



**IDPrime MD 830 with OATH & MPCOS applets  
FIPS 140-2 Cryptographic Module Security Policy  
Level 2**

# IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

## Table of Contents

References .....	5
Acronyms and definitions.....	6
1 Introduction.....	7
1.1 IDPrime MD Applet .....	8
1.2 OATH Applet .....	8
1.3 MPCOS Applet.....	9
2 Cryptographic Module Ports and Interfaces.....	10
2.1 Hardware and Physical Cryptographic Boundary .....	10
2.1.1 PIN assignments and contact dimensions .....	10
3 Cryptographic Module Specification.....	12
3.1 Firmware and Logical Cryptographic Boundary .....	12
3.2 Versions and mode of operation .....	13
3.3 Cryptographic functionality .....	18
4 Platform Critical Security Parameters .....	22
4.1 Platform Public key.....	22
4.2 IDPrime MD Applet Critical Security Parameters .....	23
4.3 IDPrime MD Applet Public Keys .....	24
4.4 OATH Applet Critical Security Parameters .....	26
4.5 MPCOS Applet Critical Security Parameters.....	26
5 Roles, authentication and services.....	27
5.1 Secure Channel Protocol (SCP) Authentication .....	28
5.2 IDPrime MD User authentication .....	29
5.3 IDPrime MD Card Application Administrator authentication .....	29
5.4 OATH User authentication .....	29
5.5 OATH Card Application Administrator authentication.....	30
5.6 MPCOS User authentication.....	30
5.7 MPCOS Card Application Administrator authentication .....	30
5.8 MPCOS Card Application Administrator for Payment authentication.....	30
5.9 Platform Services .....	31
5.10 IDPRIME MD Services.....	33
5.11 OATH Services .....	40
5.12 MPCOS Services .....	43
6 Finite State Model .....	47
7 Physical security policy .....	47
8 Operational Environment .....	47
9 Electromagnetic interference and compatibility (EMI/EMC).....	47
10 Self-test.....	48

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

<b>10.1</b>	<b>Power-on self-test</b> .....	48
<b>10.2</b>	<b>Conditional self-tests</b> .....	48
<b>11</b>	<b>Design Assurance</b> .....	49
<b>11.1</b>	<b>Configuration Management</b> .....	49
<b>11.2</b>	<b>Delivery and Operation</b> .....	49
<b>11.3</b>	<b>Guidance Documents</b> .....	49
<b>11.4</b>	<b>Language level</b> .....	49
<b>12</b>	<b>Mitigation of other attacks policy</b> .....	49
<b>13</b>	<b>Security Rules and Guidance</b> .....	49

# IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

## Table of Tables

Table 1 – References .....	6
Table 2 – Acronyms and Definitions .....	6
Table 3 – Security Level of Security Requirements .....	7
Table 4 - Contact plate pad list – Interfaces .....	11
Table 5 - Voltage and frequency ranges .....	11
Table 6 –Versions and Mode of Operations Indicators .....	16
Table 7 – Applet Version and Software Version input data .....	17
Table 8 –Applet Version returned value .....	17
Table 9 –Software Version returned values .....	17
Table 10 – Applet Version and Software Version input data .....	18
Table 11 –Applet Version returned value .....	18
Table 12 – FIPS Approved Cryptographic Functions .....	19
Table 13 – Non-FIPS Approved But Allowed Cryptographic Functions .....	19
Table 14 - Platform Critical Security Parameters .....	22
Table 15 – Platform Public Keys .....	22
Table 16 – IDPrime MD Applet Critical Security Parameters .....	24
Table 17 – IDPrime MD Applet Public Keys .....	25
Table 18 – OATH Applet Critical Security Parameters .....	26
Table 19 – MPCOS Applet Critical Security Parameters .....	26
Table 20 - Role description .....	27
Table 21 - Unauthenticated Services and CSP Usage .....	31
Table 22 – Authenticated Card Manager Services and CSP Usage .....	32
Table 23 – IDPrime MD applet Services and CSP Usage .....	38
Table 24 – MSPNP applet Services .....	39
<b>Table 26 – MPCOS Applet Services Access .....</b>	<b>46</b>
Table 27 – Power-On Self-Test .....	48

## Table of Figures

Figure 1 – Contact module views .....	10
Figure 2 – Contact plate example – Contact physical interface .....	11
Figure 3 - Module Block Diagram .....	12

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 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 2.1.1</i> , March 2003, <a href="http://www.globalplatform.org">http://www.globalplatform.org</a> <i>GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1 Amendment A</i> , March 2004 <i>GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2 Amendment D</i> , Sept 2009
[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>
[JavaCard]	<i>Java Card 2.2.2 Runtime Environment (JCRE) Specification</i> <i>Java Card 2.2.2 Virtual Machine (JCVM) Specification</i> <i>Java Card 2.2.2 Application Programming Interface</i> <i>Java Card 3.0.1 Application Programming Interface [only for algos ECDSA, SHA2]</i> Published by Sun Microsystems, March 2006
[SP800-131A]	<i>Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths</i> , January 2011
[ANS X9.31]	American Bankers Association, <i>Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)</i> , ANSI X9.31-1998 - Appendix A.2.4.
[SP 800-67]	NIST Special Publication 800-67, <i>Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher</i> , version 1.2, July 2011
[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 186-2]	NIST, <i>Digital Signature Standard (DSS)</i> , FIPS Publication 186-2, January, 2000 with Change Notice 1. (DSA, RSA and ECDSA)
[SP 800-56A]	NIST Special Publication 800-56A, <i>Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography</i> , March 2007
[FIPS 180-3]	NIST, <i>Secure Hash Standard</i> , FIPS Publication 180-3, October 2008
[AESKeyWrap]	NIST, <i>AES Key Wrap Specification</i> , 16 November 2001. This document defines symmetric key wrapping, Use of 2-Key TDEA in lieu of AES is described in [IG] D.2.
[IG]	NIST, <i>Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program</i> , last updated 29 June 2012.

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

Table 1 – References

### Acronyms and definitions

Acronym	Definition
GP	Global Platform
MMU	Memory Management Unit
OP	Open Platform
RMI	Remote Method Invocation

Table 2 – Acronyms and Definitions

# IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

## 1 Introduction

This document defines the Security Policy for the Gemalto IDCore30 platform and the ID Prime MD applet (IAS Classic V4.1) card called IDPrime MD 830 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 V1.0), the OATH Applet V2.11 and the MPCOS applet V3.8. The OATH applet and the MPCOS applet are options and the CM smart card must operate with them.

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	2
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]

## **IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2**

### **1.1 IDPrime MD Applet**

IDPrime MD Applet (called IAS Classic V4.1) 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 triple DES (Triple-DES 2-key) and 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
- Key establishment RSA , ECDH
- On board key generation (RSA, ECDSA)
- Mutual authentication between IDPrime MD Applet and the terminal (Triple-DES, AES, RSA, ECDH)
- Support of integrity on data to be signed.
- Secure Key Injection according to Microsoft scheme.

MSPNP applet is associated to IDPrime MD applet and offers:

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

### **1.2 OATH Applet**

The OATH Applet, designed for use on JavaCard 2.2.2 and Global Platform 2.1.1 compliant smart cards, provides one time password (OTP) service generation that conforms to the OATH specification for hardware tokens.

The OATH Applet features:

- Authentication of the OATH Applet User and the OATH Applet security officer
  1. Supports global PIN based authentication.
- Execution of native platform cryptographic services integrated with managed objects:
  2. Two key Triple-DES encryption and decryption.
  3. SHA1 secure hashing generation.
  4. Pseudo-random number generation.



## **IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2**

### **1.3 MPCOS Applet**

The MPCOS applet (Multi-application Payment Chip Operating System), is an applet designed for multi-purpose and payment applications. It offers secure payment and data management And could be used in a wide range of applications as electronic purse, public applications (road pricing, health care ...), multi-purpose (loyalty, retail ...), or access control.

The MPCOS applet features:

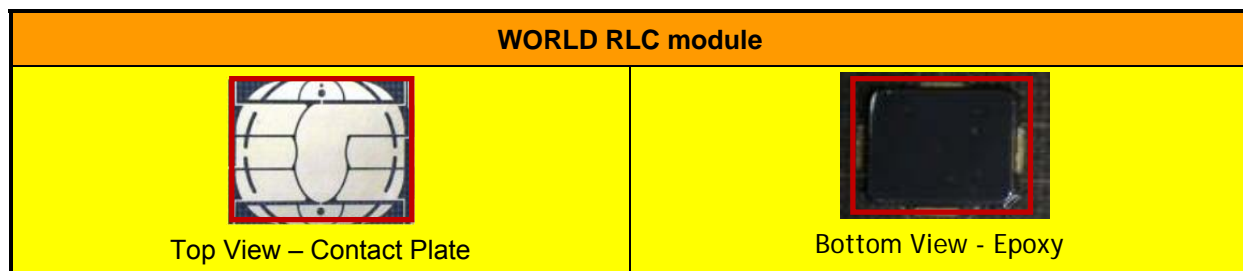
- Basic inter-industry commands and file types
- Protected by PIN (Local)
- Secure messaging based on Triple-DES algorithm to protect data integrity

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 2 Cryptographic Module Ports and Interfaces

#### 2.1 Hardware and Physical Cryptographic Boundary

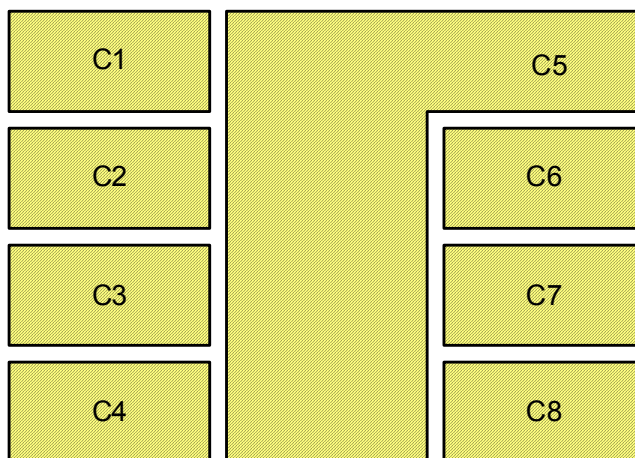
The CM is designed to be embedded into plastic card bodies, with a contact plate connection. The physical form of the CM is depicted in Figure 1 (to scale), with the cryptographic boundary indicated by the red outline. The module is a single integrated circuit die wire-bonded to a frame connected to 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.



## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

**Figure 2 – Contact plate example – 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	C8	Not connected

**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

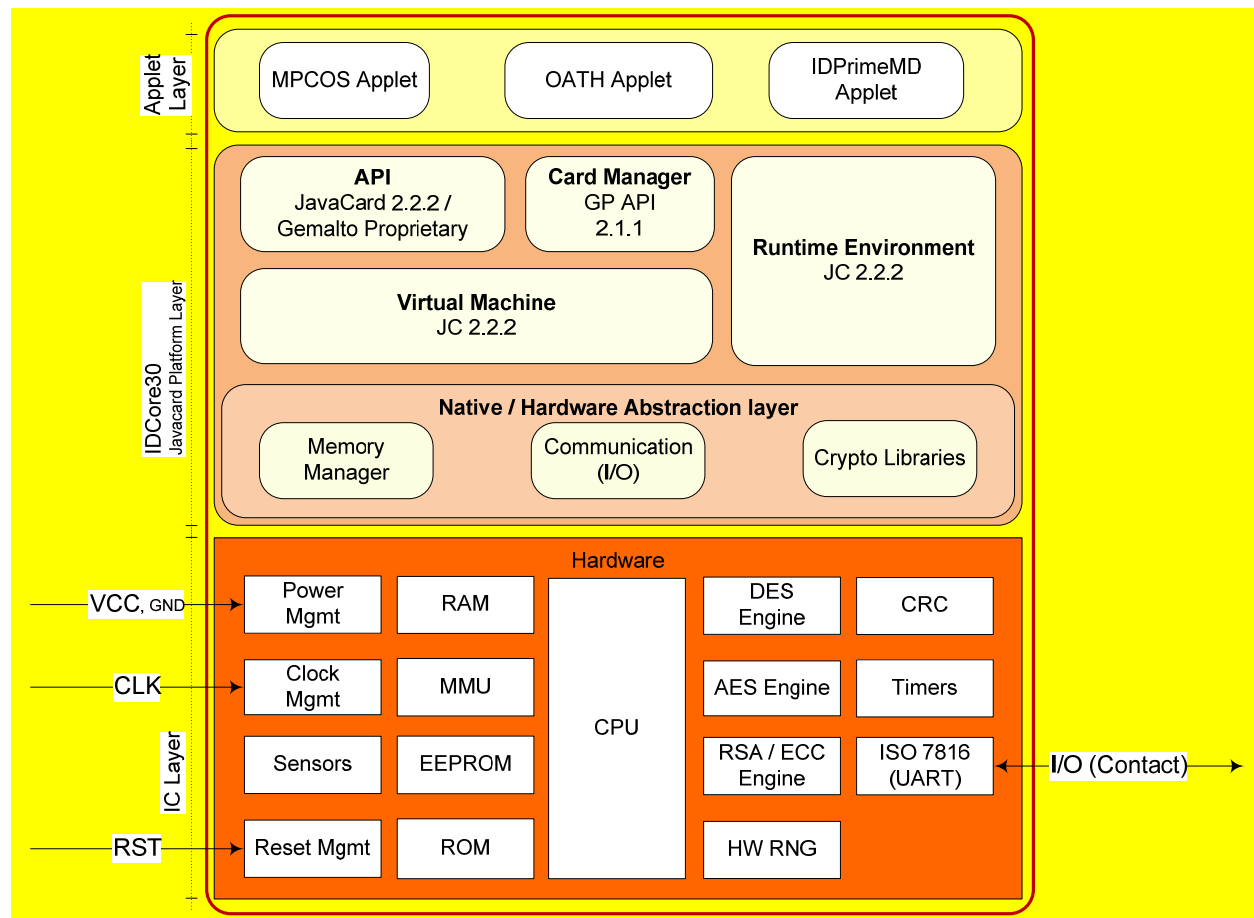
**Table 5 - Voltage and frequency ranges**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 3 Cryptographic Module Specification

#### 3.1 Firmware and Logical Cryptographic Boundary

Figure 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 on the CM, such as IDPrime MD, have access to 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, the OATH Applet and the MPCOS Applet** and performs the requested services according to its roles and services security policy.

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

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:** SLE78CFX3009P

**Firmware:** IDCore 30 Build 1.17, IDPrime MD Applet version V4.1.2.F with MSPNP Applet V1.0, OATH Applet V2.11 and MPCOS Applet V3.8

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)

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

The CM responds with the following information:

G259 Mask - CPLC data (tag 9F7F)			
Byte	Description	Value	Value meaning
1-2	IC fabricator	4090h	Infineon
3-4	IC type	7871h	SLE78CFX3009P
5-6	Operating system identifier	1291h	Gemalto
7-8	Operating system release date (YDDD) – Y=Year, DDD=Day in the year	2121h	2012 – 30 <sup>th</sup> of April
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 MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### G259 Mask - Identification data (tag 0103)

Byte	Description	Value	Value meaning
1	Gemalto Family Name	<b>B0h</b>	Javacard
2	Gemalto OS Name	<b>84h</b>	IDCore family (OA)
3	Gemalto Mask Number	<b>41h</b>	G259
4	Gemalto Product Name	<b>3Dh</b>	IDCore30
5	Gemalto Flow Version	<b>XYh</b>	<p><b>X</b> is the type of SCP:</p> <ul style="list-style-type: none"> <li>▪ 1xh for SCP0105 flows</li> <li>▪ 2xh for SCP0300 flows</li> <li>▪ 3xh for SCP0310 flows</li> </ul> <p><b>Y</b>: is the version of the flow (x=1 for version 01).</p> <p><u>For instance:</u></p> <ul style="list-style-type: none"> <li>▪ <b>11h</b> = SCP0105 - flow 01 (version 01)</li> <li>▪ <b>21h</b> = SCP0300 - flow 01 (version 01)</li> <li>▪ <b>31h</b> = SCP0310 - flow 01 (version 01)</li> </ul>
6	Gemalto Filter Set	<b>00h</b>	<ul style="list-style-type: none"> <li>▪ Major nibble: filter family = 00h</li> <li>▪ Lower nibble: version of the filter = 00h</li> </ul>
7-8	Chip Manufacturer	<b>4090h</b>	Infineon
9-10	Chip Version	<b>7871h</b>	SLE78CFX3009P
11-12	FIPS configuration	<b>8x00h</b>	<p><u>MSByte:</u></p> <p>b8 : 1 = <b>conformity to FIPS certificate</b>  b7 : 0 = not applicable  b6 : 0 = not applicable  b5 : 0 = not applicable</p> <p>b4 : 1 = ECC supported  b3 : 1 = RSA CRT supported  b2 : 1 = RSA STD supported  b1 : 1 = AES supported</p> <p><u>LSByte:</u></p> <p>b8 .. b5 : 0 = not applicable</p> <p>b4 : 0 = not applicable (ECC in contactless)  b3 : 0 = not applicable (RSA CRT in contactless)  b2 : 0 = not applicable (RSA STD in contactless)</p>

**IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2**

			<p>b1 : 0 = not applicable (AES in contactless)</p> <p><u>For instance:</u></p> <p><b>8F 00</b> = FIPS enable (CT only)–AES-RSA CRT/STD-ECC (<b>Full FIPS</b>)</p> <p><b>8D 00</b> = FIPS enable (CT only)–AES-RSA CRT-ECC (<b>FIPS PK CRT</b>) *</p> <p><b>85 00</b> = FIPS enable (CT only)–AES-RSA CRT (<b>FIPS RSA CRT</b>)</p> <p><b>00 00</b> = FIPS disable (CT only)–No FIPS mode (<b>No FIPS</b>)</p> <p>(* default configuration)</p>
13	FIPS Level for IDPrime MD product	<b>02h</b>	<p>03 = FIPS Level 3</p> <p>02 = FIPS Level 2 (default)</p>
14-29	RFU	<b>xx..xxh</b>	-

**Table 6 –Versions and Mode of Operations Indicators**



## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

The IDPrimeMD 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 input data**

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

IDPrimeMD 830 – Applet Version Data (tag DF30)	
Value	Value Meaning
34 2E 31 2E 32 2E 46	Applet Version Display value = '4.1.2.F'

**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 31 2E 32 2E 46	Software Version Display value = '4.1.2.F'
		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**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

The **OATH applet** is identified with an applet version as follow:

Field	CLA	INS	P1-P2 (Tag)	Le (Expected response length)	Purpose
Value	00	E7	05-00	05	Get Version command

**Table 10 – Applet Version and Software Version input data**

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

OATH – Applet Version Data (tag 05 00)	
Value	Value Meaning
76 32 2E 31 31	Applet Version Display value = 'v2.11'

**Table 11 –Applet Version returned value**

The **MPCOS applet** is identified with an applet version as follow:

The Get Information command with P1P2 equal to 02A4h is used to get the Pre-issuing Data:

- The CIV byte 38h in the card response indicates the applet version 3.8 (.14 describes the secure API version used for this Applet).

### 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 #
PRNG	[ANS X9.31] Pseudo Random number generator	1128
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The Module supports the 2-Key <sup>1</sup> and 3-Key options; CBC and ECB modes. Note that the Module does not support a mechanism that would allow collection of plaintext / ciphertext pairs aside from authentication, limited in use by a counter.	1413
Triple-DES MAC	[FIPS 113] Triple-DES Message Authentication Code. Vendor affirmed, based on validated Triple-DES.	1413

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

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

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.	2261
AES CMAC	AES CMAC The Module supports 128-, 192- and 256-bit key lengths.	2261
RSA	[FIPS 186-3] RSA Key pair generation: 2048-bit Signature generation: 2048-bit using SHA-2 Signature verification: 1024 and 2048-bit using SHA-1 and SHA-2	1158
RSA CRT	[FIPS 186-3] RSA Key pair generation: 2048-bit Signature generation: 2048-bit using SHA-2 Signature verification: 1024 and 2048-bit using SHA-1 and SHA-2	1163
ECDSA	[FIPS 186-3] Elliptic Curve Digital Signature Algorithm Key pair generation: P-224, P-256, P-384 and P-521 curves Signature generation: P-224, P-256, P-384 and P-521 curves using SHA-2 Signature verification: P-192, P-224, P-256, P-384 and P-521 curves using SHA-1 and SHA-2	363
ECC-CDH	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive. P-224, P-256, P-384 and P-521 curves.	41
SHA	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms. SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)	1946

**Table 12 – FIPS Approved Cryptographic Functions**

Algorithm	Description
EC Diffie-Hellman key agreement	SP 800-56A; non-compliant - NIST defined P-224, P-256, P-384 and P-521 curves; provides between 112 and 256 bits of security
Triple-DES key wrap	2-key Triple-DES key wrapping (Cert. #1413); provides 112 bits of security <sup>2</sup>
AES key wrap	AES key wrapping using 128, 192, or 256-bit keys (Cert. #2261); provides between 128 and 256 bits of security
RSA key wrap	RSA key wrapping using 2048-bit keys; provides 112 bits of security

**Table 13 – 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.

<sup>2</sup> The 112 bit claim for 2-key Triple-DES is valid because the module does not provide the means for an attacker to collect plaintext / ciphertext pairs to attempt the meet in the middle attack described in SP 800-131A.

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

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

Algorithm	Description	Cert #
RSA	[FIPS 186-3] RSA Key pair generation: 1024-bit Signature generation: 1024-bit using SHA-1/SHA-2 and 2048-bit using SHA-1	1158
RSA CRT	[FIPS 186-3] RSA Key pair generation: 1024-bit Signature generation: 1024-bit using SHA-1/SHA-2 and 2048-bit using SHA-1	1163
ECDSA	[FIPS 186-3] Elliptic Curve Digital Signature Algorithm Key pair generation: P-192 curve Signature generation: P-192 curve using SHA-1/SHA-2; P-224, P-256, P-384 and P-521 curves using SHA-1	363
ECC-CDH	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive. P-192 curve.	41
EC Diffie-Hellman key agreement	NIST defined P-192 curve; provides 80 bits of security (non-compliant)	N/A
RSA key wrap	RSA key wrapping using 1024-bit keys; provides 80 bits of security (non-compliant)	N/A

**Table 14 - Cryptographic Functions Disallowed per NIST SP 800-131A Transitions**

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

- PRNG
- Triple-DES
- Triple-DES MAC
- 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)

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

- Triple-DES
- SHA-1
- P-RNG

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

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

- Triple-DES
- P-RNG

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 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	AES-128 random key loaded into the card during pre-personalization of the card used as a seed key for the [ANS X9.31] RNG implementation.
OS-RNG-STATE	16-byte random value and 16-byte counter value used in the [ANS X9.31] RNG implementation.
OS-GLOBALPIN	4 to 16 bytes Global PIN value managed by the ISD. Character space is not restricted by the module.
OS-MKDK	2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) key used to encrypt OS-GLOBALPIN value
SD-KENC	2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Master key used by the CO role to generate SD-SENC
SD-KMAC	2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Master key used by the CO role operator to generate SD-SMAC
SD-KDEK	2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Sensitive data decryption key used by the USR role to decrypt CSPs for SCP01/03, and used to generate SD-SDEK in case of SCP02.
SD-SENC	2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Session encryption key used by the CO role to encrypt / decrypt secure channel data.
SD-SMAC	2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) Session MAC key used by the CO role to verify inbound secure channel data integrity.
SD-SDEK	2-Key Triple-DES (SCP01) or AES-128/192/256 (SCP03) Session DEK key used by the CO role to decrypt CSPs.
DAP-SYM	2-Key Triple-DES (SCP01/02) or AES-128/192/256 (SCP03) key optionally loaded in the field and used to verify the signature of packages loaded into the Module.

**Table 15 - 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 Platform Public key

Key	Description / Usage
DAP-SVK	RSA 1024 Global Platform Data Authentication Public Key. Optionally used to verify the signature of packages loaded into the Module.

**Table 16 – Platform Public Keys**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 4.2 IDPrime MD Applet Critical Security Parameters

Key	Description / Usage
IAS-SC-DKMAC-AES	AES 128/192/256 Derived Key used for Mutual Authentication
IAS-SC-DKENC-AES	AES 128/192/256 Derived Key used for Mutual Authentication
IAS-SC-DKMAC-TDES	2-Key Triple-DES Derived Key used for Mutual Authentication
IAS-SC-DKENC-TDES	2-Key Triple-DES Derived Key used for Mutual Authentication
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-SC-SMAC-TDES	2-Key Triple-DES Session key used for Secure Messaging (MAC)
IAS-SC-SENC-TDES	2-Key Triple-DES Session key used for Secure Messaging (Decryption)
IAS-AS-RSA*	1024-, 2048- private part of the RSA key pair used for Asymmetric Signature
IAS-AS-ECDSA	P-224, P-256, P-384, P-512, P-521 private part of the ECDSA key pair used for Asymmetric signature
IAS-AC-RSA*	1024-, 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-512, P-521 private part of the ECDH key pair used for shared key mechanism
IAS-KG-AS-RSA*	1024-, 2048- private part of the RSA generated key pair used for Asymmetric signature
IAS-KG-AS-ECDSA	P-224, P-256, P-384, P-512, P-521 private part of the ECDSA generated key pair used for Asymmetric signature
IAS-KG-AC-RSA*	1024-, 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-512, P-521 private part of the ECDSA generated key pair used for shared key mechanism
IAS-AS-AUTH-RSA*	1024-, 2048- private part of the RSA key pair used to Authenticate the Card
IAS-ECDSA-AUTH-ECC	P-224, P-256, P-384, P-512, P-521 private part of the ECDSA 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

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

IAS-SC-PIN-TDES	2-Key Triple-DES key used for PIN encryption (PIN History)
IAS-OWNERPIN	4 to 64 byte PIN value managed by the Applet.

**Table 17 – IDPrime MD Applet Critical Security Parameters**

\* CSPs impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Table 14).

### 4.3 IDPrime MD Applet Public Keys

Key	Description / Usage
IAS-KA-RSA-DH*	1024-, 2048- RSA DH key used for Key Agreement (Session Key computation)
IAS-KA-ECDH	P-224, P-256, P-384, P-512, P-521 ECDH key pair used for Key Agreement (Session Key computation)
IASAS-CA-RSA-PUB	1024-, 2048- CA RSA Asymmetric Public Key entered into the module used for CA certificate Verification
IASAS-CA-ECDSA-PUB	P-224, P-256, P-384, P-512, P-521 CA ECDSA Asymmetric public key entered into the module used for CA Certificate Verification.
IASAS-IFD-RSA-PUB	1024-, 2048- IFD RSA Asymmetric Public Key entered into the module used for IFD Authentication
IASAS-IFD-ECDSA-PUB	P-224, P-256, P-384, P-512, P-521 IFD ECDSA Asymmetric public key entered into the module used for IFD Authentication.
IAS-AS-RSA-PUB	1024, 2048- public part of RSA key pair used for Asymmetric Signature
IAS-AS-ECDSA-PUB	P-224, P-256, P-384, P-512, P-521 public part of ECDSA key pair used for Asymmetric signature
IAS-AC-RSA-PUB*	1024, 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-512, P-521 public part of the ECDH key pair used for shared key mechanism
IAS-KG-AS-RSA-PUB	1024, 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-512, P-521 public part of the ECDSA generated key pair used for Asymmetric signature
IAS-KG-AC-RSA-PUB	1024, 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-512, P-521 public part of the ECDSA generated key pair used for shared key mechanism
IAS-AS-AUTH-RSA-PUB	1024, 2048 public part of the RSA key pair used to Authenticate the Card



**IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2**

IAS-ECDSA-AUTH-ECC-PUB	P-224, P-256, P-384, P-512, P-521 public part of the ECDSA key used to Authenticate the card
------------------------	--

\* CSPs impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Table 14).

**Table 18 – IDPrime MD Applet Public Keys**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 4.4 OATH Applet Critical Security Parameters

CSP	Description / Usage
OTP-SC-APPLET-KMAC-TDES	2-Key Triple-DES Applet Key used for Administrative Secure Messaging (MAC)
OTP-SC-APPLET-KENC-TDES	2-Key Triple-DES Applet Key used for Administrative Decipher operation (ENC)
OTP-SC-SERV-KMAC-TDES	2-Key Triple-DES Service Key used for Administrative Secure Messaging (MAC)
OTP-SC-SERV-KENC-TDES	2-Key Triple-DES Service Key used for Administrative Decipher operation (ENC)
OTP-SC-SESSION-MAC-TDES	2-Key Triple-DES Session Key used for Administrative Secure Messaging (MAC)
OTP-SC-SESSION-KENC-TDES	2-Key Triple-DES Session Key used for Administrative Decipher operation (ENC)
OTP-SEED	Data used as Seed for OTP generation
OTP-SERVSEED	Data used as Server Seed for OTP generation
OTP-SC-SEED-TDES	2-Key Triple-DES Key used to diversify Seed used for OTP generation
OTP-SC-SERVSEED-TDES	2-Key Triple-DES Key used to diversify Server Seed used for OTP generation
OTP-OWNERPIN	4 to 8 byte PIN value managed by the Applet.

**Table 19 – OATH Applet Critical Security Parameters**

### 4.5 MPCOS Applet Critical Security Parameters

CSP	Description / Usage
MPC-SC-ADMIN-TDES	2-Key Triple-DES Key used to generate a session Key for Administrative Secure Messaging (MAC and ENC)
MPC-SC-PAY-TDES	2-Key Triple-DES Key used for Transaction certificates
MPC-SC-MULT-TDES	2-Key Triple-DES Key used for Multi-purpose function
MPC-SC-AUTH-TDES	2-Key Triple-DES Key used for Authentication
MPC-SC-SIGN-TDES	2-Key Triple-DES Key used for signature
MPC-SC-SESSION-TDES	2-Key Triple-DES Session Key used as Session Key for Secure Messaging and Payment
MPC-SC-SAUTH-TDES	2-Key Triple-DES Key used for Authentication and Session Key generation
MPC-SC-TEMP-TDES	2-Key Triple-DES Key used for Payment and Session Key generation
MPC-PSWD	4 bytes Password

**Table 20 – MPCOS Applet Critical Security Parameters**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 5 Roles, authentication and services

Next table 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.
OUSR	(User) The OATH user role is responsible for ensuring the ownership of his CM, and for not communicating his PIN to other parties. The OATH Applet authenticates the OATH user by verifying the PIN value.
OCAA	(Card Application Administrator) The OATH Card Application Administrator role represents an external application requesting the services offered by the OATH Applet. An applet authenticates the Application Administrator role by verifying possession of the OATH Card Application Administrator keys.
MUSR	(User) The MPCOS user role is responsible for ensuring the ownership of the CM, and not communicating his PIN to other parties. The MPCOS applet authenticates the MPCOS user by verifying the PIN value.
MCAA	(Card Application Administrator) The MPCOS Card Application Administrator role represents an external application requesting the services offered by the MPCOS Applet (Administrative, Authentication). An applet authenticates the MCAA role by verifying possession of the MPCOS Card Application Administrator keys.
MCAAP	(Card Application Administrator for Payment) The MPCOS Card Application Administrator for Payment role represents an external application requesting the services offered by the MPCOS Applet (Payment, Multi-purpose, Signature). An applet authenticates the MCAAP role by verifying possession of the MPCOS Card Application Administrator for Payment keys.
UA	Unauthenticated role

**Table 21 - Role description**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 5.1 Secure Channel Protocol (SCP) Authentication for ID Prime MD CO

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 SCP01 or SCP02 [SP 800-131A] Section A.1 provides the NIST rationale for 2-Key Triple-DES security strength. 2-Key Triple-DES is 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. The Module claims 112-bit security strength for its 2-Key Triple-DES operations, as the meet-in-the-middle attack rationale described in [SP 800-131A] does not apply unless the attacker has access to encrypt/decrypt pairs.

2-Key Triple-DES key establishment provides 112 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 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  $255/2^{64}$

For SCP03, AES-128, AES-192 or AES-256 keys are used instead of 2-key Triple-DES. Operations are identical to those previously described. Therefore, 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:

- $\left(\frac{1}{2^{128}}\right)$  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  $255/2^{128}$ .

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 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

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 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  $15/10^6$

### 5.4 OATH User authentication

PIN verification is the responsibility of the OATH Applet that defines and maintains its own security policy regarding PIN but uses the PIN management services provided by the platform.

The module enforces string length of 4 bytes minimum (16 bytes maximum) for the Global PIN, allowing all characters, so the strength of this authentication method is as follow:

- The probability that a random attempt at authentication will succeed is  $1/256^4$
- Based on a maximum count of 15 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is  $15/256^4$

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 5.5 OATH Card Application Administrator authentication

OCAA authentication is the responsibility of the OATH Applet using Mutual Authenticate command that involves verifying decryption of a challenge using the secret 2-Key Triple-DES key.

- The probability that a random attempt at authentication will succeed is  $1/2^{64}$  (based on block size)
- Based on the maximum rate at which the module can process authentication attempts, the probability that a random attempt will succeed over a one minute period is approximately  $495/2^{64}$

### 5.6 MPCOS 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 MPCOS Applet services to authenticate to the MUSR role.

The module enforces string length of 4 bytes for the Owner PIN, allowing all characters, so the strength of this authentication method is as follow:

- The probability that a random attempt at authentication will succeed is  $1/256^4$
- Based on a maximum count of 7 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is  $7/256^4$

### 5.7 MPCOS Card Application Administrator authentication

Using the **2-Key Triple-DES key** establishment provides 112 bits of security strength. The Module uses the MPC-SC-ADMIN-TDES to authenticate the MCAA role.

- The probability that a random attempt at authentication will succeed is  $1/2^{64}$  (based on block size)
- Based on the maximum rate at which the module can process authentication attempts, the probability that a random attempt will succeed over a one minute period is  $1200/2^{64}$

Using PIN authentication the module enforces string length of 4 bytes for the PIN, allowing all characters, so the strength of this authentication method is as follow:

- The probability that a random attempt at authentication will succeed is  $1/256^4$
- Based on a maximum count of 7 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is  $7/256^4$

### 5.8 MPCOS Card Application Administrator for Payment authentication

The **2-Key Triple-DES key** establishment provides 112 bits of security strength. The Module uses the MPC-SC-PAY--TDES, the MPC-SC-MULT-TDES, or the MPC-SC-SIGN-TDES to authenticate the MCAAP role.

- The probability that a random attempt at authentication will succeed is  $1/2^{64}$  (based on block size)
- Based on the maximum rate at which the module can process authentication attempts, the probability that a random attempt will succeed over a one minute period is  $1200/2^{64}$

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 5.9 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)	<p>Power cycle the Module by removing and reinserting it into the contact reader slot, or by reader assertion of the RST signal. The <i>Card Reset</i> service will invoke the power on self-tests described in Section <a href="#">§10-Self-test</a>.</p> <p>Moreover, on any card reset, the Module overwrites with zeros the RAM copy of, OS-RNG-STATE, SD-SENC, SD-SMAC and SD-SDEK.</p> <p>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.</p> <p>During the self-tests, the module generates the RAM copy of OS-RNG-STATE and updates the EEPROM copy of OS-RNG-STATE.</p>
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 22 - Unauthenticated Services and CSP Usage**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

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 23 – 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.



## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 5.10 IDPRIME MD Services

All services implemented by the IDPrime MD applet are listed in the table below. Each service description also describes all usage of CSPs by the service.

Service	Description	ICAA	IUSR	UA
EXTERNAL AUTHENTICATE	<p>Authenticates the external terminal to the card. Sets the secure channel mode.</p> <p><u>For symmetric keys:</u> Must be preceded by a successful GET CHALLENGE, and uses IAS-SC-DKMAC-AES, IAS-SC-DKENC-AES, IAS-SC-DKMAC-TDES, IAS-SC-DKENC-TDES or IAS-SC-DES3, to generate IAS-SC-SMAC-AES, IAS-SC-SENC-AES, IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES session keys, respectively.</p> <p><u>For Asymmetric keys:</u> Must be preceded by a successful PSO – VERIFY CERTIFICATE, and uses IASAS-IFD-RSA-PUB or IASAS-IFD-ECDSA-PUB.</p>	X	X	X
INTERNAL AUTHENTICATE*	<p>Authenticates the card to the terminal. Uses IAS-AS-AUTH-RSA or IAS-ECDSA-AUTH-ECC, with the use of: IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.</p>	X	X	X
SELECT	<p>Selects a DF or an EF by its file ID, path or name (in the case of DFs). Does not use CSPs.</p>	X	X	X
CHANGE REFERENCE DATA	<p>Changes the value of a PIN. Uses OS-GLOBALPIN or IAS-OWNERPIN. Optionally uses IAS-SC-PIN-TDES, or IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.</p>	X	X	
RESET RETRY COUNTER	<p>Unblock and optionally change the value of a PIN. Uses the OS-GLOBALPIN or the IAS-OWNERPIN. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-</p>	X		

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

Service	Description	ICAA	IUSR	UA
	SENC-AES session keys.			
VERIFY PIN	Authenticates the IUSR. Uses the OS-GLOBALPIN or the IAS-OWNERPIN. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	X
CREATE FILE	Creates an EF under the root or the currently selected DF or creates a DF under the root. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	
DELETE FILE	Deletes the current DF or EF. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	
DELETE ASYMMETRIC KEY PAIR	Deletes an RSA or ECDSA Asymmetric Key Pair: 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-AS-RSA-PUB, IAS-AS-ECDSA-PUB, IAS-AC-RSA-PUB, IAS-ECDH-ECC-PUB, IAS-KG-AS-RSA-PUB, IAS-KG-AS-ECDSA-PUB, IAS-KG-AC-RSA-PUB, IAS-KG-AC-ECDH-PUB. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	
ERASE ASYMMETRIC KEY	Erases an RSA or ELC Asymmetric Key Pair: 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-AS-RSA-PUB, IAS-AS-ECDSA-PUB, IAS-AC-RSA-PUB, IAS-ECDH-ECC-PUB, IAS-KG-AS-RSA-PUB, IAS-KG-AS-ECDSA-PUB, IAS-KG-AC-RSA-PUB, IAS-KG-AC-ECDH-PUB. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

Service	Description	ICAA	IUSR	UA
GET DATA (IDPrime MD Applet Specific)	<p>Retrieves the following information:</p> <ul style="list-style-type: none"> <li>■ CPLC data</li> <li>■ Applet version</li> <li>■ Software version (includes applet version - BER-TLV format)</li> <li>■ Available EEPROM memory</li> <li>■ Additional applet parameters</li> <li>■ PIN Policy Error</li> </ul> <p>Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.</p>	X	X	X
GET DATA OBJECT	<p>Retrieves the following information:</p> <ul style="list-style-type: none"> <li>■ Public key elements: IAS-AS-RSA-PUB, IAS-AS-ECDSA-PUB, IAS-AC-RSA-PUB, IAS-ECDH-ECC-PUB, IAS-KG-AS-RSA-PUB, IAS-KG-AS-ECDSA-PUB, IAS-KG-AC-RSA-PUB, IAS-KG-AC-ECDH-PUB IAS-AS-AUTH-RSA-PUB, IAS-ECDSA-AUTH-ECC-PUB.</li> <li>■ KICC: generates IAS-KA-RSA-DH.</li> <li>■ The contents of a specified SE</li> <li>■ Information about a specified PIN</li> </ul> <p>Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.</p>	X	X	X
PUT DATA (IDPrime MD Applet Specific)*	<p>Creates or updates a data object</p> <ul style="list-style-type: none"> <li>■ Create container<sup>3</sup></li> <li>■ Update public/private keys<sup>3</sup></li> </ul> <p>IAS-AS-RSA, IAS-AS-ECDSA, IAS-AC-RSA, IAS-ECDH-ECC (private keys), IAS-AS-RSA-PUB, IAS-AS-ECDSA-PUB, IAS-AC-RSA-PUB, IAS-ECDH-ECC-PUB (public keys).</p> <p>Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-</p>		X	

<sup>3</sup> Secure Messaging in Confidentiality is mandatory

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

Service	Description	ICAA	IUSR	UA
	SENC-AES session keys (for public keys). It becomes mandatory for private keys.			
PUT DATA (IDPrime MD Applet Specific)	Creates or updates a data object <ul style="list-style-type: none"> <li>■ Access Conditions</li> <li>■ Applet Parameters (Admin Key, Card Read Only and Admin Key Try Limit ): IAS-SC-DES3</li> <li>■ PIN info</li> </ul> Uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X		
PUT DATA (IDPrime MD Applet Specific)	Creates or updates a data object <ul style="list-style-type: none"> <li>■ Update DES or AES Secret keys3 :</li> </ul> IAS-SC-DKMAC-AES, IAS-SC-DKENC-AES, IAS-SC-DKMAC-TDES, IAS-SC-DKENC-TDES. Uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	
PUT SECURE KEY*	Imports securely an AES session key or RSA/ECC Key Pair (secure key injection). Uses IAS-AC-RSA-PUB or IAS-KG-AC-RSA-PUB (for encryption), and IAS-AC-RSA or IAS-KG-AC-RSA (for decryption) to store IAS-SC-T-SKI-AES into the card.  Optionally uses IAS-SC-SMAC-AES, IAS-SC-SENC-AES, IAS-SC-SMAC-TDES, or IAS-SC-SENC-TDES session keys.	X		
READ BINARY	Reads part of a binary file. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	X
ERASE BINARY	Erases part of a binary file. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	
UPDATE BINARY	Updates part of a binary file. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

Service	Description	ICAA	IUSR	UA
DEACTIVATE FILE	Changes the state of a file to OPERATIONAL (DEACTIVATED). Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	
ACTIVATE FILE	Changes the state of a file to OPERATIONAL (ACTIVATED). Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.	X	X	
GENERAL AUTHENTICATE	Used to generate secure messaging session keys between both entities (IFD and ICC) as part of elliptic curve asymmetric key mutual authentication. Generates IAS-KA-ECDH session key.	X	X	X
GENERATE KEY PAIR*	Generates an RSA or ECDSA key pair and stores both keys in the card: IAS-KG-AS-RSA, IAS-KG-AS-ECDSA, IAS-KG-AC-RSA, IAS-KG-AC-ECDH (private keys), and IAS-KG-AS-RSA-PUB, IAS-KG-AS-ECDSA-PUB, IAS-KG-AC-RSA-PUB, IAS-KG-AC-ECDH-PUB (public keys). 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. Uses IAS-CA-RSA-PUB or IAS-CA-ECDSA-PUB. Stores IASAS-IFD-RSA-PUB or IASAS-IFD-ECDSA-PUB. To be followed by EXTERNAL AUTHENTICATE. Uses IAS-SC-SMAC-AES and IAS-SC-SENC-AES session keys (for ECC keys only).		X	
PSO - HASH	Entirely or partially hashes data prior to a PSO– Compute Digital Signature command or prepares the data if hashed externally. Does not use CSPs.		X	

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

Service	Description	ICAA	IUSR	UA
PSO – DECIPHER*	(RSA) Deciphers an encrypted message using a decipher key stored in the card. Uses IAS-AC-RSA, IAS-KG-AC-RSA. (ECDSA) Generates a symmetric key used by the terminal. Uses IAS-ECDH-ECC, IAS-KG-AC-ECDH.		X	
PSO – COMPUTE DIGITAL SIGNATURE*	Computes a digital signature. Uses IAS-AS-RSA, IAS-KG-AS-RSA, IAS-KG-AC-RSA, IAS-AS-ECDSA, IAS-KG-AS-ECDSA. Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.		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. Generates two 4-byte-long random numbers and returns them to IFD. Does not use CSPs.	X	X	X
GET CHALLENGE	Generates an 8 or 16-byte random number. Uses IAS-SC-SMAC-AES and IAS-SC-SENC-AES session keys (for ECC keys only).			X
MANAGE SECURITY ENVIRONMENT	Supports two functions, Restore and Set. <ul style="list-style-type: none"> <li>■ Restore: replaces the current SE by an SE stored in the card.</li> <li>■ Set: sets or replaces one component of the current SE.</li> </ul> Optionally uses IAS-SC-SMAC-TDES, IAS-SC-SENC-TDES, IAS-SC-SMAC-AES, or IAS-SC-SENC-AES session keys.			X

**Table 24 – IDPrime MD applet Services and CSP Usage**

\* Services impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Table 14).

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

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"> <li>■ GUID</li> </ul> Does not use CSPs.			X

**Table 25 – MSPNP applet Services**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 5.11 OATH Services

All services implemented by the OATH applet are listed in the table below. Each service description also describes all usage of CSPs by the service.

Service	Description	OCAA	OUSR	UA
<b>SELECT</b>	Select an applet (managed by the Platform). Does not use CSPs.	X	X	X
<b>COMPUTE OTP (No Pin verification required)</b>	Compute an OTP without verification of the PIN. Uses OTP-SEED.	X	X	X
<b>COMPUTE OTP (Pin verification required)</b>	Compute an OTP with verification of the OS-GLOBALPIN or the OTP-OWNERPIN prior the computation. Uses OTP-SEED.		X	
<b>GET DATA (OATH Applet Specific)</b>	Get Data to retrieve OTP information: <ul style="list-style-type: none"> <li>▪ Profile byte</li> <li>▪ Display duration</li> <li>▪ URL address</li> </ul> Does not use CSPs.	X	X	X
<b>VERIFY PIN</b>	Authenticates the OUSR. Uses the OS-GLOBALPIN or the OTP-OWNERPIN.	X	X	X
<b>GET TOKEN DATA (Token ID, OTP Counter)</b>	Get Data to retrieve OTP information: <ul style="list-style-type: none"> <li>▪ OTP counter</li> <li>▪ Token ID</li> </ul> Does not use CSPs.	X	X	X
<b>GET TOKEN DATA ( OTP, No PIN)</b>	Get Data to retrieve OTP information. Does not use CSPs.	X	X	X
<b>GET TOKEN DATA ( OTP, PIN)</b>	Get Data to retrieve OTP information. Does not use CSPs.		X	
<b>GET MENU</b>	Retrieve part of the Menu. Does not use CSPs.	X	X	X
<b>IS MENU CHANGED</b>	Retrieve the information: "Menu has been changed"? Does not use CSPs.	X	X	X
<b>GET VERSION &amp; BATTERY COUNTER</b>	Retrieve the information on : <ul style="list-style-type: none"> <li>▪ The version of the application.</li> <li>▪ The applet code source version.</li> </ul>	X	X	X



## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

	<ul style="list-style-type: none"> <li>▪ The BATTERY_COUNTER.</li> </ul> <p>Does not use CSPs.</p>			
<b>GET CHALLENGE</b>	Initializes a secure channel and computes internal challenge (8 bytes); to be followed by MUTUAL AUTHENTICATE.	X	X	X
<b>MUTUAL AUTHENTICATE</b>	<p>Authenticates the OCAA and establishes a secure channel. Must be preceded by a successful GET CHALLENGE.</p> <p>Uses OTP-SC-APPLET-KENC-TDES, OTP-SC-APPLET-KMAC-TDES keys to generate OTP-SC-SESSION-KENC-TDES, OTP-SC-SESSION-KMAC-TDES session keys, respectively.</p>	X	X	X
<b>PUT MENU</b>	<p>Set the menu composed of menu items.</p> <p>Uses OTP-SC-SESSION-KENC-TDES, OTP-SC-SESSION-KMAC-TDES session keys.</p>	X		
<b>PUT OTP DATA &amp; TOKEN ID</b>	<p>Set the following data into the card:</p> <ul style="list-style-type: none"> <li>▪ OTP seed</li> <li>▪ OTP counter</li> <li>▪ Server seed</li> <li>▪ Token ID.</li> </ul> <p>Uses OTP-SC-SESSION-KENC-TDES, OTP-SC-SESSION-KMAC-TDES session keys. Updates OTP-SEED, OTP-SERVSEED using OTP-SC-SEED-TDES, OTP-SC-SERVSEED-TDES respectively.</p>	X		
<b>PUT DATA (OATH Applet Specific)</b>	<p>Set or Update data into the OTP referenced service.</p> <p>Uses OTP-SC-SESSION-KENC-TDES, OTP-SC-SESSION-KMAC-TDES session keys.</p>	X		
<b>COMPUTE OCRA – One way challenge response (PIN)</b>	Compute an OTP (OCRA) with verification of the OS-GLOBALPIN or the OTP-OWNERPIN prior the computation. Must be preceded by a successful GET CHALLENGE for OCRA (using the challenge returned by the command and OTP counter).		X	
<b>COMPUTE OCRA – One way challenge response (No PIN)</b>	Compute an OTP (OCRA) without verification of the PIN. Must be preceded by a successful GET CHALLENGE for OCRA (using the challenge returned by the	X	X	X

**IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2**

	command and OTP counter).			
<b>COMPUTE OCRA – Response Only (PIN)</b>	Compute an OTP (OCRA) with verification of the OS-GLOBALPIN or the OTP-OWNERPIN prior the computation. Uses the OTP counter and optional information.		X	
<b>COMPUTE OCRA – Response Only (No PIN)</b>	Compute an OTP (OCRA) without verification of the PIN. Uses the OTP counter and optional information.	X	X	X
<b>GET CHALLENGE for OCRA</b>	Computes internal challenge (8 bytes); to be followed by Compute OCRA Challenge Response.	X	X	X
<b>COMPUTE OCRA – Mutual Challenge Response (PIN)</b>	Compute an OTP (OCRA) with verification of the OS-GLOBALPIN or the OTP-OWNERPIN prior the computation. Mutual Authentication of the client and the server, using a client-challenge & a server-challenge. Uses OTP-SERVSEED.		X	
<b>COMPUTE OCRA – Mutual Challenge Response (No PIN)</b>	Compute an OTP (OCRA) without verification of the PIN. Mutual Authentication of the client and the server, using a client-challenge & a server-challenge. Uses OTP-SERVSEED.	X	X	X

**Table 26 – OATH Applet Services Access**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 5.12 MPCOS Services

All services implemented by the MPCOS applet are listed in the table below. Each service description also describes all usage of CSPs by the service.

Service	Description	MCAAP	MCAA	MUSR	UA
SELECT FILE	This command selects either a DF or an EF file. Does not use CSPs.	X	X	X	X
APPEND RECORD	The Append Record command is used to format a structured file by appending (and initializing) a new record. This command is only available for Linear Fixed EF (Not allowed for Secret Code and Keys files). Optionally uses MPC-SC-SESSION-TDES (SM).	X	X	X	X
EXTERNAL AUTH	The External Authenticate command is intended to make the Card authenticate the Outside World. Must be preceded by a successful GET CHALLENGE. Uses MPC-SC-ADMIN-TDES key to generate MPC-SC-SESSION-TDES session keys.	X	X	X	X
GET CHALLENGE	The Get Challenge command is the first step of an EXTERNAL AUTHENTICATE process and is used to make the Card generate a 8 bytes long Random Number.	X	X	X	X
INTERNAL AUTHENTICATE	The aim of the command is to make the Outside World authenticate the Card, by checking the consistency of the cryptogram. Uses MPC-SC-AUTH-TDES key to generate MPC-SC-SAUTH-TDES session keys.	X	X	X	X
READ BINARY	This command is used to read data from the transparent file. This command cannot be applicable to Secret Code and Keys files. Optionally uses MPC-SC-SESSION-TDES (SM).	X	X	X	X
READ RECORD	The Read Record command is used to read data in a structured file. This command is only available for Linear Fixed EF (Not allowed for Secret Code and Keys files). Optionally uses MPC-SC-SESSION-TDES (SM).	X	X	X	X
SELECT FILE KEY	This command is intended to set up a Session Key before issuing non-payment oriented commands with	X	X	X	X

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

Service	Description	MCAAP	MCAA	MUSR	UA
	secure messaging. Uses MPC-SC-AUTH-TDES key to generate MPC-SC-SAUTH-TDES session keys.				
SET SECRET CODE	This command is used either to unblock or to modify (substitute) the value of an existing secret code with a new value. It uses and updates MPC-PSWD. Optionally uses MPC-SC-SESSION-TDES (SM).		X		
UPDATE BINARY (Non sensitive Data file)	This command allows initiating the update of the bits already present in an EF with the bits given in the command. Optionally uses MPC-SC-SESSION-TDES (SM). (This command cannot be applicable to Secret Code)	X	X	X	X
UPDATE BINARY (Key File)	This command allows initiating the update of the bits already present in an EF with the bits given in the command. Optionally uses MPC-SC-SESSION-TDES (SM). (This command cannot be applicable to Secret Code)		X		
UPDATE RECORD	The Update Record command is used to update data in a structured file. Optionally uses MPC-SC-SESSION-TDES (SM). This command is only available for Linear Fixed EF. (Not allowed for Secret Code and Keys files)	X	X	X	X
VERIFY	This command is used to verify secret code to give authorization for some access conditions. Uses the MPC-PSWD to authenticate the MUSR role. Optionally uses MPC-SC-SESSION-TDES (SM).			X	
WRITE BINARY (non sensitive data file)	This command allows to initiates the writing of binary values into an EF using a logical OR of the bits already present in the EF with the bits given in the command. (This command cannot be applicable to Secret Code)	X	X	X	X
WRITE BINARY (Key file)	This command allows to initiates the writing of binary values into an EF using a logical OR of the bits already present in the EF with the bits given in the command. Optionally uses MPC-SC-SESSION-TDES (SM).		X		

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

Service	Description	MCAAP	MCAA	MUSR	UA
	(This command cannot be applicable to Secret Code)				
GET INFO	This command allows the retrieval of the card serial number. The data may be obtained at any moment in a session. Does not use CSPs.	X	X	X	X
GET RESPONSE	This command is used to retrieve the data prepared in RAM by the previous command. It can also be issued immediately after the ATR. Does not use CSPs.	X	X	X	X
READ MEMORY	This command is used to read the card serial number. It may be issued at any moment during a card session. Does not use CSPs.	X	X	X	X
SET CARD STATUS	This command is used to write the 3 bits in the lock byte. It can be performed only once during the life cycle of the application. Does not use CSPs.	X	X	X	X
GET DATA PTC	Get Data for Tag 9F17 (PIN Try Counter) is to be supported to get the PIN Try Counter for Global PIN. Does not use CSPs.	X	X	X	X
CREDIT	This command is used to credit an amount into the purse in EF purse. Uses either: MPC-SC-PAY-TDES, MPC-SC-MULT-TDES or MPC-SC-SIGN-TDES keys, and MPC-SC-TEMP-TDES session key.	X			
DEBIT	The Debit command is used to debit a purse. Uses MPC-SC-PAY-TDES key and MPC-SC-TEMP-TDES session key.	X		X	X
READ BALANCE	The Read Balance command is used to read the balance value of a given purse. Uses MPC-SC-TEMP-TDES session key.	X		X	X
SELECT PURSE KEY	This command is intended to set up a Session Key before issuing payment-oriented commands. Uses MPC-SC-PAY-TDES, MPC-SC-MULT-TDES or keys to generate MPC-SC-TEMP-TDES session key.	X		X	X
SET OPTIONS	This command is used to set the options of the Sign command (or to change the default options). Does not use CSPs.	X	X	X	X
SIGN	This command is used to make the Card compute a certificate of the previous transaction, based on the	X		X	

**IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2**

Service	Description	MCAAP	MCAA	MUSR	UA
	value of the Amount parameter in RAM and (option depending) on the Balance of the currently selected Purse. Uses either: MPC-SC-SIGN-TDES, MPC-SC-PAY-TDES, or MPC-SC-MULT-TDES keys and MPC-SC-TEMP-TDES session key.				
SUBSTITUTE DEBIT	The Substitute Debit command is used to cancel the previous debit performed by a terminal in a purse and to replace it with another one. The amount of this second debit is part of the data ciphered in the cryptogram. Uses MPC-SC-PAY-TDES key and MPC-SC-TEMP-TDES session key.	X			

**Table 27 – MPCOS Applet Services Access**

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 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.

Hardness testing was performed at ambient temperature. No assurance is provided for Level 3 hardness conformance at any other temperature.

### 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.

## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

### 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).
RNG	Performs ANSI X9.31 KAT with fixed inputs
Triple-DES	Performs separate encrypt and decrypt KATs using 2-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.
AES-CMAC	Performs an AES-CMAC Generate KAT using an AES 128 key. Note that AES-CMAC Verify is identical to a Generate KAT (perform Generate then compare to the input) hence a single KAT verifies both functions.
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.
ECDSA	Performs a ECDSA signature and verification KATs using an ECC P-224 key.
ECC CDH	Performs an ECC CDH KAT using an ECC P-224 key.
SHA-1	Performs a SHA-1 KAT.
SHA-256	Performs a SHA-256 KAT.
SHA-512	Performs a SHA-512 KAT.

**Table 28 – Power-On Self-Test**

#### 10.2 Conditional self-tests

On every call to the [ANS X9.31] RNG, the CM performs a stuck fault 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 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-RSA public key, the DAP-DES key or the DAP-AES



## IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic Module Security Policy Level 2

key; the signature block in this scenario is signed by an external entity using the private key corresponding to DAP-RSA or the symmetric DAP-DES key or the DAP-AES key.

### 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 Applets are Java applets 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.



**IDPrime MD 830 with OATH & MPCOS applets - FIPS 140-2 Cryptographic  
Module Security Policy Level 2**

**END OF DOCUMENT**