IDPrime MD 830-revB

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

Table of Contents

Table of Tables

Table of Figures

References

Acronym	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 *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004 *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2* Amendment D, Sept 2009
[ISO 7816]	ISO/IEC 7816-1: 1998 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification* *Java Card 2.2.2 Virtual Machine (JCVM) Specification* *Java Card 2.2.2 Application Programming Interface* *Java Card 3.0.1 Application Programming Interface [only for algos ECDSA, SHA2]* Published by Sun Microsystems, March 2006
SP800-131A Rev. 2	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019
[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 Rev 2]	NIST Special Publication 800-67 Rev 2, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, November 2017
[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 (DSA2, RSA2 and ECDSA2)
[SP 800-56A Rev. 3]	NIST Special Publication 800-56A Rev. 3, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, April 2018
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015
[AESKeyWrap]	NIST, *AES Key Wrap Specification*, 16 November 2001. This document defines symmetric key wrapping.
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 7 May 2019.

Acronym	Full Specification Name
[SP 800-90A]	NIST, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Special Publication 800-90A, January 2012.
[SP 800-108]	NIST, *Recommendation for Recommendation for Key Derivation Using Pseudorandom Functions,* Special Publication 800-108, October 2009.
[SP 800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012.

Table 1 – References

Acronyms and Definitions

Acronym	Definition
GP	Global Platform
CVC	Card Verifiable Certificate
MMU	Memory Management Unit
OP	Open Platform
RMI	Remote Method Invocation

Table 2 – Acronyms and Definitions

1 Introduction

This document defines the Security Policy for the Gemalto IDCore30-revB platform and the ID Prime MD applet (IAS Classic V4.3.5) card called IDPrime MD 830-revB and herein denoted as Cryptographic Module. The Cryptographic Module or CM, validated to FIPS 140-2 overall Level 2, is a "contact-only" secure controller module implementing the Global Platform operational environment, with Card Manager, the IDPrime MD applet (associated to MSPNP applet V1.2).

The CM is a limited operational environment under the FIPS 140-2 definitions. The CM 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 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	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 3 – Security Level of Security Requirements

The CM implementation is compliant with:

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

1.1 IDPrime MD Applet

IDPrime MD Applet (called IAS Classic V4.3.5) is a Java applet that provides all the necessary functions to integrate a smart card in a public key infrastructure (PKI) system, suitable for identity and corporate security applications. It is also useful for storing information about the cardholder and any sensitive data. IDPrime MD Applet implements state–of–the–art security and conforms to the latest standards for smart cards and PKI applications. It is also fully compliant with digital signature law.

The IDPrime MD Applet, designed for use on JavaCard 2.2.2 and Global Platform 2.1.1 compliant smart cards.

The main features of IDPrime MD Applet are as follows:

- Digital signatures—these are used to ensure the integrity and authenticity of a message. (RSA, ECDSA)
- Storage of sensitive data based on security attributes
- PIN management.
- Secure messaging based on the AES algorithms.
- Public key cryptography, allowing for RSA keys and ECDSA keys
- Storage of digital certificates—these are issued by a trusted body known as a certification authority (CA) and are typically used in PKI authentication schemes.
- CVC verification
- Decryption RSA , ECDH
- On board key generation (RSA, ECDSA)
- Mutual authentication between IDPrime MD Applet and the terminal (ECDH)
- Support of integrity on data to be signed.
- Secure Key Injection according to Microsoft scheme.
- Touch Sense feature (not available on smart card, only on Token)
- PIN Single Sign On (PIN SSO)

MSPNP applet is associated to IDPrime MD applet and offers:

- GUID tag reading, defined in Microsoft Mini Driver specification.

2 Cryptographic Module Ports and Interfaces

2.1 Hardware and Physical Cryptographic Boundary

The CM is designed to be embedded into plastic card bodies, with a contact plate connection. The physical forms of the CM are depicted in Figure 1 (to scale). The module is a single integrated circuit die wire-bonded to a frame connected to a contact plate, enclosed in epoxy and mounted in a card body. The cryptographic boundary is the contact plate surface on the top side, and the surface of the epoxy on the bottom side. The Module relies on [ISO7816] card readers as input/output devices.

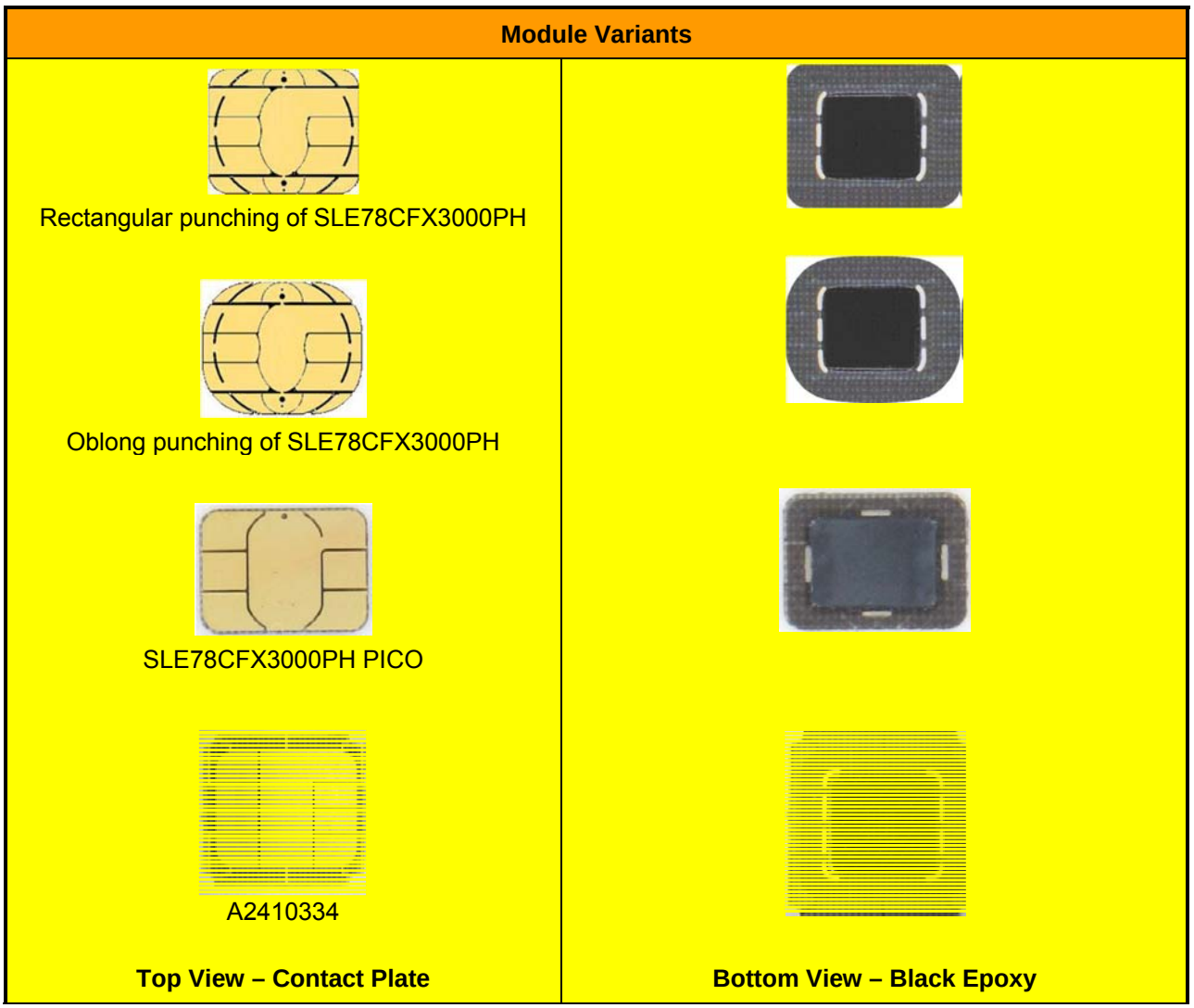

Figure 1 – Contact Module Views

2.1.1 PIN Assignments and Contact Dimensions

The CM conforms to the ISO 7816-1 and ISO 7816-2 specifications for physical characteristics, dimensions and contact location. The contact plate pads are assigned as shown below, with the corresponding interfaces given in Table 4.

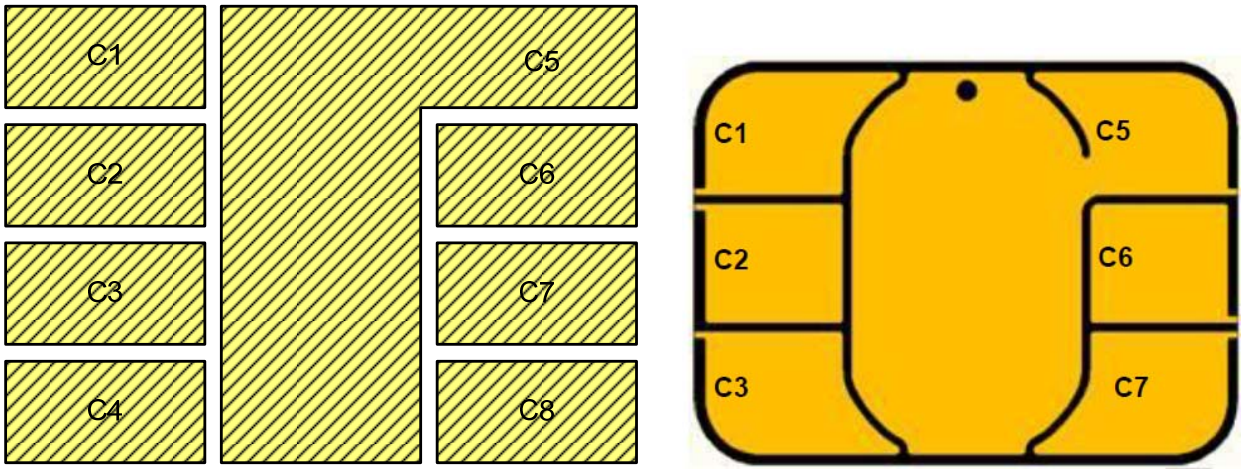

Figure 2 – Contact Plate Examples (PICO on right) – Contact Physical Interface

Contact No.	Logical interface type	Contact No.	Logical interface type
C1	VCC (Supply voltage)	C5	GND (Ground)
C2	RST (Reset signal)	C6	Not connected
C3	CLK (Clock signal)	C7	I/O : Data in, data out, control in, status out
C4	Not connected (N/A for PICO)	C8	Not connected (N/A for PICO)

Table 4 – Contact Plate Pad List – Interfaces

The CM conforms to the ISO 7816-3 specifications for electrical signals and transmission protocols, with voltage and frequency operating ranges as shown in Table 5.

Conditions	Range
Voltage	1.62 V and 5.5 V
Frequency	1MHz to 10MHz

Table 5 – Voltage and Frequency Ranges

3 Cryptographic Module Specification

3.1 Firmware and Logical Cryptographic Boundary

Figure 3 below depicts the Module operational environment and applets.

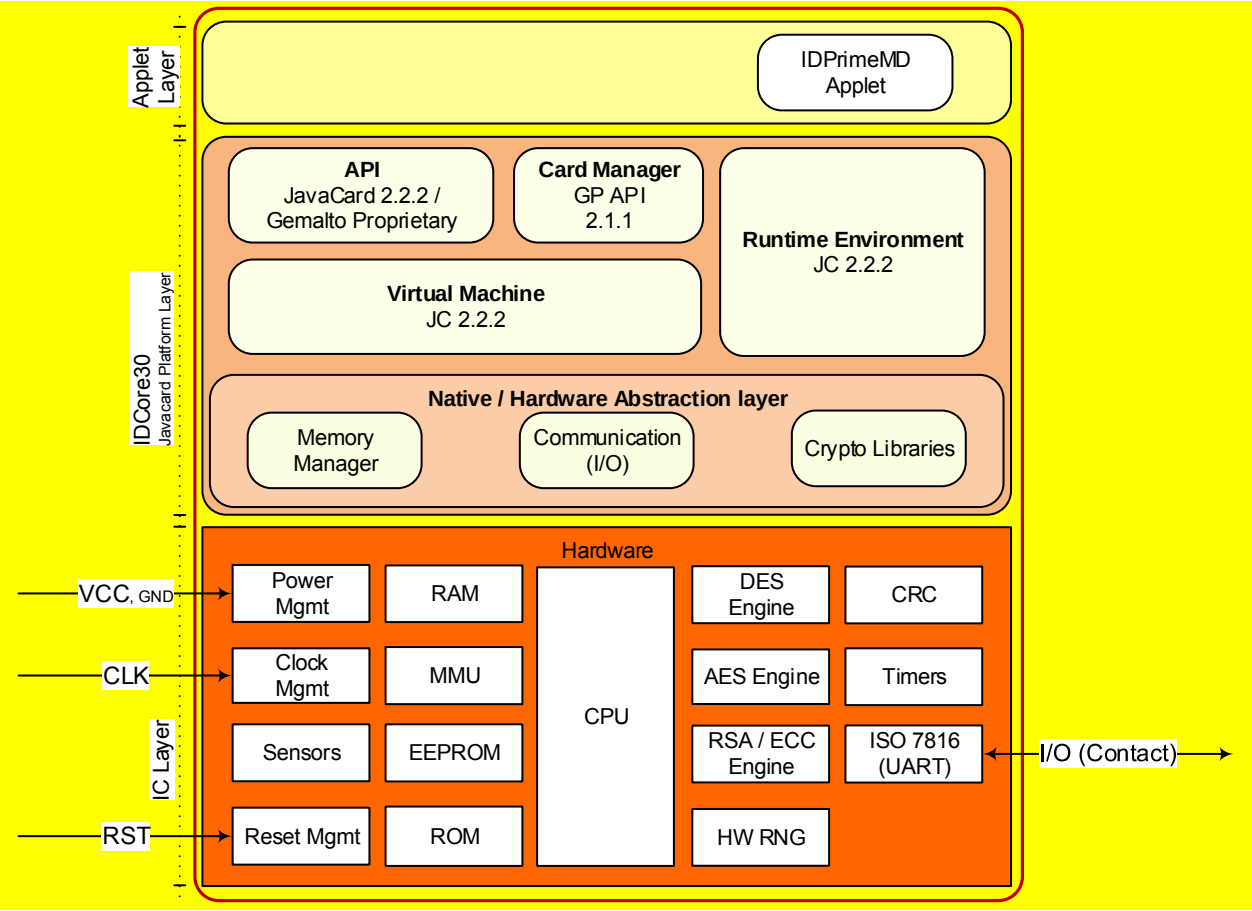

Figure 3 – Module Block Diagram

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

The CM provides services to both external devices and internal applets as the IDPrime MD.

Applets, as IDPrime MD, access module functionalities 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 provides an execution sandbox for the IDPrime MD Applet and performs the requested services according to its roles and services security policy.

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* 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* implements the dispatcher, registry, loader, logical channel and RMI 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 *Memory Manager* implements services such as memory access, allocation, deletion, garbage collector.

The *Communication* handler deals with the implementation of ATR, PSS, T=0 and T=1 protocols.

The *Cryptography Libraries* implement the algorithms listed in Section 2.

3.2 Versions and mode of operation

Hardware: SLE78CFX3000PH, SLE78CFX3000PH PICO, and A2410334
Firmware: IDCore30-revB - Build 06, IDPrime MD Applet version V4.3.5.D and MSPNP Applet V1.2

The CM supports both an Approved and non-Approved mode of operation. See Section 3.3 for information regarding the Approved and non-Approved modes.

The CM responds with the following information:

IDC30-revB - CPLC data (tag 9F7F)			
Byte	**Description**	**Value**	**Value meaning**
1-2	IC fabricator	**4090h**	Infineon
3-4	IC type	**7901**	SLE78CFX3000PH, SLE78CFX3000PH PICO and A2410334
5-6	Operating system identifier	**1291**	Gemalto
7-8	Operating system release date (YDDD) – Y=Year, DDD=Day in the year	**5356**	Operating System release Date
9-10	Operating system release level	**0200h**	V2.0
11-12	IC fabrication date	xxxxh	Filled in during IC manufacturing
13-16	IC serial number	xxxxxxxxh	Filled in during IC manufacturing
17-18	IC batch identifier	xxxxh	Filled in during IC manufacturing
19-20	IC module fabricator	xxxxh	Filled in during module manufacturing
21-22	IC module packaging date	xxxxh	Filled in during module manufacturing
23-24	ICC manufacturer	xxxxh	Filled in during module embedding
25-26	IC embedding date	xxxxh	Filled in during module embedding
27-28	IC pre-personalizer	xxxxh	Filled in during smartcard preperso
29-30	IC pre-personalization date	xxxxh	Filled in during smartcard preperso
31-34	IC pre-personalization equipment identifier	xxxxxxxxh	Filled in during smartcard preperso
35-36	IC personalizer	xxxxh	Filled in during smartcard personalization
37-38	IC personalization date	xxxxh	Filled in during smartcard personalization
39-42	IC personalization equipment identifier	xxxxxxxxh	Filled in during smartcard personalization

IDC30-revB - Identification data (tag 0103)			
Byte	**Description**	**Value**	**Value meaning**
1	Gemalto Family Name	**B0**	Javacard
2	Gemalto OS Name	**84**	IDCore family (OA)
3	Gemalto Mask Number	**56**	G286
4	Gemalto Product Name	**51**	IDCore30-revB
5	Gemalto Flow Version	**XY**	**X** is the type of SCP: ▪ 2xh for SCP0300 flows ▪ 3xh for SCP0310 flows **Y**: is the version of the flow (x=1 for version 01). For instance: ▪ **21h** = SCP0300 - flow 01 (version 01) ▪ **31h** = SCP0310 - flow 01 (version 01)
6	Gemalto Filter Set	**00**	▪ Major nibble: filter family = 00h ▪ Lower nibble: version of the filter = 00h
7-8	Chip Manufacturer	**4090**	Infineon
9-10	Chip Version	**7901**	SLE78CFX3000PH, SLE78CFX3000PH PICO and A2410334
11-12	FIPS configuration	**8D00**	MSByte: b8 : 1 = **conformity to FIPS certificate** b7 : 0 = not applicable b6 : 0 = not applicable b5 : 0 = not applicable b4 : 1 = ECC supported b3 : 1 = RSA CRT supported b2 : 1 = RSA STD supported b1 : 1 = AES supported LSByte: b8 .. b5 : 0 = not applicable b4 : 0 = not applicable (ECC in contactless) b3 : 0 = not applicable (RSA CRT in contactless) b2 : 0 = not applicable (RSA STD in contactless) b1 : 0 = not applicable (AES in contactless) For instance:

			8F 00 = FIPS enable (CT only)–AES-RSA CRT/STD-ECC **(Full FIPS)** **8D 00** = FIPS enable (CT only)–AES-RSA CRT-ECC **(FIPS PK CRT) *** **85 00** = FIPS enable (CT only)–AES-RSA CRT **(FIPS RSA CRT)** **00 00** = FIPS disable (CT only)–No FIPS mode **(No FIPS)** **(* default configuration)**
13	FIPS Level for IDPrime MD product	**02**	02 = FIPS Level 2
14-29	RFU	**xx..xxh**	-

Table 6 – Versions and Mode of Operations Indicators

The **IDPrime MD 830** is identified with an applet version and a software version as follow:

Field	CLA	INS	P1-P2 (Tag)	Le (Expected response length)	Purpose
Value	**00**	**CA**	**DF-30**	**07**	Get Applet Version
			7F-30	**19**	Get Software Version

Table 7 – Applet Version and Software Version imput data

The Applet version is returned without any TLV format as follows:

IDPrimeMD 830 – Applet Version Data (tag DF30)	
Value	**Value Meaning**
34 2E 33 2E 35 2E 44	Applet Version Display value = '4.3.5.D'

Table 8 – Applet Version returned value

The Software Version is returned in TLV format as follows:

IDPrimeMD 830 – Software Version Data (tag 7F30)					
Tag	**Length**				
7F30	17				
		Tag	**Length**	**Value**	**Value meaning**
		C0	0E	34 2E 33 2E 35 2E 44	Software Version Display value = '4.3.5.D'
		C1	07	49 41 53 20 43 6C 61 73 73 69 63 20 76 34	Applet Label Display value = 'IAS Classic v4'

Table 9 – Software Version Returned Values

3.3 Cryptographic Functionality

The Module operating system implements the FIPS Approved and Non-FIPS Approved cryptographic function listed in Tables 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 modes.	3779
AES CMAC	AES CMAC The Module supports 128-, 192- and 256-bit key lengths.	3779
ECC-CDH (CVL)	[SP 800-56A Rev. 3] The Section 5.7.1.2 ECC CDH Primitive. The Module is CAVP validated for the NIST defined P-224, P-256, P-384 and P-521 curves.	719
DRBG	[SP 800-90] Deterministic Random Number Generators [CTR_DRBG mode based on AES]	1045
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm: signature generation, verification and key pair generation. The Module is CAVP validated for the NIST defined P-224, P-256, P-384 and P-521 curves.	814
KBKDF	[SP 800-108] KDF for AES CMAC. The Module supports 128-, 192- and 256-bit key lengths.	81
KTS	[SP800-38F] Symmetric Key wrapping using 128, 192, or 256 bit keys (based on AES and AES CMAC Cert. #3779), meets the SP800-38F §3.1 ¶3. Key establishment methodology provides 128, 192, or 256 bits of strength.	3779
KTS	[SP 800-56B] RSA Key Wrapping using 2048 bit keys. Key establishment methodology provides 112 bits of strength Vendor affirmed, based on OAEP scheme as described in SP800-56B for PKCS1 v2.1. (Unwrapped output provided under Secure Messaging)	–Vendor Affirmed
RSA	[FIPS 186-4] RSA signature generation, verification, and key pair generation. The Module follows PKCS#1 and is CAVP validated for 2048 bit key length.	1946
RSA CRT	[FIPS 186-4] RSA signature generation, verification, CRT key pair generation. The Module follows PKCS#1 and is CAVP validated for 2048 bit key length.	1947
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms.	3146
Triple-DES	[SP 800-67 Rev. 2] Triple Data Encryption Algorithm. The Module supports the 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.	2100

Table 10 – FIPS Approved Cryptographic Functions

Algorithm	Description
EC Diffie-Hellman key agreement	SP 800-56A; non-compliant - key agreement using NIST defined, P-224, P-256, P-384 and P-521 curves. Key establishment methodology provides 112, 128, or 192 bits of strength.
NDRNG	Used to initialize the CTR DRNG
RSA Key Wrap	Key wrapping using 2048 bit keys. Key establishment methodology provides 112 bits of strength (for PKCS1 v1.5)

Table 11 – Non-FIPS Approved But Allowed Cryptographic Functions

The module supports the following non-Approved algorithm for use only in a non-FIPS mode of operation:

RSA key wrap	Key wrapping using 1024 and 1536 bit keys. Key establishment methodology provides less than 112 bits of strength (for PKCS1 v1.5 and PKCS v2.1 OAEP)

The CM includes an uncallable DES implementation. This algorithm is not used and no security claims are made for its presence in the Module.

FIPS approved security functions used specifically by the **IDPrime MD Applet** are:

- **DRBG**
- **AES CMAC**
- **AES**
- **RSA**
- **ECDSA**
- **SHA-1, SHA-224, SHA-256, SHA-384, SHA-512**
- **ECC-CDH**

(Note: no security function is used in **MSPNP applet**)

4 Platform Critical Security Parameters

All CSPs used by the CM are described in this section. All usages of these CSPs by the CM are described in the services detailed in Section 5.

Key	Description / Usage
OS-RNG-SEED-KEY	256-bit random drawn by the TRNG HW chip (AIS-31PTG.2), used as a seed key for the [SP 800-90A] DRBG implementation.
OS-RNG-STATE	16-byte random value and 16-byte counter value used in the [SP 800-90] DRBG implementation. 16-byte AES state V and 16-byte AES key used in the [SP800-90A] CTR DRBG implementation.
OS-GLOBALPIN	4 to 16 bytes Global PIN value managed by the ISD. Character space is not restricted by the module.
OS-MKDK	AES-128/192/256 (SCP03) key used to encrypt OS-GLOBALPIN value
SD-KENC	AES-128/192/256 (SCP03) Master key used by the CO role to generate SD-SENC
SD-KMAC	AES-128/192/256 (SCP03) Master key used by the CO role operator to generate SD-SMAC
SD-KDEK	AES-128/192/256 (SCP03) Sensitive data decryption key used by the USR role to decrypt CSPs for SCP03.
SD-SENC	AES-128/192/256 (SCP03) Session encryption key used by the CO role to encrypt / decrypt secure channel data.
SD-SMAC	AES-128/192/256 (SCP03) Session MAC key used by the CO role to verify inbound secure channel data integrity.
SD-SDEK	AES-128/192/256 (SCP03) Session DEK key used by the CO role to decrypt CSPs.
DAP-SYM	AES-128/192/256 (SCP03) key optionally loaded in the field and used to verify the signature of packages loaded into the Module.

Table 12 – Platform Critical Security Parameters

Keys with the “SD-“ prefix pertain to a Global Platform Security Domain key set. The module supports the Issuer Security Domain at minimum, and can be configured to support Supplemental Security Domains.

4.1 IDPrime MD Applet Critical Security Parameters

Key	Description / Usage
IAS-SC-SMAC-AES	AES 128/192/256 Session key used for Secure Messaging (MAC)
IAS-SC-SENC-AES	AES 128/192/256 Session key used for Secure Messaging (Decryption)
IAS-AS-RSA	2048- private part of the RSA key pair used for Asymmetric Signature
IAS-AS-ECDSA	P-224, P-256, P-384, P-521 private part of the ECDSA key pair used for Asymmetric signature
IAS-AC-RSA	2048- private part of the RSA key pair used for Asymmetric Cipher (key wrap, key unwrap)
IAS-ECDH-ECC	P-224, P-256, P-384, P-521 private part of the ECDH key pair used for shared key mechanism
IAS-KG-AS-RSA	2048- private part of the RSA generated key pair used for Asymmetric signature
IAS-KG-AS-ECDSA	P-224, P-256, P-384, P-521 private part of the ECDSA generated key pair used for Asymmetric signature
IAS-KG-AC-RSA	2048- private part of the RSA generated key pair used for Asymmetric cipher (key wrap, key unwrap)
IAS-KG-AC-ECDH	P-224, P-256, P-384, P-521 private part of the ECDSA generated key pair used for shared key mechanism
IAS-ECDSA-AUTH-ECC	P-224, P-256, P-384, P-521 private part of the ECDSA private key used to Authenticate the card
IAS-SC-DES3	3-Key Triple-DES key used for authentication.
IAS-SC-P-SKI-AES	AES 128/192/256 Session key used for Secure Key Injection
IAS-SC-T-SKI-AES	AES 128/192/256 Session key used for Secure Key Injection
IAS-SC-PIN-TDES	3-Key Triple-DES key used for PIN encryption (PIN History)
IAS-OWNERPIN	4 to 64 byte PIN value managed by the Applet.

Table 13 – IDPrime MD Applet Critical Security Parameters

4.2 IDPrime MD Applet Public Keys

Key	Description / Usage
IAS-KA-ECDH	P-224, P-256, P-384, P-521 ECDH key pair used for Key Agreement (Session Key computation)
IASAS-CA-ECDSA-PUB	P-224, P-256, P-384, P-521 CA ECDSA Asymmetric public key entered into the module used for CA Certificate Verification.
IASAS-IFD-ECDSA-PUB	P-224, P-256, P-384, P-521 IFD ECDSA Asymmetric public key entered into the module used for IFD Authentication.
IAS-AS-RSA-PUB	2048- public part of RSA key pair used for Asymmetric Signature
IAS-AS-ECDSA-PUB	P-224, P-256, P-384, P-521 public part of ECDSA key pair used for Asymmetric signature
IAS-AC-RSA-PUB	2048 public part of the RSA key pair used for Asymmetric Cipher (key wrap, key unwrap)
IAS-ECDH-ECC-PUB	P-224, P-256, P-384, P-521 public part of the ECDH key pair used for shared key mechanism
IAS-KG-AS-RSA-PUB	2048- public part of the RSA generated key pair used for Asymmetric signature
IAS-KG-AS-ECDSA-PUB	P-224, P-256, P-384, P-521 public part of the ECDSA generated key pair used for Asymmetric signature
IAS-KG-AC-RSA-PUB	2048- public part of the RSA generated key pair used for Asymmetric cipher (key wrap, key unwrap)
IAS-KG-AC-ECDH-PUB	P-224, P-256, P-384, P-521 public part of the ECDSA generated key pair used for shared key mechanism
IAS-ECDSA-AUTH-ECC-PUB	P-224, P-256, P-384, P-521 public part of the ECDSA key pair used to Authenticate the card

Table 14 – IDPrime MD Applet Public Keys

5 Roles, Authentication and Services

Table 15 lists all operator roles supported by the Module. This Module does not support a maintenance role. The Module clears previous authentications on power cycle. The Module supports GP logical channels, allowing multiple concurrent operators. Authentication of each operator and their access to roles and services is as described in this section, independent of logical channel usage. Only one operator at a time is permitted on a channel. Applet de-selection (including Card Manager), card reset or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services. Authentication data is encrypted during entry (by SD-SDEK), is stored encrypted (by OS-MKDK) and is only accessible by authenticated services.

Role ID	Role Description
CO	(Cryptographic Officer) This role is responsible for card issuance and management of card data via the Card Manager applet. Authenticated using the SCP authentication method with SD-SENC.
IUSR	(User) The IDPrime MD User, authenticated by the IDPrime MD applet – see below for authentication mechanism.
ICAA	(Card Application Administrator) The IDPrime MD Card Application Administrator authenticated by the IDPrime MD applet – see below for authentication mechanism.
UA	Unauthenticated role

Table 15 – Role Description

5.1 Secure Channel Protocol (SCP) Authentication

The Open Platform Secure Channel Protocol authentication method is performed when the EXTERNAL AUTHENTICATE service is invoked after successful execution of the INITIALIZE UPDATE command. These two commands operate as described next.

The SD-KENC and SD-KMAC keys are used along with other information 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).

For SCP03, AES-128, AES-192 or AES-256 keys are used for Global Platform secure channel operations, in which the Module derives session keys from the master keys and a handshake process, performs mutual authentication, and decrypts data for internal use only. 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. AES key establishment provides a minimum of 128 bits of security strength. The Module uses the SD-KDEK key to decrypt critical security parameters, and does not perform encryption with this key or output data decrypted with this key.

The strength of GP mutual authentication relies on AES key length, and the probability that a random attempt at authentication will succeed is:

- $\left(\frac{1}{2^{128}}\right)$ for AES 16-byte-long keys;
- $\left(\frac{1}{2^{192}}\right)$ for AES 24-byte-long keys;
- $\left(\frac{1}{2^{256}}\right)$ for AES 32-byte-long keys;

Based on the maximum count value of the failed authentication blocking mechanism, the minimum probability that a random attempt will succeed over a one minute period is 255/2^128.

5.2 IDPrime MD User Authentication

This authentication method compares a PIN value sent to the Module to the stored PIN values if the two values are equal, the operator is authenticated. This method is used in the IDPrime MD Applet services to authenticate to the IUSR role.

The module enforces string length of 4 bytes minimum (16 bytes maximum) for the Global PIN and 8 bytes for the Session PIN.

For the Global PIN, an embedded PIN Policy allows at least a combination of Numeric value (‘30’ to ‘39’) or alphabetic upper case (‘A’ to ‘Z’) or alphabetic lower case (‘a’ to z’), so the possible combination of value for the Global PIN is greater than 10^6. Then the strength of this authentication method is as follow:

- The probability that a random attempt at authentication will succeed is lower than 1/10^6
- 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 lower than 15/10^6

5.3 IDPrime MD Card Application Administrator Authentication (ICAA)

a) **The 3-Key Triple-DES key** establishment provides 168 bits of security strength. The Module uses the IAS-SC-DES3 to authenticate the ICAA role.

- The probability that a random attempt at authentication will succeed is 1/2^64 (based on block size)
- Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^64

b) PIN Authentication

This authentication method compares a PIN value sent to the Module to the stored OWNERPIN values if the two values are equal, the operator is authenticated. This method is used in the IDPrime MD Applet services to authenticate the ICAA role.
The module enforces string length of 4 bytes minimum (64 bytes maximum).
An embedded PIN Policy allows at least a combination of Numeric value (‘30’ to ‘39’) or alphabetic

upper case ('A' to 'Z') or alphabetic lower case ('a' to z'), so the possible combination of value for the Global PIN is greater than 10^6. Then the strength of this authentication method is as follow:

- The probability that a random attempt at authentication will succeed is lower than1/10^6
- 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 lower than 15/10^6

5.4 Platform Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Service	Description
Card Reset (Self-test)	Power cycle the Module by removing and reinserting it into the contact reader slot, or by reader assertion of the RST signal. The *Card Reset* service will invoke the power on self-tests described in Section §10-Self-. Moreover, on any card reset, the Module overwrites with zeros the RAM copy of, OS-RNG-STATE, SD-SENC, SD-SMAC and SD-SDEK. The Module can also write the values of all CSPs stored in EEPROM as a consequence of restoring values in the event of card tearing or a similar event. During the self-tests, the module generates the RAM copy of OS-RNG-STATE and updates the EEPROM copy of OS-RNG-STATE.
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. Uses SD-SENC and SD-SMAC.
INITIALIZE UPDATE	Initializes the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. Uses the SD-KENC, SD-KMAC and SD-KDEK master keys to generate the SD-SENC, SD-SMAC and SD-SDEK session keys, respectively.
GET DATA	Retrieve a single data object. Optionally uses SD-SENC, SD-SMAC (SCP).
MANAGE CHANNEL	Open and close supplementary logical channels. Optionally uses SD-SENC, SD-SMAC (SCP).
SELECT	Select an applet. Does not use CSPs.

Table 16 – Unauthenticated Services and CSP Usage

Service	Description	CO
DELETE	Delete an applet from EEPROM. This service is provided for the situation where an applet exists on the card, and does not impact platform CSPs. Optionally uses SD-SENC, SD-SMAC (SCP).	X
GET STATUS	Retrieve information about the card. Does not use CSPs. Optionally uses SD-SENC, SD-SMAC (SCP).	X
INSTALL	Perform Card Content management. Optionally uses SD-SENC, SD-SMAC (SCP). Optionally, the Module uses the DAP-SYM key to verify the package signature.	X
LOAD	Load a load file (e.g. an applet). Optionally uses SD-SENC, SD-SMAC (SCP).	X
PUT DATA	Transfer data to an application during command processing. Optionally uses SD-SENC, SD-SMAC (SCP).	X
PUT KEY	Load Card Manager keys The Module uses the SD-KDEK key to decrypt the keys to be loaded. Optionally uses SD-SENC, SD-SMAC (SCP).	X
SET STATUS	Modify the card or applet life cycle status. Optionally uses SD-SENC, SD-SMAC (SCP).	X
STORE DATA	Transfer data to an application or the security domain (ISD) processing the command. Optionally, updates OS-GLOBALPIN. Optionally uses SD-SENC, SD-SMAC (SCP).	X
GET MEMORY SPACE	Monitor the memory space available on the card. Optionally uses SD-SENC, SD-SMAC (SCP).	X
SET ATR	Change the card ATR. Optionally uses SD-SENC, SD-SMAC (SCP).	X

Table 17 – Authenticated Card Manager Services and CSP Usage

All of the above commands use the SD-SENC and SD-SMAC keys for secure channel communications, and SD-SMAC for firmware load integrity.

The card life cycle state determines which modes are available for the secure channel. In the SECURED card life cycle state, all command data must be secured by at least a MAC. As specified in the GP specification, there exist earlier states (before card issuance) in which a MAC might not be necessary to send Issuer Security Domain commands. Note that the LOAD service enforces MAC usage.

5.5 IDPRIME MD Services

All services implemented by the IDPrime MD applet are listed in the table below.

Service	Description	ICAA	IUSR	UA
EXTERNAL AUTHENTICATE	Authenticates the external terminal to the card. Sets the secure channel mode.	X	X	X
INTERNAL AUTHENTICATE	Authenticates the card to the terminal	X	X	X
SELECT	Selects a DF or an EF by its file ID, path or name (in the case of DFs).	X	X	X
CHANGE REFERENCE DATA	Changes the value of a PIN. (Note : User Auth is always done within the command itself by providing previous PIN)	X	X	
RESET RETRY COUNTER	Unblocks and changes the value of a PIN	X	X	
CREATE FILE	Creates an EF under the root or the currently selected DF or creates a DF under the root.	X	X	
DELETE FILE	Deletes the current DF or EF.	X	X	
DELETE ASYMMETRIC KEY PAIR	Deletes an RSA or ECDSA Asymmetric Key Pair	X	X	
ERASE ASYMMETRIC KEY	Erases an RSA or ELC Asymmetric Key Pair	X	X	
GET DATA (IDPrime MD Applet Specific)	Retrieves the following information: ■ CPLC data ■ Applet version ■ Software version (includes applet version - BER-TLV format) ■ Available EEPROM memory ■ Additional applet parameters ■ PIN Policy Error ■ Applet install parameter (DF0Ah tag)	X	X	X
GET DATA OBJECT	Retrieves the following information: ■ Public key elements ■ KICC	X	X	X

Service	Description	ICAA	IUSR	UA
	■ The contents of a specified SE ■ Information about a specified PIN ■ Key generation flag ■ Touch Sense flag			
PUT DATA (IDPrime MD Applet Specific)	Creates or updates a data object ■ Create container[1] ■ Update public/private keys(1)		X	
PUT DATA (IDPrime MD Applet Specific)	Creates or updates a data object ■ Access Conditions ■ Applet Parameters (Admin Key, Card Read Only and Admin Key Try Limit) ■ PIN Info	X		
PUT DATA (IDPrime MD Applet Specific)	Creates or updates a data object ■ Update DES or AES Secret keys(1)	X	X	
READ BINARY	Reads part of a binary file.	X	X	X
ERASE BINARY	Erases part of a binary file.	X	X	
UPDATE BINARY	Updates part of a binary file.	X	X	
GENERATE AUTHENTICATE	Used to generate secure messaging session keys between both entities (IFD and ICC) as part of elliptic curve asymmetric key mutual authentication.	X	X	X
GENERATE KEY PAIR	Generates an RSA or ECDSA key pair and stores both keys in the card. It returns the public part as its response.		X	
PSO – VERIFY CERTIFICATE	Sends the IFD certificate C_CV.IFD.AUT used in asymmetric key mutual authentication to the card for verification. No real reason to use it in the personalization phase, but it is allowed.		X	
PSO - HASH	Entirely or partially hashes data prior to a PSO–Compute Digital Signature command or prepares the data if hashed externally		X	

[1] Secure Messaging in Confidentiality is mandatory

Service	Description	ICAA	IUSR	UA
PSO – DECIPHER*	(RSA) Deciphers an encrypted message using a decipher key stored in the card. (Uses IAS-AC-RSA and IAS-AC-RSA-PUB for RSA key unwrap) (ECDSA) Generates a shared symmetric key.		X	
PSO – COMPUTE DIGITAL SIGNATURE	Computes a digital signature.		X	
PUT SECURE KEY	Secure Key Injection Scheme from Microsoft Minidriver spec V7		X	
UNAUTHENTICATE EXT	Breaks a secure messaging session, or invalidates an MS3DES3 External Authentication.			X
CHECK RESET AND APPLET SELECTION	Tells the terminal if the card has been reset or the applet has been reselected since the previous time that the command was performed.	X	X	X
GET CHALLENGE	Generates an 8 or 16-byte random number.			X
MANAGE SECURITY ENVIRONMENT	Supports two functions, Restore and Set. ■ Restore: replaces the current SE by an SE stored in the card. ■ Set: sets or replaces one component of the current SE.			X
VERIFY	Authenticates the user to the card by presenting the User PIN. The User Authenticated status is granted with a successful PIN verification.		X	

Table 18 – IDPrime MD Applet Services and CSP Usage

* - Service also available for non-Approved of operation when using key sizes that provide less than 112 bits of security strength.

All services implemented by the MSPNP applet are listed in the table below.

Service	Description	ICAA	IUSR	UA
GET DATA (MSPNP applet specific)	Retrieves the following information: ■ GUID			X

Table 19 – MSPNP applet Services

6 Finite State Model

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

The CM includes Power on/off states, Cryptographic Officer states, User services states, applet loading states, Key/PIN loading states, Self-test states, Error states, and the GP life cycle states.

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 CM is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The CM uses standard passivation techniques and is protected by passive shielding (metal layer coverings opaque to the circuitry below) and active shielding (a grid of top metal layer wires with tamper response). A tamper event detected by the active shield places the Module permanently into the Card Is Killed error state.

The CM is mounted in a plastic smartcard; physical inspection of the Module boundaries is not practical after mounting. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process. The Module also provides a key to protect the Module from tamper during transport and the additional physical protections listed in Section 12 below.

8 Operational Environment

This section does not apply to CM. No code modifying the behavior of the CM operating system can be added after its manufacturing process.

Only authorized applets can be loaded at post-issuance under control of the Cryptographic Officer. Their execution is controlled by the CM operating system following its security policy rules.

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

Each time the CM is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-on self–tests are available on demand by power cycling the CM.

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

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code located in Flash memory (for OS, Applets and filters).
DRBG	Performs DRBG SP 800-90 KAT with fixed inputs (no derivation function and no reseeding)
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES 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.
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 signature and verification KATs using an RSA 2048 bit key, and a RSA PKCS#1 signature KAT using the RSA CRT implementation with a 2048 bit key.
ECC CDH	Performs an ECC CDH KAT using an ECC P-224 key.(same crypto engine than for ECDSA KAT)
SHA-1	Performs a SHA-1 KAT.
SHA-256	Performs a SHA-256 KAT.
SHA-512	Performs a SHA-512 KAT.

Table 20 – Power-On Self-Test

10.2 Conditional Self-Tests

On every call to the [SP 800-90] DRBG, the FIPS 140-2 Continuous RNG test to assure that the output is different than the previous value.

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

When new firmware is loaded into the CM using the LOAD command, the CM verifies the integrity and authenticity of the new firmware (applet) using the SD-SMAC key for MAC process. Optionally, the CM may

also verify a signature of the new firmware (applet) using the DAP-AES key; the signature block in this scenario is signed by an external entity using the DAP-AES key.

When any new RSA asymmetric key pair generated or pushed into the CM is used for first time to perform a key unwrap, CM performs a pair-wise consistency test before allowing unwrapping operation.

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 software 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 section: Roles, Authentication and Services.

11.4 Language Level

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

TheIDPrime MD 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 Module.
- In accordance to NIST guidance, operators are responsible for insuring that a single Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit data blocks.

END OF DOCUMENT