gemalto
security to be free

# IDCore 3130 Platform

# FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

## Table of Contents

References ..... 4
Acronyms and Definitions ..... 5
1. Introduction ..... 6
2. Cryptographic Module Ports and Interfaces ..... 7
2.1 Hardware and Physical Cryptographic Boundary ..... 7
2.2 PIN assignments - Contact & Combi modules: ..... 8
3. Cryptographic Module Specification ..... 9
3.1 Firmware and Logical Cryptographic Boundary ..... 9
3.2 Versions and Mode of Operation ..... 10
3.3 Cryptographic Functionality ..... 11
4. Platform Critical Security Parameters ..... 12
4.1 Platform Critical Security Parameters ..... 12
4.2 Demonstration Applet Critical Security Parameters ..... 14
4.3 Platform Public Keys ..... 14
4.4 Demonstration Applet Public Keys ..... 14
5. Roles, Authentication and Services ..... 15
5.1 Secure Channel Protocol Authentication Method ..... 15
5.2 Demonstration applet Authentication Method ..... 16
5.3 Services ..... 16
6. Finite State Model ..... 19
7. Physical Security Policy ..... 20
8. Operational Environment ..... 20
9. Electromagnetic Interference and Compatibility (EMI/EMC) ..... 20
10. Self-test ..... 20
10.1 Power-on Self-test ..... 20
10.2 Conditional Self-tests ..... 21
10.3 Reducing the number of Known Answer Tests ..... 21
11. Design Assurance ..... 21
11.1 Configuration Management ..... 21
11.2 Delivery and Operation ..... 22
11.3 Guidance Documents ..... 22
11.4 Language Level ..... 22
12. Mitigation of Other Attacks Policy ..... 22
13. Security Rules and Guidance ..... 22

## Table of Tables

Table 1 – References ........ 5
Table 2 – Acronyms and Definitions ........ 5
Table 3 – Security Level of Security Requirements ........ 6
Table 4 – Module Physical Ports and Corresponding Logical Interfaces ........ 8
Table 5 - Voltage and Frequency Ranges ........ 8
Table 6 – Contactless voltage and Frequency Ranges ........ 8
Table 7 – FIPS Approved Cryptographic Functions ........ 12
Table 8 – FIPS Non-Approved but Allowed Cryptographic Functions ........ 12
Table 9 – Platform Critical Security Parameters ........ 13
Table 10 – Demonstration Applet Critical Security Parameters ........ 14
Table 11 – Platform Public Keys ........ 14
Table 12 – Demonstration Applet Public Keys ........ 14
Table 13 - Roles Supported by the Module ........ 15
Table 14 - Unauthenticated Services ........ 16
Table 15 – Authenticated Services ........ 16
Table 16 – CSP Access by Service ........ 18
Table 17 – Power-On Self-Test ........ 21

## Table of Figures

Figure 1– Physical form and Cryptographic Boundary ........ 7
Figure 2 - Module Block Diagram ........ 9

## References

| Acronym | Full Specification Name |
|---|---|
| [FIPS140-2] | NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001 |
| [GlobalPlatform] | *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1,* January 2011, http://www.globalplatform.org |
| [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 3.0.5 Runtime Environment (JCRE) Specification*<br>*Java Card 3.0.5 Virtual Machine (JCVM) Specification*<br>*Java Card 3.0.5 Application Programming Interface*<br>Published by Sun Microsystems, October 2015. |
| [SP800-131A] | NIST Special Publication 800-131A revision 1, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, November 2015 |
| [SP 800-133] | NIST Special Publication 800-133, *Recommendation for Cryptographic Key Generation*, December 2012 |
| [SP 800-38B] | NIST Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication*, May 2005 |
| [SP 800-90A] | NIST Special Publication 800-90A revision 1, *Recommendation for the Random Number Generation Using Deterministic Random Bit Generators (Revised)*, June 2015 |
| [SP 800-67] | NIST Special Publication 800-67 revision 2, *Recommendation for the Triple Data Encryption Algorithm (Triple-DES) Block Cipher*, November 2017 |
| [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 186-4] | NIST, Digital Signature Standard (DSS), FIPS Publication 186-4, July, 2013 |
| [SP 800-56A] | NIST Special Publication 800-56A revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013 |
| [SP 800-56B] | NIST Special Publication 800-56B revision 1, *Recommendation for Pair-Wise Key-* |

| Acronym | Full Specification Name |
|---|---|
| | *Establishment Schemes Using Integer Factorization Cryptography*, September 2014 |
| [FIPS 180-4] | NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015 |
| [SP 800-38F] | NIST Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012 |
| [IG] | NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated January 19th |

**Table 1 – References**

## Acronyms and Definitions

| Acronym | Definition |
|---|---|
| API | Application Programming Interface |
| CM | Cryptographic Module |
| CSP | Critical Security Parameter |
| DAP | Data Authentication Pattern, see [GlobalPlatform] |
| DM | Delegated Management, 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] |
| SSD | Supplementary Security Domain, see [GlobalPlatform] |
| SPA | Simple Power Analysis |

**Table 2 – Acronyms and Definitions**

## 1. Introduction

This document defines the Security Policy for the Gemalto IDCore 3130 Platform cryptographic module, herein denoted the *Module*. The *Module*, validated to FIPS 140-2 overall Level 3, is a single-chip “dual” 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**

The CM implementation is compliant with:

- [ISO 7816] Parts 1-4
- [JavaCard]
- [GlobalPlatform]

# 2. Cryptographic Module Ports and Interfaces

## 2.1 Hardware and Physical Cryptographic Boundary

The *Module* is designed to be embedded into a plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna. The physical form of the *Module* is depicted in Figure 1 (to scale). The cryptographic boundary is defined as the surfaces and edges of the packages as shown in Table 4 and figure 1. The *Module* relies on [ISO 7816] and/or [ISO 14443] card readers as input/output devices.

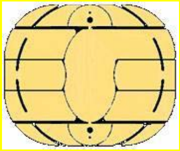
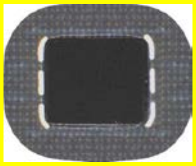
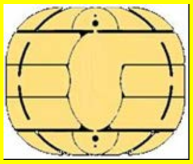
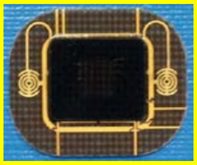
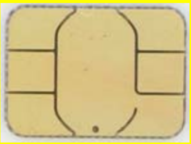
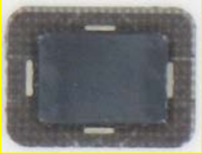
| **WORLD RLT module (SLE78CFX400VPH)** | |
|---|---|
| <br>Oblong punching<br>**Top View – Contact Plate** | <br>**Bottom View - Black Epoxy with RLT technology** |
| **WORLD Combi RLT module (SLE78CLFX400VPH)** | |
| <br>Oblong punching<br>**Top View – Combi Plate** | <br>**Bottom View - Black Epoxy with RLT technology** |
| **PICO RLV module (SLE78CFX400VPH)** | |
| <br>**Top View – Contact Plate** | <br>**Bottom View - Black Epoxy with RLV technology** |

**Figure 1– Physical form and Cryptographic Boundary**

### 2.2 PIN assignments - Contact & Combi modules:

WORLD Combi RLT module has access to contact and contactless interfaces. The WORLD RLT and PICO RLV modules only have access to the contact interface.

| Contact No. | Description | Logical interface type |
|---|---|---|
| VCC | Supply voltage | Power |
| RST | Reset signal | Control in |
| CLK | Clock signal | Control in |
| GND | Ground | Power |
| I/O | Input/output | Data in, data out, control in, status out |
| LA | Antenna coil connection (combi only) | Power, Data in, Data out, Control in, Status out |
| LB | Antenna coil connection (combi only) | Power, Data in, Data out, Control in, Status out |

**Table 4 – Module Physical Ports and Corresponding Logical Interfaces**

For contact interface operation, the *Module* conforms to [ISO 7816] part 1 and part 2. The electrical signals and transmission protocols follow the [ISO 7816] part 3. The conditions of use are the following:

| Conditions | Range |
|---|---|
| Voltage | 1.8V, 3 V and 5.5 V |
| Frequency | 1MHz to 10MHz |

**Table 5 - Voltage and Frequency Ranges**

For contactless interface operation, the *Module* conforms to [ISO 14443] part 1 for physical connections, and to [ISO 14443] parts 2, 3 and 4 for radio frequencies and transmission protocols.

The conditions of use are the following:

| Conditions | Range |
|---|---|
| Supported bit rate | 106 Kbits/s, 212 Kbits/s, 424 Kbits/s, 848 Kbits/s |
| Operating field | Between 1.5 A/m and 7.5 A/m rms |
| Frequency | 13.56 MHz +- 7kHz |

**Table 6 – Contactless voltage and Frequency Ranges**

# 3. Cryptographic Module Specification

## 3.1 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment and applets.

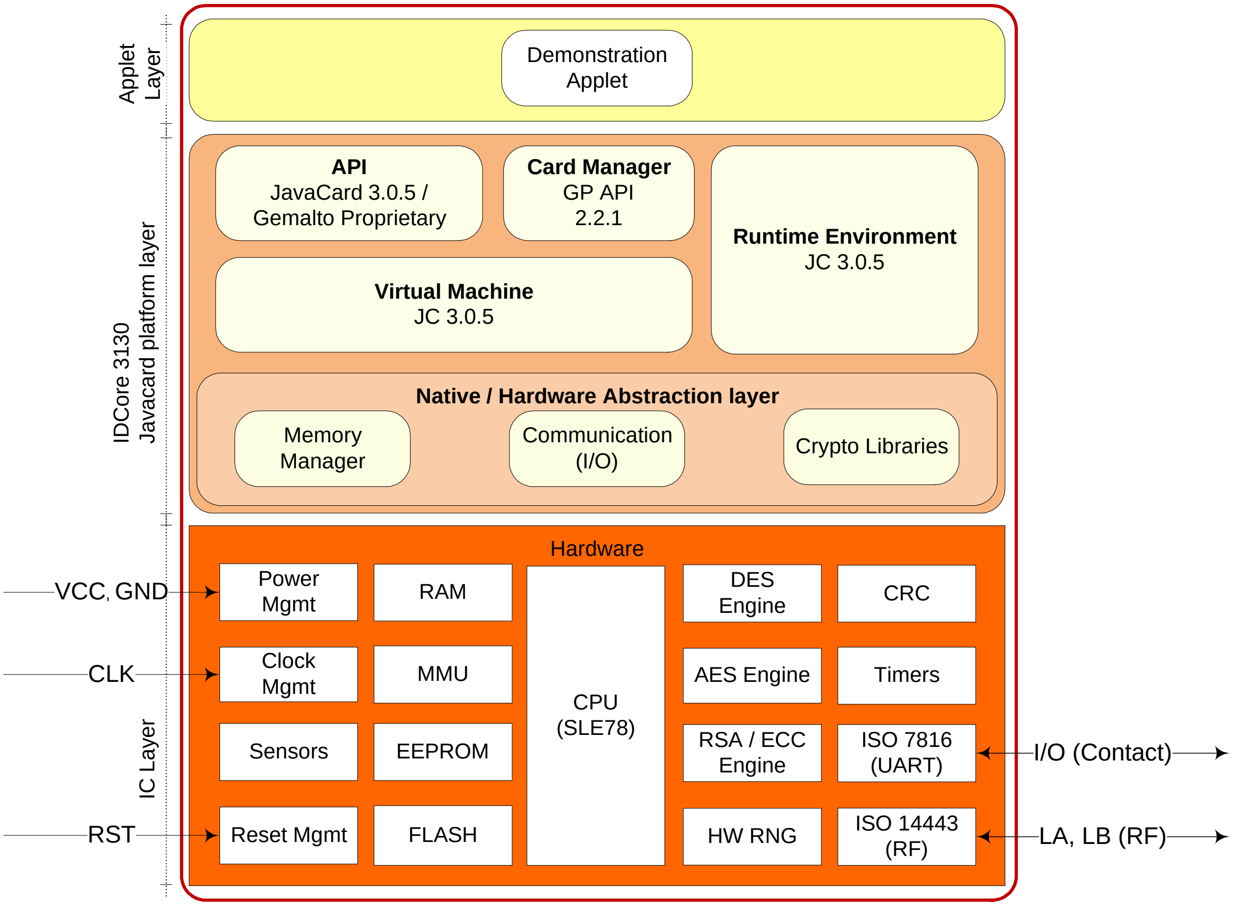


**Figure 2 - Module Block Diagram**

The CM supports [ISO7816] T=0, T=1 and T=CL communication protocols.

The CM provides an execution sandbox for Applets, performing the requested services as described in this security policy. Applets access module functionality via internal API entry points that are not exposed to external entities. External devices have access to CM services by sending APDU commands.

The CM inhibits all data output via the data output interface while the module is in error state and during self-tests.

The *JavaCard API (JCAPI)* is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

The *JavaCard Runtime Environment (JCRE)* implements the dispatcher, registry, loader, and logical channel functionalities.

The *Virtual Machine (VM)* 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. In case of delegated management (DM), the Supplementary Security Domain (SSD) behaves similarly to the Card Manager in term of card content, keys and life cycle states.

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 in contactless mode and dual mode.

The *Cryptography Libraries* implement the algorithms listed in Section 3.3.

## 3.2 Versions and Mode of Operation

**Hardware:**

Infineon SLE78CLFX400VPH
Infineon SLE78CFX400VPH

**Firmware**:

IDCore 3130 (Build09C), Demonstration Applet version V1.6

This Module is available in one of the three possible packaging options:

- World RLT: P/N (Part Number) = **A1977038** (Contact only)
- World Combi RLT: P/N = **A1714221** (Combi)
- Pico RLV: P/N = **A2023188** (Contact only)

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 Info* service (specifically, the GET DATA command with tag 012F). The *Module* responds with a single byte, where the explicit indicator of the FIPS approved mode is stored and will be 01.

### 3.3 Cryptographic Functionality

The Module implements the *FIPS Approved* cryptographic functions listed in Table 7 below:

| Algorithm | Description | Cert # |
|---|---|---|
| AES | [FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128-, 192- and 256-bit key lengths with ECB and CBC encrypt/ decrypt modes. | 5243 |
| AES CMAC | [SP 800-38B] The Module supports 128-, 192- and 256-bit key lengths. | 5243 |
| CKG | [SP 800-133] Section 6.1, Section 7.1: The Module generates symmetric keys and seeds to be used in asymmetric key generation directly from unmodified DRBG output. | Vendor Affirmed |
| CVL (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. | 1713 |
| CVL (RSADP) | [SP 800-56B] RSA key decryption primitive using 2048-bit keys (same RSA implementation validated below). | 1715<br>1716 |
| CVL (RSASP1) | [FIPS 186-4] [PKCS#1 v2.1] RSA signature generation primitive using 2048-bit keys (same RSA implementation validated below). | 1714<br>1717 |
| DRBG | [SP 800-90A] Deterministic Random Bits Generator (256-bit security strength CTR-DRBG based on AES). | 2005 |
| ECDSA | [FIPS 186-4] Elliptic Curve Digital Signature Algorithm using the NIST defined curves.<br>– Key pair generation: P-224, P-256, P-384 and P-521 curves.<br>– Signature generation: P-224, P-256, P-384 and P-521 curves with SHA-2.<br>– Signature verification: P-192 (not used), P-224, P-256, P-384 and P-521 curves (approved SHA sizes of the CM). | 1365 |
| KAS | [SP 800-56A] The Module supports OnePAssDH P-256 with SHA-256 for OPACITY secure Messaging (not used). | 165 |
| KBKDF | [SP 800-108] The Module supports AES CMAC 128-, 192- and 256-bit key lengths. | 177 |
| KTS | [SP 800-38F] Use of approved AES encryption method with the combination of approved Authentication method AES CMAC, in accordance with SP 800-38F.<br>The Module supports 128-, 192- and 256-bit key lengths. | 5243 |
| RSA | [FIPS 186-4] [PKCS#1 v1.5 and PSS] 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-bit keys (approved SHA sizes of the CM). Note that RSA-1024 verification and the use of SHA-1 for any RSA verification is allowed for legacy-use only. | 2802 |

| | | |
|---|---|---|
| RSA CRT | [FIPS 186-2] [PKCS#1 v1.5 and PSS] RSA CRT algorithm.<br>– Signature verification using 4096-bit key with SHA-2.<br>[FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA CRT algorithm.<br>– Key pair generation using 2048- and 3072-bit keys;<br>– Signature generation using 2048, 3072 and 4096-bit keys with SHA-2;<br>– Signature verification using 1024-, 2048-and 3072-bit keys (approved SHA sizes of the CM). Note that RSA-1024 verification and the use of SHA-1 for any RSA verification is allowed for legacy-use only. | 2803 |
| | [FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA CRT algorithm.<br>– Key pair generation using 4096-bit keys;<br>– Signature generation using 4096-bit keys (PKCS#1 v1.5) with SHA-2;<br>– Signature verification using 4096-bit keys (approved SHA sizes of the CM). Note that the use of SHA-1 for any RSA verification is allowed for legacy-use only. | Approved per IG A.14<br>(Cert. #2803) |
| SHA-1<br>SHA-2 | [FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms. The Module supports the SHA-1 (160 bits), SHA-2 (224- bit, 256-bit, 384-bit, 512-bit) variants. | 4221 |
| Triple-DES | [SP 800-67] Triple Data Encryption Algorithm (not used). The Module supports the 3-Key options; CBC and ECB encrypt/ decrypt modes, and 2-key decryption for legacy use only. | 2651 |

**Table 7 – FIPS Approved Cryptographic Functions**

The Module also implements the *FIPS Non Approved but Allowed* cryptographic functions listed in Table 8 below:

| Algorithm | Description |
|---|---|
| NDRNG | True Random Number Generator |

**Table 8 – FIPS Non-Approved but Allowed Cryptographic Functions**

## 4. Platform 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 5.

### 4.1 Platform Critical Security Parameters

| Key | Description / Usage |
|---|---|
| OS-DRBG-EI | 272-bit random drawn by the NDRNG HW chip during startup and used as entropy input for the [SP800-90A] DRBG implementation. Provides at least 256 bits of entropy. |
| OS-DRBG-STATE | 16-byte AES state V and 32-byte AES key used in the [SP800-90A] CTR DRBG implementation. |
| OS-GLOBALPIN | 4 to 16 byte Global PIN value managed by the ISD. Character space is not restricted by the module. |
| OS-MKDK | AES-128 (SCP03) key used to encrypt OS-GLOBALPIN value. |

| | |
|---|---|
| SD-KENC | AES-128/192/256 (SCP03) encryption master key used to derive SD-SENC. |
| SD-KMAC | AES-128/192/256 (SCP03) Security Domain MAC master key, used by the CO to derive SD-SMAC. |
| SD-KDEK | AES-128/192/256 (SCP03) Sensitive data decryption key used by the User role to decrypt CSPs. |
| SD-SENC | AES-128/192/256 (SCP03) Session encryption key used by the Module role to encrypt / decrypt secure channel data. |
| SD-SMAC | AES-128/192/256 (SCP03) Security Domain Session MAC key, used to verify secure channel message integrity. |
| DAP-SYM | AES-128 (DAP) key optionally loaded in the field and used to verify the MAC signature of packages loaded into the Module. |
| DM-TOKEN-SYM | AES-128 Delegate Management Token Symmetric key. |
| DM-RECEIPT-SYM | AES-128 Delegate Management Receipt Symmetric key. |

**Table 9 – Platform Critical Security Parameters**

### 4.2 Demonstration Applet Critical Security Parameters

| Key | Description / Usage |
|---|---|
| DEM-EDK | AES-128 encryption / decryption key used by the Demonstration Applet *Symmetric Cipher* service to import or export CSPs into or out of the module. |
| DEM-MAC | AES-128 key used by Demonstration Applet *Message Authentication* service. |
| DEM-SGV-PRI | 2048-, 3072-, 4096-bit RSA or P-224, P-256, P-384, P-521 ECDSA private key used by Demonstration Applet *Digital Signature* service. |
| DEM-KAP-PRI | P-224, P-256, P-384, P-521 ECDSA private key used by the Demonstration Applet *Generate Key Pair* and *Key Agreement Primitives* services. |
| DEM-KGS-PRI | 2048-bit RSA or P-224, P-256, P-384, P-521 ECDSA private key used by Demonstration Applet *Generate Key Pair and RSADP Primitive* services. |

**Table 10 – Demonstration Applet Critical Security Parameters**

### 4.3 Platform Public Keys

| Key | Description / Usage |
|---|---|
| DAP-ASYM | 2048-bit RSA Data Authentication Pattern Asymmetric key, used to verify package loading process. |
| DM-TOKEN-ASYM | 2048-bit RSA Delegate Management Token Asymmetric key. |

**Table 11 – Platform Public Keys**

### 4.4 Demonstration Applet Public Keys

| Key | Description / Usage |
|---|---|
| DEM-KAP-PUB | P-224, P-256, P-384, P-521 ECDSA public key used by the Demonstration Applet *Key Agreement Primitives* service. |
| DEM-KGS-PUB | 2048-bit RSA or 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 12 – Demonstration Applet Public Keys**

## 5. 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-KDEK), is stored in plaintext and is only accessible by authenticated services.

Table 13 lists all operator roles supported by the Module.

| Role ID | Role Description |
|---|---|
| CO | Cryptographic Officer - Role that manages Module content and configuration, including issuance and management of Module data via the ISD or SSD 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 13 - Roles Supported by the Module**

### 5.1 Secure Channel Protocol Authentication Method

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

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

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

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:

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

### 5.2 Demonstration applet Authentication Method

This authentication method compares a PIN value sent to the Module over an encrypted channel to be stored OS-GLOBALPIN values; 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 4 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 1/256^4.
- 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 15/256^4.

### 5.3 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 if self-test flag is set. |
| Run Cryptographic KATs | Resets a flag so that cryptographic KATs may be performed on demand via Module Reset. |

**Table 14 - 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 (inclusive of RSASP1) and ECDSA digital signature generation and verification. | | X |
| Generate Key Pair | Demonstrate RSA and ECDSA key generation. | | X |
| ECC CDH Primitive | Demonstrate EC Diffie-Hellman primitive. | | X |
| RSADP Primitive | Demonstrate RSADP primitive. | | X |
| Message Authentication | Demonstrate AES CMAC. | | X |
| Symmetric Cipher | Demonstrate use of AES for encryption and decryption. | | X |

**Table 15 – Authenticated Services**

The provided demonstration applet enforces the restrictions of algorithms, modes, and key sizes per NIST SP 800-131A Revision 1.

| CSPs | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Service | OS-DRBG-SEI | OS-DRBG-STATE | OS-GLOBALPIN | OS-MKDK | SD-KENC | SD-KMAC | SD-KDEK | SD-SENC | SD-SMAC | DAP-SYM | DAP-ASYM | DM-TOKEN-SYM | DM-RECEIPT-SYM | DM-TOKEN-ASYM | DEM-EDK | DEM-MAC | DEM-SGV-PRI | DEM-KGS-PRI | DEM-KAP-PRI | DEM-KAP-PUB | DEM-KGS-PUB | DEM-SGV-PUB |
| Module Reset | ZEW | ZEGW | -- | -- | -- | -- | -- | Z | Z | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Run Cryptographic KATs | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Module Info (Unauth) | -- | -- | -- | -- | -- | -- | -- | E[1] | E[1] | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Context | -- | -- | -- | -- | -- | -- | -- | Z | Z | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Secure Channel | -- | EW | -- | E | E | E | E | GE[1] | GE[1] | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Manage Content | -- | -- | W | E | W | WE | WE | E[1] | E[1] | EW | EW | EW | EW | EW | -- | -- | -- | -- | -- | -- | -- | -- |
| Lifecycle | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z |
| Module Info (Auth) | -- | -- | -- | -- | -- | -- | -- | E[1] | E[1] | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Symmetric Cipher | -- | -- | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | ERZ | -- | -- | -- | -- | -- | -- | -- |
| Message Authentication | -- | -- | -- | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | EZ | -- | -- | -- | -- | -- | -- |
| Digital Signature | -- | EW | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | ERWZ | -- | -- | -- | -- | ERWZ |
| Generate Key Pair | -- | EW | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | GERWZ | -- | -- | GERWZ | -- |

[1] "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.

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ECC CDH Primitive | -- | EW | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | ERWZ | ERWZ | -- | -- |
| RSADP Primitive | -- | EW | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | ERWZ | ERWZ | -- | -- |

**Table 16 – 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.

## 6. Finite State Model

The CM is designed using a finite state machine model that explicitly specifies every operational and error state.

An additional document (Finite State Machine document) identifies and describes all the states of the module including all corresponding state transitions.

## 7. 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* has been tested for hardness at nominal (20ºC), high (120ºC) and low (-40ºC) temperatures.

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 12 Mitigation of Other Attacks Policy below.

## 8. 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.

## 9. 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.

## 10. Self-test

### 10.1 Power-on Self-test

On power-on or reset, the *Module* performs self-tests described in Table 17. 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 or *Card is Killed* error state, depending on number of failures.

| Test Target | Description |
|---|---|
| Firmware Integrity | 16 bit CRC performed over all code located in FLASH and EEPROM memory (for OS, Applets). |
| AES | Performs decrypt KAT using an AES 128 key in ECB mode. AES encrypt is self-tested as an embedded algorithm of AES-CMAC. |
| DRBG | Performs DRBG SP 800-90A Section 11.3 instantiate and generate health test KAT with fixed inputs (derivation function and no reseeding supported). |
| ECC CDH | Performs an ECC CDH KAT using an ECC P-224 key. |
| ECDSA | Performs separate ECDSA signature and verification KATs using an ECC P-224 key. |
| KBKDF AES-CMAC | Performs a KDF AES-CMAC KAT using an AES 128 key and 32-byte derivation data. The KAT computes session keys and verifies the result. Note that KDF KAT is identical to an AES-CMAC KAT; the only difference is the size of input data. |
| RSA | Performs separate RSA PKCS#1.5 signature and verification KATs using an |

| Test Target | Description |
|---|---|
| | RSA 2048 bit key, and a RSA PKCS#1.5 signature KAT using the RSA CRT implementation with a 2048 bit key. RSA CRT signature verification is tested as part of the RSA signature verification KAT as described above. |
| SHA-1, SHA-2 | Performs separate KATs for SHA-1, SHA-256 and SHA-512. |
| Triple-DES | Performs separate encrypt and decrypt KATs using 3-Key TDEA in ECB mode. |

**Table 17 – Power-On Self-Test**

### 10.2 Conditional Self-tests

On every call to the [SP 800-90] DRBG, the CM performs the FIPS 140-2 Continuous RNG test (CRNGT) to assure that the output is different than the previous value. Note that the DRBG is seeded only once per power cycle and therefore a CRNGT is not required to be performed on the NDRNG per IG 9.8.

When any asymmetric key pair is generated (for RSA or ECC keys) the CM performs a pairwise consistency test.

When new firmware is loaded into the CM using the Manage content service, the CO verifies the integrity and authenticity of the new firmware (applet) using the SD-SMAC key for MAC process.

Optionally, the CO may also verify a MAC or a signature of the new firmware (applet) using the DAP-SYM key or DAP-ASYM key respectively. The signature or MAC block in this scenario is generated by an external entity using the key corresponding to the asymmetric key DAP-ASYM or the secret key DAP-SYM.

### 10.3 Reducing the number of Known Answer Tests

The CM implements latest [IG], reducing the number of Known Answer tests (KAT) described at chapter 9.11.

On the 1st reset of the CM, it performs “Firmware Integrity” test and all Cryptographic KATs.

On each next reset of the CM, it performs only “Firmware Integrity test” as permitted by [IG] document.

The cryptographic KATs are also available on demand and can be played by any operator with the Run Cryptographic KATs service (see Section 5.3 – Services).

## 11. Design Assurance

The CM meets the Level 3 Design Assurance section requirements.

### 11.1 Configuration Management

An additional document (Configuration Management Plan document) defines the methods, mechanisms and tools that allow to identify and place under control all the data and information concerning the specification, design, implementation, generation, test and validation of the card firmware throughout the development and validation cycle.

### 11.2 Delivery and Operation

Some additional documents (‘Delivery and Operation’, ‘Reference Manual’, ‘Card Initialization Specification’ documents) define and describe the steps necessary to deliver and operate the CM securely.

### 11.3 Guidance Documents

The Guidance document provided with CM is intended to be the ‘Reference Manual’. This document includes guidance for secure operation of the CM by its users as defined in the Roles, Authentication and Services chapter.

### 11.4 Language Level

The CM operational environment is implemented using a high level language. A limited number of firmware modules have been written in assembly to optimize speed or size.

The Demonstration Applet is a Java applet designed for the Java Card environment.

## 12. 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

## 13. 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 Mo*d*ule.

**END OF DOCUMENT**