



IDPrime 930 / 3930
FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy Level 3

Table of Contents

References.....	4
Acronyms and definitions	5
1 Introduction.....	6
1.1 IDPrime Applet.....	7
2 Cryptographic Module Ports and Interfaces.....	8
2.1 Hardware and Physical Cryptographic Boundary.....	8
2.1.1 PIN Assignments and Contact Dimensions	9
3 Cryptographic Module Specification	10
3.1 Firmware and Logical Cryptographic Boundary	10
3.2 Versions and mode of operation	11
3.3 Cryptographic Functionality	16
4 Module Critical Security Parameters.....	19
4.1 Platform Critical Security Parameters	19
4.2 IDPrime Applet Critical Security Parameters	19
4.3 IDPrime Applet Public Keys	21
5 Roles, Authentication and Services.....	22
5.1 Secure Channel Protocol (SCP) Authentication	22
5.2 IDPrime User Authentication	23
5.3 IDPrime Card Application Administrator Authentication (ICAA)	23
5.4 IDPrime Init Key Authentication (Initialization Officer Role).....	24
5.5 Platform Services	24
5.6 IDPRIME Services.....	27
6 Finite State Model	32
7 Physical Security Policy.....	33
8 Operational Environment.....	33
9 Electromagnetic Interference and Compatibility (EMI/EMC)	33
10 Self-test.....	34
10.1 Power-on Self-test	34
10.2 Conditional Self-tests	34
10.3 Reducing the number of Known Answer Tests.....	35
11 Design Assurance	35
11.1 Configuration Management.....	35
11.2 Delivery and Operation	35
11.3 Guidance Documents	35
11.4 Language Level.....	35
12 Mitigation of Other Attacks Policy	35
13 Security Rules and Guidance	36

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..... 9

Table 5 - Voltage and Frequency Ranges..... 9

Table 6 – Contactless voltage and Frequency Ranges 10

Table 7 – Versions and Mode of Operations Indicators 14

Table 8 – Applet Version and Software Version input data 15

Table 9 –Applet Version returned value..... 15

Table 10 –Software Version Returned Values..... 15

Table 11 – FIPS Approved Cryptographic Functions 17

Table 12 – Non-FIPS Approved But Allowed Cryptographic Functions 18

Table 13 - Platform Critical Security Parameters..... 19

Table 14 – IDPrime Applet Critical Security Parameters 20

Table 15 – IDPrime Applet Public Keys..... 21

Table 16 - Role Description 22

Table 17 - Unauthenticated Services 24

Table 18 – Authenticated Card Manager Services 25

Table 19 – Platform CSP Access by Service 26

Table 20 – IDPrime Applet Services and CSP Usage 30

Table 21 – MSPNP applet Services 30

Table 22 – IDPrime CSP Access by Service..... 32

Table 23 – Power-On Self-Test 34

Table of Figures

Figure 1– Physical form and Cryptographic Boundary 9

Figure 2 - Module Block Diagram 10

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, <i>Security Requirements for Cryptographic Modules</i> , May 25, 2001
[GlobalPlatform]	<i>GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1</i> , January 2011, http://www.globalplatform.org
[ISO 7816]	ISO/IEC 7816-1:1998 <i>Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics</i> ISO/IEC 7816-2:2007 <i>Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts</i> ISO/IEC 7816-3:2006 <i>Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols</i> ISO/IEC 7816-4:2005 <i>Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange</i>
[ISO 14443]	<i>Identification cards – Contactless integrated circuit cards – Proximity cards</i> ISO/IEC 14443-1:2008 Part 1: <i>Physical characteristics</i> ISO/IEC 14443-2:2010 Part 2: <i>Radio frequency power and signal interface</i> ISO/IEC 14443-3:2011 Part 3: <i>Initialization and anticollision</i> ISO/IEC 14443-4:2008 Part 4: <i>Transmission protocol</i>
[JavaCard]	<i>Java Card 3.0.5 Runtime Environment (JCRE) Specification</i> <i>Java Card 3.0.5 Virtual Machine (JCVM) Specification</i> <i>Java Card 3.0.5 Application Programming Interface</i> Published by Sun Microsystems, October 2015.
[SP800-131A]	NIST Special Publication 800-131A revision 2, <i>Transitioning the Use of Cryptographic Algorithms and Key Lengths</i> , March 2019
[SP 800-133]	NIST Special Publication 800-133, <i>Recommendation for Cryptographic Key Generation</i> , December 2012
[SP 800-38B]	NIST Special Publication 800-38B, <i>Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication</i> , May 2005
[SP 800-90A]	NIST Special Publication 800-90A revision 1, <i>Recommendation for the Random Number Generation Using Deterministic Random Bit Generators (Revised)</i> , June 2015
[SP 800-67]	NIST Special Publication 800-67 revision 2, <i>Recommendation for the Triple Data Encryption Algorithm (Triple-DES) Block Cipher</i> , November 2017
[FIPS113]	NIST, <i>Computer Data Authentication</i> , FIPS Publication 113, 30 May 1985.
[FIPS 197]	NIST, <i>Advanced Encryption Standard (AES)</i> , FIPS Publication 197, November 26, 2001.
[PKCS#1]	<i>PKCS #1 v2.1: RSA Cryptography Standard</i> , RSA Laboratories, June 14, 2002
[FIPS 186-4]	NIST, <i>Digital Signature Standard (DSS)</i> , FIPS Publication 186-4, July, 2013
[SP 800-56A]	NIST Special Publication 800-56A revision 2, <i>Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography</i> , May 2013
[SP 800-56B]	NIST Special Publication 800-56B revision 1, <i>Recommendation for Pair-Wise Key-</i>

Acronym	Full Specification Name
	<i>Establishment Schemes Using Integer Factorization Cryptography</i> , September 2014
[FIPS 180-4]	NIST, <i>Secure Hash Standard</i> , FIPS Publication 180-4, August 2015
[SP 800-38F]	NIST Special Publication 800-38F, <i>Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping</i> , December 2012
[IG]	NIST, <i>Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program</i> , last updated May 7, 2019

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 Thales IDCore3130 platform and the IDPrime applet (IAS Classic V4.5) card called IDPrime 930 (contact-only) or IDPrime 3930 (contact and contactless) and herein denoted as Cryptographic Module, Module, or CM. The Cryptographic Module or CM, validated to FIPS 140-2 overall Level 3, is a “contact and contactless” secure controller module implementing the Global Platform operational environment, with Card Manager, the IDPrime applet (associated to MSPNP applet V1.2).

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]

1.1 IDPrime Applet

IDPrime Applet (called IAS Classic V4.5) 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 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 Applet, designed for use on JavaCard 3.0.5 and Global Platform 2.2.1 compliant smart cards.

The main features of IDPrime 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 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)
- Reinit feature
- Extended APDU support



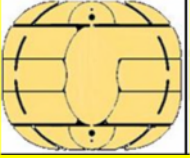
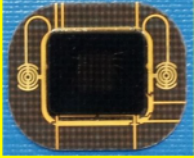
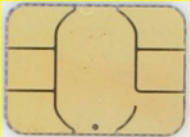
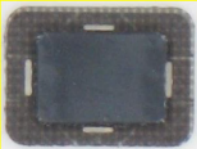
MSPNP applet is associated to IDPrime applet and offers:

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

2 Cryptographic Module Ports and Interfaces

2.1 Hardware and Physical Cryptographic Boundary

The *Module* is designed to be embedded into a plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or contactless antenna connection. 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 - A1977038)	
 Oblong punching Top View – Contact Plate	 Bottom View - Black Epoxy with RLT technology
WORLD Combi RLT module (SLE78CLFX400VPH - A1714221)	
 Oblong punching Top View – Combi Plate	 Bottom View - Black Epoxy with RLT technology
PICO module (SLE78CFX400VPH - A2023188)	
 Top View – Contact Plate	 Bottom View - Black Epoxy with RLV technology
G8 module (SLE78CFX400VPH - A2410334)	

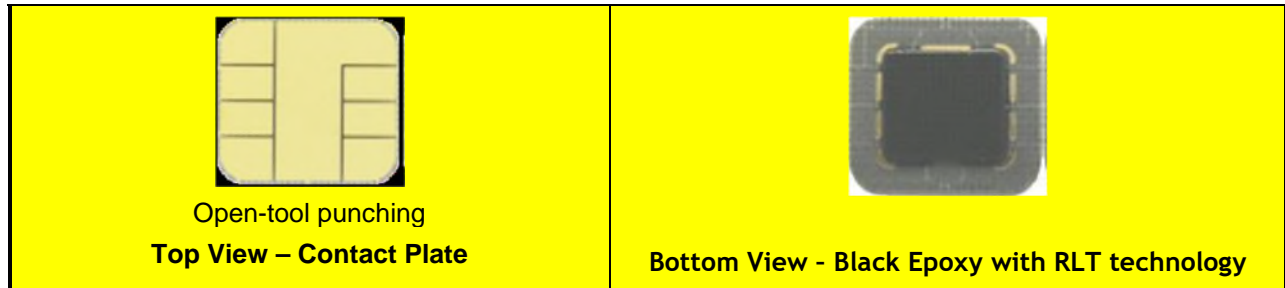


Figure 1– Physical form and Cryptographic Boundary

2.1.1 PIN Assignments and Contact Dimensions

WORLD Combi RLT module has access to contact and contactless interfaces. The WORLD RLT, PICO and G8 modules only have access to the contact interface. The contactless ports, when supported, require connection to an antenna.

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 below depicts the Module operational environment and applets.

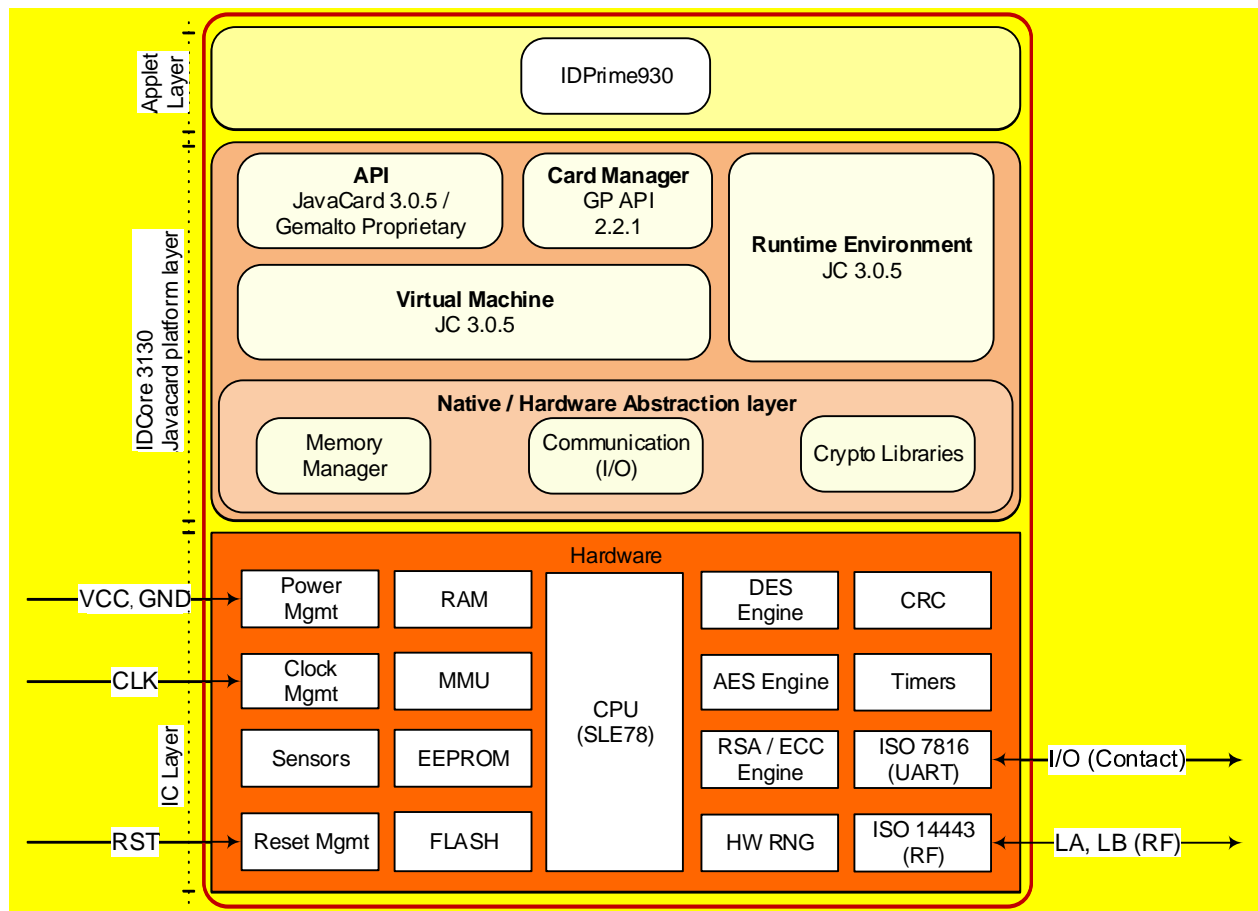


Figure 2 - Module Block Diagram

The CM supports [ISO7816] T=0 and T=1, and also [ISO14443] T=CL communication protocols.

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

Applets, as IDPrime, 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 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/ATS, PSS, T=0 T=1 and T=CL protocols.

The *Cryptography Libraries* implement the algorithms listed in [Table 11 – FIPS Approved Cryptographic Functions](#).

3.2 Versions and mode of operation

Hardware: SLE78CFX400VPH (A1977038), SLE78CFX400VPH (A2410334), SLE78CFX400VPH (A2023188), SLE78CLFX400VPH (A1714221)

Firmware: IDCore3130 - Build11D, IDPrime 930 / 3930 Applet version V4.5 and MSPNP Applet V1.2

The CM is always in the approved mode of operation. To verify that a CM is in the approved mode of operation, select the Card Manager and send the GET DATA commands shown below:

Field	CLA	INS	P1-P2 (Tag)	Le (Expected response length)	Purpose
Value	00	CA	9F-7F	2A	Get CPLC data
			01-03	1D	Identification information (proprietary tag)

The CM responds with the following information:

IDC3130 - CPLC data (tag 9F7F)			
Byte	Description	Value	Value meaning
1-2	IC fabricator	4090h	Infineon
3-4	IC type	7861	SLE78CLFX400VPHM
5-6	Operating system identifier	1291	Gemalto
7-8	Operating system release date (YDDD) – Y=Year, DDD=Day in the year	7334	Operating System release Date
9-10	Operating system release level	0100h	V1.0
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

IDPrime 930 / 3930

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy Level 3

IDC3130 - Identification data (tag 0103)

Byte	Description	Value	Value meaning
1	Gemalto Family Name	B0	Javacard
2	Gemalto OS Name	84	IDCore family
3	Gemalto Mask Number	60	G286
4	Gemalto Product Name	61	IDCore3130 for IDPrime 930 / 3930
5	Gemalto Flow Version	XX	<p>XX is the version of the flow:</p> <ul style="list-style-type: none"> ▪ 01h for flow version 01 ▪
6	Gemalto Filter Set	00	<ul style="list-style-type: none"> ▪ Major nibble: filter family = 00h ▪ Lower nibble: version of the filter = 00h
7-8	Chip Manufacturer	4090	Infineon
9-10	Chip Version	7861	SLE78CLFX400VPHM
11-12	FIPS configuration	8F00	<p><u>MSByte:</u> 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</p> <p><u>LSByte:</u> 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)</p> <p><u>For instance:</u> 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)</p>

IDPrime 930 / 3930

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy Level 3

13	FIPS Level for IDPrime product	03	03 = FIPS Level 3 02 = FIPS Level 2
14-15	Specific chip ID	01 30	01 30 = Contact only (IDPrime930 product) 31 30 = Combi (IDPrime3930 product)
16-29	RFU	xx..xxh	-

Table 7 – Versions and Mode of Operations Indicators

IDPrime 930 / 3930

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy Level 3

The IDPrime 930 / 3930 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 8 – Applet Version and Software Version input data

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

IDPrime 930 / 3930 – Applet Version Data (tag DF30)	
Value	Value Meaning
34 2E 35 2E 30 2E 45	Applet Version Display value = '4.5.0.E'

Table 9 –Applet Version returned value

The Software Version is returned in TLV format as follows:

IDPrime 930 / 3930 – Software Version Data (tag 7F30)					
Tag	Length				
7F30	17				
		Tag	Length	Value	Value meaning
		C0	0E	34 2E 35 2E 30 2E 45	Software Version Display value = '4.5.0.E'
		C1	07	49 41 53 20 43 6C 61 73 73 69 63 20 76 34	Applet Label Display value = 'IAS Classic v4'

Table 10 –Software Version Returned Values

IDPrime 930 / 3930

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy Level 3

3.3 Cryptographic Functionality

The Module operating system implements the FIPS Approved and Non-FIPS Approved cryptographic function listed in Tables below.

There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.

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 1716
CVL (RSASP1)	[FIPS 186-4] [PKCS#1 v2.1] RSA signature generation primitive using 2048-bit keys (same RSA implementation validated below).	1714 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. <ul style="list-style-type: none"> - Key pair generation: P-224, P-256, P-384 and P-521 curves. - Signature generation: P-224 (SHA-224), P-256 (SHA-224, SHA-256), P-384 (SHA-224, SHA-256, SHA-384) and P-521 (SHA-224, SHA-256, SHA-384, SHA-512) curves. - Signature verification: P-224 (SHA-224), P-256 (SHA-224, SHA-256), P-384 (SHA-224, SHA-256, SHA-384) and P-521 (SHA-224, SHA-256, SHA-384, SHA-512) curves. 	1365
KBKDF	[SP 800-108] The Module supports AES CMAC 128-, 192- and 256-bit key lengths.	177
KTS	Use of approved [FIPS 197] AES encryption method with the combination of approved Authentication method [SP 800-38B] AES CMAC The Module supports 128-, 192- and 256-bit key lengths. The Module supports 256-bit key length for Applet Secure Messaging.	5243
RSA	[FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA algorithms. <ul style="list-style-type: none"> - Key pair generation using 2048-bit keys. - Signature generation using 2048-bit keys with SHA-2. - 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

IDPrime 930 / 3930

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy Level 3

RSA CRT	<p>[FIPS 186-2] [PKCS#1 v1.5 and PSS] RSA CRT algorithm.</p> <ul style="list-style-type: none"> - Signature verification using 4096-bit key with SHA-2. <p>[FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA CRT algorithm.</p> <ul style="list-style-type: none"> - Key pair generation using 2048-, 3072- and 4096-bit keys; - Signature generation using 2048-, 3072- and 4096-bit keys with SHA-2; - Signature verification using 1024-, 2048-, 3072- and 4096-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
SHA-1 SHA-2	<p>[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.</p>	4221
Triple-DES	<p>[SP 800-67] Triple Data Encryption Algorithm. The Module supports the 3-Key options; CBC and ECB encrypt/ decrypt modes, and 2-key decryption for legacy use only. The CM restricts Triple-DES encryptions to 2¹⁶ per key. After a counter for a given key reach 2¹⁶, the key is blocked.</p>	2651
RSA Key Wrap (KTS)	<p>SP 800-56B Key wrapping using 2048 bit keys.</p> <p>Key establishment methodology provides 112 bits of strength</p> <p>Vendor affirmed, based on OAEP scheme as described in SP800-56B for PKCS1 v2.1. (Unwrapped output provided under Secure Messaging)</p>	Vendor Affirmed

Table 11 – FIPS Approved Cryptographic Functions

Algorithm	Description
RSA Key Unwrap	Key unwrapping using 2048, 3072 or 4096 bit keys. Key establishment methodology provides between 112 and 150 bits of encryption strength) (for PKCS1 v1.5)
EC Diffie-Hellman key agreement	NIST defined, P-224, P-256, P-384 and P-521 curves. Key establishment methodology provides 112, 128, 192 or 256 bits of strength. CVL cert. #1713.
NDRNG	True Random Number Generator

Table 12 – Non-FIPS Approved But Allowed Cryptographic Functions

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 Applet** are:

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

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

4 Module 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.

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 (or Nonce) 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 OS. The PIN Policy is managed by applet.
OS-MKDK	AES-128 (SCP03) key used to encrypt OS-GLOBALPIN value.
SD-KENC	AES-128/192/256 (SCP03) master key used by the CO role to derive SD-SENC.
SD-KMAC	AES-128/192/256 (SCP03) master key used by the CO role to derive SD-SMAC.
SD-KDEK	AES-128/192/256 (SCP03) decryption key used by the CO role to decrypt secure channel data.
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 secure channel data 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.
DAP-ASYM	2048-bit public part of RSA key pair used for Asymmetric Signature verification used to verify the 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.
DM-TOKEN-ASYM	2048-bit public part of RSA key pair used for Delegated Management Token

Table 13 - 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.

4.2 IDPrime Applet Critical Security Parameters

Key	Description / Usage
-----	---------------------

IAS-SC-SMAC-AES	AES 256 Session key used for Secure Messaging (MAC)
IAS-SC-SENC-AES	AES 256 Session key used for Secure Messaging (Decryption)
IAS-AS-RSA	2048/3072/4096- 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	2048/3072/4096- 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	2048/3072/4096- 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	2048/3072/4096- private part of the RSA generated key pair used for Asymmetric cipher (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 Admin (ICAA Role) 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.
IAS-INITK-AES	256bits AES key used to authenticate in IO Role

Table 14 – IDPrime Applet Critical Security Parameters

4.3 IDPrime 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	2048/3072/4096 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	2048/3072/4096- 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	2048/3072/4096- public part of the RSA generated key pair used for Asymmetric cipher
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 15 – IDPrime Applet Public Keys

5 Roles, Authentication and Services

Table 16 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. The module supports identity-based authentication.

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 User, authenticated by the IDPrime applet – see below for authentication mechanism.
ICAA	(Card Application Administrator) The IDPrime Card Application Administrator authenticated by the IDPrime applet – see below for authentication mechanism.
UA	Unauthenticated role
IO	Initialization Officer. This role is responsible for recycling/reinitializing the card using Reinit Authentication - see below for authentication mechanism.

Table 16 - 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 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 Applet services to authenticate to the IUSR role. There can be several OWNER PIN and one GlobalPIN. Both kind are User PINs.

The module enforces string length of 4 bytes minimum (16 bytes maximum for Global PIN / 64 bytes maximum for OWNER PIN).

For the User 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 User PIN is at minimum 62^4 , greater than 10^7 . Consequently 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 $15/10^7$

5.3 IDPrime Card Application Administrator Authentication (ICAA)

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 challenge 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 $255/2^{64}$

5.4 IDPrime Init Key Authentication (Initialization Officer Role)

The **AES-256 key** provides 256 bits of security strength. The Module uses the IAS-INITK-AES to authenticate the IO role.

- The probability that a random attempt at authentication will succeed is $1/2^{256}$ (based on challenge 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 $15/2^{256}$

5.5 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
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 17 - Unauthenticated Services

Service	Description	CO
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

Table 18 – Authenticated Card Manager Services

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.

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
Module Reset	ZE W	ZE GW	--	--	--	--	--	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	W	W	E ¹	E ¹	E W	E W	E W	E W	E W
Lifecycle	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

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.

Module Info (Auth)	--	--	--	--	--	--	--	E ¹	E ¹	--	--	--	--	--
--------------------	----	----	----	----	----	----	----	----------------	----------------	----	----	----	----	----

Table 19 – Platform 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.

IDPrime 930 / 3930

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy Level 3

5.6 IDPRIME Services

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

Service	Description	ICAA	IUSR	UA	IO
EXTERNAL AUTHENTICATE	Authenticates the external terminal to the card. Sets the secure channel mode.	X	X	X	X
INTERNAL AUTHENTICATE	Authenticates the card to the terminal	X	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	X
CHANGE REFERENCE DATA	Changes the value of a PIN. (Note : User Auth is always done within the command itself by providing previous PIN) Secure Messaging is enforced for this command.	X	X		
RESET RETRY COUNTER	Unblocks and changes the value of a PIN Secure Messaging is enforced for this command.	X	X		
CREATE FILE	Creates an EF under the root or the currently selected DF or creates a DF under the root.	X	X		X
DELETE FILE	Deletes the current DF or EF.	X	X		X
DELETE ASYMMETRIC KEY PAIR	Deletes an RSA or ECDSA Asymmetric Key Pair	X	X		X
ERASE ASYMMETRIC KEY	Erases an RSA or ELC Asymmetric Key Pair	X	X		X
GET DATA (IDPrime Applet Specific)	Retrieves the following information: <ul style="list-style-type: none"> ■ 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	X
GET DATA OBJECT	Retrieves the following information:	X	X	X	X

Service	Description	ICAA	IUSR	UA	IO
	<ul style="list-style-type: none"> ■ Public key elements ■ KICC ■ The contents of a specified SE ■ Information about a specified PIN ■ Key generation flag ■ Touch Sense flag 				
PUT DATA (IDPrime Applet Specific)	Creates or updates a data object <ul style="list-style-type: none"> ■ Create container² ■ Update public/private keys(2) 		X		X
PUT DATA (IDPrime Applet Specific)	Creates or updates a data object <ul style="list-style-type: none"> ■ Access Conditions ■ Applet Parameters (Admin Key, Card Read Only and Admin Key Try Limit) ■ PIN Info 	X			X
PUT DATA (IDPrime Applet Specific)	Creates or updates a data object <ul style="list-style-type: none"> ■ Update DES or AES Secret keys(2) 	X	X		X
READ BINARY	Reads part of a binary file.	X	X	X	X
ERASE BINARY	Erases part of a binary file.	X	X		X
UPDATE BINARY	Updates part of a binary file.	X	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	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		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	X	X	X
PSO - HASH	Entirely or partially hashes data prior to a PSO–Compute Digital Signature command or		X		X

² Secure Messaging in Confidentiality is mandatory

Service	Description	ICAA	IUSR	UA	IO
	prepares the data if hashed externally				
PSO - DECIPHER	(RSA) Deciphers an encrypted message using a decipher key stored in the card. (ECDSA) Generates a shared symmetric key. Secure Messaging is enforced for this command.		X		X
PSO – COMPUTE DIGITAL SIGNATURE	Computes a digital signature.		X		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	X	X	X
CHECK RESET AND APPLLET 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	X
GET CHALLENGE	Generates an 8, 16 or 32-byte random number.	X	X	X	X
MANAGE SECURITY ENVIRONMENT	Supports two functions, Restore and Set. <ul style="list-style-type: none"> ■ Restore: replaces the current SE by an SE stored in the card. ■ Set: sets or replaces one component of the current SE. 	X	X	X	X
VERIFY	Authenticates the user to the card by presenting the User PIN. The User Authenticated status is granted with a successful PIN verification. Secure Messaging is enforced for this command.		X		
EXTERNAL AUTHENTICATION (ADMIN)	Performs external authentication for ADMIN role (using Triple-DES challenge response)	X			
REINIT (Authenticate)	Command used to grand the IO role using a challenge based AES256 authentication.				X
REINIT (Key Update)	Updates the Init Key used for IO role authentication and its ratification counter.				X
REINIT (Reinit)	Process the reinit command, actions depends on options (in any cases, erase of all user keys). During reinit process IO can process all the				X

Service	Description	ICAA	IUSR	UA	IO
	commands for which he has rights.				
REINIT (End Reinit)	End the reinit process	X	X	X	X
REINIT (Get Counters)	Get ratification and retry counters for Init Key	X	X	X	X
PUT DATA (PIN)	Creates PIN objects on card (only possible if the PIN was not existing, or erased during reinit process)				X

Table 20 – IDPrime Applet Services and CSP Usage

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: <ul style="list-style-type: none"> ■ GUID 			X

Table 21 – MSPNP applet Services

CSP																	
Service	IAS-SC-SMAC-AES	IAS-SC-SENC-AES	IAS-AS-RSA	IAS-AS-ECDSA	IAS-AC-RSA	IAS-ECDH-ECC	IAS-KG-AS-RSA	IAS-KG-AS-ECDSA	IAS-KG-AC-RSA	IAS-KG-AC-ECDH	IAS-ECDSA-AUTH-ECC	IAS-SC-DES3	IAS-SC-P-SKI-AES	IAS-SC-T-SKI-AES	IAS-SC-PIN-TDES	IAS-OWNERPIN / OS-GLOBALPIN	IAS-INITK-AES
EXTERNAL AUTHENTICATE	E	F	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
INTERNAL AUTHENTICATE	E	F	-	-	-	-	-	-	-	-	F	-	-	-	-	-	-
SELECT	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CHANGE REFERENCE DATA	E	F	-	-	-	-	-	-	-	-	-	-	-	-	F	F W Z	-

CSP																	
Service	IAS-SC-SMAC-AES	IAS-SC-SENC-AES	IAS-AS-RSA	IAS-AS-ECDSA	IAS-AC-RSA	IAS-ECDH-ECC	IAS-KG-AS-RSA	IAS-KG-AS-ECDSA	IAS-KG-AC-RSA	IAS-KG-AC-ECDH	IAS-ECDSA-AUTH-ECC	IAS-SC-DES3	IAS-SC-P-SKI-AES	IAS-SC-T-SKI-AES	IAS-SC-PIN-TDES	IAS-OWNERPIN / OS-GLOBALPIN	IAS-INITK-AES
RESET RETRY COUNTER	E	E	--	--	--	--	--	--	--	--	--	E	--	--	E	E W N	--
CREATE FILE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
DELETE FILE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
DELETE ASYMMETRIC KEY PAIR	--	--	Z	Z	Z	Z	Z	Z	Z	--	Z	--	--	--	--	--	--
ERASE ASYMMETRIC KEY	--	--	Z	Z	Z	Z	Z	Z	Z	--	Z	--	--	--	--	--	--
GET DATA (IDPrime MD Applet Specific)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
GET DATA OBJECT	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PUT DATA (IDPrime MD Applet Specific)	E	E	WZ	WZ	WZ	WZ	WZ	WZ	WZ	--	WZ	--	--	--	--	--	--
PUT DATA (IDPrime MD Applet Specific)	--	--	--	--	--	--	--	--	--	--	--	W Z	--	--	--	--	--
READ BINARY	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
ERASE BINARY	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
UPDATE BINARY	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
GENERATE AUTHENTICATE	G	G	--	--	--	E	--	--	--	GE	--	--	--	--	--	--	--
GENERATE KEY PAIR	E	E	--	--	--	--	G	G	G	--	--	--	--	--	--	--	--
PSO – VERIFY CERTIFICATE	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PSO - HASH	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PSO – DECIPHER	--	--	--	--	E	--	--	--	E	--	--	--	--	--	--	--	--
PSO – COMPUTE DIGITAL SIGNATURE	--	--	E	E	--	--	E	E	--	--	--	--	--	--	--	--	--
PUT SECURE KEY	--	--	WZ	WZ	WZ	WZ	WZ	WZ	WZ	--	WZ	--	E	EWZ	--	--	--
UNAUTHENTICATE EXT	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

CSP																	
Service	IAS-SC-SMAC-AES	IAS-SC-SENC-AES	IAS-AS-RSA	IAS-AS-ECDSA	IAS-AC-RSA	IAS-ECDH-ECC	IAS-KG-AS-RSA	IAS-KG-AS-ECDSA	IAS-KG-AC-RSA	IAS-KG-AC-ECDH	IAS-ECDSA-AUTH-ECC	IAS-SC-DES3	IAS-SC-P-SKI-AES	IAS-SC-T-SKI-AES	IAS-SC-PIN-TDES	IAS-OWNERPIN / OS-GLOBALPIN	IAS-INITK-AES
CHECK RESET AND APPLET SELECTION	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
GET CHALLENGE	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
MANAGE SECURITY ENVIRONMENT	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
VERIFY	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--
EXTERNAL AUTHENTICATION (ADMIN)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--
REINIT (Authenticate)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E
REINIT (Key Update)	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	WZ
REINIT (Reinit)	E	E	Z	Z	Z	--	Z	Z	Z	--	--	--	WZ	--	--	--	--
REINIT (End Reinit)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
REINIT (Get Counters)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PUT DATA (PIN)	E	E	--	--	--	--	--	--	--	--	--	--	--	--	E	WZ	--

Table 22 – IDPrime CSP Access by Service

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.

The CM has been tested for hardness at nominal (22°C), high (120°C) and low (-40°C) temperatures.

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

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 *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 v1.5 signature and verification KATs using an RSA 2048 bit key, and a RSA PKCS#1 v1.5 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. RSA PKCS#1 v1.5 decryption KAT with a 2048 bit key is also performed.
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 23 – Power-On Self-Test

10.2 Conditional Self-tests

On every call to the [SP 800-90A] 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 5.5– Platform 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 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.

The IDPrime 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.

When the module enters the “Card is killed” error state, the user / operator will return his card to the local security officer and obtain a new card.

END OF DOCUMENT