state. The Flash Firmware Integrity check is performed on every reset or on demand.

Pre-operational Self-Tests

- Firmware Integrity: 32-bit CRC performed over all code located in Flash.

Conditional Self-Tests

- Cryptographic Algorithm Self-Tests
 - AES CBC 128-bit Encrypt KAT ◦ AES CBC 128-bit Decrypt KAT ◦ AES CMAC 128-bit Encrypt KAT ◦ AES CMAC 128-bit Decrypt KAT
 - CTR_DRBG 256-bit KAT (Health Tests: Generate, Reseed, Instantiate functions per Section 11 in NIST SP800-90Ar1)
 - ECDSA P-521 SHA-256 Signature Generation KAT
 - ECDSA P-521 SHA-256 Signature Verification KAT
 - HMAC-SHA2-256 KAT
 - KAS-ECC-SSC P-256 KAT
 - KDF TLS 1.2 KAT
 - KDA KAT (One-Step KDF per SP800-56Cr1 for both Cert. #A2714 and #A2715)
 - KDA KAT (Two-Step KDF KAT (HKDF) per SP800-56Cr1 for Cert.#A2713)
 - NIST KDF SP800-108 KAT (Counter mode with AES-128)
 - NIST KDF SP800-108 KAT (Feedback Mode with HMAC-SHA1)
 - NIST SP800-132 KDF KAT (with HMAC-SHA-1)
 - RSA 2048-bit SHA2-256 Signature Generation KAT
 - RSA 2048-bit SHA2-256 Signature Verification KAT
 - SHA-1 KAT (for both Cert. #A2713 and #A2714)
 - SHA2-256 KAT (for both Cert. #A2713 and #A2714 (inclusive of SHA2-224, per IG 10.3.A))
 - SHA2-512 KAT (for both Cert. #A2713 and #A2714 (inclusive of SHA2-384, per IG 10.3.A))
 - NIST SP800-90B ENT (P) Repetition Count Test (RCT) performed on raw data

- NIST SP800-90B ENT (P) Developer Defined Heath Test Transition Count Test performed on the raw data
- NIST SP800-90B ENT (P) Developer Defined Heath Test Chi-Square Test performed on the conditioned data
- NIST SP800-90B ENT (P) Developer Defined Heath Test Amplitude Limiter Analog Test on the analog data
- Pairwise Consistency Tests
 - Generate PCT: Pairwise consistency test performed when an asymmetric key pair is generated for RSA or ECC. The conditional test is implemented at the applet level
 - Signature PCT: Pairwise consistency test performed when a signature is generated for RSA or ECDSA
- Firmware Load Test: Signature Verification based on ECDSA P-256 with SHA2-256

Note: The module does not support loading of external firmware by the operator (it is limited to the vendor, NXP Semiconductors, at factory pre-shipment of the module). The Firmware Load Test above is performed by the module in support of the same.

All the 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. In case of a failure, the module enters a hard error (MUTE) state and returns a code/status indicator. The APDU code 9000 signifies success and 66A7 is the error indicator corresponding to the MUTE error state. The JCOP OS is intended to execute pre-operational self-tests (rather than conditional self- tests) periodically, since these tests are pre-defined to be executed post resets. The periodic time will thus always start from zero. RAM can be used to manage the periodic time interval which is the number of execution events e.g., number of APDUs/commands received (the tests are repeated after every 500,000 CAPDUs/commands).

11 Life-Cycle Assurance

All configuration management items are managed using an automated configuration management system. The module is designed to allow the testing of all provided security-related services. All firmware is implemented using a high-level language and is designed in a manner that avoids the use of code, parameters, or symbols not necessary for the module's functionality and execution.

While the module can be delivered with the Approved mode enabled by default, customers also have the option to receive a module which is in the unconfigured state, i.e., non-Approved mode. To comply with and maintain the FIPS 140-3 validation, it would be the CO's responsibility to enable the Approved mode of operation as follows (this information can also be found in the *JCOP 4.5 User guidance and administrator manual* document):

1. Install SEMS Lite applet to run in Approved mode of operation.
2. Install the IoT applet and configure the applet to run in Approved mode of operation.
3. Configure the Operation System to run in Approved mode of operation.

In each of these steps, it is in the CO's responsibility to apply proper security conditions and to ensure that once the device is put into Approved mode of operation, it will not be set into non-Approved mode of operation ever again. The operator can verify that the module is operating in the Approved mode by following instructions specified in Section 2 in this document.

There are no specific maintenance requirements for this module.

12 Mitigation of Other Attacks

The module is protected against the following non-invasive attacks: 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, fault induction mitigations like light sensors, voltage glitch sensors and an active shield, and detection of illegal address or instruction.

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. In addition to the non-invasive attacks, the module also uses standard passivation techniques and is protected by active shielding (a grid of top metal layer wires with tamper response) which qualifies for classification under mitigation of other attacks.

END OF DOCUMENT