THALES
Building a future we can all trust

eToken 5300 Mini MD 4.3.5

FIPS 140-2 Cryptographic Module

Non-Proprietary Security Policy Level 3

Document Information

Product Version	MD 4.3.5
Document Part Number	Doc Number TBD
Release Date	3 June 2021

Revision History

Revision	Date	Reason
A	3 June 2021	Initial release in Thales format

infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE

This document defines the Security Policy for the Thales eToken 5300 Mini which comprises the 5300 USB MCU FW supporting Touch Sense Button (TSB), the IDCore 30-revB platform and the MD Applet 4.3.5 and herein denoted as Cryptographic Module (CM). The Cryptographic Module or CM, validated to FIPS 140-2 overall Level 3, is a USB token that contains a secure controller module implementing the Global Platform operational environment, with Card Manager, and the MD Applet 4.3.5 supporting the TSB flow.

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001 CHANGE NOTICES (12-03-2002)
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1,* March 2003, www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004 *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2* Amendment D, Sept 2009
[ISO 7816]	ISO/IEC 7816-1: 1998 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification* *Java Card 2.2.2 Virtual Machine (JCVM) Specification* *Java Card 2.2.2 Application Programming Interface* *Java Card 3.0.1 Application Programming Interface [only for algos ECDSA, SHA2]* Published by Sun Microsystems, March 2006
[SP800-131A]	NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 1, November 2015
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[FIPS 113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS 197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013 (DSA2, RSA2 and ECDSA2)
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-3, August 2015

Acronym	Full Specification Name
[AESKeyWrap]	NIST Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012. This document defines symmetric key wrapping, Use of 2-Key TDES in lieu of AES is described in [IG] D.2.
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 20 November 2015.
[SP 800-90A]	NIST, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Special Publication 800-90A Revision 1, June 2015.
[SP 800-108]	NIST, *Recommendation for Recommendation for Key Derivation Using Pseudorandom Functions,* Special Publication 800-108, October 2009.

Table 1 – References

Acronyms and Definitions

Acronym	Definition
CVC	Card Verifiable Certificate
CM	Cryptographic Module
GP	GlobalPlatform
MMU	Memory Management Unit
OP	Open Platform
RMI	Remote Method Invocation
SC	Smart Card

Table 2 – Acronyms and Definitions

CHAPTER 1: Introduction

The CM is a limited operational environment under the FIPS 140-2 definitions. The CM SC 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 CM also includes the USB MCU FW firmware load service to support necessary updates of the USB controller FW.

The TSB is a physical button that any operator with physical access to the module can depress. The button press acts as a security measure (presence detection) in addition to the user PIN.

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]

IDPrime MD Applet

IDPrime MD Applet (called IAS Classic V4.3.5) is a Java applet that provides all the necessary functions to integrate a smart card in a public key infrastructure (PKI) system, suitable for identity and corporate security applications. It is also useful for storing information about the cardholder and any sensitive data. IDPrime MD Applet implements state–of–the–art security and conforms to the latest standards for smart cards and PKI applications. It is also fully compliant with digital signature law.
The IDPrime MD Applet, designed for use on JavaCard 2.2.2 and GlobalPlatform 2.1.1 compliant smart cards.

The main features of IDPrime MD Applet are as follows:

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

MSPNP applet is associated to IDPrime MD applet and offers:

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

CHAPTER 2: Hardware and Physical Cryptographic Boundary

Hardware and Physical Cryptographic Boundary

The eToken 5300 Mini is a multi-chip standalone composed of two (2) single chips. Two (2) ICs are mounted on a PCB assembly with a connector and passive components, covered by epoxy on both sides, exposing only the LED, the USB connector and a Touch Sense Button contact. The Module is intended to be covered within a plastic enclosure. Physical inspection inside the Module boundary is not practical, as the epoxy layer is opaque.

The Module meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations.

eToken 5300 Mini Crypto Boundary

Figure 1 depicts the Module at the cryptographic boundary. Figure 2 shows the Module with the outer enclosure, which is not within the cryptographic boundary.

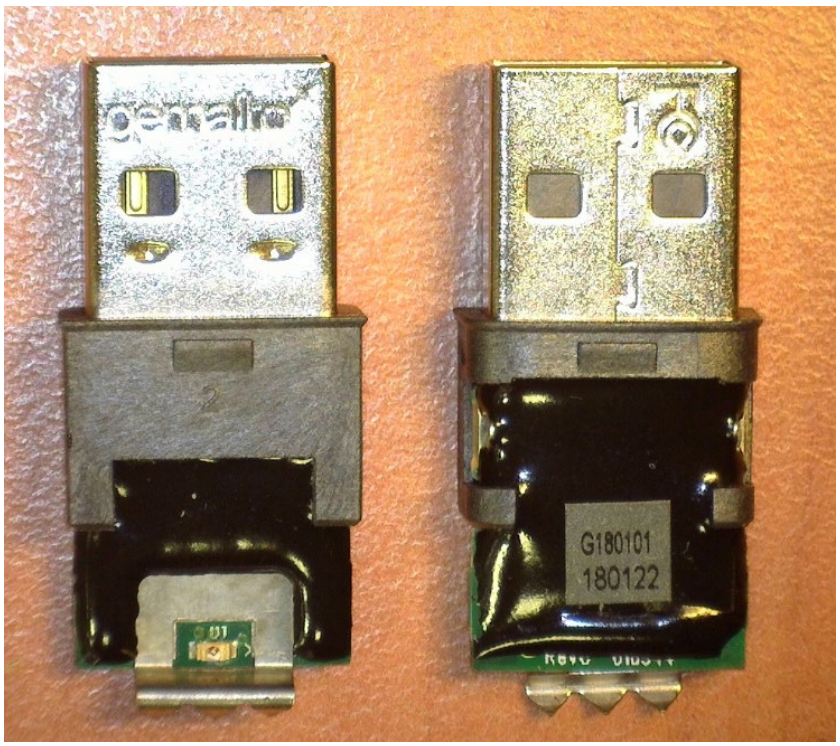

Figure 1 – eToken 5300 Mini Crypto Boundary

Figure 2 – eToken 5300 Mini with Outer Enclosure

Ports and Interfaces

The Module functions as a USB slave device to process and respond to commands. This module provides a contact interface that is fully compliant with USB 2.0, a contact interface for LED indicator and a contact interface for Touch Sense Button.

Ports	Description
USBDM	USB D- differential data
USBDP	USB D+ differential data
VBus	Power supply input
GND	Ground (reference voltage)
LED, LEDA	LED indicator
TOUCH POINT	Touch Sense Button contact

Table 4 – Ports

The I/O ports of the platform provide the following logical interfaces:

Interface	Ports
Data In	USBDM, USBDP
Data Out	USBDM, USBDP
Status Out	USBDM, USBDP, LED, LEDA
Control In	USBDM, USBDP, TOUCH POINT
Power	VBus, GND

Table 5 – Logical Interfaces

CHAPTER 3: Cryptographic Module Specification

USB MCU Firmware and Logical Cryptographic Boundary

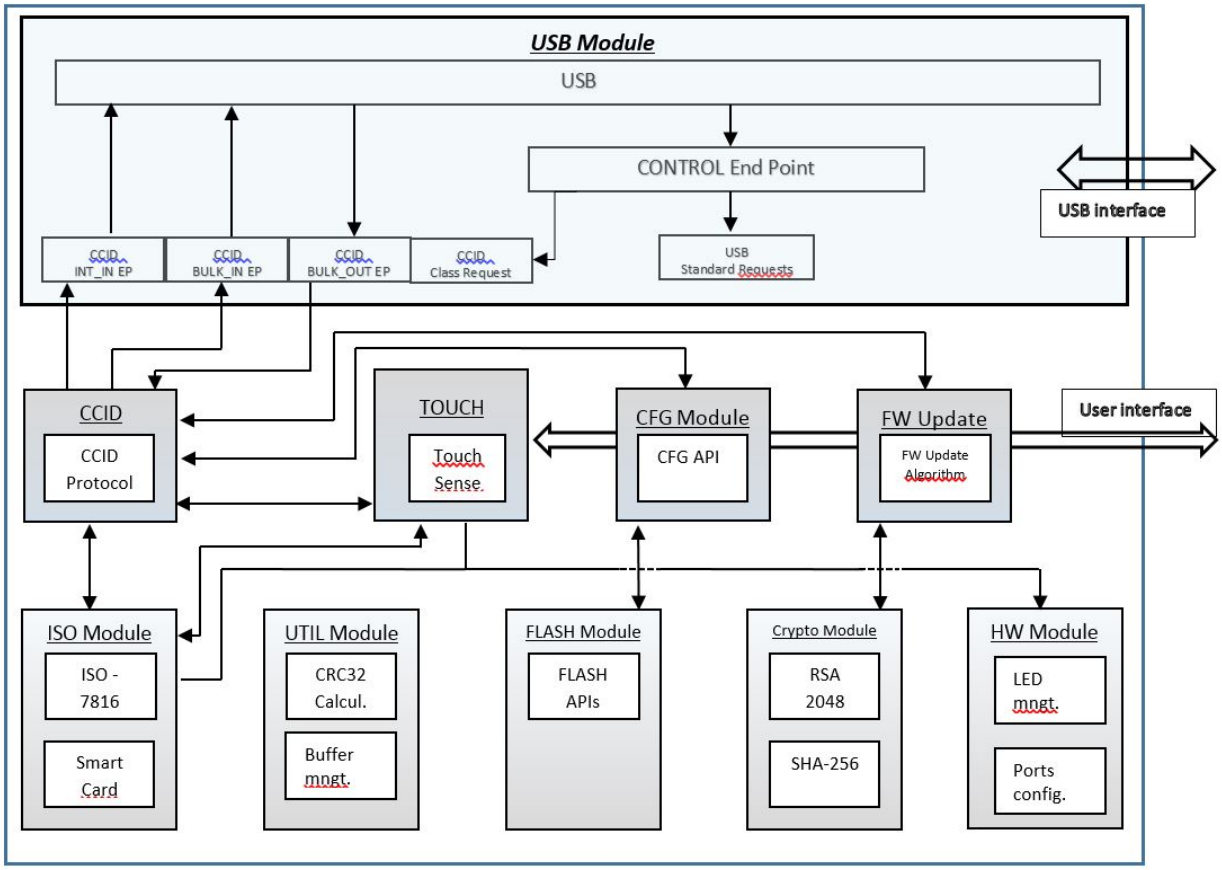

Figure 3 – USB MCU Block Diagram

The CM provides framework for the USB Standard and Class requests including the API dedicated to the CCID protocol. The CM defines an interface for USB MCU firmware update service secured with RSA-2048 PKCS#1 RSASSA-PKCS1-v1_5 signature. The USB MCU FW communicates with the SC OS using ISO-7816 T1 protocol.

The LED functions as status indicator with no connection to Critical Security Parameters, and thus cannot output any sensitive information.

The Touch Sense Button inputs button press indication to the MCU with no connection to Critical Security Parameters, and thus cannot output any sensitive information.

USB MCU FW Versions

eToken 5300 Mini:

Product Number	214-010381-001	ASSY,PCB,SAFENET 5300,MINI
USB MCU	STMicro	STM32F042K6U6TR
Firmware	5300 FIPS	FW ver-14.0.15

The MCU FW version is retrieved via an escape command through the CCID channel; The FW version is encoded in the kernelVerMajor, kernelVerMinor, kernelBuild Fields.

Get FW version

Get FW Version Request

Offset	Field	Size (bytes))	Value	Field Description
0x00	Command Id	1	0x02	Get firmware version

Table 6 – Get FW Version Request Structure

Get FW Version Answer

It is important that the answer starts with 'Gem' (for compatibility with the Thales PC/SC driver)

Offset	Field	Size (bytes)	Value	Field Description
0x00	String answer	20		"GemP53-XX.YY.ZZZZ-X2" Where: "P53" to indicate PKI eToken 5300. XX : Firmware major version. ⇨ 14 for eToken 5300 YY : Firmware minor version (max 99). ZZZZ: Firmware build (max 9999).

Table 7 - Get FW Version Answer Structure

SC Firmware and Logical Cryptographic Boundary

The figure below depicts the SC operational environment and applets.

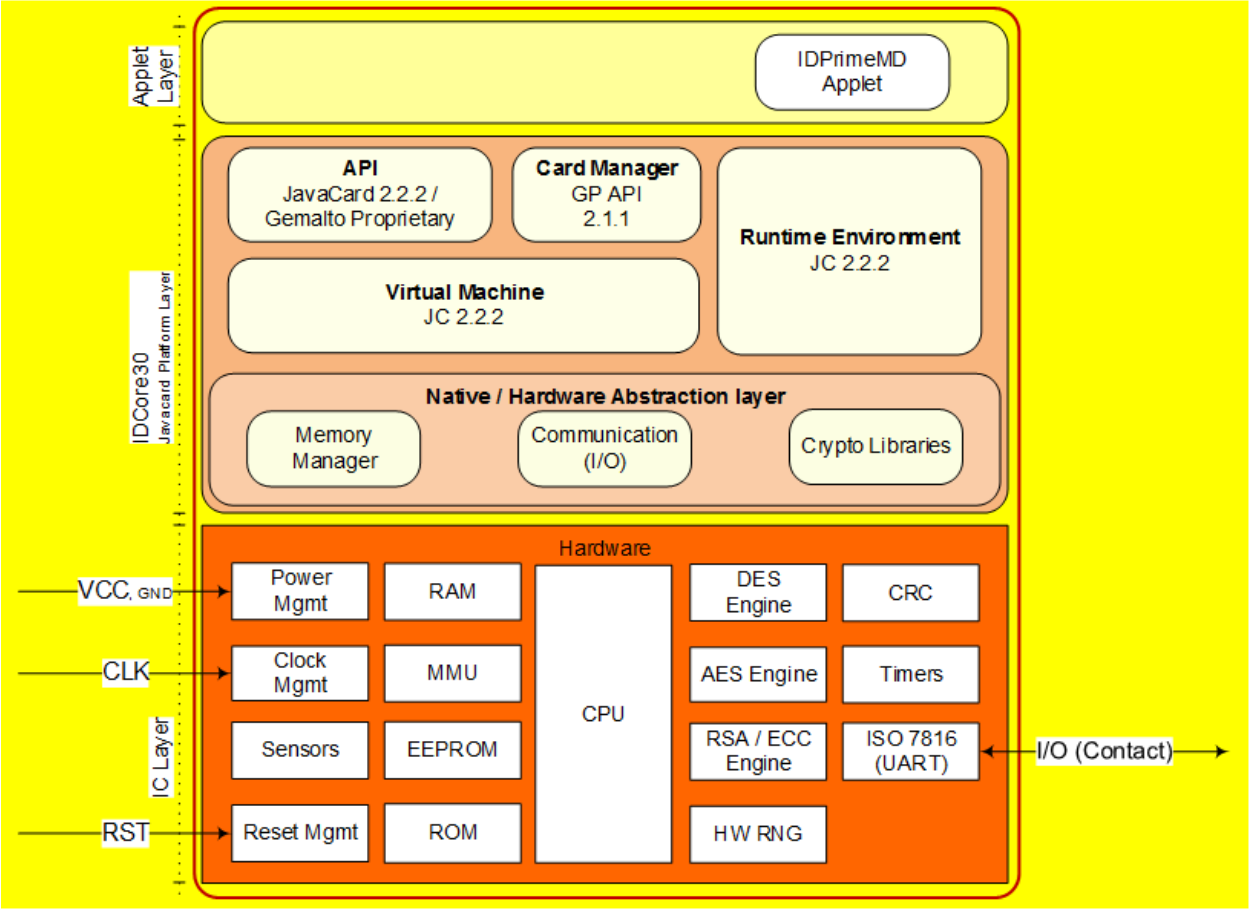

Figure 4 - Smart Card Block Diagram

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

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

Applets, as IDPrime MD, access module functionalities via internal API entry points that are not exposed to external entities. External devices have access to SC services by sending APDU commands encapsulated in the USB CCID commands supported by the USB MCU.

The SC provides an execution sandbox for the IDPrime MD Applet and performs the requested services according to its roles and services security policy.

The SC 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 Chapter 2.

Secure Controller Versions

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

The **IDPrime MD 830** is identified with an applet version and a software version with the two (2) following APDU commands encapsulated in the USB command ***TPDU Reader Level request*** and ***TPDU Reader Level answer***:

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:

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

Table 9 – Applet Version Returned Value

The Software Version is returned in TLV format as follows:

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

Table 10 –Software Version Returned Values

Cryptographic Module Mode of Operation

The Cryptographic Module 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 - which are encapsulated in the USB CCID commands supported by the USB MCU - 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)

Table 11 – GET DATA APDU Command

The SC responds with the following information:

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

IDC30-revB - Identification data (tag 0103)			
Byte	Description	Value	Value meaning
1	Thales Family Name	**B0**	Javacard
2	Thales OS Name	**84**	IDCore family (OA)
3	Thales Mask Number	**56**	G286
4	Thales Product Name	**51**	IDCore30-revB
5	Thales Flow Version	**XY**	**X** is the type of SCP: ▪ 2xh for SCP0300 flows ▪ 3xh for SCP0310 flows **Y**: is the version of the flow (x=1 for version 01). For instance: ▪ **21h** = SCP0300 - flow 01 (version 01) ▪ **31h** = SCP0310 - flow 01 (version 01)
6	Thales Filter Set	**00**	▪ Major nibble: filter family = 00h Lower nibble: version of the filter = 00h
7-8	Chip Manufacturer	**4090**	Infineon
9-10	Chip Version	**7901**	SLE78CFX3000PH
11-12	FIPS configuration	**8D00**	MSByte: b8 : 1 = **conformity to FIPS certificate** b7 : 0 = not applicable b6 : 0 = not applicable b5 : 0 = not applicable b4 : 1 = ECC supported b3 : 1 = RSA CRT supported b2 : 1 = RSA STD supported b1 : 1 = AES supported LSByte: b8 .. b5 : 0 = not applicable b4 : 0 = not applicable (ECC in contactless) b3 : 0 = not applicable (RSA CRT in contactless) b2 : 0 = not applicable (RSA STD in contactless) b1 : 0 = not applicable (AES in contactless) For instance: **8F 00** = FIPS enable (CT only)–AES-RSA CRT/STD-ECC **(Full FIPS)** **8D 00** = FIPS enable (CT only)–AES-RSA CRT-ECC **(FIPS PK CRT) *** **85 00** = FIPS enable (CT only)–AES-RSA CRT **(FIPS RSA CRT)** **00 00** = FIPS disable (CT only)–No FIPS mode **(No FIPS)** **(* default configuration)**

IDC30-revB - Identification data (tag 0103)			
Byte	Description	Value	Value meaning
13	FIPS Level for IDPrime MD product	**03**	03 = FIPS Level 3
14-29	RFU	**xx..xxh**	-

Table 12 – SC Versions and Mode of Operations Indicators

Cryptographic Functionality

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

Algorithm	Description	Cert #
AES	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128-, 192- and 256-bit key lengths with ECB and CBC modes.	3779
AES CMAC	[SP800-38B] AES CMAC The Module supports 128-, 192- and 256-bit key lengths.	3779
CKG	[SP 800-133] Cryptographic key generation compliant with 6.1, 6.2 7.1, 7.2, and 7.4	Vendor Affirmed
CVL ECC-CDH	[SP 800-56A] ECC Cofactor Diffie-Hellman primitive component (5.7.1.2). The Module supports NIST defined P-224, P-256, P-384 and P-521 curves.	719
DRBG	[SP 800-90] Deterministic Random Number Generators, CTR_DRBG mode based on AES-128, derivation function is not used.	1045
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm: signature generation, verification and key pair generation. The Module supports NIST defined P-224, P-256, P-384 and P-521 curves. P-192 is not used by the Module.	814
KBKDF	[SP 800-108] KDF for AES CMAC. The Module supports 128-, 192- and 256-bit key lengths.	81
KTS	[SP800-38F] Symmetric Key wrapping using 128, 192, or 256 bit keys (based on AES and AES CMAC Cert. #3779), meets the SP800-38F §3.1 ¶3 requirements for symmetric key wrapping. Key establishment methodology provides between 128 and 256 bits of encryption strength.	3779
KTS	[SP 800-56B] Key wrapping using 2048-bit keys. Key establishment methodology provides 112 bits of encryption strength Vendor affirmed, based on OAEP scheme as described in SP800-56B for PKCS1 v2.1. (Unwrapped output provided under Secure Messaging)	Vendor Affirmed
RSA	[FIPS 186-4] RSA signature generation, verification, and key pair generation. The Module follows PKCS#1 v1.5 and PSS and supports 2048-bit key. 1024-bit keys are not supported.	1946

Algorithm	Description	Cert #
RSA CRT	[FIPS 186-4] RSA signature generation and CRT key pair generation. The Module follows PKCS#1 v1.5 and PSS, and supports 2048-bit key. The signature verification is not performed by this algorithm. 1024-bit keys are not supported.	1947
RSA Signature Verification (In the USB MCU FW)	[FIPS 186-4] RSA signature verification. The Module follows PKCS#1 v1.5 and supports 2048-bit key.	2622
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms.	3146
SHA256 (In the USB MCU FW)	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms.	3928
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The Module supports the 3-Key options; CBC and ECB modes. Note that the Module does not support a mechanism that would allow collection of plaintext / ciphertext pairs aside from authentication, limited in use by a counter. Per IG A.13, the operator is responsible for ensuring the module's limit to 2^16 encryptions with the same Triple-DES key	2100

Table 13 – FIPS Approved Cryptographic Functions

Algorithm	Description
EC Diffie-Hellman key agreement	NIST defined P-224, P-256, P-384 and P-521 curves. EC DH key agreement calls CVL ECC-CDH Cert. #719. Key establishment methodology provides between 112 and 256 bits of encryption strength.
NDRNG	Used to seed the [SP800-90A] DRBG.
RSA key wrap	Key wrapping using 2048-bit keys. Key establishment methodology provides 112 bits of encryption strength (for PKCS1 v1.5)

Table 14 – 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 MD Applet** are:

- **DRBG**
- **AES CMAC**
- **AES**
- **Triple-DES**
- **RSA**
- **ECDSA**
- **SHA-1, SHA-224, SHA-256, SHA-384, SHA-512**

- **ECC-CDH**

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

CHAPTER 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 CHAPTER 5.

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

IDPrime MD Applet Critical Security Parameters

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

Table 16 – IDPrime MD Applet Critical Security Parameters

IDPrime MD Applet Public Keys

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

Table 17 – IDPrime MD Applet Public Keys

USB MCU FW Public Keys

Key	Description / Usage
ID_FW_DOWNLOAD_RSA_KEY_PUBLIC_CORE	2048-bit RSA Public key embedded in the USB MCU FW – used by the FW to validate the new FW signature during FW Download. It concerns the Core part of the FW.
ID_FW_DOWNLOAD_RSA_KEY_PUBLIC_KERNEL	2048-bit RSA Public key embedded in the USB MCU FW – used by the FW to validate the new FW signature during FW Download. It concerns the kernel low & high parts of the FW.

Table 18 – USB MCU FW Public Keys

CHAPTER 5: Roles, Authentication and Services

Table 19 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. CO 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 fIDPrime MD applet – see below for authentication mechanism.
ICAA	(Card Application Administrator) The IDPrime MD Card Application Administrator authenticated by the IDPrime MD applet – see below for authentication mechanism.
UA	Unauthenticated role

Table 19 - Role Description

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-SMAC 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.

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 (0 to 9) 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 1/62^4 which 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 15/62^4 which is lower than 1/10^5

IDPrime MD Card Application Administrator Authentication (ICAA)

a) The 3-Key Triple-DES key establishment provides 112 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 (0 to 9) 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 1/62^4 which 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 15/62^4 which is lower than 1/10^5

Platform Services

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

Service	Description
Card Reset (Self-test)	Power cycle the Module by removing and reinserting it into the contact reader slot, or by reader assertion of the reset signal. The *Card Reset* service will invoke the power on self-tests described in Section §9-Self-test. Moreover, on any card reset, the Module overwrites with zeros the RAM copy of, OS-RNG-STATE, SD-SENC, SD-SMAC and SD-SDEK. The Module can also write the values of all CSPs stored in EEPROM as a consequence of restoring values in the event of card tearing or a similar event. During the self-tests, the module generates the RAM copy of OS-RNG-STATE and updates the EEPROM copy of OS-RNG-STATE.
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. Uses SD-SENC and SD-SMAC.
INITIALIZE UPDATE	Initializes the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. Uses the SD-KENC, SD-KMAC and SD-KDEK master keys to generate the SD-SENC, SD-SMAC and SD-SDEK session keys, respectively.
GET DATA	Retrieve a single data object. Optionally uses SD-SENC, SD-SMAC (SCP).
MANAGE CHANNEL	Open and close supplementary logical channels. Optionally uses SD-SENC, SD-SMAC (SCP).
SELECT	Select an applet. Does not use CSPs.

Table 20 - Unauthenticated Services and CSP Usage

Service	Description	CO
DELETE	Delete an applet from EEPROM. This service is provided for the situation where an applet exists on the card, and does not impact platform CSPs. Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X
GET STATUS	Retrieve information about the card. Does not use CSPs. Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X
INSTALL	Perform Card Content management. Uses SD-SMAC, uses SD-SENC optionally (SCP03). Optionally, the Module uses the DAP-SYM key to verify the package signature.	X
LOAD	Load a load file (e.g. an applet). Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X
PUT DATA	Transfer data to an application during command processing. Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X
PUT KEY	Load Card Manager keys The Module uses the SD-KDEK key to decrypt the keys to be loaded. Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X
SET STATUS	Modify the card or applet life cycle status. Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X
STORE DATA	Transfer data to an application or the security domain (ISD) processing the command. Optionally, updates OS-GLOBALPIN. Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X
GET MEMORY SPACE	Monitor the memory space available on the card. Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X
SET ATR	Change the card ATR. Uses SD-SMAC, uses SD-SENC optionally (SCP03).	X

Table 21 – 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 Services

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

Service	Description	ICAA	IUSR	UA
EXTERNAL AUTHENTICATE	Authenticates the external terminal to the card. Sets the secure channel mode.	X	X	X
INTERNAL AUTHENTICATE	Authenticates the card to the terminal	X	X	X
SELECT	Selects a DF or an EF by its file ID, path or name (in the case of DFs).	X	X	X
CHANGE REFERENCE DATA	Changes the value of a PIN. (Note : User Auth is always done within the command itself by providing previous PIN) 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	
DELETE FILE	Deletes the current DF or EF.	X	X	
DELETE ASYMMETRIC KEY PAIR	Deletes an RSA or ECDSA Asymmetric Key Pair	X	X	
ERASE ASYMMETRIC KEY	Erases an RSA or ECC Asymmetric Key Pair	X	X	
GET DATA (IDPrime MD Applet Specific)	Retrieves the following information: • CPLC data • Applet version • Software version (includes applet version - BER-TLV format) • Available EEPROM memory • Additional applet parameters • PIN Policy Error • Applet install parameter (DF0Ah tag)	X	X	X
GET DATA OBJECT	Retrieves the following information: • Public key elements • KICC • The contents of a specified SE • Information about a specified PIN • Key generation flag • Touch Sense flag	X	X	X
PUT DATA (IDPrime MD Applet Specific)	Creates or updates a data object		X	

Service	Description	ICAA	IUSR	UA
	• Create container[1] • Update public/private keys(1)			
PUT DATA (IDPrime MD Applet Specific)	Creates or updates a data object Access Conditions • Applet Parameters (Admin Key, Card Read Only and Admin Key Try Limit) • PIN Info	X		
PUT DATA (IDPrime MD Applet Specific)	Creates or updates a data object • Update Triple-DES or AES Secret keys(1)	X	X	
READ BINARY	Reads part of a binary file.	X	X	X
ERASE BINARY	Erases part of a binary file.	X	X	
UPDATE BINARY	Updates part of a binary file.	X	X	
GENERATE AUTHENTICATE	Used to generate secure messaging session keys between both entities (IFD and ICC) as part of elliptic curve asymmetric key mutual authentication (EC DH key agreement).	X	X	X
GENERATE KEY PAIR	Generates an RSA or ECDSA key pair and stores both keys in the card. It returns the public part as its response.		X	
PSO – VERIFY CERTIFICATE	Sends the IFD certificate C_CV.IFD.AUT used in asymmetric key mutual authentication to the card for verification. No real reason to use it in the personalization phase, but it is allowed.		X	
PSO - HASH	Entirely or partially hashes data prior to a PSO–Compute Digital Signature command or prepares the data if hashed externally		X	
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	
PSO – COMPUTE DIGITAL SIGNATURE	Computes a digital signature.		X	
PUT SECURE KEY	Secure Key Injection Scheme from Microsoft Minidriver spec V7		X	

[1] Secure Messaging in Confidentiality is mandatory

Service	Description	ICAA	IUSR	UA
UNAUTHENTICATE EXT	Breaks a secure messaging session, or invalidates an MS3DES3 External Authentication.			X
CHECK RESET AND APPLET SELECTION	Tells the terminal if the card has been reset or the applet has been reselected since the previous time that the command was performed.	X	X	X
GET CHALLENGE	Generates an 8 or 16-byte random number.			X
MANAGE SECURITY ENVIRONMENT	Supports two functions, Restore and Set. • Restore: replaces the current SE by an SE stored in the card. • Set: sets or replaces one component of the current SE.			X
VERIFY	Authenticates the user to the card by presenting the User PIN. The User Authenticated status is granted with a successful PIN verification. Secure Messaging is enforced for this command.		X	

Table 22 – IDPrime MD 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: • GUID			X

Table 23 – MSPNP applet Services

All services implemented by the USB MCU FW are listed in the table below.

Service	Description	UA
USB SC	This module provides framework for the USB Standard and Class requests, CCID protocols, to allow ISO7816 communication with the SC.	X
USB MCU	This module provides framework for the USB commands, which are directed to the FW such as FW get Info, etc.	X
FW Update	This module defines an interface for firmware update process; FW is protected by an RSA 2048 PKCS#1 v1.5 SHA256 signatures. The signature verification is for the purposes of authenticating the USB FW download. No-Thales signed FWs will be rejected by the USB MCU.	X
TSB	The Touch Sense Button acts as a security measure (presence detection) in addition to the user PIN.	X

Table 24 – USB MCU FW Services

CHAPTER 6: Physical Security Policy

The eToken 5300 Mini MD 4.3.5 is a multiple-Chip standalone cryptographic module, 2 ICs are mounted on a PCB assembly with a connector and passive components, covered by epoxy on both sides, exposing only the LED, the Touch Sense Button and USB connector. The Module is intended to be covered within a plastic enclosure. Physical inspection inside the Module boundary is not practical, as the epoxy layer is opaque.

The LED functions as status indicator and this is the reason it is kept non-covered with epoxy. The LED has no connection to Critical Security Parameters, and thus cannot output any sensitive information.

The Touch Sense Button inputs button press indication to the MCU and this is the reason it is kept non-covered with epoxy.

The Touch Sense Button has no connection to Critical Security Parameters, and thus cannot output any sensitive information.

CHAPTER 7: Operational Environment

This section does not apply to SC platform. No code modifying the behavior of the SC 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.

Only authorized (Signed by Thales private keys) USB MCU FW can be loaded at post-issuance while no-Thales signed FWs will be rejected by the USB MCU.

New firmware versions (applet or USB MCU) within the scope of this validation must be validated through the CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

CHAPTER 8: 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.

CHAPTER 9: Self-test

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 will enter in an error state and the LED will blink following given sequences or the module will not answer (SC is mute).

The FW performs self-tests during power up. A failure of these operations will lead to an error state.

Test Target	Description
Firmware Integrity	32 bit CRC performed over all code located in USB MCU Flash memory.
	16 bit CRC performed over all code located in SC Flash memory (for OS, Applets and filters).
DRBG	Performs DRBG SP 800-90 KAT with fixed inputs (no derivation function and no reseeding) and health test.
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
AES	Performs decrypt KAT using an AES 128 key in ECB mode. AES encrypt is self-tested as an embedded algorithm of AES-CMAC.
KBKDF AES-CMAC	Performs a KDF AES-CMAC KAT using an AES 128 key and 32-byte derivation data. The KAT computes session keys and verifies the result. Note that KDF KAT is identical to an AES-CMAC KAT; the only difference is the size of input data.
RSA	Performs separate RSA PKCS#1 signature and verification KATs using an RSA 2048 bit key, and a RSA PKCS#1 signature KAT using the RSA CRT implementation with a 2048 bit key.
ECC CDH	Performs an ECC CDH KAT using an ECC P-224 key.(same crypto engine than for ECDSA KAT)
SHA-1	Performs a SHA-1 KAT.
SHA-256	Performs a SHA-256 KAT.
SHA-512	Performs a SHA-512 KAT.
SHA-256 (USB MCU)	Performs a SHA-256 on a constant message stored in memory. Result given by the operation is compared with the expected result. If they are the same, self-test is OK.
RSA SIGN Verification (USB MCU)	Performs a RSA PKCS#1 signature verification - 2048-bit key on a constant key (modulus & exponent) and message and the expected result stored in memory. If the signature verification is successful, self-test is OK.

Table 25 – Power-On Self-Test

Conditional Self-tests

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

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

When new firmware is loaded into the SC using the LOAD command, the SC verifies the integrity and authenticity of the new firmware (applet) using the SD-SMAC key for MAC process. Optionally, the SC may also verify a signature of the new firmware (applet) using the DAP-SYM key; the signature block in this scenario is signed by an external entity using the DAP-SYM key.

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

When a new FW is downloaded to the USB MCU, the existing MCU FW validates the integrity of the new FW by verifying the new FW signatures using 2048-bit RSA Public keys embedded in the USB MCU existing FW.

CHAPTER 10: Design Assurance

The CM meets the Level 3 Design Assurance section requirements.

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.

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.

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.

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 MD Applet is a Java applet designed for the Java Card environment.

CHAPTER 11: 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

CHAPTER 12: 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. All keys and CSPs of the module can be zeroized by various zeroization services. For example, complete Applet zeroization can be done by the CO role via the applet Delete service (required ISD key), while User Keys can be zeroized by the user or the Admin (ICAA). For more details about the eToken 5300 zeroization services customization – please contact Thales product support.
- The Module does not support manual key entry, output plaintext CSPs or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
- In accordance to NIST guidance, operators are responsible for insuring that a single Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit data blocks.