# MultiApp V3 Platform
# FIPS 140-2 Cryptographic Module Security Policy

# Table of Contents

# Table of Tables

# Table of Figures

## References

| Reference | Full Specification Name |
|---|---|
| [FIPS140-2] | NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001 |
| [GlobalPlatform] | *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1,* March 2003, http://www.globalplatform.org<br>*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004 |
| [ISO 7816] | ISO/IEC 7816-1: 1998 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics*<br>ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts*<br>ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols*<br>ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange* |
| [ISO 14443] | *Identification cards -- Contactless integrated circuit cards -- Proximity cards*<br>ISO/IEC 14443-1:2008 Part 1*: Physical characteristics*<br>ISO/IEC 14443-2:2010 Part 2: *Radio frequency power and signal interface*<br>ISO/IEC 14443-3:2011 Part 3: *Initialization and anticollision*<br>ISO/IEC 14443-4:2008 Part 4: *Transmission protocol* |
| [JavaCard] | *Java Card 2.2.2 Runtime Environment (JCRE) Specification*<br>*Java Card 2.2.2 Virtual Machine (JCVM) Specification*<br>*Java Card 2.2.2 Application Programming Interface*<br>Published by Sun Microsystems, March 2006 |
| [SP800-131A] | *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011 |
| [ANS X9.31] | American Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1998 - Appendix A.2.4. |
| [SP 800-67] | NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011 |
| [FIPS113] | NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985. |
| [FIPS 197] | NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001. |
| [PKCS#1] | *PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002 |
| [FIPS 186-2] | NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-2, January, 2000 with Change Notice 1. (DSA, RSA and ECDSA) |
| [SP 800-56A] | NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007 |
| [FIPS 180-3] | NIST, *Secure Hash Standard*, FIPS Publication 180-3, October 2008 |

| Reference | Full Specification Name |
|---|---|
| [AESKeyWrap] | NIST, *AES Key Wrap Specification*, 16 November 2001. This document defines symmetric key wrapping, Use of 2-Key TDEA in lieu of AES is described in [IG] D.2. |
| [IG] | NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 2 May 2012. |

**Table 1 - References**

## Acronyms and definitions

| Acronym | Definition |
|---|---|
| API | Application Programming Interface |
| CM | Card Manager, see [GlobalPlatform] |
| CSP | Critical Security Parameter |
| DAP | Data Authentication Pattern, see [GlobalPlatform] |
| DPA | Differential Power Analysis |
| GP | Global Platform |
| HID | Human Interface Device (Microsoftism) |
| IC | Integrated Circuit |
| ISD | Issuer Security Domain, see [GlobalPlatform] |
| KAT | Known Answer Test |
| OP | Open Platform (predecessor to Global Platform) |
| PCT | Pairwise Consistency Test |
| PKI | Public Key Infrastructure |
| SCP | Secure Channel Protocol, see [GlobalPlatform] |
| SPA | Simple Power Analysis |

**Table 2 - Acronyms and Definitions**

# 1 Introduction

This document defines the Security Policy for the Gemalto MultiApp V3 cryptographic module, hereafter denoted *the Module*. The Module, validated to FIPS 140-2 overall Level 3, is a single chip smartcard module implementing the Global Platform operational environment, with Card Manager and a Demonstration Applet.

The Demonstration Applet is available only to demonstrate the complete cryptographic capabilities of the Module for FIPS 140-2 validation, and is not intended for general use. The term *platform* herein is used to describe the chip and operational environment, not inclusive of the Demonstration Applet.

The Module is a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load function to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

The FIPS 140-2 security levels for the Module are as follows:

| Security Requirement | Security Level |
|---|---|
| Cryptographic Module Specification | 3 |
| Cryptographic Module Ports and Interfaces | 3 |
| Roles, Services, and Authentication | 3 |
| Finite State Model | 3 |
| Physical Security | 3 |
| Operational Environment | N/A |
| Cryptographic Key Management | 3 |
| EMI/EMC | 3 |
| Self-Tests | 3 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | 3 |

**Table 3 - Security Level of Security Requirements**

## 1.1 Versions and mode of operation

**Hardware:** M7820 SLE78CLX1600P (Contact-only),
M7820 SLE78CLX1600P (Contactless-only)

**Firmware:** MultiApp V3.0, Demonstration Applet version V1.2

The Module implements only an Approved mode of operation, as delivered from the manufacturing environment. The explicit indicator of FIPS mode is available using the *Module Information* service (specifically, the GET DATA command with tag 0103). The Module responds with a multi-byte data set; the most significant bit of the 5th byte set to 1 is the explicit indicator of the FIPS Approved mode.

Specifically, the first five bytes will be:

B0 85 43 3F **81** (represented in hexadecimal, with the 5th byte shown in bold red font)

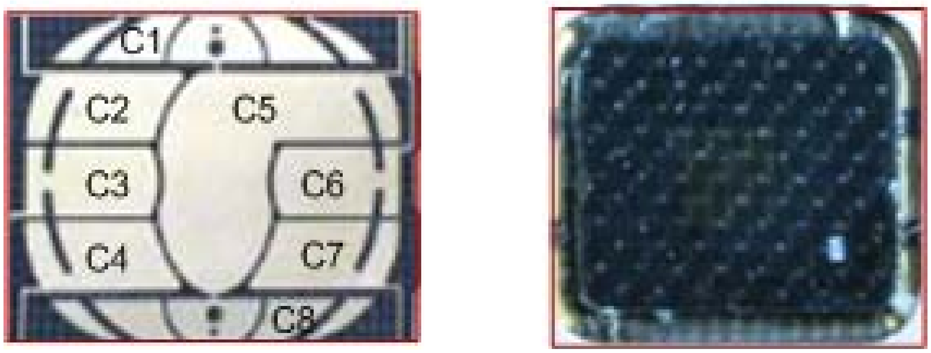
where the 5th byte is **1**000 0001 (represented in binary, with FIPS Approved mode indicator in bold red font).

## 1.2 Hardware and Physical Cryptographic Boundary

### *1.2.1 Contact-Only Configuration*

The Contact-only Module, intended for use in a plastic card body, is a single integrated circuit die wire-bonded to a frame connected to a contact plate, enclosed in epoxy. The cryptographic boundary is the contact plate surface on the top side, and the surface of the epoxy on the bottom side. The physical form of the Module is depicted in Figure 1.

The Module relies on [ISO 7816] card readers as input/output devices.



**Top (Contact Plate)**

**Bottom (Epoxy)**

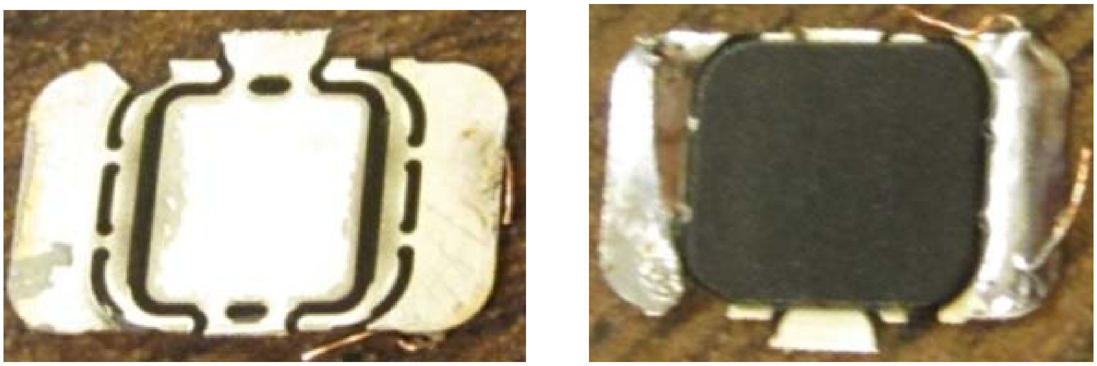
**Figure 1 - Physical Form of the Contact-Only Module**

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

**Table 4 - Ports and Interfaces**

### *1.2.2 Contactless-Only Configuration*

The Contactless-only Module, intended for use in a plastic card body, is a single integrated circuit die wire-bonded to a frame connected to an antenna coil connection plate, enclosed in epoxy. The cryptographic boundary is the antenna coil connection plate surface on the top side, and the epoxy surface on the bottom side. The physical form of the Module is depicted in Figure 2.



**Top (Antenna Coil Connection Plate)** **Bottom (Epoxy Coating)**

**Figure 2 - Physical Form of the Contactless-Only Module**

| Contact No. | Description | Logical interface type |
|---|---|---|
| LA, LB | Antenna coil connects | Power, data in, data out, control in, status out |

**Table 5 - Ports and Interfaces**

## 1.3 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment and applets.

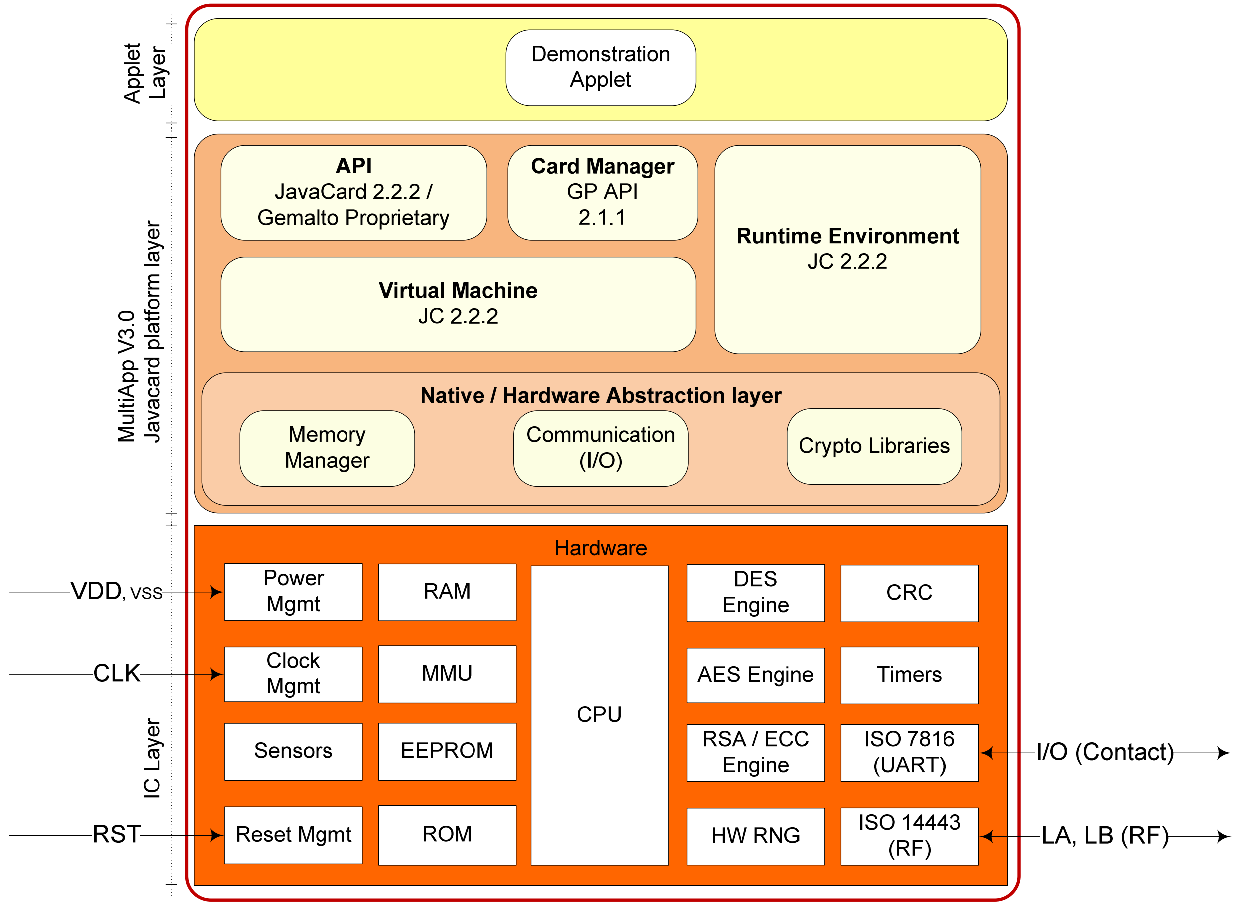


**Figure 3 - Module Block Diagram**

The *JavaCard API* is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary). The *Cryptography Libraries* implement the algorithms listed in Section 2. The *Javacard Runtime Environment* implements the dispatcher, registry, loader, and logical channel functionalities. The *Virtual Machine* implements the byte code interpreter, firewall, exception management and byte code optimizer functionalities.

The *Card Manager* is the card administration entity, allowing authorized users to manage the card content, keys, and life cycle states. The Card Manager behaves similarly to an applet, but is properly represented as a constituent of the platform. The *Memory Manager* implements functions such as memory access, allocation, deletion and garbage collection.

The *Communication* handler implements the ISO 7816 and ISO 14443 communications protocols.

The Module memory configuration is 280 Kb ROM, 7872 bytes RAM, and 160 Kb NVM.

Section 3 describes applet functionality in greater detail.

## 2 Cryptographic functionality

The Module operating system implements the *FIPS Approved* and *Non-Approved but Allowed* cryptographic function listed in Table 6 and Table 7 below.

| Algorithm | Description | Cert # |
|---|---|---|
| PRNG | [ANSI X9.31] AES-128 Pseudo Random number generator. | 1128 |
| Triple-DES | [SP 800-67] Triple Data Encryption Algorithm. The Module supports the 2-Key[1] and 3-Key options; CBC and ECB modes. Note that the Module does not support a mechanism that would allow collection of plaintext / ciphertext pairs aside from authentication, limited in use by a counter. | 1413 |
| Triple-DES MAC | [FIPS113] Triple-DES Message Authentication Code. Vendor affirmed, based on validated Triple-DES. | 1413 |
| AES | [FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128-, 192- and 256-bit key lengths with ECB and CBC modes. | 2261 |
| AES CMAC | [SP 800-38D] The Module supports 128-, 192- and 256-bit key lengths. | 2261 |
| SHA-1<br>SHA-2 | [FIPS 180-2] Secure Hash Standard compliant one-way (hash) algorithms. The module supports the SHA-1 (160-bit) and all SHA-2 (224-bit, 256-bit, 384-bit and 512-bit) variants. | 1946 |
| RSA | [FIPS 186-2] [PKCS#1] RSA algorithms.<br>– Key pair generation using 2048-bit keys;<br>– Signature generation using 2048-bit keys with SHA-2;<br>– Signature verification using 1024-, 2048-, 3072-and 4096-bit keys (any SHA size).<br>[FIPS 186-4] [PKCS#1] RSA algorithms.<br>– Key pair generation using 2048-bit keys;<br>– Signature generation using 2048-bit keys with SHA-2;<br>– Signature verification using 1024-, 2048-and 3072-bit keys (any SHA size).<br>This algorithm implementation has been CAVP validated for conformance to [FIPS 186-2] and [FIPS 186-4], because the module supports the 4096 bit key size which is not testable under [FIPS 186-4]. | 1287 |
| RSA CRT | [FIPS 186-2] [PKCS#1] RSA CRT algorithms.<br>– Key pair generation using 2048-bit keys;<br>– Signature generation using 2048-bit, 3072-bit and 4096-bit keys with SHA-2.<br>[FIPS 186-4] [PKCS#1] RSA CRT algorithms.<br>– Key pair generation using 2048-bit keys;<br>– Signature generation using 2048-and 3072-bit keys with SHA-2;<br>– Signature verification using 1024-, 2048-and 3072-bit keys (any SHA size).<br>This algorithm implementation has been CAVP validated for conformance to [FIPS 186-2] and [FIPS 186-4], because the module supports the 4096 bit key size which is not testable under [FIPS 186-4]. | 1288 |

[1] Per NIST SP 800-131A: Through December 31, 2015, the use of 2-key Triple DES for encryption is restricted: the total number of blocks of data encrypted with the same cryptographic key shall not be greater than $2^{20}$. *After December 31, 2015, 2-key Triple DES shall not be used for encryption.* Decryption using 2-key Triple DES is allowed for legacy-use.

| Algorithm | Description | Cert # |
|---|---|---|
| ECDSA | [FIPS 186-4] Elliptic Curve Digital Signature Algorithm using the NIST defined curves.<br>– Key pair generation using P-224, P-256, P-384, and P-521;<br>– Signature generation using P-224, P-256, P-384, and P-521 with SHA-2;<br>– Signature verification using P-192, P-224, P-256, P-384, and P-521 (any SHA size). | 363 |
| ECC CDH | [SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive using the NIST defined curves: P-224, P-256, P-384 and P-521. | 41 (CVL) |

**Table 6 - FIPS Approved Cryptographic Functions**

| Algorithm | Description |
|---|---|
| EC DH | Elliptic Curve Diffie-Hellman key agreement, non-compliant to SP 800-56A as allowed by IG D.8 Scenario 4 and SP 800-131A. Used for demonstration purposes only in the Demonstration Applet.<br>EC Diffie-Hellman using P-256, P-384, and P-521 curves (key agreement; key establishment methodology provides 112 to 256 bits of encryption strength). |
| Symmetric key wrap | The Module supports symmetric key wrapping using 2-Key TDEA or AES-128, as allowed by IG D.9.<br>Triple-DES (Cert. #1413, key wrapping; key establishment methodology provides 112 bits[2] of encryption strength)<br>AES (Cert. #2261, key wrapping; key establishment methodology provides 128 bits of encryption strength) |

**Table 7 - FIPS Non-Approved But Allowed Cryptographic Functions**

The module implements algorithms, modes and key sizes that are Disallowed as of January 1, 2014 per the NIST SP 800-131A transitions. Algorithms providing less than 112 bits of security strength (Disallowed per NIST SP 800-131A) are not allowed in the FIPS Approved mode of operation for use by Federal agencies. The Disallowed algorithms, modes and key sizes are listed in Table 8 below.

| Algorithm | Description | Cert # |
|---|---|---|
| RSA | [FIPS 186-2] [PKCS#1] RSA algorithms.<br>– Key pair generation using 1024-bit keys;<br>– Signature generation using 1024-bit keys with SHA-1/SHA-2 and 2048-bit keys with SHA-1.<br>[FIPS 186-4] [PKCS#1] RSA algorithms.<br>– Key pair generation using 1024-bit keys;<br>– Signature generation using 1024-bit keys with SHA-1/SHA-2 and 2048-bit keys with SHA-1. | 1287 |

[2] The Module claims 112-bit security strength for its 2-Key Triple-DES operations, as the meet-in-the-middle attack rationale described in SP 800-131A does not apply unless the attacker has access to encrypt/decrypt pairs.

| Algorithm | Description | Cert # |
|---|---|---|
| RSA CRT | [FIPS 186-2] [PKCS#1] RSA CRT algorithms.<br>– Key pair generation using 1024-bit keys;<br>– Signature generation using 1024-bit keys with SHA-1/SHA-2 and 2048-bit (or larger) keys with SHA-1.<br>[FIPS 186-4] [PKCS#1] RSA CRT algorithms.<br>– Key pair generation using 1024-bit keys;<br>– Signature generation using 1024-bit keys with SHA-1/SHA-2 and 2048-bit (or larger) RSA keys with SHA-1. | 1288 |
| ECDSA | [FIPS 186-4] Elliptic Curve Digital Signature Algorithm.<br>– Key pair generation using P-192;<br>– Signature generation using P-192 with SHA-1/SHA-2 and P-224, P-256, P-384, and P-521 with SHA-1. | 363 |
| ECC CDH | [SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive using P-192. | 41 (CVL) |
| EC DH | Elliptic Curve Diffie-Hellman key agreement, non-compliant to SP 800-56A. Used for demonstration purposes only in the Demonstration Applet.<br>EC Diffie-Hellman using P-192 curve (key agreement; key establishment methodology provides <112 bits of encryption strength; non-compliant). | N/A |
| FFC DH | Finite Field Cryptography Diffie-Hellman key agreement, non-compliant to SP 800-56A. Used for demonstration purposes only in the Demonstration Applet.<br>Diffie-Hellman using 1024-bit modulus size (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant). | N/A |

**Table 8 - Cryptographic Functions Disallowed per NIST SP 800-131A Transitions**

## 2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module are described in the services detailed in Section 4. In the tables below, the OS prefix denotes operating system, the SD prefix denotes the Global Platform Security Domain, the DAP prefix denotes the Global Platform Data Authentication Protocol, and the DEM prefix denotes a Demonstration Applet CSP.

| Key | Description / Usage |
|---|---|
| OS-RNG-SEED-KEY | [ANS X9.31] RNG AES-128 seed key. |
| OS-RNG-STATE | [ANS X9.31] RNG 128-bit block and 128-bit counter values. |
| OS-GLOBALPIN | 6 to 16 byte Global PIN value. Character space is not restricted by the module. |
| SD-KENC | 2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) encryption master key, used to derive SD-SENC. |
| SD-KMAC | 2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Security Domain MAC master key, used to derive SD-SMAC. |
| SD-KDEK | 2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Security Domain sensitive data decryption key. |

| Key | Description / Usage |
|---|---|
| SD-SENC | 2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Security Domain session decryption key, used to decrypt secure channel messages. |
| SD-SMAC | 2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Security Domain session MAC key, used to verify secure channel message integrity. |
| SD-SDEK | 2-Key TDES (SCP01) or AES-128/192/256 (SCP03) Session DEK key used by the CO role to decrypt CSPs. |
| DAP-SYM | 2-Key TDES (SCP01/02) or AES-128/192/256 (SCP03) key optionally loaded in the field and used to verify the MAC of packages loaded into the Module. |
| DEM-EDK | 2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) encryption / decryption key used by the Demonstration Applet *Symmetric Cipher* service. |
| DEM-KAP-PRI* | P-192, P-224, P-256, P-384, P-521 ECDSA private key used by the Demonstration Applet *Key Agreement Primitives* service. |
| DEM-KGS-PRI* | 1024- or 2048-bit RSA or P-192, P-224, P-256, P-384, P-521 ECDSA private key used by Demonstration Applet *Generate Asymmetric Key Pair* service. |
| DEM-MAC | 2-Key Triple-DES MAC (SCP01/02) or AES-128/192/256 CMAC (SCP03) key used by Demonstration Applet *Message Authentication* service. |
| DEM-MK | 2-Key Triple-DES master key used to encrypt or decrypt Demonstration Applet CSPs exported out of or imported into the Module. |
| DEM-SGV-PRI* | 1024-, 2048-, 3072-, 4096-bit RSA or P-192, P-224, P-256, P-384, P-521 ECDSA private key used by Demonstration Applet Asymmetric Signature service. |

**Table 9 - Critical Security Parameters**

* CSPs impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Table 8).

## 2.2 Public Keys

| Key | Description / Usage |
|---|---|
| DAP-SV-PUB | RSA 1024 GlobalPlatform Data Authentication Public Key used to verify the signature of packages loaded into the Module. |
| DEM-KAP-PUB | P-192, P-224, P-256, P-384, P-521 ECDSA public key used by the Demonstration Applet *Key Agreement Primitives* service. |
| DEM-KGS-PUB | 1024-, 2048-bit RSA or P-192, P-224, P-256, P-384, P-521 ECDSA public key used by Demonstration Applet *Generate Asymmetric Key Pair* service. |
| DEM-SGV-PUB | 1024-, 2048-, 3072-, 4096-bit RSA or P-192, P-224, P-256, P-384, P-521 ECDSA public key used by Demonstration Applet Asymmetric Signature service. |

**Table 10 - Public Keys**

# 3 Roles, authentication and services

The Module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage. Only one operator at a time is permitted on a channel.

Applet deselection (including Card Manager), card reset or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services.

Authentication data is encrypted during entry (by SD-SDEK), is stored in plaintext and is only accessible by authenticated services.

Table 11 lists all operator roles supported by the Module.

| Role ID | Role Description |
|---|---|
| CO | Cryptographic Officer – role that manages Module content and configuration, including issuance and management of Module data via the ISD. Authenticated as described in *Secure Channel Protocol Authentication* below. |
| User | User - The User role for FIPS 140-2 validation purposes, authenticated as described in *Demonstration Applet Authentication* below. |

**Table 11 - Roles Supported by the Module**

## 3.1 Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method is provided by the *Secure Channel* service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The SD-SENC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module in the CO role).

[SP 800-131A] Section A.1 provides the NIST rationale for 2-Key TDEA security strength. The Module encrypts a total of one block (the mutual authentication cryptogram) over the life of the session encryption key; no decrypted data is output by the Module. The Module claims 112-bit security strength for its 2-Key TDEA operations, as the meet-in-the-middle attack rationale described in [SP 800-131A] does not apply unless the attacker has access to encrypt/decrypt pairs.

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

- 1/2^64 = 5.4E-20 (for 2-Key Triple-DES SD-KENC/SD-SENC)
- 1/2^128 = 2.9E-39 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

The Module enforces a maximum of 255 failed SCP authentication attempts. The probability that a random attempt will succeed over a one minute interval is:

- 255/2^64 = 1.30E-18 (for 2-Key Triple-DES SD-KENC/SD-SENC)
- 255/2^128 = 7.5E-37 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

### 3.2 Demonstration Applet Authentication Method

This authentication method compares a PIN value sent to the Module over an encrypted channel to the stored OS-GLOBALPIN value; if the two values are equal, the operator is authenticated. This method is used in the Demonstration Applet services to authenticate to the User role.

The module enforces OS-GLOBALPIN string length of 6 bytes minimum (16 bytes maximum), allowing all characters, so the strength of this authentication method is as follows:

- The probability that a random attempt at authentication will succeed is 1/256^6.
- Based on a maximum count of 15 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is 15/256^6.

### 3.3 Services

All services implemented by the Module are listed in the tables below.

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

**Table 12 - Unauthenticated Services**

| Service | Description | CO | User |
|---|---|---|---|
| Lifecycle | Modify the card or applet life cycle status. | X | |
| Manage Content | Load and install application packages and associated keys and data. | X | |
| Module Info (Auth) | Read module configuration or status information (privileged data objects) | X | |
| Secure Channel | Establish and use a secure communications channel. | X | |
| Digital Signature* | Demonstrate RSA and ECDSA digital signature generation and verification. | | X |
| Generate Key Pair* | Demonstrate RSA and ECDSA key generation | | X |
| Key Agreement* | Demonstrate Approved FFC and EC Diffie-Hellman key agreement. | | X |
| Message Authentication | Demonstrate Triple-DES Mac and AES CMAC. | | X |
| Symmetric Cipher | Demonstrate use of Triple-DES and AES for encryption and decryption. | | X |

**Table 13 - Authenticated Services**

* Services impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Table 8).

| Service | CSPs | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | OS-RNG-SEED-KEY | OS-RNG-STATE | OS-GLOBALPIN | SD-KENC | SD-KMAC | SD-KDEK | SD-SENC | SD-SMAC | SD-SDEK | DAP-SYM | DEM-EDK | DEM-MAC | DEM-SGV-PRI | DEM-KGS-PRI | DEM-KAP-PRI | DEM-MK |
| Module Reset | E<br>W | ZEG<br>W | -- | -- | -- | -- | Z | Z | Z | -- | -- | -- | -- | -- | -- | -- |
| Module Info (Unauth) | -- | -- | | -- | -- | -- | E[3] | E[1] | E[1] | -- | -- | -- | -- | -- | -- | -- |
| Context | -- | -- | | -- | -- | -- | Z | Z | Z | -- | -- | -- | -- | -- | -- | -- |
| Secure Channel | -- | EW | | E | E | E | GE[1] | GE[1] | GE[1] | -- | -- | -- | -- | -- | -- | -- |
| Manage Content | -- | -- | W | W | W | W | E[1] | E[1] | E[1] | EW | -- | -- | -- | -- | -- | -- |
| Lifecycle | Z | Z | Z | Z | Z | -- | -- | -- | -- | Z | Z | -- | Z | Z | Z | Z |
| Module Info (Auth) | -- | -- | -- | -- | -- | -- | E[1] | E[1] | E[1] | | | | | | | |
| Symmetric Cipher | -- | -- | E | -- | -- | -- | -- | -- | -- | -- | EW<br>Z | -- | -- | -- | -- | E |
| Message Authentication | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | EW<br>Z | -- | -- | -- | -- |
| Digital Signature | -- | EW | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | ER<br>WZ | -- | -- | E |
| Generate Key Pair | -- | EW | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | GE<br>RW<br>Z | -- | E |
| Key Agreement Primitives | -- | -- | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | ER<br>WZ | E |

**Table 14 - CSP Access by Service**

- G = Generate: The Module generates the CSP.
- R = Read: The Module reads the CSP (read access to the CSP by an outside entity).
- E = Execute: The Module executes using the CSP.
- W = Write: The Module writes the CSP. The write access is typically performed after a CSP is imported into the Module or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure)
- -- = Not accessed by the service.

[3] "E" for Secure Channel keys is included for situations where a Secure Channel has been established and all traffic is received encrypted. The Secure Channel establishment includes authentication to the module.

# 4 Self-test

## 4.1 Power-on self-test

On power-on or reset, the Module performs self-tests as described in Table 15 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the *Card Is Mute* error state.

| Test Target | Description |
|---|---|
| FW integrity | 16 bit CRC performed over all code located in EEPROM. This integrity test is not required or performed for code stored in masked ROM code memory. |
| ANS X9.31 | Performs a KAT using fixed values of OS-RNG-SEED and OS-RNG-STATE. |
| Triple-DES | Performs separate encrypt and decrypt KATs using 3-Key TDEA in ECB mode. |
| AES | Performs decrypt KAT using an AES 128 key in ECB mode. AES encrypt is self-tested as an embedded algorithm of AES-CMAC. |
| AES CMAC | Performs an AES-CMAC Generate KAT using an AES 128 key. Note that AES-CMAC Verify is identical to a Generate KAT (perform Generate then compare to the input) hence a single KAT verifies both functions. |
| ECDSA | Performs separate ECDSA signature and verification KATs using p-224. |
| RSA | Performs separate RSA PKCS#1 signature and verification KATs using an RSA 2048 bit key. |
| RSA CRT | Performs RSA PKCS#1 signature KAT using an RSA 2048-bit key. |
| SHA-1, SHA-2 | Performs separate KATs for SHA-1, SHA-256 and SHA-512. |
| ECC CDH | Performs a KAT for ECC CDH using p-224 keys constituents. |

**Table 15 - Power-On Self-Test**

## 4.2 Conditional self-tests

On every call to the ANSI X9.31 RNG, the Module performs the AS09.42 RNG test to assure that the output is different than the previous value.

When an RSA or ECDSA key pair is generated the Module performs a pairwise consistency test.

When new firmware is loaded into the Module using the *Manage Content* service, the Module verifies the integrity of the new firmware (applet) using MAC verification with the SD-SMAC key. Optionally, the Module may also verify a signature of the new firmware (applet) using the DAP-SV-PUB public key or the DAP-SYM key; the signature block in this scenario is generated by an external entity using the private key corresponding to DAP-SV-PUB or the symmetric DAP-SYM.

## 5 Physical security policy

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques

The Module is designed to be mounted in a plastic smartcard or similar package; physical inspection of the epoxy side of the Module is not practical after mounting. The Module also provides a key to protect the Module from tamper during transport and the additional physical protections listed in Section 8 below.

Note: Module hardness testing was only performed at ambient temperature; no assurance is provided for Level 3 hardness conformance at any other temperature.

## 6 Operational environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

## 7 Electromagnetic interference and compatibility (EMI/EMC)

The Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

## 8 Mitigation of other attacks policy

The Module implements defenses against:

- Fault attacks
- Side channel analysis (Timing Analysis, SPA/DPA, Simple/Differential Electromagnetic Analysis)
- Probing attacks
- Card tearing

## 9 Security Rules and Guidance

The Module implementation also enforces the following security rules:

- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support manual key entry, output plaintext CSPs or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

END OF DOCUMENT