HID Global

HID Global ActivID Applet 2.7.7 & 2.7.8 on Thales IDCore 3230 Platform

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 10
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 13
2.8 RBG and Entropy 13
2.9 Key Generation 13
2.10 Key Establishment 14
2.10.1 Key Agreement 14
2.10.2 Key Transport 14
2.11 Industry Protocols 14
3 Cryptographic Module Interfaces 14
3.1 Ports and Interfaces 14
4 Roles, Services, and Authentication 15
4.1 Authentication Methods 15
4.2 Roles 16
4.3 Approved Services 16
4.4 Non-Approved Services 21
4.5 External Software/Firmware Loaded 21
5 Software/Firmware Security 22
5.1 Integrity Techniques 22
5.2 Initiate on Demand 22
6 Operational Environment 22
6.1 Operational Environment Type and Requirements 22
7 Physical Security 22
7.1 Mechanisms and Actions Required 22
7.5 EFP/EFT Information 23
7.6 Hardness Testing Temperature Ranges 23
8 Non-Invasive Security 23

9 Sensitive Security Parameters Management 23
9.1 Storage Areas 23
9.2 SSP Input-Output Methods 24
9.3 SSP Zeroization Methods 24
9.4 SSPs 25
10 Self-Tests 32
10.1 Pre-Operational Self-Tests 32
10.2 Conditional Self-Tests 32
10.3 Periodic Self-Test Information 34
10.4 Error States 34
10.5 Operator Initiation of Self-Tests 35
10.6 Additional Information 35
11 Life-Cycle Assurance 36
11.1 Installation, Initialization, and Startup Procedures 36
11.2 Administrator Guidance 36
11.3 Non-Administrator Guidance 36
11.6 End of Life 36
11.7 Additional Information 36
12 Mitigation of Other Attacks 37

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 9
Table 4: Approved Algorithms 11
Table 5: Vendor-Affirmed Algorithms 11
Table 6: Security Function Implementations 13
Table 7: Entropy Certificates 13
Table 8: Entropy Sources 13
Table 9: Ports and Interfaces 15
Table 10: Authentication Methods 16
Table 11: Roles 16
Table 12: Approved Services 21
Table 13: Mechanisms and Actions Required 22
Table 14: EFP/EFT Information 23
Table 15: Hardness Testing Temperatures 23
Table 16: Storage Areas 24
Table 17: SSP Input-Output Methods 24
Table 18: SSP Zeroization Methods 24
Table 19: SSP Table 1 28
Table 20: SSP Table 2 32
Table 21: Pre-Operational Self-Tests 32
Table 22: Conditional Self-Tests 33
Table 23: Pre-Operational Periodic Information 34
Table 24: Conditional Periodic Information 34
Table 25: Error States 35

List of Figures

Figure 1: Block Diagram 6
Figure 2 : Tags for Tracking Data (Approved Mode) 9
Figure 3 : Card Production Life Cycle Data 9
Figure 4 : Versions and Operations Indicators 10

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the **HID Global ActivID Applet 2.7.7 & 2.7.8 on the Thales IDCore 3230 Platform** Cryptographic Module. This document may freely be reproduced and distributed in its entirety. This Security Policy describes the security services provided by the module and describes how the module meets the requirements of FIPS 140-3 (Federal Information Processing Standards 140-3) for an overall Security Level 2 implementation.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	3
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

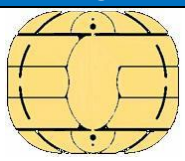
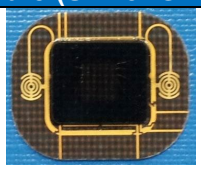
2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The *Module* is designed to be embedded into a plastic card body, USB key, secure element etc., with a contact plate connection and/or RF antenna.

The physical form of the *Module* is depicted in following pictures (to scale). The cryptographic boundary is defined as the surfaces and edges of the packages. The *Module* relies on [ISO 7816] and/or [ISO 14443] card readers as input/output devices.

WORLD Combi RLT module (SLC37GDA512) for 3230	
 Oblong punching **Top View – Combi Plate**	 **Bottom View – Black Epoxy with RLT technology**

Purpose and Use:

This document defines the Security Policy for the HID Global ActivID Applet 2.7.7 & 2.7.8 on the Thales IDCore 3230 Platform cryptographic module, herein denoted the *Module*. The *Module*, validated to FIPS 140-3 overall Level 2, is a single-chip "contact and contactless" module implementing the Global Platform operational environment, with Card Manager and the HID Global ActivID Applet.
The term *platform* herein is used to describe the chip and operational environment, not inclusive of the ActivID Applet.

The *Module* has a limited operational environment. The *Module* includes a firmware load function to support necessary updates. New firmware versions within the scope of this Security Policy and certificate must be validated through the FIPS 140-3 CMVP. Any other firmware loaded onto this module is out of the scope of this validation and requires a separate FIPS 140-3 validation.

The Module is designed to be embedded into a plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna.

Module Type: Hardware

Module Embodiment: SingleChip

Module Characteristics:

Cryptographic Boundary:

Figure 1 below depicts the Module's block diagram, with a red outline highlighting the cryptographic boundary. The cryptographic boundary encompasses all the components. included on the single chip.

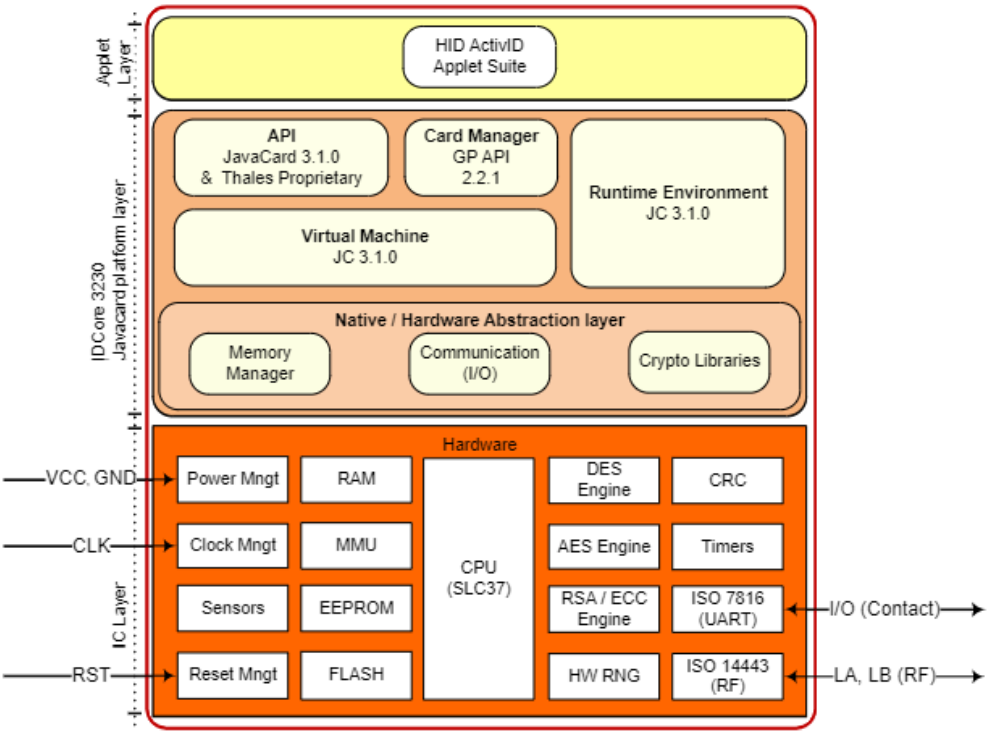


Figure 1: Block Diagram

The Cryptographic Module (CM) is fully compliant with two major cards industry standards: Oracle Java Card 3.1.0 Classic Edition and GlobalPlatform (GP) Card Specification version 2.2.1.

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

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

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

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

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

The *Virtual Machine (VM)* implements the byte code interpreter, firewall, exception management and byte code optimizer functionalities.

The *Card Manager* is the card administration entity, allowing authorized users to manage the card content, keys, and life cycle states. The Card Manager behaves similarly to an applet, but is properly represented as a constituent of the platform. In case of delegated management (DM), the Supplementary Security Domain (SSD) behaves similarly to the Card Manager in term of card content, keys and life cycle states.

The *Memory Manager* implements functions such as memory access, allocation, deletion and garbage collection.

The *Communication* handler implements the ISO 7816 and ISO 14443 communications protocols in contactless mode and dual mode.

The *Cryptography Libraries* implement the Approved services listed in Section 2.5.

The HID Global ActivID Applet 2.7.7 & 2.7.8 comprises:

- *ASC Library package* – This is the library package that implements functions required by other HID applets. The library functions are not directly accessible via the cryptographic Module command interface.
- *Access Control Applet (ACA)* – This applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. Three off-card entity authentication methods – GP secure messaging, PIN, and External Authentication are included by default in the ACA applet.
- *PKI / Generic Container (PKI/GC) Applet* – The PKI/GC Applet provides secure storage for PKI credentials, and other data that are required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based cryptographic operations using the RSA private key stored in the PKI buffers. This applet is compliant with GSC-IS 2.1.
- *PIV EP Wrapper Applet* – This Applet aligns with [SP800-73-4] (both at card-edge and data model levels). This Applet is a wrapper on top of the ActivID Applet (ASCLIB, ACA, GC/PKI). Its purpose is to access the PIV card-edge and objects although objects are physically stored in the GC/PKI applet instance. This Applet cannot operate in standalone mode and must interface with the ACA and GC/PKI applets and library to operate properly.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

The Module is designed to be embedded into a plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna.

The Module's single chip is the SLC37GDA512. It is presented on one form factor: WORLD Combi RLT module (contact and contactless)

Application Firmware:

HID Global ActivID Applet 2.7.7 is comprised of
- ASCLIB: 2.7.7.3
- ACA: 2.7.7.3
- GC/PKI: 2.7.7.3
- PIV EP Wrapper: 2.7.7.5

HID Global ActivID Applet 2.7.8 is comprised of
- ASCLIB: 2.7.8.2
- ACA: 2.7.8.7
- GC/PKI: 2.7.8.7
- PIV EP Wrapper: 2.7.8.4

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
World Combi RLT module/ PN: A2848344	SLC37GDA512 Mask number: G322	Firmware: IDCore 3230-BUILD6.9; ActivID Applet 2.7.7 or ActivID Applet 2.7.8	Infineon SLC37GDA512	Java Card 3.1.0 GlobalPlatform (GP) 2.2.1 Interface: contact with protocol communication; T=0 and T=1; Contactless with protocol communication T=CL

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

None

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	This is the module's only mode of operation	Approved	"8900" in byte 11-12 of tag 0103

Table 3: Modes List and Description

The module is acting in an approved mode of operation when the module provides the services described in the Approved Services table. These services use the security functions listed in the Approved Algorithm table in an approved manner. The security service indicator provides confirmation that an approved service has been provided.
Once the module has been delivered outside of the factory, the CM is always in Approved mode. The configuration cannot be changed outside the factory. The CM does not support a non-approved mode of operation.

To identify the CM, 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	2Dh	Get CPLC data (tag 9F 7F)
			01-03	1Dh	Get Identification data (tag 01 03)
			01-2F	10h	Get Approved mode parameters (tag 01 2F):

Figure 2 : Tags for Tracking Data (Approved Mode)

The CM production life cycle data can be checked using GET DATA command with tag '9F7F'. The Module responds with 42 bytes composed of:

IDCore 3230 – CPLC data (tag 9F7F)			
Byte	Description	Value	Value meaning
1-2	IC fabricator	**4090h**	Infineon
3-4	IC type	**0039h**	SLC37GDA512
5-6	Operating system identifier	**1291h**	Thales
7-8	Operating system release date (YDDD) – Y=Year, DDD=Day in the year	**YDDDh**	Operating System release Date
9-10	Operating system release level	**0100h**	V1.0
11-12	IC fabrication date	xxxxh	Filled in during IC manufacturing
13-16	IC serial number	xxxxxxxxh	Filled in during IC manufacturing
17-18	IC batch identifier	xxxxh	Filled in during IC manufacturing
19-20	IC module fabricator	xxxxh	Filled in during module manufacturing
21-22	IC module packaging date	xxxxh	Filled in during module manufacturing
23-24	ICC manufacturer	xxxxh	Filled in during module embedding
25-26	IC embedding date	xxxxh	Filled in during module embedding
27-28	IC pre-personalizer	xxxxh	Filled in during smartcard preperso
29-30	IC pre-personalization date	xxxxh	Filled in during smartcard preperso
31-34	IC pre-personalization equipment identifier	xxxxxxxxh	Filled in during smartcard preperso
35-36	IC personalizer	xxxxh	Filled in during smartcard personalization
37-38	IC personalization date	xxxxh	Filled in during smartcard personalization
39-42	IC personalization equipment identifier	xxxxxxxxh	Filled in during smartcard personalization

Figure 3 : Card Production Life Cycle Data

The CM identification data can be checked using GET DATA command with tag '0103'. The Module responds with 29 bytes composed of:

IDCORE 3230 – Identification data (tag 0103)			
Byte	Description	Value	Value meaning
1	Thales Family Name	B0	Javacard
2	Thales OS Name	84	IDCore family
3	Thales Mask Number	66	G322
4	Thales Product Name	69	IDCore3230
5	Thales Version	06	Major Version
6	Thales Version (Minor)	09	Minor Version
7-8	Chip Manufacturer	4090	Infineon
9-10	Chip Version	7305	SLC37GDA512
11-12	Operational Mode	8900	Approved mode
13	FIPS Level for product	02	02 = FIPS Level 2
14-15	Specific chip ID	32 30	32 30 = Contact and Contactless
16-17	HID Piv applet version	02 77	02 77 = ActivID Applet 2.7.7 02 78 = ActivID Applet 2.7.8
18-29	RFU	xx..xxh	RFU

Figure 4 : Versions and Operations Indicators

The status of the Approved mode of operation can be checked using GET DATA command with tag '012F'. The Module responds with 16 bytes composed of:

- 4 bytes for CAST status
- 2 bytes for Error log
- 4 bytes for Periodic Self-Test counter
- 4 bytes for Periodic Self-Test maximum counter value
- 1 byte for Operational Mode
- 1 byte for Flag

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2877	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A2877	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-ECB	A2877	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
Counter DRBG	A2877	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A2877	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - extra bits	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC Sp800-56Ar3	A2877	Domain Parameter Generation Methods - P-256 Function - Partial Validation Scheme - onePassDh - KAS Role - Responder KDF Methods - oneStepKdf - Key Length - 512	SP 800-56A Rev. 3
KDF SP800-108	A2877	KDF Mode - Counter Supported Lengths - Supported Lengths: 128-256 Increment 64	SP 800-108 Rev. 1
KTS-IFC	A2877	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg1-basic, rsakpg1-crt Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Key Length - 512	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A2877	Key Generation Mode - probable Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Primality Tests - 2pow100 Modulo - 2048, 3072 Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A2877	Modulo - 2048, 3072 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A2877	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA2-224	A2877	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A2877	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-384	A2877	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A2877	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

NOTE: Only the algorithms specified in the table above are supported by the module in approved mode of operation.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	SP800-133r2 Section 4, Example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Digital Signature Generation RSA	DigSig-SigGen	Signature Generation		RSA SigGen (FIPS186-5): (A2877)
Digital Signature Verification RSA	DigSig-SigVer	Signature Verification		RSA SigVer (FIPS186-5): (A2877)
Encryption - Decryption	BC-UnAuth	Block cipher unauthenticated	Strength:128, 192, 256 bits	AES-CBC: (A2877) Sizes: 128, 192, 256 bits AES-ECB: (A2877) Sizes: 128, 192, 256 bits
Generate Key Pair EC (CKG)	AsymKeyPair-KeyGen	Demonstrate ECC key generation		ECDSA KeyGen (FIPS186-5): (A2877) Counter DRBG: (A2877) CKG: () Key Type: Asymmetric
Generate Key Pair RSA (CKG)	AsymKeyPair-KeyGen	Demonstrate RSA key generation		RSA KeyGen (FIPS186-5): (A2877) Counter DRBG: (A2877) CKG: () Key Type: Asymmetric
KDF	KBKDF	Key-Based Key Derivation		AES-CMAC: (A2877) Sizes: 128,192, 256 KDF SP800-108: (A2877)
KTS	KTS-Wrap	Key Transport using AES ECB or CBC for encryption and AES-CMAC for authentication	Strength:Key transport methodology providing between 128 and 256 bits of security strength Standard:SP 800-38F IG D.G:Approved method #2	AES-CBC: (A2877) Sizes: 128,192, 256 AES-CMAC: (A2877) Sizes: 128,192, 256 AES-ECB: (A2877)
KTS-IFC	KTS-Encap	Key Transport Encapsulation	Strength:Key establishment methodology providing between 112 and 128 bits of security strength Standard:SP 800-56Br2 IG D.G:Approved method #1	KTS-IFC: (A2877) Modulus: 2048, 3072
Message Authentication	MAC	Message Authentication		AES-CMAC: (A2877) Sizes: 128,192, 256
Opacity Secure Channel (KAS)	KAS-Full	Key Agreement Scheme, SP800-56Cr2 Key Derivation, Message Authentication for key confirmation	IG:IG D.F Scenario 2, path 2 Key Derivation:SP 800-56Cr2 KDA (Tested as part of KAS	KAS-ECC Sp800-56Ar3: (A2877) AES-CMAC: (A2877) Sizes: 128 Counter DRBG: (A2877)

Name	Type	Description	Properties	Algorithms
			certificate) Key Confirmation:Yes	
Secure Hash	SHA	Compute the hash value		SHA2-224: (A2877) SHA2-256: (A2877) SHA2-384: (A2877) SHA2-512: (A2877)

Table 6: Security Function Implementations

The table lists the security functions provided by the HID Global ActivID Applet 2.7.7 & 2.7.8 on the Thales IDCore 3230 Platform Cryptographic Module.

2.7 Algorithm Specific Information

SP 800-56Ar3 Assurances:

The module is systematically checking the key in mode FULL VALIDATION at EC public key generation and key agreement, it implements assurances for SP800-56Ar3 section 5.6.2.3.3 for ECC full public key validation.

2.8 RBG and Entropy

Cert Number	Vendor Name
E107	Infineon

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
SLC37 32-bit Security Controller	Physical	N/A	32 bits	Min-entropy claimed: 13.376 bits per 32-bit blocks.	N/A

Table 8: Entropy Sources

ESV certificate (#E107) has been procured for this entropy source.

The output of the entropy source is used to directly feed the DRBG. The DRBG uses CTR_DRBG from [SP800-90Ar1] with Derivation Function (DF) enabled. 1024-bits of entropy at 13.376 bits per 32-bits min-entropy are fed to the DF which accounts for 428.032 -bits of entropy which exceed the 256-bits required by CTR_DRBG to claim full entropy output of the DRBG. A separate nonce is created for the DRBG based on output from entropy source.

2.9 Key Generation

The module uses unmodified output from its Counter DRBG to generate seeds used for asymmetric key generation.

The module supports the following CKG methodologies:

- FIPS 186-5 RSA Key generation per SP 800-133r2, sections 4 and 5.1
- FIPS 186-5 and SP 800-56Ar3 ECC Key generation per SP 800-133r2, sections 4, 5.1 and 5.2

2.10 Key Establishment

2.10.1 Key Agreement

The module implements the following approved key agreement scheme as specified in FIPS 140-3 IG D.F, Scenario 2, path 2 which has been CAVP tested and validated:

- SP 800-56Ar3 KAS-ECC with SP 800-56Cr2 OneStep KDA.

2.10.2 Key Transport

The module implements the following approved key transport methods as specified in FIPS 140-3 IG D.G, the underlying algorithms of which have been CAVP tested and validated:

- SP 800-56Br2 KTS-IFC (Approved method #1 from IG D.G)
- SP 800-38F Key Transport using AES ECB/CBC for encryption and AES-CMAC for authentication. (Approved method #2 from IG D.G)

2.11 Industry Protocols

Not Applicable

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The WORLD Combi RLT module has access to contact and contactless interfaces.

VCC, RST, CLK, GND and IO are for contact interface. as specified into ISO7816 standard.
When the contactless smart card is within the reader's electromagnetic field, the antenna receives the RF energy, which powers the IC chip via the LA and LB connections, enabling the chip to communicate with the reader in contactless. As specified into ISO14443 standard.

Physical Port	Logical Interface(s)	Data That Passes
VCC	Power	Supply Voltage
RST	Control Input	Reset Signal
CLK	Control Input	Clock Signal
GND	Power	Ground
I/O	Data Input Data Output Control Input Status Output	Commands and responses, protocol and control data

Physical Port	Logical Interface(s)	Data That Passes
LA	Data Input Data Output Control Input Status Output Power	Supply ,clock signal, commands and responses, protocol and control data
LB	Data Input Data Output Control Input Status Output Power	Supply ,clock signal, commands and responses, protocol and control data

Table 9: Ports and Interfaces

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

The operating conditions for the contact interfaces of this module are:

Conditions	Range
Voltage	1.8V, 3 V and 5.5 V DC
Frequency[1]	1MHz to 10MHz

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

The operating conditions for the contactless interfaces of this module are:

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

Both contact and contactless interfaces share the same data storage, processing, SSPs, and services.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Secure Channel Protocol authentication method	In accordance to SP 800-63B, this Authenticator type is best described as Single-Factor Cryptographic Software (Section 5.1.6). This authentication method employs AES CMAC used along with AES ECB/CBC as part of a challenge-response mechanism. This method is performed when the EXTERNAL AUTHENTICATE	KTS	The strength of Global Platform mutual authentication relies on AES key length, and the probability that a random attempt at authentication will succeed is: (1/2^128) for AES 16-byte-long keys; (1/2^192) for AES 24-byte-long keys;	The module enforces a maximum count of 15 consecutive failed authentication attempts. After 15 consecutive unsuccessful attempts, the secure channel authentication is permanently blocked

[1] Frequency of the internal clock as supplied by the CLK physical interface.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	command is invoked after successful execution of the INITIALIZE UPDATE command.		(1/2^256) for AES 32-byte-long keys	
Symmetric Cryptographic Authentication method	In accordance to SP 800-63B, this Authenticator type is best described as Single-Factor Cryptographic Software (Section 5.1.6). This authentication method decrypts (using ACA-SPAK) an encrypted challenge (128-bits) sent to the module by an external entity and compares the challenge to the expected value. This method is used to authenticate to the AA role.	Encryption - Decryption	The strength of Symmetric Cryptographic Authentication method relies on AES-CBC key length (128 bits), and the probability that a random attempt at authentication will succeed is: 1/(2^128)	The execution of this authentication mechanism is rate limited - the module can perform no more than 2^16 attempts per minute. Therefore, the probability that a random attempt will succeed over a one minute period is (2^16)/(2^128) = 1.93E - 34
Secret Value authentication method	In accordance to SP 800-63B, this Authenticator type is best described as Memorized Secrets (Section 5.1.1). This authentication method compares a value sent to the Module to the stored ACA-PIN value; if the two values are equal, the operator is authenticated.	Encryption - Decryption	The probability of false authentication of this authentication method is as follows: 1/(256^8) = 5.4E20	Based on the [SP800-73-4] defined maximum count of 15 for failed authentication attempts, the probability that a random attempt will succeed over a one minute period is: 15/(256^8) = 8.1E-19

Table 10: Authentication Methods

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage. Only one operator at a time is permitted on a channel.
Applet deselection (including Card Manager), card reset or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services.
Applet reselection (except Card Manager that close systematically the GlobalPlatform secure channel) is leaving the secure channel unchanged and it is up to the applet policy to close it or not.
The module clears previous authentications on each power cycle. It also supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Identity	Crypto Officer.	Secure Channel Protocol authentication method
AA	Identity	Application Administrator	Symmetric Cryptographic Authentication method
USR	Identity	User	Secret Value authentication method

Table 11: Roles

The module provides Identity-based authentication using either the Security Channel Protocol Authentication or the Secret Value Authentication Method above.
The Module does not support a maintenance role.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Lifecycle	Modify the card or applet life cycle status. Performs zeroization.	IND_1	Set / Get Status : life cycle state to update/ empty	Return Status Word / life cycle state and package list	None	CO - OS-DRBG-EI : Z - OS-DRBG-S : Z - OS-DRBG-V : Z - OS-DRBG-KEY : Z - OS-MKDK : Z - SD-KENC: Z - SD-KMAC: Z - SD-KDEK: Z - SD-SENC: Z - SD-SMAC: Z - DAP-SYM: Z - OPACITY-SENC : Z - OPACITY-SMAC: Z - OPACITY-SRMAC : Z - OPACITY-SCONFIRMATION: Z - ACA-PIN: Z - ACA-PUK: Z - ACA-PC: Z - SMA-OPRI: Z - PIV-RPAK: Z - PIV-RDSK: Z - PIV-RCAK: Z - PIV-RKDK: Z - PIV-RPAK-PUB: Z - PIV-RKDK-PUB: Z - SMA-OPRI-PUB: Z - ACA-SPAK: Z
Manage Content	Load, install, and delete application packages and associated keys and data	IND_1	Applications and associated data	Return Status Word	Message Authentication	CO - SD-SMAC: E - DAP-SYM: E - ACA-PIN: Z - ACA-PUK: Z - ACA-PC: Z - ACA-SPAK: Z - PIV-RPAK: Z - PIV-RDSK: Z - PIV-RCAK: Z - PIV-RKDK: Z - SMA-OPRI: Z - PIV-RPAK-PUB: Z - PIV-RDSK-PUB: Z - PIV-RCAK-PUB: Z - SMA-OPRI-PUB: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Module Info (Auth)	Read module configuration or status information (privileged data objects). Shows module versioning and status information.	IND_1	Tags and module information	Module configuration status information return Status Word	Message Authentication	CO - SD-SMAC: E
Secure Channel	Establish and use a secure communications channel	IND_1	Random, diversification data	Authentication data, return Status Word	Encryption - Decryption KDF KTS Message Authentication	CO - OS-DRBG-EI : G,E - OS-DRBG-S : G,E - OS-DRBG-V : G,E - OS-DRBG-KEY : G,E - SD-KENC: E - SD-KMAC: E - SD-KDEK: E - SD-SMAC: G,E - SD-SENC: G,E - SD-MDAP-KDEK: E - SD- MDAP - KENC: E - SD- MDAP - KMAC: E
Request for autotest	Performs self-tests. Sets a flag to see that a specific cryptographic KAT has been performed on demand via Module Reset.	IND_1	CAST bit field	return Status Word	None	Unauthenticated
Generate HID Applet RSA 2048/3072 Key pair using the secure channel.	Generate HID Applet RSA 2048/3072 Key pair using the secure channel. PIV Authentication RSA Key Pair Generation PIV Signature RSA Key Pair Generation PIV Card Authentication RSA Key Pair Generation HID Applet 2.7.7 supports 2048 RSA keypair generation. HID Applet 2.7.8 supports both 2048 and 3072 RSA Keypair generation.	IND_1	HID applet application parameters for generating RSA key pair	The response message contains the modulus corresponding to the private key generated in the card, and return Status Word	Generate Key Pair RSA (CKG) Message Authentication	CO - PIV-RPAK: G,Z - PIV-RDSK: G,Z - PIV-RCAK: G,Z - PIV-RPAK-PUB: G - PIV-RDSK-PUB: G - PIV-RCAK-PUB: G - SD-SMAC: E
PUT Key (RSA)	Put HID Applet RSA 2048/3072 Encryption Private Key using the secure channel Inject PIV Encryption RSA Private Key (put key)	IND_1	HID applet application parameters for injecting RSA Private	Return Status Word	KTS	CO - PIV-RKDK: W,Z - SD-KDEK: E - SD-SENC: E - SD-SMAC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Inject Retired Encryption Private Key 1-5 (Put key) Private Key components wrapped with SD-KDEK HID Applet 2.7.7 supports 2048 RSA Private Key Put Key. HID Applet 2.7.8 support both 2048 and 3072 RSA Private Key Put Key		Key component			
PUT Certificate	Put HID Applet RSA 2048/3072 Certificate using the secure channel Put PIV Authentication Certificate Put PIV Signature Certificate Put PIV Card Authentication Certificate Put PIV Encryption Certificate Put PIV Retired 1-5 Key Certificate HID Applet 2.7.7 supports Put RSA 2048 certificate service only. HID Applet 2.7.8 supports Put RSA 2048 and 3072 certificate service	IND_1	HID applet application parameters for putting certificate T/V data	Return Status Word	Message Authentication	CO - SD-SMAC: E - PIV-RPAK-PUB: W - PIV-RDSK-PUB: W - PIV-RCAK-PUB: W - PIV-RKDK-PUB: W
PUT AES 128 using Symmetric Cryptographic Authentication	Manage AES 128 using Symmetric Cryptographic Authentication Put AES 128 key used by ACA applet to authenticate the AA role (0-8 keys) Legacy use Key wrapped by SD-KDEK	IND_1	HID Applet application parameters	Return Status Word	KTS	CO - ACA-SPAK: W,Z - SD-KDEK: E - SD-SMAC: E
Manage Security value	Manage Security value using the secure channel PIN, PUK, Pairing Code	IND_1	HID Applet application parameters	Return Status Word	KTS	CO - ACA-PIN: W - ACA-PUK: W - ACA-PC: W - SD-SENC: E - SD-SMAC: E
OPACITY ECC Key Pair generation	OPACITY ECC Key Pair generation	IND_1	HID Applet Application parameters	Return Status Word	Generate Key Pair EC (CKG) Message Authentication	CO - SMA-OPRI: G - SD-SMAC: E - SMA-OPRI-PUB: G
Manage HID Applet Configuration	Register/Unregister applet instance, set its associated identifier, and related	IND_1	HID Applet Application Parameters	HID Applet application response and status word	KDF Message Authentication	CO - SD-SMAC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	ACR configuration in ACA, and Instance properties					
Read HID Applet info	Retrieve applet instance properties, public ACR and associated properties, secure messaging certificate (CVC). ACR configuration defined which role is allowed to perform the service.	IND_1	HID Applet Application Parameters	HID Applet application response and status word	None	AA USR Unauthenticated
PIV Authentication	Authentication of the PIV application by an external system, Required PIN verification	IND_1	Data to sign.	Signature, return Status Word	Digital Signature Verification RSA	USR - PIV-RPAK: E
PIV Card Authentication	Authentication by an external system	IND_1	Data to sign	Signature, return Status Word	Digital Signature Verification RSA	Unauthenticated - PIV-RCAK: E
PIV Digital Signature	Sign an externally generated Hash, Required PIN verification	IND_1	Data to sign	Signature, return status	Digital Signature Generation RSA	USR - PIV-RDSK: E
PIV System Key service	Unwrap a key provided by the host. The key is not established into or used by the module, Required PIN verification	IND_1	Wrapped data to unwrap	Unwrapped data, return status	KTS-IFC	USR - PIV-RKDK: E
PIV Read Data	Read PIV Data objects	IND_1	Specified in NIST.SP.800-73-4	PIV Data. Specified in NIST.SP.800-73-4	None	USR
Verify	Verify the PIN, Pairing Code, and PUK	IND_1	PIN, Pairing Code or PUK	Return Status Word	Encryption - Decryption	Unauthenticated - OS-MKDK : E - ACA-PIN: E - ACA-PUK: E - ACA-PC: E
OPACITY Secure Message	Establish OPACITY-ZKM secure messaging	IND_1	Data	Control byte + nonce + cryptogram + cert return Status Word	Opacity Secure Channel (KAS) Secure Hash	Unauthenticated - OS-DRBG-EI : G,E - OS-DRBG-S : G,E - OS-DRBG-V : G,E - OS-DRBG-KEY : G,E - OPACITY-SENC : G,E - OPACITY-SMAC: G,E - OPACITY-SRMAC : G,E - OPACITY-SCONFIRMATION:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E,Z - SMA-OPRI: E - SMA-OPRI-PUB: R - OPACITY-Z: G,E,Z - ROE-PUB: E
Read Certificates	Read Certificate from a user card, that is configured as read always in ACA ACR configuration as SP-800-73-4	IND_1	Input Data defined in SP-800-73-4	Certificate, data format defined in SP-800-73-4	None	Unauthenticated - PIV-RPAK-PUB: R - PIV-RDSK-PUB: R - PIV-RCAK-PUB: R - PIV-RKDK-PUB: R
Symmetric Cryptographic Authentication	Use of AES for encryption	IND_1	HID Application Parameter	Encrypted Data + Status Word	Encryption - Decryption	AA - ACA-SPAK: E

Table 12: Approved Services

In the ‘Roles SSP Access’ column:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroize: The module zeroizes the SSP

In the ‘Indicator Column’:

IND_1: The status conditions for successfully completed execution is 90 00

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module has a limited operational environment.

In the Approved mode of operation, the Cryptographic Officer (Crypto Officer) has access to the firmware load service. Only applets that are validated under FIPS 140-3 shall be loaded and installed. The firmware loading service relies on the DAP Verification specified in Global Platform Specification v2.3, whereby the DAP Verification (DAP-SYM) key uses AES-CMAC (Cert. #A2877) as the approved data authentication technique. The firmware load test verifies the validity of the firmware package to be loaded.

5 Software/Firmware Security

5.1 Integrity Techniques

The CM's firmware integrity is checked on startup and when periodic self-test period is over.

Periodic Self-Tests (PST) are performed and run the firmware integrity tests.

The integrity technique is based on EDC (CRC-16), which is approved for a hardware module. The firmware image size covered by the integrity technique is roughly 200 KB.

Failure of firmware integrity self-tests during Periodic Self-Tests (PST) will trigger a module halt. Recovery from this state will require the module to be restarted and for the detected fault to have cleared. Otherwise the module will re-halt during POST following restart. The module's FIPS error log is updated regarding the encountered issue and the card goes into an error state.

5.2 Initiate on Demand

The integrity test can be triggered on demand by setting the specific flag with the proprietary command "Request for autotest".

Restarting the module will cause the integrity check to be rerun.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The module includes a limited Operating Environment.
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.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Single-Chip Packaging	On receipt of module following transport. Before each module use.	In the event of any observed damage, photograph the card and contact Thales to confirm whether observed anomalies are to be expected or are confirmed signs of potential tampering

Table 13: Mechanisms and Actions Required

The module is a hardware module claiming level 3 **physical security** and of embodiment single-chip.
The module 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 *Module* is designed to be mounted in a plastic smartcard or similar package; physical inspection of the epoxy side of the Module is not practical after mounting.

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-45°C	EFP	shutdown
HighTemperature	+130°C	EFP	shutdown
LowVoltage	1.6 V	EFP	shutdown
HighVoltage	5.5 V	EFP	shutdown

Table 14: EFP/EFT Information

The module's hardware is designed to sense and respond to out-of-range temperature conditions as well as out-of-range voltage conditions. The temperature and voltage conditions are only monitored in the powered-on state.

The module supports an EFP mechanism that will trigger module shutdown if low or high temperature extremes and out-of-range voltage conditions are detected whilst the module is active.

In the event that the module senses an out-of-range temperature or over voltage the module will reset itself, clearing all working memory.

The module can be reset and placed back into operation when in-bound operating conditions have been restored.

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-25°C
HighTemperature	85°C

Table 15: Hardness Testing Temperatures

8 Non-Invasive Security

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Random Access Memory	Dynamic
FLASH	Electronic non-volatile memory storage	Static

Table 16: Storage Areas

All SSPs used by the CM are described in this section. All usages of these SSPs by the CM are described in the services. In addition, all keys stored in RAM are zeroized upon power-cycle of the CM.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
PutKey or Writing with Secure Channel (contact)	Entered	FLASH	Encrypted	Manual	Electronic	KTS
PutKey or Writing with Secure Channel (contactless)	Entered	FLASH	Encrypted	Wireless	Electronic	KTS
PUT Key (RSA) (contact)	Entered	FLASH	Encrypted	Manual	Electronic	KTS
PUT Key (RSA) (contactless)	Entered	FLASH	Encrypted	Wireless	Electronic	KTS
PUT Certificate (contact)	Entered	FLASH	Encrypted	Manual	Electronic	Message Authentication
PUT Certificate (contactless)	Entered	FLASH	Encrypted	Wireless	Electronic	Message Authentication
PUT AES 128 (contact)	Entered	FLASH	Encrypted	Manual	Electronic	KTS
PUT AES 128 (contactless)	Entered	FLASH	Encrypted	Wireless	Electronic	KTS
Manage Security value (contact)	Entered	FLASH	Encrypted	Manual	Electronic	KTS
Manage Security value(contactless)	Entered	FLASH	Encrypted	Wireless	Electronic	KTS
OPACITY Secure Message input (contact)	Entered	RAM	Plaintext	Manual	Electronic	Opacity Secure Channel (KAS)
OPACITY Secure Message input (contactless)	Entered	RAM	Plaintext	Wireless	Electronic	Opacity Secure Channel (KAS)
OPACITY Secure Message output (contact)	FLASH	Output	Plaintext	Manual	Electronic	Opacity Secure Channel (KAS)
OPACITY Secure Message output (contactless)	FLASH	Output	Plaintext	Wireless	Electronic	Opacity Secure Channel (KAS)
Read Certificates (contact)	FLASH	Output	Plaintext	Manual	Electronic	
Read Certificates (contactless)	FLASH	Output	Plaintext	Wireless	Electronic	

Table 17: SSP Input-Output Methods

‘PutKey or Writing with Secure channel’ keys are encrypted by SD-KDEK; key identifier entity association during manufacturing. This command is only used only during manufacturing.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Module entering TERMINATED state	Using the Manage Content / Lifecycle service of the CO, the CM is able to enter the TERMINATED state, through the Set Status command, destroying the SSPs by overwriting with zero values.	Overwrite with zero values	yes
Power-cycling the module	Using the Module Reset service, the CM is able to destroy the SSPs by overwriting with zero values (in RAM memory).	Overwrite with zero values	Yes
Closing SCP secure channel	Using the Secure Channel service of the CO, the CM is able to destroy the SSPs of this service, at the closing of SCP secure channel by overwriting with zero values	Overwrite with zero values	Yes
Uninstallation of applet	Using the Manage Content / Delete service of the CO, the CM is able to destroy the SSPs of applet, through the Delete command (uninstall method).	Overwrite with zero values	Yes
Zeroize after use	Zeroize immediately after use	Overwrite with zero values	No

Table 18: SSP Zeroization Methods

All SSPs stored in RAM are zeroized upon power-cycle of the CM.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
OS-DRBG-EI	Entropy Input 1024-bit random drawn by an external entropy source populated during CM initialization and used as entropy input for the [SP 800-90Ar1] DRBG implementation	1024 bit - 256 bits	Entropy Input - CSP	Entropy Source (E107)		Generate Key Pair EC (CKG) Generate Key Pair RSA (CKG)
OS-DRBG-S	Seed 48 bytes seed output from AES_DF used for instantiation of the [SP800-90Ar1] DRBG implementation	768 bits - 256 bits	Seed - CSP	Entropy Source (E107)		Generate Key Pair EC (CKG) Generate Key Pair RSA (CKG)
OS-DRBG-V	DRBG "V" value 16-byte AES state V used in the [SP 800-90Ar1] CTR DRBG implementation	128 bits - 128 bits	DRBG "V" Value - CSP	Counter DRBG (A2877)		Generate Key Pair EC (CKG) Generate Key Pair RSA (CKG)
OS-DRBG-KEY	DRBG "Key" value 32-byte AES key used in the [SP 800-90Ar1] CTR DRBG implementation	256 bits - 256 bits	DRBG "Key" value - CSP	Counter DRBG (A2877)		Generate Key Pair EC (CKG) Generate Key Pair RSA (CKG)
OS-MKDK	Encryption key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Encryption Symmetric Key - CSP			Encryption - Decryption
SD-KENC	Decryption Key AES-128/192/256 master key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Decryption Symmetric Key - CSP			KDF
SD-KMAC	Signature verification Key AES-128/192/256 master key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Message Authentication; Symmetric Key - CSP			KDF
SD-KDEK	Encryption decryption AES-128/192/256 key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Encryption / Decryption Symmetric Key - CSP			Encryption - Decryption KDF
SD-SENC	Session decryption key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Decryption Symmetric Key - CSP	KDF		Encryption - Decryption
SD-SMAC	Session Signature verification Key	128, 192, 256 bits -	Message Authentication	KDF		Message Authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128 bits, 192 bits, 256 bits	Symmetric Key - CSP			
SD-MDAP-KDEK	Encryption decryption AES-128/192/256 key for SD with MDAP	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Encryption / Decryption Symmetric Key - CSP			Encryption - Decryption
SD- MDAP -KENC	Decryption Key AES-128/192/256 key for SD with MDAP	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Decryption Symmetric Key - CSP			Encryption - Decryption
SD- MDAP -KMAC	Signature verification Key AES-128/192/256 key for SD with MDAP	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Message Authentication Symmetric Key - CSP			Message Authentication
DAP-SYM	DAP verification key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Signature verification Symmetric Key - CSP			Message Authentication
OPACITY-SENC	Card OPACITY Secure Messaging Session Encryption Key	128, 256 bits - 128 bits, 256 bits	Encryption Symmetric Key - CSP		Opacity Secure Channel (KAS)	Encryption - Decryption
OPACITY-SMAC	Card OPACITY Secure Messaging Session MAC Key	128, 256 bits - 128 bits, 256 bits	Message Authentication Symmetric Key - CSP		Opacity Secure Channel (KAS)	Message Authentication
OPACITY-SRMAC	Card OPACITY Secure Messaging Session Response MAC Key	128, 256 bits - 128 bits, 256 bits	Signature generation Symmetric Key - CSP		Opacity Secure Channel (KAS)	Message Authentication
OPACITY-SCONFIRMATION	Card OPACITY Secure Messaging Session Confirmation Key	128, 256 bits - 128 bits, 256 bits	Signature generation confirmation Symmetric Key - CSP		Opacity Secure Channel (KAS)	Opacity Secure Channel (KAS)
OPACITY-Z	Shared secret generated during opacity secure channel establishment	256 bits - 256 bits	Shared secret - CSP		Opacity Secure Channel (KAS)	Opacity Secure Channel (KAS)
ACA-PIN	Enter by User. Use for USR Verification	64 bits - 64 bits	Personal Identification Number - CSP			
ACA-PUK	Use for USR PIN unlock	64 bits - 64 bits	PIN Unblocking Key - CSP			
ACA-PC	PIV VCI Pairing Code Verification PIN	64 bits - 64 bits	Pairing Code - CSP			
SMA-OPRI	Card OPACITY Secure Channel ECC Keypair	P-256 - 256 bits	Key Agreement Asymmetric Key - CSP	Generate Key Pair EC (CKG)		Opacity Secure Channel (KAS)
PIV-RPAK	PIV-RPAK is Private Key performs Digital Signature PIV-RPAK: PIV Authentication	Applet 2.7.8: 2048 bits , 3072 bits; Applet	Signature generation Asymmetric Key - CSP	Generate Key Pair RSA (CKG)		Digital Signature Verification RSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	(9A) RSA authentication Key	2.7.7: 2048 bits - 112 bits, 128 bits				
PIV-RDSK	Private Key performs Digital Signature PIV-RDSK: PIV Card Authentication (9C) RSA Authentication Key	Applet 2.7.8: 2048 bits , 3072 bits; Applet 2.7.7: 2048 bits - 112 bits, 128 bits	Signature generation Asymmetric Key - CSP	Generate Key Pair RSA (CKG)		Digital Signature Generation RSA
PIV-RCAK	Private Key performs Digital Signature, PIV-RCAK: PIV Card Authentication (9E) RSA Authentication Key	Applet 2.7.8: 2048 bits , 3072 bits; Applet 2.7.7: 2048 bits - 112 bits, 128 bits	Signature generation Asymmetric Key - CSP	Generate Key Pair RSA (CKG)		Digital Signature Verification RSA
PIV-RKDK	PIV-RKDK: PIV Key Management (9D) RSA private decryption key and up to 5 copies of this key may be stored in retired key locations "82" thought "86"	Applet 2.7.8: 2048 bits , 3072 bits; Applet 2.7.7: 2048 bits - 112 bits, 128 bits	Decryption - CSP			KTS-IFC
PIV-RPAK-PUB	PIV Digital Authentication (9A)'s RSA Public Key with certificate (No Private Key). The module stores the certificate, but does not perform Security Function with this certificate.	Applet 2.7.8: 2048 bits , 3072 bits; Applet 2.7.7: 2048 bits - 112 bits, 128 bits	Public - PSP	Generate Key Pair RSA (CKG)		KTS-IFC
PIV-RDSK-PUB	PIV Card Signature (9C)'s RSA Public Key with certificate (No Private Key). The module stores the certificate, but does not perform Security Function with this certificate.	Applet 2.7.8: 2048 bits , 3072 bits; Applet 2.7.7: 2048 bits - 112 bits, 128 bits	Public - PSP	Generate Key Pair RSA (CKG)		
PIV-RCAK-PUB	PIV Key Card Authentication (9E)'s RSA Public Key with certificate. The module stores the public certificate.	Applet 2.7.8: 2048 bits , 3072 bits; Applet 2.7.7: 2048 bits - 112 bits, 128 bits	Public - PSP	Generate Key Pair RSA (CKG)		
PIV-RKDK-PUB	PIV Key management (9D)'s RSA Public Key with certificate. The	Applet 2.7.8: 2048 bits , 3072 bits; Applet 2.7.7: 2048	Public - PSP	Generate Key Pair RSA (CKG)		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	module stores public the certificate	bits - 112 bits, 128 bits				
SMA-OPRI-PUB	Hash of the certificate is one of parameters to generate session keys of OPACITY secure channel.	2048 bits - P-256	Public - PSP	Generate Key Pair EC (CKG)		Opacity Secure Channel (KAS)
ACA-SPAK	AES, Use for AA authentication	128 bits - 128 bits	Encryption Symmetric Key - CSP			Encryption - Decryption
ROE-PUB	Reader ephemeral public key used for opacity	P-256 - 2048 bits	Public - PSP			Opacity Secure Channel (KAS)

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
OS-DRBG-EI		RAM:Plaintext	Duration of the module session	Module entering TERMINATED state	OS-DRBG-V :Derives OS-DRBG-KEY :Derives
OS-DRBG-S		RAM:Plaintext	Duration of the module session	Module entering TERMINATED state Power-cycling the module	OS-DRBG-V :Derives OS-DRBG-KEY :Derives
OS-DRBG-V		RAM:Plaintext	Duration of the module session	Module entering TERMINATED state Power-cycling the module	OS-DRBG-EI :Derived From OS-DRBG-S :Derived From
OS-DRBG-KEY		RAM:Plaintext	Duration of the module session	Module entering TERMINATED state	OS-DRBG-EI :Derived From OS-DRBG-S :Derived From
OS-MKDK	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure Channel (contactless)	FLASH:Plaintext		Module entering TERMINATED state	ACA-PIN:Encrypts
SD-KENC	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure Channel (contactless)	FLASH:Plaintext		Module entering TERMINATED state	SD-SENC:Derives SD-KDEK:Wrapped by
SD-KMAC	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure	FLASH:Plaintext		Module entering TERMINATED state	SD-KDEK:Wrapped by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Channel (contactless)				
SD-KDEK	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure Channel (contactless)	FLASH:Plaintext		Module entering TERMINATED state	SD-KENC:Encrypts SD-KMAC:Encrypts SD-KDEK:Encrypts ACA-PIN:Encrypts ACA-PUK:Encrypts ACA-PC:Encrypts SMA-OPRI:Encrypts PIV-RPAK:Encrypts PIV-RDSK:Encrypts PIV-RCAK:Encrypts PIV-RKDK:Encrypts PIV-RPAK-PUB:Encrypts PIV-RDSK-PUB:Encrypts PIV-RCAK-PUB:Encrypts PIV-RKDK-PUB:Encrypts SMA-OPRI-PUB:Encrypts ACA-SPAK:Encrypts
SD-SENC		RAM:Plaintext	Duration of the SCP secure channel	Power-cycling the module Closing SCP secure channel	SD-KENC:Derived From
SD-SMAC		RAM:Plaintext	Duration of the SCP secure channel	Power-cycling the module Closing SCP secure channel	SD-KMAC:Derived From
SD-MDAP-KDEK	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure Channel (contactless)	FLASH:Plaintext		Module entering TERMINATED state	SD-MDAP-KDEK:Encrypts SD- MDAP -KENC:Encrypts SD- MDAP -KMAC:Encrypts DAP-SYM:Encrypts
SD- MDAP -KENC	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure Channel (contactless)	FLASH:Plaintext		Module entering TERMINATED state	SD-MDAP-KDEK:Wrapped by
SD- MDAP -KMAC	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure Channel (contactless)	FLASH:Plaintext		Module entering TERMINATED state	SD-MDAP-KDEK:Wrapped by
DAP-SYM	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure Channel (contactless)	FLASH:Plaintext		Module entering TERMINATED state	SD-MDAP-KDEK:Wrapped by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
OPACITY-SENC		RAM:Plaintext	Duration of the SCP secure channel	Power-cycling the module Closing SCP secure channel	OPACITY-Z:Derived From
OPACITY-SMAC		RAM:Plaintext	Duration of the SCP secure channel	Power-cycling the module Closing SCP secure channel	OPACITY-Z:Derived From
OPACITY-SRMAC		RAM:Plaintext	Duration of the SCP secure channel	Power-cycling the module Closing SCP secure channel	OPACITY-Z:Derived From
OPACITY-SCONFIRMATION		RAM:Plaintext	Duration of the SCP secure channel establishment	Power-cycling the module Closing SCP secure channel	OPACITY-Z:Derived From
OPACITY-Z		RAM:Plaintext	Duration of the SCP secure channel establishment	Zeroize after use	SMA-OPRI:Derived From OPACITY-SENC :Derives OPACITY-SMAC:Derives OPACITY-SRMAC :Derives OPACITY-SCONFIRMATION:Derives
ACA-PIN	Manage Security value (contact) Manage Security value(contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	OS-MKDK :Wrapped by
ACA-PUK	Manage Security value (contact) Manage Security value(contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	
ACA-PC	Manage Security value (contact) Manage Security value(contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	
SMA-OPRI	PutKey or Writing with Secure Channel (contact) PutKey or Writing with Secure Channel (contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	SMA-OPRI-PUB:Paired With OPACITY-Z:Derives
PIV-RPAK		FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-RPAK-PUB:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
PIV-RDSK		FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-RDSK-PUB:Paired With
PIV-RCAK		FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-RCAK:Paired With
PIV-RKDK	PUT Key (RSA) (contact) PUT Key (RSA) (contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-RKDK-PUB:Paired With
PIV-RPAK-PUB	PUT Certificate (contact) PUT Certificate (contactless) Read Certificates (contact) Read Certificates (contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-RPAK:Paired With
PIV-RDSK-PUB	PUT Certificate (contact) PUT Certificate (contactless) Read Certificates (contact) Read Certificates (contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-RDSK:Paired With
PIV-RCAK-PUB	PUT Certificate (contact) PUT Certificate (contactless) Read Certificates (contact) Read Certificates (contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-RCAK:Paired With
PIV-RKDK-PUB	PUT Certificate (contact) PUT Certificate (contactless) Read Certificates (contact) Read Certificates (contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-RKDK:Paired With
SMA-OPRI-PUB	OPACITY Secure Message output (contact) OPACITY Secure Message output (contactless)	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	SMA-OPRI:Paired With
ACA-SPAK	PUT AES 128 (contact)	FLASH:Plaintext		Module entering TERMINATED	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	PUT AES 128 (contactless)			state Uninstallation of applet	
ROE-PUB	OPACITY Secure Message input (contact) OPACITY Secure Message input (contactless)	RAM:Plaintext	Duration of the SCP secure channel establishment	Zeroize after use	OPACITY-Z:Derives

Table 20: SSP Table 2

The following table lists Sensitive Security Parameters (SSP) used to perform approved security function supported by the cryptographic module.

The following notes should be observed when reading the table:

- 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
- The “PRI” suffix indicates that this is a private key
- The “PUB” suffix indicates that this is a public key
- The “SYM” suffix indicates that this is a symmetric key
- The “ASYM” suffix indicates that this is an asymmetric key
- The “ACA” prefix is used for the HID ACA Applet keys.
- The “SMA” prefix is used for HID PIV Applet OPACITY keys

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Integrity test	EDC (16-bit CRC)	KAT	SW/FW Integrity	Bit32 of flag set to 1	Comparison with known value

Table 21: Pre-Operational Self-Tests

On power-on or reset, the *Module* performs integrity testing using an EDC (16-bit CRC) performed over all code located in FLASH and EEPROM memory (for OS and Applets).

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A2877)	decrypt KAT using an AES 128-bit key in ECB mode.	KAT	CAST	Bit 18 of flag set to 1	decrypt	COND_1
KDF SP800-108 (A2877)	generates AES-CMAC message performs a KDF AES-CMAC KAT using an AES 128-byte key and 32-byte derivation data	KAT	CAST	Bit 18 of flag set to 1	encrypt sign	COND_1

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-5) (A2877)	Performs an RSA PKCS#1 v1.5 signature generation using an RSA 2048-bit private STD key implementation	KAT	CAST	Bit 27 of flag set to 1	Sign	COND_1
RSA SigVer (FIPS186-5) (A2877)	Performs an RSA PKCS#1 v1.5 signature verification using an RSA 2048-bit public STD key	KAT	CAST	Bit 26 of flag set to 1	Verify	COND_1
KAS-ECC Sp800-56Ar3 (A2877)	Performs a Key Agreement Scheme Standalone Shared Secret ECC using an ECC P-224 key	KAT	CAST	Bit 29 of flag set to 1	Key Agreement	COND_1
SHA2-256 (A2877)	SHA2-256: hashes a 24-bytes message	KAT	CAST	Bit 21 of flag set to 1	Hashing	COND_1
SHA2-512 (A2877)	SHA2-512: hashes a 24-bytes message	KAT	CAST	Bit 21 of flag set to 1	Hashing	COND_1
Counter DRBG (A2877)	Gets a random value with specific nonce (48 bytes) and entropy (128 bytes) SP 800-90AR1 Tests 11.3 (11.3.1-11.3.3)	KAT	CAST	Bit 3 of flag set to 1	DRBG	COND_1
ECDSA KeyGen (FIPS186-5) (A2877)	Sign a fixed pattern and verify with the public key in order to validate the key pair	PCT	PCT	IND 3	Sign, Verify	COND_2
RSA KeyGen (FIPS186-5) (A2877)	Performs signature generation and verification using the key pair	PCT	PCT	IND 3	Encrypt , Decrypt	COND_2
SP 800-90B RCT	Entropy error event	Fault-Detection test	CAST	IND 2	TRNG Error	COND_1
SP 800-90B APT	Statistic error event	Fault-Detection test	CAST	IND 2	TRNG Error	COND_1
Firmware Load	MAC verification with AES CMAC (128-256 bit key)	Signature	SW/FW Load	IND_4	MAC verification with AES CMAC	COND_3

Table 22: Conditional Self-Tests

KDF SP800-108 KAT covers: KDF SP800-108 and AES-CMAC

The module maintains a flag in RAM memory that stores the state (self-test passed or not) for each Cryptographic algorithm that is approved. This flag indicates if an algorithm has been already self-tested.
The Module performs self-test of an algorithm prior the first operational use (corresponding flag is not set) and if the self-test succeeds, the corresponding flag is set otherwise the card logs the self-test error and entered into a Card Is Mute error state or Card is Killed error state, depending on number of failures.
On each reset, all flags for cryptographic algorithm self-tests are cleared.
In the ‘Indicator Column’:

IND_2: In case of error detection, the module enters into specific error states such as "Card Is Mute" or "Card is Killed."

IND_3: If the test fails, the error is logged in error log of “Approved mode parameters”

IND_4: An unsuccessful execution returns the status word: Security Conditions not satisfied

In the ‘Condition Column’:

COND_1: The self-test is executed before the first operational use of the algorithm if the indicator is not set

COND_2: The test is executed at each Key pair generation requested by the module

COND_3: The test is executed on each APDU Command

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Integrity test	KAT	SW/FW Integrity	Periodic counter value	Count of APDU received by the CM

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A2877)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
KDF SP800-108 (A2877)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
RSA SigGen (FIPS186-5) (A2877)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
RSA SigVer (FIPS186-5) (A2877)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
KAS-ECC Sp800-56Ar3 (A2877)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
SHA2-256 (A2877)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
SHA2-512 (A2877)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
Counter DRBG (A2877)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
ECDSA KeyGen (FIPS186-5) (A2877)	PCT	PCT	N/A	N/A
RSA KeyGen (FIPS186-5) (A2877)	PCT	PCT	N/A	N/A
SP 800-90B RCT	Fault-Detection test	CAST	N/A	N/A
SP 800-90B APT	Fault-Detection test	CAST	N/A	N/A
Firmware Load	Signature	SW/FW Load	N/A	N/A

Table 24: Conditional Periodic Information

RSA KeyGen , ECDSA KeyGen , SP 800-90B RCT, SP 800-90Ar1 APT, and Firmware Load tests are not strictly periodic but are triggered whenever the module calls on the services they depend on.

The Module supports an internal counter and an associated maximum value. The counter is set to its maximum value on power on and it is decremented when receiving an APDU.
When the counter reaches zero, the integrity test is executed (see 10.1), the counter is reset to its maximum value, and the flag for on-demand tests is reset so that at the next individual cryptographic algorithm usage, the CAST for that algorithm are executed again (see 10.2.1). No interruption to the module's operation is expected while the CASTs are executed. The periodic counter is stored in RAM and defined during the init flow.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Card is Mute	The module Resource Manager has shut down	Fault Detected	Reset card	Error log is stored
Card is killed	The module Resource Manager has shut down. It no longer responds to the command, service	Fault Detected	N/A	No answer from module

Table 25: Error States

10.5 Operator Initiation of Self-Tests

The cryptographic KATs are executed automatically, in a mode named “on demand”, when a cryptographic service is requested.
Self-tests can be run by any operator using the “autotests management” APDU command, corresponding to the “Request for autotest” service. The operator can choose from the list of self-test executions by providing the appropriate self-test flag.

10.6 Additional Information

The module performs continuous health tests of the entropy using the repetition count test and the adaptative Proportion test.

The cryptographic module performs a pair-wise consistency test for every generated public and private key pair. If this test fails, the error is logged into the error log.

The module performs a validity check of the public static key and the ephemeral keys according to the SP 800-56Ar3 specification. If this test fails, the error is logged into the error log.

The module performs hardware fault detection tests (APT and RCT tests). If a fault is detected, the module will handle the error by entering entered into a “Card Is Mute” error state or “Card is Killed” error state.

In case of failure, the module will handle the error by entering entered into a “Card Is Mute” error state or “Card is Killed” error state, depending on number of failures. If 8 consecutive failures occur, the module irreversibly enters the “Card is Killed” state.
In case of “Card Is Mute”, the crypto module provides an error log an error log that is accessible by an authorized operator of the module.

Following are the details on specific ADPU return codes returned upon specific self-test failures:

- AT_LOG_INTEGRITY_ERROR **[0xA1]** - This error code is used when memory integrity fails
- AT_LOG_CAST_SHA2_256 **[0xA3]** - This error code is used when SHA2 256 bits CAST result is not matching with expecting pattern
- AT_LOG_CAST_SHA2_512 **[0xA4]** - This error code is used when SHA2 512 bits CAST result is not matching with expecting pattern
- AT_LOG_CAST_DRBG (Counter DRBG) **[0xA9]** - This error code is used when DRBG CAST result is not matching with expecting pattern
- AT_LOG_CAST_AES **[0xAA]** - This error code is used when AES CAST result is not matching with expecting pattern

- AT_LOG_CAST_KDF_SP800_56CREV2 (KDA OneStep SP800-56Cr2) **[0xAC]** - This error code is used when KDF (based on SP800-56CRev2) CAST result is not matching with expecting pattern
- AT_LOG_CAST_RSA_CRT (RSA SigGen (FIPS186-5) CRT) **[0xAF]** - This error code is used when RSA CRT CAST result is not matching with expecting pattern
- AT_LOG_CAST_RSA_STD (RSA SigVer (FIPS186-5) STD) **[0xB0]** - This error code is used when RSA STD CAST result is not matching with expecting pattern
- AT_LOG_CAST_RSA_PUB (RSA primitive encryption, KTS_IFC) **[0xB1]** - This error code is used when RSA Pub CAST result is not matching with expecting pattern
- AT_LOG_CAST_RSA_CONSISTENCY (conditional test perform after RSA KeyGen (FIPS186-5)) **[0xB2]** - This error code is used when RSA consistency check fails
- AT_LOG_CAST_ECC_CONSISTENCY (conditional test perform after Generate Key Pair EC) **[0xB3]** - This error code is used when ECC consistency check fails
- AT_LOG_CAST_CS2 (KAS-ECC OnePassDH algorithm relying on Crypto Suite 2) **[0xB5]** - CAST ONE PASS DH CS2 Error

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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. Once the module has been delivered outside of the factory, the CM is always in Approved mode. The configuration cannot be changed outside the factory.

Product documentation, technical notes are available on The Customer Support Portal https://supportportal.thalesgroup.com.

11.2 Administrator Guidance

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

11.3 Non-Administrator Guidance

Please refer to section 11.2.

11.6 End of Life

When the module has reached end of life and is no longer deployed or intended for further use, it shall be placed in the TERMINATED state by the Crypto Officer. Following this, the module shall be taken to a suitable electronics recycling facility that assures physical destruction of electronic waste.

11.7 Additional Information

The *Module* implementation also enforces the following security rules:
- No additional interface or service is implemented by the *Module* which would provide access to SSPs.
- Data output is inhibited during key generation, self-tests, zeroisation, and error states.
- The zeroisation service is applied with no restrictions on all keys or SSPs of the CM.

- The *Module* does not support manual key entry, output plaintext SSPs or output intermediate key values.
- Status information does not contain SSPs or sensitive data that if misused could lead to a compromise of the Module.

In addition, the guidance below must be followed to operate the Module in accordance with the conditions of the FIPS 140-3 validation.
The PIV applet always checks all 8 bytes and does not restrict character space in PIN values. However, an external system may impose rules which restrict character space or include padding schemes. PIV Applet administrators are required to procedurally enforce usage policy that ensures end user's PIV PIN values meet the conditions as described in [SP800-73-4].

12 Mitigation of Other Attacks