

Thales

IDPrime PIV 4.0 FIDO on IDCore3230 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	9
2.3 Excluded Components	10
2.4 Modes of Operation	10
2.5 Algorithms	12
2.6 Security Function Implementations	16
2.7 Algorithm Specific Information	20
2.8 RBG and Entropy	20
2.9 Key Generation	20
2.10 Key Establishment	21
2.10.1 Key Agreement	21
2.10.2 Key Transport	22
2.11 Industry Protocols	22
3 Cryptographic Module Interfaces	22
3.1 Ports and Interfaces	22
4 Roles, Services, and Authentication	24
4.1 Authentication Methods	24
4.2 Roles	27
4.3 Approved Services	27
4.4 Non-Approved Services	63
4.5 External Software/Firmware Loaded	64
5 Software/Firmware Security	64
5.1 Integrity Techniques	64
5.2 Initiate on Demand	64
6 Operational Environment	64
6.1 Operational Environment Type and Requirements	64
7 Physical Security	65
7.1 Mechanisms and Actions Required	65
7.2 EFP/EFT Information	65
7.3 Hardness Testing Temperature Ranges	66

8 Non-Invasive Security	66
9 Sensitive Security Parameters Management.....	66
9.1 Storage Areas	66
9.2 SSP Input-Output Methods	66
9.3 SSP Zeroization Methods	67
9.4 SSPs	69
9.5 Transitions	99
10 Self-Tests	99
10.1 Pre-Operational Self-Tests	100
10.2 Conditional Self-Tests.....	100
10.3 Periodic Self-Test Information.....	103
10.4 Error States	104
10.5 Operator Initiation of Self-Tests	105
10.6 Additional Information	105
11 Life-Cycle Assurance	106
11.1 Installation, Initialization, and Startup Procedures.....	106
11.2 Administrator Guidance	106
11.3 Non-Administrator Guidance.....	106
11.4 Design and Rules	106
11.5 End of Life	106
11.6 Additional Information	106
12 Mitigation of Other Attacks	107

List of Tables

Table 1: Security Levels	5
Table 2: Tested Module Identification – Hardware	10
Table 3: Modes List and Description	10
Table 4: Approved Algorithms	15
Table 5: Vendor-Affirmed Algorithms	15
Table 6: Security Function Implementations	20
Table 7: Entropy Certificates	20
Table 8: Entropy Sources	20
Table 9: Ports and Interfaces	23
Table 10: Authentication Methods	26
Table 11: Roles	27
Table 12: Approved Services	63
Table 13: Mechanisms and Actions Required	65
Table 14: EFP/EFT Information	65
Table 15: Hardness Testing Temperatures	66
Table 16: Storage Areas	66
Table 17: SSP Input-Output Methods	67
Table 18: SSP Zeroization Methods	69
Table 19: SSP Table 1	82
Table 20: SSP Table 2	99
Table 21: Pre-Operational Self-Tests	100
Table 22: Conditional Self-Tests	102
Table 23: Pre-Operational Periodic Information	103
Table 24: Conditional Periodic Information	104
Table 25: Error States	104

List of Figures

Figure 1 : Block Diagram	8
Figure 2 : Tags for Tracking Data (Approved Mode)	11
Figure 3 : Card Production Life Cycle Data	11
Figure 4 : Versions and Operations Indicators	12

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Thales IDCore230/3230 platform with the IDPrime PIV 4.0 and FIDO2 2.1 applets, **IDPrime PIV 4.0 FIDO on IDcore 3230**. 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.

The Module, validated to FIPS 140-3 overall Level 2, is a single-chip cryptographic platform. The Module implements the Global Platform operational environment, including the Card Manager, and supports the deployment of the following configurable application environments:

- PIV Applet
- PIV Admin Applet
- MoC Server Applet (for Biometric Match-on-Card)
- FIDO Applet

The *Module* is a limited operational environment under the FIPS 140-3 definitions

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	3
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

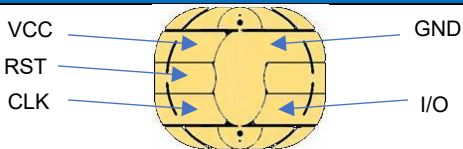
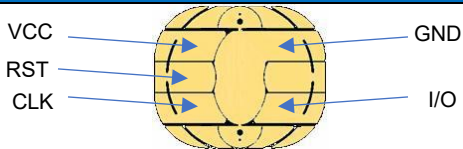
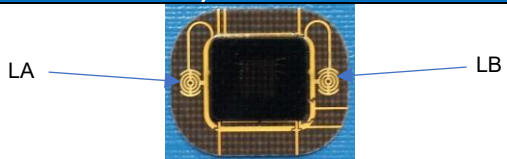
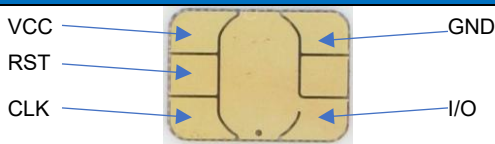
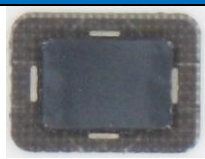
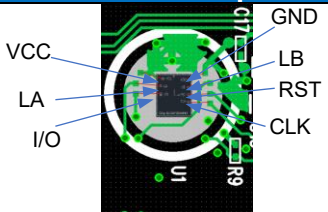
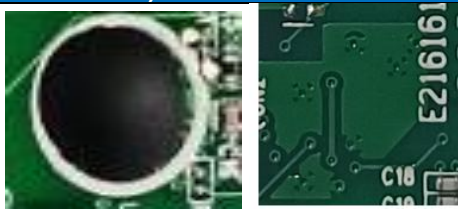
2.1 Description

The Module is running on the single chip: SLC37GDA512, and can be manufactured using the following hardware part numbers:

- WORLD RLT module (contact)
- WORLD Combi RLT module (contact and contactless, aka "Dual")
- PICO RLV module (contact)

- Chip On Board module (contact)

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 RLT module (SLC37GDA512) for 230	
 Top View – Contact Plate	 Bottom View – Black Epoxy with RLT technology
WORLD Combi RLT module (SLC37GDA512) for 3230	
 Top View – Combi Plate	 Bottom View – Black Epoxy with RLT technology
PICO RLV module (SLC37GDA512) for 230	
 Top View – Contact Plate	 Bottom View – Black Epoxy with RLV technology
Chip on Board module (SLC37GDA512) for 230	
 Top View - without Black Epoxy	 Top View - with Black Epoxy / Bottom View with PCB

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* 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.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics:

Cryptographic Boundary:

Below depicts the Module's block diagram:

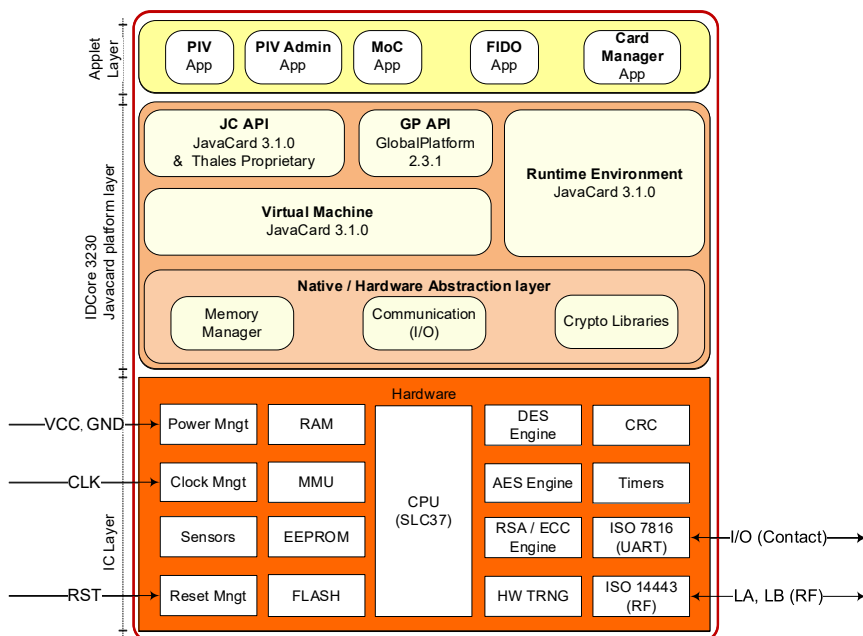


Figure 1 : Block Diagram

The Cryptographic Module (CM) is fully compliant with two major card industry standards: Oracle JavaCard (JC) 3.1.0 Classic Edition and GlobalPlatform (GP) Card Specification version 2.3.1.

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

The CM provides an execution sandbox for the *PIV, MoC Server, and FIDO applets* and performs the requested services according to its roles and services security policy.

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

The *JavaCard API (JC 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 (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 terms 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 CM supports T=0, T=1 and T=CL communication protocols

The *Cryptography Libraries* implement the algorithms listed in Section 2.5.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
COB Module	SLC37GDA512 Mask number: G322	IDCore 230-BUILD6.11 with Firmware: IDCore 3230-BUILD6.11; IDPrimePIV 4.0 Applet (version 4.0.0) MoC Server applet (version 1.1) FIDO 2.1 Applet (version 2.1.0.B)	Infineon SLC37GDA512	Java Card 3.1.0 GlobalPlatform (GP) 2.3.1 Contact with protocol communication T=0 and T=1
PICO RLV Module / A3138921	SLC37GDA512 Mask number: G322	IDCore 230-BUILD6.11 with Firmware: IDCore 3230-BUILD6.11; IDPrimePIV 4.0 Applet (version 4.0.0) MoC Server applet (version 1.1) FIDO 2.1 Applet (version 2.1.0.B)	Infineon SLC37GDA512	Java Card 3.1.0 GlobalPlatform (GP) 2.3.1 Contact with protocol communication T=0 and T=1
World Combi RLT module / A2848344	SLC37GDA512 Mask number: G322	Firmware: IDCore 3230-BUILD6.11; IDPrimePIV 4.0 Applet (version 4.0.0) MoC Server applet (version 1.1) FIDO 2.1 Applet (version 2.1.0.B)	Infineon SLC37GDA512	Java Card 3.1.0 GlobalPlatform (GP) 2.3.1 Contact with protocol communication T=0 and T=1 Contactless with protocol communication T=CL

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
World RLT module / A3103037	SLC37GDA512 Mask number: G322	IDCore 230-BUILD6.11 with Firmware: IDCore 3230-BUILD6.11; IDPrimePIV 4.0 Applet (version 4.0.0) MoC Server applet (version 1.1) FIDO 2.1 Applet (version 2.1.0.B)	Infineon SLC37GDA512	Java Card 3.1.0 GlobalPlatform (GP) 2.3.1 Contact with protocol communication T=0 and T=1

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.

2.3 Excluded Components

None

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	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

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 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 3230/230 - 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	1981h	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 3230/230 - 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	6B	IDCore3230 / 230
5	Thales Version	06	Major Version
6	Thales Version (Minor)	11	Minor Version1
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	FIPS Level 2
14-15	Specific chip ID	32 30	32 30 = Contact and Contactless 02 30 = Contact
16-17	PKI applet version	0400	0400 = Piv applet version 4.0
18-19	FIDO applet version	0210	021 = FIDO applet version 2.1
20-29	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:

¹ Bytes 5 and 6, as indicated in Table 6 above collective indicate the validated Firmware version number, "IDCore 3230-BUILD6.11".

Algorithm	CAVP Cert	Properties	Reference
AES-CBC, AES-ECB	A2877	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A2877	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 128-256 Increment 8	SP 800-38B
Counter DRBG	A2877	Prediction Resistance - No Supports Reseed - No Mode - AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 1024 Nonce - Nonce: 384 Personalization String Length - Personalization String Length: 0 Returned Bits - 128	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A2877	Curve - P-256, P-384 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A2877	Curve - P-256, P-384 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA2-256	A2877	MAC - MAC: 256 Key Length - Key Length: 128, 256	FIPS 198-1
KAS-ECC Sp800-56Ar3	A2877	Domain Parameter Generation Methods - P-256, P-384 Function - Partial Validation iutId - 123456ABCD Scheme - onePassDh - KAS Role - Responder KDF Methods - oneStepKdf - Auxiliary Function Methods - Auxiliary Function Name - SHA2-384 Fixed Info Pattern - algorithmId uPartyInfo vPartyInfo Fixed Info Encoding - Concatenation Key Confirmation Methods - Key Confirmation Directions - Key Confirmation Roles - Key Confirmation MAC Methods - CMAC - Key Length - 256 MAC Length - 128 Key Length - 1024	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A2877	Domain Parameter Generation Methods - P-256, P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A2877	Fixed Info Pattern - uPartyInfo vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 512 Shared Secret Length - Shared Secret Length: 256 HMAC Algorithm - SHA2-256 Perform Multiple Expansion Tests - No	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A2877	Auxiliary Function Methods - Auxiliary Function Name - SHA2-256 Fixed Info Pattern - uPartyInfo vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 256 Shared Secret Length - Shared Secret Length: 256	SP 800-56C Rev. 2
KDF SP800-108	A2877	KDF Mode - Counter MAC Mode - CMAC-AES128, CMAC-AES192, CMAC-AES256 Supported Lengths - Supported Lengths: 128-256 Increment 64 Fixed Data Order - In the Middle of Fixed Data Counter Length - 8 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KTS-IFC	A2877	IUT ID - CAFECafe Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg1-crt Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Encoding - concatenation 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 Modulo - 2048, 3072, 4096	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
		p mod 8 - 0 Primality Tests - 2pow100 q mod 8 - 0 Fixed Public Exponent - 010001 Info Generated By Server - No Private Key Format - crt, standard Public Exponent Mode - fixed	
RSA SigGen (FIPS186-5)	A2877	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - MGF1	FIPS 186-5
SHA2-224, SHA2-256, SHA2-384, SHA2-512	A2877	Message Length - Message Length: 8-65536 Increment 8 Function - SHA2	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 and Symmetric	N/A	SP800-133r2 Section 4, Example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

There are no non-approved, allowed algorithms in this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

There are no non-approved, allowed algorithms with no security claimed in this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

There are no Non-Approved, Not Allowed Algorithms in this module.

2.6 Security Function Implementations

The table lists the security functions provided by the IDPrime PIV 4.0 FIDO on IDcore 3230 module.

Name	Type	Description	Properties	Algorithms
CKG Symmetric	CKG	Symmetric key generation for AES		Counter DRBG: (A2877) AES-CBC: (A2877)
Digital Signature Generation ECC	DigSig- SigGen	Signature Generation		ECDSA SigGen (FIPS186-5): (A2877) P-224: SHA2- 224, SHA2-256, SHA2-384, SHA2-512 P-256: SHA2- 256, SHA2- 384, SHA2-512 P-384: SHA2- 384, SHA2-512 P-521: SHA2- 512 SHA2-224: (A2877) SHA2-256: (A2877) SHA2-384: (A2877) SHA2-512: (A2877)
Digital Signature Generation RSA	DigSig- SigGen	Signature Generation		RSA SigGen (FIPS186-5): (A2877) Modulus and Hash values: n=2048, 3072, 4096 with PKCS v1.5 and PKCS PSS SHA2- (224, 256, 384, 512) SHA2-224: (A2877) SHA2-256: (A2877) SHA2-384: (A2877)

Name	Type	Description	Properties	Algorithms
				SHA2-512: (A2877)
DRBG	DRBG	Counter DRBG		Counter DRBG: (A2877) AES-CBC: (A2877)
Encryption - Decryption	BC-UnAuth	Block cipher- decipher unauthenticated	Strength:128, 192, 256 bits	AES-CBC: (A2877) AES-ECB: (A2877)
Entropy Source	ENT-ESV	NIST SP 800-90B Physical Entropy Source	NIST SP 800- 90B Physical Entropy Source:	
FIDO Authentication	DigSig- SigGen KAS-56CKDF MAC SHA KAS-Full	FIDO Authentication Service	IG: D.F Scenario 2, path (2), split Key Confirmation: No Key Derivation: KDA (tested as part of KAS certificate) Caveat: Key establishment methodology provides between 112 and 256 bits of security strength	ECDSA SigGen (FIPS186-5): (A2877) KDA HKDF SP800-56Cr2: (A2877) HMAC-SHA2- 256: (A2877) SHA2-256: (A2877) KAS-ECC-SSC Sp800-56Ar3: (A2877)
FIDO KTS	KTS-Wrap	FIDO wrap using AES CBC for encryption and HMAC for authentication used to transport key handle	Strength:Key transport methodology providing 128 bits of security strength	HMAC-SHA2- 256: (A2877) AES-CBC: (A2877) SHA2-256: (A2877)
FIDO Registration	AsymKeyPair- KeyGen KAS-56CKDF MAC CKG	FIDO Registration service		ECDSA KeyGen (FIPS186-5): (A2877) Counter DRBG: (A2877) CKG: () KDA HKDF SP800-56Cr2: (A2877) AES-CBC: (A2877) HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				256: (A2877) SHA2-256: (A2877)
Generate Key Pair EC	AsymKeyPair-KeyGen	Demonstrate ECC key generation		ECDSA KeyGen (FIPS186-5): (A2877) Counter DRBG: (A2877) CKG: () Key Type: Asymmetric
Generate Key Pair RSA	AsymKeyPair-KeyGen	Demonstrate RSA key generation		RSA KeyGen (FIPS186-5): (A2877) Counter DRBG: (A2877) CKG: () Key Type: Asymmetric
GP Secure Channel	KTS-Unwrap KTS-Wrap	AES encryption method with the combination of approved Authentication method AES CMAC, in accordance with SP 800-38F.	IG D.G: Approved method #2 Strength: Key transport methodology provides between 128 and 256 bits of security strength	AES-CBC: (A2877) AES-CMAC: (A2877) AES-ECB: (A2877)
HMAC	MAC	Message Authentication		HMAC-SHA2-256: (A2877) SHA2-256: (A2877)
IFC-Encrypt	AsymKeyPair-Decap	Key Transport Decapsulation		KTS-IFC: (A2877) SHA2-224: (A2877) SHA2-256: (A2877) SHA2-384: (A2877) SHA2-512: (A2877)
KDA HKDF	KAS-56CKDF	Key Derivation		KDA HKDF SP800-56Cr2: (A2877) SHA2-256:

Name	Type	Description	Properties	Algorithms
				(A2877) HMAC-SHA2-256: (A2877)
KDF	KBKDF	Key-Based Key Derivation		AES-CMAC: (A2877) KDF SP800-108: (A2877) AES-CBC: (A2877)
Key Agreement	KAS-SSC	Shared Secret Calculation	IG: D.F Scenario 2, path (2), split Key Confirmation: No Key Derivation: KDA (tested as part of KAS certificate) Caveat: Key establishment methodology provides between 112 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A2877)
Message Authentication	MAC	Message Authentication		AES-CMAC: (A2877) AES-CBC: (A2877)
Opacity Secure Channel	KAS-Full	Key Agreement Scheme SP800-56Cr2 Key Derivation Message Authentication for key confirmation	IG: D.F Scenario 2, path 2, end-to-end Key Confirmation: Yes Key Derivation: SP 800-56Cr2 KDA (Tested as part of KAS certificate) Caveat: Key establishment methodology provides between 112 to 256 bits of security Strength	KAS-ECC Sp800-56Ar3: (A2877) KDA OneStep SP800-56Cr2: (A2877) AES-CMAC: (A2877) HMAC-SHA2-256: (A2877) SHA2-256: (A2877) AES-CBC: (A2877)
Secure Hash	SHA	Compute the hash value		SHA2-224: (A2877)

Name	Type	Description	Properties	Algorithms
				SHA2-256: (A2877) SHA2-384: (A2877) SHA2-512: (A2877)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

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	Infineon SLC37 32-bit Security Controller V11	1 bit	0.418	non-vetted conditioning function

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 symmetric keys and 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

The module uses unmodified output from its Counter DRBG as symmetric key generation. The module supports the following CKG methodologies:

- SP800-133r2 6.1: "Direct Generation of Symmetric Keys
- SP800-133r2 6.3: Symmetric Keys Derived by Combining Multiple Keys and Other Data, which involves a key-extraction process

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.

The module implements the following approved key agreement scheme as specified in FIPS 140-3 IG D.F, Scenario 2, path 1 which has been CAVP tested and validated

- SP 800-56Ar3 KAS-ECC-SSC for Shared Secret Computation.

The module implements the following approved Key-Establishment Schemes HKDF as specified in FIPS 140-3 IG D.F, which has been CAVP tested and validated:

- SP 800-56Ar3 KAS-ECC with SP 800-56Cr2 HKDF 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 800-38F Key Transport using AES ECB/CBC for encryption and AES-CMAC for authentication. (Approved method #2 from IG D.G)
- SP 800-38F Key Transport using AES ECB/CBC for encryption and HMAC for authentication. (Approved method #2 from IG D.G)

2.11 Industry Protocols

N/A

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

All cryptographic modules within this processor family incorporate physical interfaces for both contact (ISO/IEC 7816) and contactless (ISO/IEC 14443) communications at the hardware level.

During manufacturing, activation of these interfaces is determined by the selected form factor (see part 2.1 description of the Cryptographic Module Specification) **and** the presence/absence of antenna integration in the product.

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: Used to supply power to the module in contact mode; The module starts when interface is powered -as specified in ISO17816 -3 (part 5.2.1).
RST	Control Input	Reset signal: If a signal is sent on this interface on contact mode, the module will reboot (active low) as specified in ISO17816 -3.
CLK	Control Input	Clock signal: The interface is used by an external device (ex: smartcard reader) to provide a clock signal to the IC in contact mode as specified in ISO17816 -3.
GND	Power	Ground
I/O	Data Input Data Output Control Input	Commands and responses, protocol and control data. The interface is used to communicate with an external entity (ex: SmartCard reader) in contact mode as specified in ISO17816 -3.

Physical Port	Logical Interface(s)	Data That Passes
	Status Output	
LA	Data Input Data Output Control Input Status Output Power	Supply, clock signal, commands and responses, protocol and control data This interface is used to communicate with an external entity (ex: smartcard reader) in contactless mode; It is also used to set the internal clock and to supply power to the module as specified in ISO14443 -2
LB	Data Input Data Output Control Input Status Output Power	Supply, clock signal, commands and responses, protocol and control data This interface is used to communicate with an external entity (ex: smartcard reader) in contactless mode; It is also used to set the internal clock and to supply power to the module as specified in ISO14443 -2

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 ²	1MHz to 10MHz

Table : Voltage and Frequency Ranges

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

The 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

Table: Contactless voltage and Frequency Ranges

² Frequency of the internal clock as supplied by the CLK physical interface.

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 described as Single-Factor Cryptographic Software (Section 5.1.6) This method is performed when the EXTERNAL AUTHENTICATE command is invoked after successful execution of the INITIALIZE UPDATE command. This method is used to authenticate the CO role.	GP Secure Channel	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, $(1/2^{256})$ for AES 32-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.
Secret Value authentication method (PIN)	In accordance to SP 800-63B, this Authenticator type is described as Memorized Secrets (Section 5.1.1). This authentication method compares an encrypted PIN value sent to the Module to the stored encrypted PIN values. If the two values are equal, the Card Holder is authenticated. This method is used to authenticate the CH role.	Encryption - Decryption	The probability that a random attempt at authentication will succeed is $(1/10^8)$.	Based on a maximum count of 5 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one-minute period is lower than $5/10^8$.
Secret Value authentication method (PC)	In accordance to SP 800-63B, this Authenticator type is described as	Encryption - Decryption	The probability that a random attempt at authentication	The probability that a random attempt will succeed over a

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	Memorized Secrets (Section 5.1.1).this authentication method compares an encrypted Pairing Code value sent to the Module to the stored encrypted Pairing Code value. If the two values are equal, the Card Holder is authenticated. This method is used to authenticate the CHPC role.		will succeed is $(1/10^8)$.	one-minute period is $(59/10^8)$.
Secret Value authentication method (PUK)	In accordance to SP 800-63B, this Authenticator type is described as Memorized Secrets (Section 5.1.1).This authentication method compares an encrypted PUK value sent to the Module to the stored encrypted PUK value if the two values are equal, the Card Holder II is authenticated. This method is used to authenticate the CHII role.	Encryption - Decryption	The probability that a random attempt at authentication will succeed is lower than $(1/256^8)$.	Based on a maximum count of 15 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one-minute period is lower than $(15/256^8)$.
PIV Symmetric Cryptographic Authentication method	In accordance to SP 800-63B, this Authenticator type is described as Single-Factor Cryptographic Software (Section 5.1.6).The Module uses the PIV-AUTH-AES to authenticate the CAA role.	Encryption - Decryption	128/192/256 bits. The probability that a random attempt at authentication will succeed is $1/2^{128}$ (for 128-bit length).	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 $(255/2^{128})$ for AES 16-byte-long keys, $(255/2^{192})$ for

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
				AES 24-byte-long keys, $(255/2^{256})$, for AES 32-byte-long keys.
Secret Value authentication method	In accordance to SP 800-63B, this Authenticator type is described as Memorized Secrets (Section 5.1.1). This authentication method runs an OnCardComparison (OCC) of a candidate fingerprint template as defined by [FIPS 2012]. This method is used to authenticate the CHOCC role.	Memorized secret for on-card comparison	The probability that a random attempt at authentication will succeed is $1/10^4$.	Based on a maximum count of 5 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one-minute period is lower than $5/10^4$.
FIDO User Authentication	In accordance to SP 800-63B, this Authenticator type is described as Memorized Secrets (Section 5.1.1). This authentication method compares a PIN value sent to the Module to the stored FID-UV-PIN. If the two values are equal, the operator is authenticated. This method is used to authenticate the FUSR role.	Encryption - Decryption SHA	The probability that a random attempt at authentication will succeed is lower than $1/2^{48}$.	Based on a maximum count of 8 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one-minute period is $8/2^{48}$.

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, but only one operator can operate per channel at the same time, thus allowing two concurrent operators for the two corresponding applets supported by the module.

4.2 Roles

The module provides Identity-based authentication. The Module does not support a maintenance role.

Name	Type	Operator Type	Authentication Methods
CO	Identity	Cryptographic Officer	Secure Channel Protocol authentication method
CAA	Identity	User	PIV Symmetric Cryptographic Authentication method
CH	Identity	User	Secret Value authentication method (PIN)
CHII	Identity	User	Secret Value authentication method (PUK)
CHPC	Identity	User	Secret Value authentication method (PC)
CHOCC	Identity	User	Secret Value authentication method
FUSR	Identity	User	FIDO User Authentication

Table 11: Roles

The Cryptographic Officer (CO) role is responsible for card issuance and management of card data via the Card Manager Authenticated using The SCP authentication method with SD-SENC. The Card Application Administrator (CAA) is the PIV Card Application Administrator role. It represents an external application requesting the services offered by the PIV Applet.

The PIV Card Holder (CH) role is responsible for ensuring the ownership of his MODULE, and for not communicating his PIN to other parties.

The PIV Card Holder II (CHII) role is responsible for unblocking and/or changing the Card Holder PIN.

The PIV Card Holder Pairing Code (CHPC) role is responsible for ensuring the ownership of his MODULE, and for not communicating his Pairing Code to other parties.

The Card Holder On Card Comparison (CHOCC) role is responsible for ensuring the ownership of his MODULE. The PIV Applet authenticates the CHOCC role by verifying the biometric fingerprint through the MoC Server Applet.

The FIDO user (FUSR) role is allowed to perform cryptographic authentication operation with the PIN (key handles) when user verification is required by the Relaying Party. This role is responsible for changing the PIN as well.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authenticator_Reset (FIDO Service)	Reset the	IND 1	none	none	CKG Symm	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	applet, rendering all credentials created useless				etric KDA HKDF Key Agreement HMAC	- FID- ECDH- ECC: E - FID- KG-AS- ECDSA- PUB: Z - FID- KG-RK- ECDSA: Z - FID- PIN- KEY: G - FID- RK- HMAC- NONCE: Z - FID- SC- AUTH- HMAC: G - FID- SC- ENC- AES: G - FID- SEED: Z - FID- SHARE D- SECRET : E,G - FID- SHARE D- SECRET -INTER: E,G,Z - OS- DRBG- EI: E - OS- DRBG-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						KEY: G,E - OS- DRBG- S: E - OS- DRBG- V: G,E
Context - Select an applet or manage logical channels. (Platform service)	Select an applet or manage logical channels.	IND_1	data	return Status Word		Unauthenticated - FID- PIN- KEY: Z - FID- SHARE D- SECRET : Z - SD- SENC: Z - SD- SMAC: Z
CTAP2_ClientPIN_GetPinToken CTAP2_ClientPin_GetPinUvAuthTokenUsingPinWithPermissions (FIDO service)	Retrieve the authentication nonce of the application	IND_1	CTAP data including encrypted pin	ctap data, status word	Key Agreement CKG Symmetric KDA HKDF Encryption - Decryption	FUSR - FID- ECDH- ECC: E - FID- PIN- KEY: G,E - FID- PLAT- ECDH- PUB: W,E,Z - FID- SHARE D- SECRET : E,G - FID- TOKEN- NONCE- V2: G,R - OS- DRBG-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						EI: E - OS-DRBG-KEY: G,E - OS-DRBG-S: E - OS-DRBG-V: G,E
CTAP2_ClientPIN_ChangePin (FIDO service)	Update the pin of the application	IND_1	CTAP data including encrypted pin	status word	HMAC KDA HKDF Key Agreement Encryption - Decryption Secure Hash Generate Key Pair EC	FUSR - FID-ECDH-ECC: E,G - FID-ECDH-ECC-PUB: G - FID-PIN-KEY: G,E - FID-PLAT-ECDH-PUB: W,E,Z - FID-SHARE D-SECRET : G,E - FID-SHARE D-SECRET -INTER: G,E,Z - FID-UV-PIN: W,E - FID-UV-PIN-Hash: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- OS-MKDK: E
CTAP2_ClientPIN_GetKeyAgreement (FIDO service)	Return the number transient ECDH public key of the application	IND_1	CTAP data	ctap data, status word		Unauthenticated - FID-ECDH-ECC-PUB: R
CTAP2_ClientPIN_GetRetries (FIDO service)	Return the number of remaining attempt for the PIN	IND_1	CTAP data	ctap data, status word		Unauthenticated
CTAP2_ClientPIN_SetPin (FIDO service)	Set the pin of the application	IND_1	CTAP data including encrypted pin	status word	Generate Key Pair EC KDA HKDF Secure Hash Encryption - Decryption HMAC Key Agreement	Unauthenticated - FID-ECDH-ECC: E,G - FID-ECDH-ECC-PUB: G - FID-PIN-KEY: G,E - FID-PLAT-ECDH-PUB: W,E,Z - FID-SHARE D-SECRET: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- FID-SHARE D-SECRET -INTER: G,E,Z - FID-UV-PIN: W,E - FID-UV-PIN-Hash: G - OS-MKDK: E
CTAP2_Config_SettingAMinimumPINLength (FIDO service)	Used to set a minimum PIN Length	IND_1	CTAP data	status word	HMAC	FUSR - FID-TOKEN-NONCE-V2: E
CTAP2_Config_ToggleAlwaysRequireUserVerification (FIDO service)	Used to enforce User Verification	IND_1	CTAP data	status word	HMAC	FUSR - FID-TOKEN-NONCE-V2: E
CTAP2_ControlEnd (FIDO service)	Deactivate the applet, until the applet is explicitly selected again	IND_1	none	status word	None	Unauthenticated
CTAP2_CredentialManagement_EnumeratingCredentialsForAnRP_Begin_EnumeratingCredentialsForAnRP_Next (FIDO service)	Used for enumeration of Credentials for a RP present on the	IND_1	CTAP data	ctap data, status word	HMAC	FUSR - FID-TOKEN-NONCE-V2: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	authenticator					
CTAP2_CredentialManagement_EnumeratingRPs_Begin_EnumeratingRPs_Next (FIDO service)	Used for enumeration of RPs present on the authenticator	IND_1	CTAP data	ctap data, status word	HMAC	FUSR - FID-TOKEN-NONCE-V2: E
CTAP2_CredentialManagement_GettingCredentialsMetadata (FIDO service)	Used to get credentials metadata	IND_1	CTAP data	ctap data, status word	HMAC	FUSR - FID-TOKEN-NONCE-V2: E
CTAP2_CredentialManagement_DeleteCredential (FIDO service)	Used to delete a credential	IND_1	CTAP data	status word	HMAC	FUSR - FID-KG-RK-ECDSA: Z - FID-KG-RK-ECDSA-PUB: Z - FID-RK-HMAC-NONCE: Z - FID-TOKEN-NONCE-V2: E
CTAP2_CredentialManagement_UpdatingUserInformation (FIDO service)	Used to update user information associated to a credential	IND_1	CTAP data	status word	HMAC	FUSR - FID-TOKEN-NONCE-V2: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
CTAP2_GetAssertion CTAP2_GetNextAssertion (FIDO service)	initiate a CTAP2 token authentication	IND_1	CTAP data	ctap data, status word	CKG Symmetric Digital Signature Generation ECC Encryption - Decryption FIDO Authentication FIDO KTS FIDO Registration HMAC KDA HKDF	FUSR - FID-HMAC-NONCE: E,G - FID-KG-AS-ECDSA: E - FID-KG-RK-ECDSA: E - FID-RK-HMAC-NONCE: E - FID-SC-AUTH-HMAC: E - FID-SC-ENC-AES: E - FID-SEED: E,W - FID-TOKEN-NONCE-V2: E
CTAP2_GetInfo (FIDO service)	Retrieve the authenticator information	IND_1	none	getInfo data return Status Word		Unauthenticated
CTAP2_MakeCredential (FIDO service)	Generates a new key pair for token	IND_1	ctap data	ctap data, status word	FIDO KTS FIDO Registration	FUSR - FID-AT-ECDSA: E - FID-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	registration					AT-ECDSA-PUB: R - FID-HMAC-NONCE: G - FID-KG-AS-ECDSA: G - FID-KG-AS-ECDSA-PUB: G,R - FID-KG-RK-ECDSA: G - FID-KG-RK-ECDSA-PUB: G - FID-RK-HMAC-NONCE: G - FID-SC-AUTH-HMAC: E - FID-SC-ENC-AES: E - FID-SEED: G,R - FID-TOKEN-NONCE-V2: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
FIDO GetData (Applet Info) (FIDO service)	Retrieve the authenticator information	IND_1	none	return Status Word / info data		Unauthenticated
FIDO Select (FIDO service)	allows the platform to let a user select a certain authenticator	IND_1	datas such as a DF an EF by its file ID, path or name	return Status Word	None	CO Unauthenticated
Get Approved mode parameters (Platform service)	Get information of the approved mode of operation	IND_1	none	data return Status Word		Unauthenticated
Lifecycle (Platform service)	Modify the card or applet life cycle status. May be employed to perform zeroization.	IND_1	Set / Get Status : life cycle state to update/ empty	return Status Word / life cycle state and package list	None	CO - FID-HMAC-NONCE: Z - DAP-SYM: Z - FID-AT-ECDSA: Z - FID-AT-ECDSA-PUB: Z - FID-ECDH-ECC: Z - FID-ECDH-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECC-PUB: Z - FID-KG-AS-ECDSA: Z - FID-KG-AS-ECDSA-PUB: Z - FID-KG-RK-ECDSA: Z - FID-PIN-KEY: Z - FID-RK-HMAC-NONCE: Z - FID-SEED: Z - FID-SHARE D-SECRET: Z - FID-TOKEN-NONCE-V2: Z - FID-UV-PIN: Z - MOC-OCC: Z - OPACITY-SCONFIRMATION: Z - OPACITY

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Y-SENS: Z - OPACIT Y- SMAC: Z - OPACIT Y- SRMAC: Z - OS- DRBG- EI: Z - OS- DRBG- KEY: Z - OS- DRBG- S: Z - OS- DRBG- V: Z - PIV- AKM- ECC: Z - PIV- AKM- RSA: Z - PIV- AS-ECC: Z - PIV- AS-ECC- PUB: Z - PIV- AS-RSA: Z - PIV- AS-RSA- PUB: Z - PIV- AUTH- AES: Z - PIV- AUTH-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECC: Z - PIV-AUTH-ECC-PUB: Z - PIV-AUTH-RSA: Z - PIV-AUTH-RSA-PUB: Z - PIV-AUTH-CH-AES: Z - PIV-AUTH-CH-ECC: Z - PIV-AUTH-CH-RSA: Z - PIV-KS-ECC: Z - PIV-KS-RSA: Z - PIV-PC: Z - PIV-PIN: Z - PIV-PUK: Z - PIV-SM-ECC: Z - PIV-SM-ECC-PUB: Z - SD-KDEK: Z - SD-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						KENC: Z - SD- KMAC: Z - SD- SENC: Z - SD- SMAC: Z
Manage Content (Platform service)	Load, install, and delete application packages	IND_1	Applications and associated data	return Status Word	GP Secure Channel Message Authentication	CO - DAP-SYM: E,Z - FID-AT-ECDSA: Z - FID-AT-ECDSA-PUB: Z - FID-ECDH-ECC: Z - FID-ECDH-ECC-PUB: Z - FID-KG-AS-ECDSA: Z - FID-KG-AS-ECDSA-PUB: Z - FID-KG-RK-ECDSA: Z - FID-PIN-KEY: Z - FID-RK-HMAC-NONCE: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- FID-SC-ENC-AES: Z - FID-SEED: Z - FID-SHARE D-SECRET : Z - FID-TOKEN-NONCE-V2: Z - FID-UV-PIN: Z - MOC-OCC: Z - OPACITY-SCONFIRMATION: Z - OPACITY-SENC: Z - OPACITY-SMAC: Z - OPACITY-SRMAC: Z - OS-DRBG-EI: Z - OS-DRBG-KEY: Z - OS-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG-S: Z - OS- DRBG-V: Z - PIV- AKM-ECC: Z - PIV- AKM-RSA: Z - PIV- AS-ECC: Z - PIV- AS-ECC-PUB: Z - PIV- AS-RSA: Z - PIV- AS-RSA-PUB: Z - PIV- AUTH-AES: Z - PIV- AUTH-ECC: Z - PIV- AUTH-ECC-PUB: Z - PIV- AUTH-RSA: Z - PIV- AUTH-RSA-PUB: Z - PIV- AUTH-CH-AES: Z - PIV- AUTH-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						CH-ECC: Z - PIV-AUTH-CH-RSA: Z - PIV-KS-ECC: Z - PIV-KS-RSA: Z - PIV-PC: Z - PIV-PIN: Z - PIV-PUK: Z - PIV-SM-ECC: Z - PIV-SM-ECC-PUB: Z - SD-KDEK: Z - SD-KENC: Z - SD-KMAC: Z - SD-SENC: E,Z - SD-SMAC: E,Z
Manage keys (Platform service)	Put Keys	IND_1	Command parameters (data objects, SSPs)	return Status Word	Encryption - Decryption GP Secure Channel	CO - DAP-SYM: W - OS-MKDK: W - PIV-AUTH-AES: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PIV-AUTH-CH-AES: W - SD-MDAP-KENC: W - SD-MDAP-KMAC: W - SD-KDEK: E,W - SD-KENC: W - SD-KMAC: W - SD-MDAP-KDEK: W - SD-SENC: E - SD-SMAC: E
Module Info (Auth) (Platform service)	Read module configuration or status information (privileged data objects).	IND_1	Tags and module information	module configuration status information, return Status Word	GP Secure Channel Message Authentication	CO - SD-SENC: E - SD-SMAC: E
Module Info (Platform service)	Read unprivileged data	IND_1	data	return Status Word		Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	objects, e.g., module configuration or status information, including version information..					
Module Reset (Platform service)	Power cycle or reset the Module . Includes Integrity Self-Test, periodic self-test counter set-up and self-test flag is reset	IND_1	none	ATR (Answer To Reset)	DRBG Entropy Source	Unauthenticated - SD-SENC: Z - SD-SMAC: Z - OS-DRBG-EI: Z,G,E - OS-DRBG-S: Z,G,E - OS-DRBG-KEY: Z,G,E - OS-DRBG-V: Z,G,E - FID-ECDH-ECC: Z - FID-HMAC-NONCE: Z - FID-SHARE D-SECRET : Z - FID-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						TOKEN-NONCE-V2: Z - OPACITY-SCONFIRMATION: Z - OPACITY-SENC: Z - OPACITY-SMAC: Z - OPACITY-SRMAC: Z
OPACITY Secure Message (PIV Service)	Establish OPACITY-ZKM secure messaging	IND_1	data	control byte + nonce + cryptogram + cert return Status Word	Message Authentication Opacity Secure Channel Secure Hash CKG Symmetric Encryption - Decryption	Unauthenticated - OPACITY-SCONFIRMATION: G,E,Z - OPACITY-SENC: G,E - OPACITY-SMAC: G,E - OPACITY-SRMAC: G,E - OPACITY

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Y-Z: G,E,Z - OS- DRBG- EI: E - OS- DRBG- KEY: G,E - OS- DRBG- S: E - OS- DRBG- V: G,E - PIV- SM- ECC- PUB: R - ROE- PUB: W,E
PIV Admin Garbage collector command (PIV Service)	Performs a memory clean up	IND_1	N/A	return Status Word	GP Security Channel	CO - SD- SENC: E - SD- SMAC: E
PIV Admin Get data (Prop) (PIV Service)	Retrieves the data content of - Data Object Control Parameter (DOCP) of SE, PIN, Key or data object, Applet person	IND_1	object name	Object data content, return Status Word		Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	alization data					
PIV Admin Get pin last error code (PIV Service)	Retrieves the last error encounter regarding the pin policy verification	IND_1	N/A	last error code, return Status Word		Unauthenticated
PIV Admin Manage PIN (PIV Service)	Unlock a pin or change its value without any knowledge of the current value	IND_1	PIN Reference new PIN	return Status Word	Encryption - Decryption GP Secure Channel	CO - OS-MKDK: E - PIV-PC: W,E - PIV-PIN: W,E - PIV-PUK: W,E - PIV-AUTH-CH-AES: E
PIV Admin Reinit command (PIV Service)	Clear the data model content, keeping the data object header but deleting the value of Sensitive	IND_1	object data, Admin keyID	return Status Word	GP Secure Channel	CO - PIV-AKM-ECC: Z - PIV-AKM-ECC-PUB: Z - PIV-AKM-RSA: Z - PIV-AKM-RSA-PUB: Z - PIV-AS-ECC: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Security Parameters and PIV Objects					- PIV-AS-ECC-PUB: Z - PIV-AS-RSA: Z - PIV-AS-RSA-PUB: Z - PIV-AUTH-AES: W - PIV-AUTH-ECC: Z - PIV-AUTH-CH-AES: Z - PIV-AUTH-CH-ECC: Z - PIV-AUTH-CH-ECC-PUB: Z - PIV-AUTH-CH-RSA: Z - PIV-AUTH-CH-RSA-PUB: Z - PIV-KS-ECC: Z - PIV-KS-ECC-PUB: Z - PIV-KS-RSA: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PIV-KS-RSA-PUB: Z - PIV-SM-ECC: Z - PIV-SM-ECC-PUB: Z - SD-SENC: E - SD-SMAC: E - PIV-PIN: Z
PIV Admin Select (PIV Service)	Select admin applet	IND_1	datas such as a DF and EF by its file ID, path or name	return Status Word		Unauthenticated
PIV Administrator Authentication (PIV Service)	Performs, external authentication, or mutual authentication.	IND_1	Random, cryptogram, algorithm reference, key reference, data	Cryptogram, nonce, return Status Word	DRBG Encryption - Decryption	CAA - OS-DRBG-EI: G,E - OS-DRBG-KEY: G,E - OS-DRBG-S: G,E - OS-DRBG-V: G,E - PIV-AUTH-AES: E - PIV-AUTH-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						CH-AES: E
PIV Authentication (PIV Service)	Authentication by an external system, or authenticates the card holder to an external entity	IND_1	Data to sign	Signature, return Status Word	Digital Signature Generation ECC Digital Signature Generation RSA Encryption - Decryption	CH - PIV-AS-ECC: E - PIV-AUTH-AES: E - PIV-AUTH-CH-AES: E - PIV-AUTH-CH-ECC: E - PIV-AUTH-CH-RSA: E Unauthenticated - PIV-AS-ECC: E - PIV-AUTH-ECC: E - PIV-AUTH-RSA: E - PIV-AUTH-CH-AES: E - PIV-AUTH-CH-ECC: E - PIV-AUTH-CH-RSA: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
PIV Change Reference Data (CRD) (PIV Service)	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.	IND_1	PIN Reference, Current PIN, new PIN	return Status Word	Encryption - Decryption Opacity Secure Channel Message Authentication	CH - OPACITY-SENC: E - OPACITY-SMAC: E - OPACITY-SRMAC: E - OS-MKDK: E - PIV-PC: W,E,Z - PIV-PIN: W,E,Z - PIV-PUK: W,E,Z CHII - OPACITY-SENC: E - OPACITY-SMAC: E - OPACITY-SRMAC: E - OS-MKDK: E - PIV-PC: W,E,Z - PIV-PIN:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E,Z CHPC - OPACITY-SENC: E - OPACITY-SMAC: E - OPACITY-SRMAC: E - PIV-PC: W,E,Z - PIV-PIN: W,E,Z - PIV-PUK: W,E,Z
PIV digital signature (PIV Service)	Digital signature mode pin always	IND_1	off card hash data	Signature, return Status Word	Digital Signature Generation ECC Digital Signature Generation RSA	CH - PIV-AS-ECC: E - PIV-AS-RSA: E - PIV-AUTH-CH-ECC: E - PIV-AUTH-CH-RSA: E CHOCC - PIV-AS-ECC: E - PIV-AS-RSA: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PIV-AUTH-CH-ECC: E - PIV-AUTH-CH-RSA: E
PIV Generate asymmetric key pair (PIV Service)	Generates an RSA or EC Asymmetric Key Pair	IND_1	key reference, algorithm, data	PSP key value, return Status Word	Generate Key Pair EC Generate Key Pair RSA	CAA - OS-DRBG-EI: E - OS-DRBG-KEY: G,E - OS-DRBG-S: E - OS-DRBG-V: G,E - PIV-AKM-ECC: G - PIV-AKM-ECC-PUB: G,R - PIV-AKM-RSA: G - PIV-AKM-RSA-PUB: G,R - PIV-AS-ECC-PUB: G - PIV-AS-RSA: G - PIV-AS-RSA-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PUB: G,R - PIV- AUTH- ECC: G - PIV- AUTH- ECC- PUB: G,R - PIV- AUTH- RSA: G - PIV- AUTH- RSA- PUB: G,R - PIV- AUTH- CH- ECC: G,E - PIV- AUTH- CH- ECC- PUB: G - PIV- AUTH- CH-RSA: G - PIV- AUTH- CH- RSA- PUB: G,R - PIV- SM- ECC: G - PIV- SM- ECC- PUB: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
PIV Get data (PIV Service)	Retrieves the data content of the single data object whose tag is given in the data field.	IND_1	object name	Object data content, return Status Word		CH - MOC-OCC: E - PIV-AKM-ECC-PUB: R - PIV-AKM-RSA-PUB: R - PIV-AS-RSA-PUB: R - PIV-AUTH-ECC-PUB: R - PIV-AUTH-RSA-PUB: R - PIV-AUTH-CH-ECC-PUB: R - PIV-AUTH-CH-RSA-PUB: R - PIV-KS-ECC-PUB: R - PIV-KS-RSA-PUB: R - PIV-PIN: E CHOCC - MOC-OCC: E - PIV-PIN: E CHPC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- MOC-OCC: E - PIV-PIN: E Unauthenticated - MOC-OCC: E - PIV-AUTH-CH-RSA-PUB: R - PIV-PIN: E
PIV KTS (PIV Service)	Used with the key management key ('9D') and the retired key management keys ('82' - '95') to realize key establishment schemes specified in SP 800-78 (ECDH and RSA)	IND_1	Wrapped data to unwrap	Unwrapped data, return status	Key Agreement IFC-Encrypt	CH - ECDH_R KEY: W,E,Z - PIV-AKM-ECC: E - PIV-AKM-RSA: E - PIV-KS-ECC: E - PIV-KS-RSA: E - PIV-SYM-KEY: R,W,Z - PIV-Z: R,G,Z
PIV Put data (PIV Service)	Create, update or	IND_1	object data	return Status Word		CAA - MOC-OCC: W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	deletes an object value in the data model.					- PIV-AKM-ECC: W,Z - PIV-AKM-ECC-PUB: W,Z - PIV-AKM-RSA: W,Z - PIV-AKM-RSA-PUB: W,Z - PIV-AS-ECC: W,Z - PIV-AS-ECC-PUB: W,Z - PIV-AS-RSA: W,Z - PIV-AS-RSA-PUB: W,Z - PIV-AUTH-ECC: W,Z - PIV-AUTH-ECC-PUB: W,Z - PIV-AUTH-RSA: W,Z - PIV-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						AUTH-RSA-PUB: W,Z - PIV-AUTH-CH-AES: W,Z - PIV-AUTH-CH-ECC: W,Z - PIV-AUTH-CH-ECC-PUB: W,Z - PIV-AUTH-CH-RSA: W,Z - PIV-AUTH-CH-RSA-PUB: W,Z - PIV-KS-ECC: W,Z - PIV-KS-ECC-PUB: W,Z - PIV-KS-RSA: W,Z - PIV-KS-RSA-PUB: W,Z - PIV-SM-ECC:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,Z - PIV-SM-ECC-PUB: W,Z - PIV-PIN: Z
PIV Reset Retry Counter (RRC) (PIV Service)	Unblocks and changes the value of a PIN. Secure Messaging is enforced for this command.	IND_1	"Reset retry counter" reference data	return Status Word	Encryption - Decryption	CHII - OS-MKDK: E - PIV-AUTH-CH-AES: E - PIV-PIN: W - PIV-PUK: E
PIV Select (PIV Service)	Selects a DF or an EF by its file ID, path or name (in the case of DFs).	IND_1	Data such as a DF, an EF by its file ID, path or name	return Status Word		CAA CH CHII CHOCC CHPC Unauthenticated
PIV Verify (MOC-OCC) (PIV Service)	Authenticates the user (CHOC C) to the card by presenting the MOC-OCC template	IND_1	finger print reference	return Status Word		CHOCC - MOC-OCC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	e (aka Finger Print or Minutiae). The User Authenticated status is granted with a successful On Card Comparison.					
PIV Verify (PIN) (PIV Service)	Authenticates the user (CH) to the card by presenting the User PIN. The User Authenticated status is granted with a successful PIN verification.	IND_1	Pin reference	return Status Word	Encryption - Decryption	CH - OS-MKDK: E - PIV-PIN: E CHPC - OS-MKDK: E - PIV-PC: E
Request for autotest (Platform service)	Resets specific cryptographic flag to	IND_1	data	return Status Word		Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	request autotest					
Secure Channel (Platform service)	Establish and use a secure communications channel	IND_1	random, diversification data	authentication data, return Status Word	DRBG Encryption - Decryption GP Secure Channel KDF Message Authentication CKG Symmetric	CO - OS-DRBG-EI: E - OS-DRBG-KEY: G,E - OS-DRBG-S: E - OS-DRBG-V: G,E - SD-MDAP-KENC: E - SD-MDAP-KMAC: E - SD-KDEK: E - SD-KENC: E - SD-KMAC: E - SD-MDAP-KDEK: E - SD-SENC: G,E,Z - SD-SMAC: G,E,Z
U2F_Get Version (FIDO service)	Retrieve protocol version implemented by the	IND_1	none	Version return Status Word		Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	authenticator					
Authenticator Select (FIDO service)	Selects the authenticator on the current channel	IND_1	None	return Status Word		Unauthenticated
Manage Content (data) (Platform Service)	PutData Storedata platform command	IND_1	Tags and module information	return Status Word	GP Secure Channel	CO - SD-SENC: E - SD-SMAC: E
PIV Admin MOC-OCC template (PIV Service)	Zeroize and Delete all the MOC-OCC templates.	IND_1	None	return Status Word	GP Secure Channel	CO - MOC-OCC: Z - SD-SENC: E - SD-SMAC: 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.

The module does not support non-approved services.

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. The cryptographic module performs a pair-wise consistency test for every generated public and private key pair.

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 CM meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The CM uses standard passivation techniques and is protected by passive shielding (opaque glue coating) 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

7.2 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.

7.3 Hardness Testing Temperature Ranges

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

Table 15: Hardness Testing Temperatures

8 Non-Invasive Security

No assured mitigations to ‘other attacks’ are covered in this security policy

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

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

PutKey command protected, keys are encrypted by SD-KDEK; key identifier entity association during manufacturing. This command is only used only during manufacturing.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Change Reference Data (CRD)	Entered	FLASH	Plaintext	Manual	Electronic	
CTAP2_ClientPIN_ChangePin	Entered	FLASH	Encrypted	Manual	Electronic	FIDO KTS
CTAP2_ClientPIN_GetKeyAgreement	FLASH	Host	Plaintext	Manual	Electronic	
CTAP2_ClientPIN_SetPin	Entered	FLASH	Plaintext	Manual	Electronic	
CTAP2_ClientPIN_GetPinToken CTAP2_ClientPin_GetPinUvAuthToken UsingPinWithPermissions input	Entered	FLASH	Encrypted	Manual	Electronic	FIDO KTS

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
CTAP2_ClientPIN_GetPinToken CTAP2_ClientPin_GetPinUvAuthToken UsingPinWithPermissions output	FLASH	Host	Encrypted	Automated	Electronic	Encryption - Decryption
CTAP2_GetAssertion CTAP2_GetNextAssertion input	Entered	FLASH	Encrypted	Manual	Electronic	FIDO Authentication
CTAP2_MakeCredential output	FLASH	Host	Encrypted	Manual	Electronic	FIDO Registration
OPACITY Secure Message input	Entered	RAM	Plaintext	Manual	Electronic	
OPACITY Secure Message output	FLASH	Output	Plaintext	Manual	Electronic	
PIV Admin Manage PIN	Entered	FLASH	Encrypted	Manual	Electronic	Encryption - Decryption
PIV Admin Reinit command	Entered	FLASH	Plaintext	Manual	Electronic	
PIV Generate Asymmetric KeyPair	FLASH	Output	Plaintext	Manual	Electronic	
PIV Get Data	FLASH	Output	Plaintext	Manual	Electronic	
PIV KTS input	Entered	RAM	Encrypted	Manual	Electronic	IFC-Encrypt
PIV KTS output	RAM	Output	Plaintext	Manual	Electronic	
PIV Put Data	Entered	FLASH	Plaintext	Manual	Electronic	
PutKey command protected	Entered	FLASH	Encrypted	Manual	Electronic	Encryption - Decryption
Reset Retry Counter (RRC)	Entered	FLASH	Plaintext	Manual	Electronic	

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operation or Initiation
Applet deselection	Deselection of the current applet	Overwrite with zero values	Yes
Authenticator_Reset	Using Authenticator_Reset service	Overwrite with zero values	Yes
Closing secure channel	When the Secure Channel (Platform service) service or the Opacity Secure Message (Platform service) service is terminated, the SSPs linked to the service are erased by overwriting them with zero values.	Overwrite with zero values	Yes
FIDO DeleteCredential	Using FIDO DeleteCredential service. CTAP2_CredentialManagement_DeleteCredential CTAP2_CredentialManagementPreview_DeleteCredential	Overwrite with zero values	Yes
Module entering TERMINATED state	Using the Lifecycle, the module is set to TERMINATED state, through the Set Status command, the SSPs are destroyed by overwriting with zero values	Overwrite with zero values	Yes
PIV Admin MOC-OCC template	Using PIV Admin MOC-OCC template (PIV Service) to zeroize and delete all MOC-OCC templates.	Overwrite with zero values	Yes
PIV Admin Reinit command	Clear the data model content, keeping the data object header but deleting the value of Sensitive Security Parameters and PIV Objects	Overwrite with zero values	Yes
PIV Change Reference Data (CRD)	Using PIV Change Reference Data (CRD) service	Overwrite with zero values	Yes
PIV PUT Data Mode Clear	Using PIV Put Data service in clear mode	Overwrite with zero values	Yes (CO only)
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
Uninstallation of applet	Using the Manage Content service of the CO, the CM is able to destroy the SSPs of the applet, through the Delete command (uninstall method).	Overwrite with zero values	Yes

Zeroization Method	Description	Rationale	Operator Initiation
Zeroize after use	Clear 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

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
- Keys with “OS” prefix are used by the platform operating system
- Keys with “PIV” prefix are used by the PIV Application
- Keys with “FID” prefix are used by the FIDO Application

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DAP-SYM	DAP Signature verification AES CMAC key	128, 192, 256 bits - 128, 192, 256 bits	Signature verification Symmetric Key - CSP	Generated in factory		Message Authentication
ECDH_RKEY	Reader ephemeral public key used for PIV KTS service	P-256, P-384 - 128 bits, 192 bits	Public key - PSP			Key Agreement

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
FID-AT-ECDSA	P-256 private part of the authenticator attestation key pair. The public part is stored in the device attestation certificate. It is used as shared domain for the generation of FID-KG-AS-ECDSA, FID-KG-RK-ECDSA, FID-KG-AS-ECDSA-PUB, FID-KG-RK-ECDSA-PUB, FID-ECDH-ECC, FID-ECDH-ECC-PUB.	P-256 - 128 bits	FIDO authenticator attestation key - CSP	Generated in factory		FIDO Registration
FID-AT-ECDSA-PUB	The public component of the FIDO Authenticator Attestation ECDSA key pair (ECC P-256)	P-256 - 128 bits	FIDO Authenticator attestation public key - PSP	Generated in factory		
FID-ECDH-ECC	P-256 private part of the ECDH key pair used for shared secret mechanism	P-256 - 128 bits	FIDO ephemeral private key - CSP	Generate Key Pair EC		Key Agreement
FID-ECDH-ECC-PUB	P-256 public part of the ECDH key pair used for shared key mechanism	P-256 - 128 bits	FIDO ephemeral public key - PSP	Generate Key Pair EC		
FID-HMAC-NONCE	256 bits key, used to process the HMAC-secret extension (for non-Resident Credential)	256 bits - 256 bits	FIDO key associated to the HMAC-secret extension nonce - CSP		KDA HKDF	HMAC
FID-KG-AS-ECDSA	P-256 private part of the user key pair used in services CTAP2_MakeCredential, CTAP2_GetAssertion, CTAP12_GETNextAssertion	P-256 - 128 bits	FIDO authentication key - CSP	FIDO Registration		FIDO Authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
FID-KG-AS-ECDSA-PUB	P-256 public part of the user key pair	P-256 - 128 bits	FIDO authentication public key - CSP	FIDO Registration		
FID-KG-RK-ECDSA	P-256 private part of the user key pair ECDSA for Discoverable Credential	P-256 - 128 bits	FIDO Registration private key - CSP	FIDO Registration		Digital Signature Generation ECC
FID-KG-RK-ECDSA-PUB	P-256 public part of the user key pair ECDSA for Discoverable Credential	P-256 - 128 bits	FIDO discoverable credential public key - PSP	FIDO Registration		
FID-PIN-KEY	The authenticator secret key used for decryption of PIN (FID-UV-PIN); AES CBC 256 bits key.	256 bits - 256 bits	FIDO PIN Decryption key - CSP	KDA HKDF		Encryption - Decryption
FID-PLAT-ECDH-PUB	P-256 public part of the ECDH key pair from the server used for shared key mechanism.	P-256 - 128 bits	FIDO ephemeral public key - PSP			Key Agreement
FID-RK-HMAC-NONCE	256 bits nonce, used to process the HMAC-secret extension for Discoverable Credential	256 bits - 256 bits	FIDO key associated to the HMAC-secret extension nonce for resident key - CSP	FIDO Registration		HMAC
FID-SC-AUTH-HMAC	HMAC 128-bit authenticator secret key used for authentication of key handles with HMAC-SHA256 used in services U2F_Register,	128 bits - 128 bits	FIDO authenticator authentication	FIDO Registration		FIDO KTS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	U2F_Authenticate, CTAP2_MakeCredential, CTAP2_GetAssertion, CTAP12_GETNextAssertion		key - CSP			
FID-SC-ENC-AES	AES authenticator secret key used for encryption and decryption of key handles with AES CBC used in services CTAP2_MakeCredential, CTAP2_GetAssertion, CTAP12_GETNextAssertion.	128 bits - 128 bits	FIDO authenticator encryption decryption key - CSP	CKG Symmetric Generated in factory		FIDO KTS
FID-SEED	Used on CTAP2_MakeCredential, CTAP2_GetAssertion or CTAP2_GetNextAssertion, services.	256 bits - 256 bits	FIDO nonce - CSP	Generated in factory		KDA HKDF
FID-SHARED-SECRET	The shared secret established during client pin key agreement in service CTAP2_ClientPIN_GetKeyAgreement	256 bits - 256 bits	FIDO signature key - CSP	KDA HKDF		HMAC
FID-SHARED-SECRET-INTER	The shared secret established during client pin key agreement in service CTAP2_ClientPIN_GetKeyAgreement.	256 bits - 128 bits	FIDO signature key - CSP		Key Agreement	KDA HKDF
FID-TOKEN-NONCE-V2	256 bits nonce used to authenticator client commands in the Client PIN protocol V2 (equivalent to a session PIN) in services CTAP2_ClientPIN_GetPinToken and CTAP2_ClientPin_GetPinUvAuthTokenUsingPinWithPermissions	256 bits - 256 bits	FIDO nonce - CSP	CKG Symmetric		HMAC FIDO KTS
FID-UV-PIN	The reference user verification data (6 to 63 bytes) used to authenticate the user.	48-504 bits - 48-504 bits	FIDO User PIN code - CSP			Secure Hash
FID-UV-PIN-Hash	Hash value of FID-UV-PIN	256 bits - 256 bits	Hash value of FID-UV-	Secure Hash		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
			PIN - CSP			
MOC-OCC	MoC template (or Finger Print / Minutiae) for On Card Comparison (OCC) according to [SP800-76-2].	1968 bits (246 bytes max in update apdu command so 82 Minutiae max) - 1968 bits	Authentication data - CSP			
OPACITY-SCONFIRMATION	Card OPACITY Secure Messaging Session Confirmation Key (AES CMAC)	128, 192 bits - 128, 192 bits	Signature generation confirmation Symmetric Key - CSP		Opacity Secure Channel	Opacity Secure Channel
OPACITY-SENC	Card OPACITY Secure Messaging Session Encryption AES ECB/CBC Key	128, 256 bits - 128 bits, 256 bits	Encryption Symmetric Key - CSP		Opacity Secure Channel	Encryption - Decryption
OPACITY-SMAC	Card OPACITY Secure Messaging Session MAC AES ECB/CBC Key	128, 192 bits - 128, 192 bits	Signature verification Symmetric Key - CSP		Opacity Secure Channel	Message Authentication
OPACITY-SRMAC	Card OPACITY Secure Messaging Session	128, 192 bits -	Signature generation		Opacity Secur	Message

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Response MAC AES-128/192/256 Key	128, 192 bits	on Symmetric Key - CSP		e Channel	Authentication
OPACITY-Z	Shared secret generated during opacity secure channel establishment	256 bits - 256 bits	Shared secret - CSP		Opacity Secure Channel	Opacity Secure Channel
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		Counter DRBG (A2877)
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)		Counter DRBG (A2877)
OS-DRBG-S	Seed 48 bytes seed output from AES_DF used for instantiation of the [SP800-90Ar1] DRBG implementation	384 bits - 256 bits	Seed - CSP	Entropy Source		Counter DRBG (A2877)
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)		Counter DRBG (A2877)
OS-MKDK	Encryption key AES CBC/ECB	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Encryption Symmetric Key - CSP	Generated in factory		Encryption - Decryption
PIV-AKM-ECC	PIV Key Management Key (9D): P-256 or P-384 Private part of ECC key pair used to compute a shared secret.	P-256, P-384 - 128	Asymmetric private	Generate Key Pair EC		Key Agreement

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Using this key authenticates the card holder to an external entity (physical access rights).	bits, 192 bits	Key - CSP			
PIV-AKM-ECC-PUB	PIV Key Management Key (9D): P-256 or P-384 public part of ECC key pair used for Key Management	P-256, P-384 - 128 bits, 192 bits	Decryption asymmetric public Key - PSP	Generate Key Pair EC		
PIV-AKM-RSA	PIV Key Management Key (9D): used to realize key establishment schemes specified in SP 800-78	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Asymmetric private Key - CSP	Generate Key Pair RSA		IFC-Encrypt
PIV-AKM-RSA-PUB	PIV Key Management Key (9D): Public part of the RSA key pair used for Key Management.	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Decryption asymmetric public Key - PSP	Generate Key Pair RSA		
PIV-AS-ECC	PIV Digital Signature Key (9C): used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).	P-256, P-384 - 128 bits, 192 bits	Signature generation asymmetric private Key - CSP	Generate Key Pair EC		Digital Signature Generation ECC
PIV-AS-ECC-PUB	PIV Digital Signature Key (9C): used for Asymmetric	P-256,	Signature	Generate Key		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	signature (Asymmetric key protected by PIN Always used for signature).	P-384 - 128 bits, 192 bits	generation asymmetric public Key - PSP	Pair EC		
PIV-AS-RSA	PIV Digital Signature Key (9C): used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Signature generation asymmetric private Key - CSP	Generate Key Pair RSA		Digital Signature Generation RSA
PIV-AS-RSA-PUB	PIV Digital Signature Key (9C): used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Signature generation asymmetric public Key - PSP	Generate Key Pair RSA		
PIV-AUTH-AES	PIV Card Application Administration ECB/ CBC AES-128/192/256 key (9B): used by the PIV Applet. External authenticate using this key grant CAA rights	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Symmetric encryption / decryption key - CSP			Encryption - Decryption
PIV-AUTH-ECC	PIV authentication Key (9A): Used to encrypt a challenge (nonce). Internal authenticate using this key, in combination with PIN	P-256, P-384 - 128 bits,	Authentication asymmetric private	Generate Key Pair EC		Digital Signature Generation ECC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	verification, authenticates the CAA to an external entity (physical access rights).	192 bits	Key - CSP			
PIV-AUTH-ECC-PUB	PIV authentication Key (9A): P-256 or P-384 public part of ECC key pair used for Authentication	P-256, P-384 - 128 bits, 192 bits	Authentication public key - PSP	Generate Key Pair EC		
PIV-AUTH-RSA	PIV authentication Key (9A): Used to encrypt a challenge (nonce). Internal authenticate using this key, in combination with PIN verification, authenticates the card holder to an external entity (physical access rights).	2048 bits - 112 bits	Authentication asymmetric private Key - CSP	Generate Key Pair RSA		Digital Signature Generation RSA
PIV-AUTH-RSA-PUB	PIV authentication Key (9A): Public part of the RSA key pair used for Authentication	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Authentication public key - PSP	Generate Key Pair RSA		
PIV-AUTH-CH-AES	PIV Card Authentication Key (9E): used by the PIV Applet. Internal authenticate using this key authenticates the card holder to an external entity (physical access rights).	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Symmetric encryption / decryption key - CSP			Encryption - Decryption
PIV-AUTH-CH-ECC	PIV Card Authentication Key (9E): used to sign a challenge (nonce). Internal authenticate using this key authenticates the card holder	P-256, P-384 - 128 bits,	Authentication asymmetric private	Generate Key Pair EC		Digital Signature Generation ECC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	to an external entity (physical access rights).	192 bits	Key - CSP			
PIV-AUTH-CH-ECC-PUB	PIV Card Authentication Key (9E): used for Internal authenticate using to authenticate the card holder (physical access rights). Used to decrypt a challenge. Using this key authenticates the card holder to an external entity (physical access rights).	P-256, P-384 - 128 bits, 192 bits	Decryption asymmetric public Key - PSP	Generate Key Pair EC		
PIV-AUTH-CH-RSA	PIV Card Authentication Key (9E): used to sign a challenge (nonce). Internal authenticate using this key authenticates the card holder to an external entity (physical access rights).	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Authentication asymmetric private Key - CSP	Generate Key Pair RSA		Digital Signature Generation RSA
PIV-AUTH-CH-RSA-PUB	PIV Card Authentication Key (9E): used for Internal authenticate using to authenticate the card holder (physical access rights). Used to decrypt a challenge. Using this key authenticates the card holder to an external entity (physical access rights)	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Decryption asymmetric public Key - PSP	Generate Key Pair RSA		
PIV-KS-ECC	Retired Key Management (82 up to 95): P-256 or P-384 Private part of ECC key pair corresponding to a certificate that has expired, been revoked, or has otherwise been superseded. Managed by PIV Card application Crypto Officer to store keys history	P-256, P-384 - 128 bits, 192 bits	Asymmetric private Key - CSP			Key Agreement

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PIV-KS-ECC-PUB	Retired Key Management (82 up to 95): used for Key Storage, managed by PIV Card application Crypto Officer to store keys history	P-256, P-384 - 128 bits, 192 bits	Retired public Key - PSP			
PIV-KS-RSA	Retired Key Management (82 up to 95): Private part of the RSA key pair corresponding to a certificate that has expired, been revoked, or has otherwise been superseded. Managed by PIV Card application Crypto Officer to store keys history.	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Asymmetric Private Key - CSP			IFC-Encrypt
PIV-KS-RSA-PUB	Retired Key Management (82 up to 95): used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.	2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 140 bits	Retired public Key - PSP			
PIV-PC	PIV card Pairing Code: 8 byte-long, used for Virtual Contact Interface (VCI), in numerical format.	64 bits - 64 bits	Pairing Code - CSP	Generated in factory		Encryption - Decryption
PIV-PIN	Between 6 and 8 byte-long, PIV Card Application PIN (Local PIN 80, Global PIN 00), in numerical format	64 bits - 64 bits	Personal Identification Number - CSP	Generated in factory		Encryption - Decryption
PIV-PUK	8 byte-long PIV card PUK (81) and may be any 8-byte binary value. That is, the bytes comprising the PUK may have any value in the range 0x00 - 0xFF.	64 bits - 64 bits	Personal Unblock PIN - CSP	Generated in factory		Encryption - Decryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PIV-SM-ECC	PIV Card OPACITY Secure Messaging Key (04): for PIV Secure Messaging Establishment, aka OPACITY (ECC-P-256 or P-384).	P-256, P-384 - 128 bits, 192 bits	Asymmetric private Key - CSP	Generate Key Pair EC		Opacity Secure Channel
PIV-SM-ECC-PUB	Used for OPACITY PIV Secure Messaging Establishment.	P-256, P-384 - 128 bits, 192 bits	Public - PSP	Generate Key Pair EC		
PIV-SYM-KEY	Unwrapped key. The unwrapped key is for the outside system and is not used by the module.	80 - 256 bits - 80 - 256 bits	Encryption decryption AES-128/192/256 key - Neither			
PIV-Z	Shared secret generated during key agreement.	256 bits - 256 bits	Shared secret - CSP		Key Agreement	
ROE-PUB	Reader ephemeral public key used for opacity.	256, 384 bits - 128 bits, 192 bits	Public - PSP			Opacity Secure Channel
SD-MDAP-KENC	Derivation AES ECB/CBC key for SD with MDAP	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Decryption Key AES-128/192/256 key for SD with MDA - CSP	Generated in factory		Encryption - Decryption
SD-MDAP-KMAC	Derivation Key AES ECB/CBC Key for SD with MDAP	128, 192, 256 bits -	Signature verification on Key	Generated in factory		Message Authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128, 192, 256 bits	AES-128/192/256 key for SD with MDAP - CSP			
SD-KDEK	Encryption decryption AES CBC/ECB key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Encryption / Decryption Symmetric Key - CSP	Generated in factory		Encryption - Decryption
SD-KENC	Derivation Key AES CBC/ECB master key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Derivation Symmetric Key - CSP	Generated in factory		KDF
SD-KMAC	Derivation Key AES CBC/ECB master key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Derivation Symmetric Key - CSP	Generated in factory		KDF
SD-MDAP-KDEK	Encryption decryption AES ECB/CBC key for SD with MDAP	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Encryption decryption AES-128/192/256 key for SD with	Generated in factory		Encryption - Decryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		256 bits	MDAP - CSP			
SD-SENC	Session decryption AES ECB/CBC key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Decryption Symmetric Key - CSP	KDF		Encryption - Decryption GP Secure Channel
SD-SMAC	Session Signature verification AES ECB/CBC/CMAC key	128, 192, 256 bits - 128 bits, 192 bits, 256 bits	Signature verification Symmetric Key - CSP	KDF		GP Secure Channel Message Authentication

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DAP-SYM	PutKey command protected	FLASH:Plaintext		Module entering TERMINATED state	SD-MDAP-KDEK:Encrypted by
ECDH_RKEY	PIV KTS input	RAM:Plaintext	Automatically zeroized after use	Zeroize after use	PIV-Z:Derives PIV-KS-ECC:Used with PIV-AKM-ECC:Used with
FID-AT-ECDSA	CTAP2_MakeCredential output	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	FID-AT-ECDSA-PUB:Paired With
FID-AT-ECDSA-PUB	CTAP2_MakeCredential output	FLASH:Plaintext		Module entering TERMINATED state	FID-AT-ECDSA:Paired With FID-SC-ENC-AES:Wrapped

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Uninstallati on of applet	by FID-SC-AUTH- HMAC:Authenti cated by FID-KG-AS- ECDSA:Used With
FID- ECDH- ECC		FLASH:Pla intext	Duratio n of Module session	Module entering TERMINAT ED state Power- cycling the module	FID-ECDH- ECC- PUB:Paired With FID-SHARED- SECRET- INTER:Derives OS-DRBG- KEY:Generated by OS-DRBG- V:Generated by
FID- ECDH- ECC-PUB	CTAP2_ClientPIN_Get KeyAgreement	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet	FID-ECDH- ECC:Paired With OS-DRBG- KEY:Generated by OS-DRBG- V:Generated by
FID- HMAC- NONCE		RAM:Pla intext	Duratio n of Fido session	Module entering TERMINAT ED state Power- cycling the module	FID- SEED:Derived from
FID-KG- AS- ECDSA		FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet	FID-KG-AS- ECDSA- PUB:Paired With FID-SC-ENC- AES:Wrapped by FID-SC-ENC- AES:Unwrappe d by FID-SC-Auth- HMAC:Authenti cated by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
FID-KG-AS-ECDSA-PUB	CTAP2_MakeCredential output	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	FID-KG-AS-ECDSA:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
FID-KG-RK-ECDSA		FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet FIDO DeleteCredential	FID-KG-RK-ECDSA-PUB:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
FID-KG-RK-ECDSA-PUB	CTAP2_MakeCredential output	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet FIDO DeleteCredential	FID-KG-RK-ECDSA:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
FID-PIN-KEY		RAM:Plaintext	Duration of FIDO session	Module entering TERMINATED state Uninstallation of applet Applet deselection	FID-SHARED-SECRET-INTER:Derived From FID-UV-PIN:Wrapps FID-TOKEN-NONCE-V2:Encrypts
FID-PLAT-ECDH-PUB	CTAP2_ClientPIN_ChangePin CTAP2_ClientPIN_SetPin CTAP2_ClientPIN_GetPinToken CTAP2_ClientPin_Get	RAM:Plaintext	Duration of the key agreement	Zeroise after use	FID-SHARED-SECRET-INTER:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	PinUvAuthToken UsingPinWithPermissions input				
FID-RK-HMAC-NONCE		FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet Authentication or Reset	OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
FID-SC-AUTH-HMAC		FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	FID-KG-AS-ECDSA:Authenticates FID-KG-RK-ECDSA:Authenticates FID-UV-PIN:Authenticates SD-SENC:Wrapped by SD-SMAC:Authenticated by OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
FID-SC-ENC-AES		FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	FID-KG-AS-ECDSA:Wraps FID-KG-AS-ECDSA:Unwraps FID-KG-RK-ECDSA:Wraps FID-UV-PIN:Wraps SD-SENC:Wrapped by SD-SMAC:Authenticated by OS-DRBG-

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					KEY:Generated by OS-DRBG-V:Generated by
FID-SEED	CTAP2_GetAssertion CTAP2_GetNextAssertion input CTAP2_MakeCredential output	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by FID-KG-AS-ECDSA:Derives FID-KG-RK-ECDSA:Derives FID-HMAC-NONCE:Derives
FID-SHARED-SECRET		RAM:Plaintext	Duration of key establishment	Power-cycling the module Zeroise after use	FID-SHARED-SECRET-INTER:Derived From
FID-SHARED-SECRET-INTER		RAM:Plaintext	Duration of Module session	Zeroise after use	FID-ECDH-ECC:Derived from FID-PLAT-ECDH-PUB:Derived from FID-PIN-KEY:Derives FID-SHARED-SECRET:Derives
FID-TOKEN-NONCE-V2	CTAP2_ClientPIN_GetPinToken CTAP2_ClientPin_GetPinUvAuthToken UsingPinWithPermissions output	RAM:Plaintext	Duration of Module session	Module entering TERMINATED state Power-cycling the module	OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by FID-PIN-KEY:Encrypted by
FID-UV-PIN	CTAP2_ClientPIN_ChangePin CTAP2_ClientPIN_GetPinToken CTAP2_ClientPin_GetPinUvAuthToken	FLASH:Obscured		Authenticate or_Reset Module entering TERMINATED state	FID-UV-PIN-Hash:Derives FID-SHARED-SECRET:Authenticated by FID-PIN-

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	UsingPinWithPermissions input			Uninstallati on of applet	KEY:Wrapped by
FID-UV- PIN-Hash	CTAP2_ClientPIN_Ch angePin CTAP2_ClientPIN_Get PinToken CTAP2_ClientPin_Get PinUvAuthToken UsingPinWithPermissi ons input	FLASH:En crypte		Authenticat or_Reset Module entering TERMINAT ED state Uninstallati on of applet	FID-UV- PIN:Derived from OS- MKDK:Encrypte d by
MOC-OCC	PIV Put Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin MOC-OCC template	
OPACITY- SCONFIR MATION	OPACITY Secure Message output	RAM:Plaint ext	Duratio n of SCP secure channel	Power- cycling the module Closing secure channel Module entering TERMINAT ED state	OPACITY- Z:Derived From
OPACITY- SENC		RAM:Plaint ext	Duratio n of SCP secure channel	Power- cycling the module Closing secure channel Module entering TERMINAT ED state	OPACITY- Z:Derived From PIV-PIN:Wraps
OPACITY- SMAC		RAM:Plaint ext	Duratio n of SCP secure channel	Power- cycling the module Closing secure	OPACITY- Z:Derived From PIV- PIN:Authenticat es

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				channel Module entering TERMINATED state	
OPACITY-SRMAC		RAM:Plaintext	Duration of SCP secure channel	Power-cycling the module Closing secure channel Module entering TERMINATED state	OPACITY-Z:Derived From
OPACITY-Z		RAM:Plaintext	Duration of SCP secure channel	Zeroise after use	PIV-SM-ECC:Derived From ROE-PUB:Derived From OPACITY-SENC:Derives OPACITY-SMAC:Derives OPACITY-SRMAC:Derives OPACITY-SCONFIRMATION:Derives
OS-DRBG-EI		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-KEY		RAM:Plaintext	Duration of the module session	Module entering TERMINATED state Power-cycling the module	OS-DRBG-S:Derived From OS-DRBG-EI:Derived From FID-ECDH-ECC:Generates FID-KG-AS-ECDH:Generates

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					tes FID-KG-RK- ECDSA:Genera tes FID-RK-HMAC- NONCE:Gener ates FID- SEED:Generat es FID-TOKEN- NONCE- V2:Generates PIV-AS- ECC:Generates PIV-AKM- RSA:Generates PIV-AKM- ECC:Generates PIV-AS- RSA:Generates PIV-AUTH- ECC:Generates PIV-AUTH- RSA:Generates PIV-AUTH_CH- ECC:Generates PIV-AUTH_CH- RSA:Generates PIV-SM- ECC:Generates FID-SC-AUTH- HMAC:Generat es FID-SC-ENC- AES:Generates
OS- DRBG-S		RAM:Plaint ext	Duratio n of the module session	Module entering TERMINAT ED state Power- cycling the module	OS-DRBG- V:Derives OS-DRBG- KEY:Derives
OS- DRBG-V		RAM:Plaint ext	Duratio n of the module session	Module entering TERMINAT ED state	OS-DRBG- S:Derived From OS-DRBG- EI:Derived

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Power-cycling the module	From FID-ECDH-ECC:Generates FID-KG-AS-ECDSA:Generates FID-KG-RK-ECDSA:Generates FID-RK-HMAC-NONCE:Generates FID-SEED:Generates FID-TOKEN-NONCE-V2:Generates PIV-AS-ECC:Generates PIV-AKM-RSA:Generates PIV-AKM-ECC:Generates PIV-AS-RSA:Generates PIV-AUTH-ECC:Generates PIV-AUTH-RSA:Generates PIV-AUTH_CH-ECC:Generates PIV-AUTH_CH-RSA:Generates PIV-SM-ECC:Generates FID-SC-AUTH-HMAC:Generates FID-SC-ENC-AES:Generates
OS-MKDK	PutKey command protected	FLASH:Plaintext		Module entering TERMINATED state	PIV-PIN:Encrypts PIV-PC:Encrypts PIV-PUK:Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					PIV-UV-PIN-Hash:Encrypts SD-KDEK:Wrapped by
PIV-AKM-ECC	PIV Put Data	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AKM-ECC-PUB:Paired With ECDH_RKEY:Used with PIV-Z:Derives OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
PIV-AKM-ECC-PUB	PIV Put Data PIV Get Data PIV Generate Asymmetric KeyPair	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AKM-ECC:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
PIV-AKM-RSA	PIV Put Data	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AKM-RSA-PUB:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by PIV-SYM-KEY:Decrypts
PIV-AKM-RSA-PUB	PIV Put Data PIV Get Data PIV Generate Asymmetric KeyPair	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-AKM-RSA:Paired With OS-DRBG-KEY:Generated by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				PIV PUT Data Mode Clear PIV Admin Reinit command	OS-DRBG- V:Generated by
PIV-AS-ECC	PIV Put Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AS-ECC- PUB:Paired With OS-DRBG- KEY:Generated by OS-DRBG- V:Generated by
PIV-AS-ECC-PUB	PIV Put Data PIV Get Data PIV Generate Asymmetric KeyPair	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AS- ECC:Paired With OS-DRBG- KEY:Generated by OS-DRBG- V:Generated by
PIV-AS-RSA	PIV Put Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AS-RSA- PUB:Paired With OS-DRBG- KEY:Generated by OS-DRBG- V:Generated by
PIV-AS-RSA-PUB	PIV Put Data PIV Get Data PIV Generate Asymmetric KeyPair	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati	PIV-AS- RSA:Paired With OS-DRBG- KEY:Generated

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	by OS-DRBG- V:Generated by
PIV-AUTH-AES	PIV Put Data PIV Admin Reinit command	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear	
PIV-AUTH-ECC	PIV Put Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AUTH-ECC-PUB:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
PIV-AUTH-ECC-PUB	PIV Put Data PIV Get Data PIV Generate Asymmetric KeyPair	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AUTH-ECC:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
PIV-AUTH-RSA	PIV Put Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT	PIV-AUTH-RSA-PUB:Paired With OS-DRBG-KEY:Generated by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Data Mode Clear PIV Admin Reinit command	OS-DRBG-V:Generated by
PIV-AUTH-RSA-PUB	PIV Put Data PIV Get Data PIV Generate Asymmetric KeyPair	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AUTH-RSA:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
PIV-AUTH-CH-AES	PIV Put Data	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet PIV PUT Data Mode Clear PIV Admin Reinit command	
PIV-AUTH-CH-ECC	PIV Put Data	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AUTH-CH-ECC-PUB:Paired With OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
PIV-AUTH-CH-ECC-PUB	PIV Put Data PIV Get Data PIV Generate Asymmetric KeyPair	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet	PIV-AUTH-CH-ECC:Paired With OS-DRBG-KEY:Generated by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				PIV PUT Data Mode Clear PIV Admin Reinit command	OS-DRBG- V:Generated by
PIV-AUTH-CH-RSA	PIV Put Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AUTH-CH- RSA- PUB:Paired With OS-DRBG- KEY:Generated by OS-DRBG- V:Generated by
PIV-AUTH-CH-RSA-PUB	PIV Put Data PIV Get Data PIV Generate Asymmetric KeyPair	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-AUTH-CH- RSA:Paired With OS-DRBG- KEY:Generated by OS-DRBG- V:Generated by
PIV-KS-ECC	PIV Put Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-KS-ECC- PUB:Paired With PIV-Z:Derives ECDH_RKEY:U sed with
PIV-KS-ECC-PUB	PIV Put Data PIV Get Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati	PIV-KS- ECC:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	
PIV-KS-RSA	PIV Put Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-KS-RSA- PUB:Paired With PIV-SYM- KEY:Decrypts
PIV-KS-RSA-PUB	PIV Put Data PIV Get Data	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-KS- RSA:Paired With
PIV-PC	PIV Put Data Change Reference Data (CRD) Reset Retry Counter (RRC) PIV Admin Manage PIN	FLASH:Pla intext		Module entering TERMINAT ED state Uninstallati on of applet PIV Change Reference Data (CRD)	OS- MKDK:Encrypte d with SD- SENC:Unwrapp ed by SD- SMAC:authenti cated by
PIV-PIN	Change Reference Data (CRD) Reset Retry Counter (RRC) PIV Admin Manage PIN	FLASH:En crypted		Module entering TERMINAT ED state Uninstallati on of applet	OS- MKDK:Encrypte d by OS-DRBG- KEY:Generated by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				PIV PUT Data Mode Clear PIV Admin Reinit command	SD-SMAC:Unwrapped by SD-SMAC:Authenticated by
PIV-PUK	Change Reference Data (CRD) PIV Admin Manage PIN	FLASH:Encrypted		Module entering TERMINATED state Uninstallation of applet PIV Change Reference Data (CRD)	OS-MKDK:Encrypted with SD-SENC:Unwrapped by SD-SMAC:Authenticated by
PIV-SM-ECC	PIV Put Data	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-SM-ECC-PUB:Paired With OPACITY-Z:Derives SD-KDEK:Encrypted by OS-DRBG-KEY:Generated by OS-DRBG-V:Generated by
PIV-SM-ECC-PUB	PIV Put Data OPACITY Secure Message output PIV Generate Asymmetric KeyPair	FLASH:Plaintext		Module entering TERMINATED state Uninstallation of applet PIV PUT Data Mode Clear PIV Admin Reinit command	PIV-SM-ECC:Paired With OPACITY-Z:Derives SD-KDEK:Encrypted by
PIV-SYM-KEY	PIV KTS output PIV KTS input	RAM:Plaintext	Duration of service execution	Zeroise after use	PIV-KS-RSA:Decrypted by PIV-AKM-RSA:Decrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
PIV-Z	PIV KTS output	RAM:Plaintext	Duration of service execution	Zeroise after use	PIV-KS-ECC:Derived from ECDH_RKEY:Derived from PIV-AKM-ECC:Derived from
ROE-PUB	OPACITY Secure Message input	FLASH:Plaintext	Duration of SCP secure channel	Module entering TERMINATED state Closing secure channel	OPACITY-Z:Derives PIV-SM-ECC:Used with
SD-MDAP-KENC	PutKey command protected	FLASH:Plaintext		Module entering TERMINATED state	SD-MDAP-KDEK:Encrypted by
SD-MDAP-KMAC	PutKey command protected	FLASH:Plaintext		Module entering TERMINATED state	SD-MDAP-KDEK:Encrypted by
SD-KDEK	PutKey command protected	FLASH:Plaintext		Module entering TERMINATED state	SD-KENC:Encrypts SD-KMAC:Encrypts SD-KDEK:Encrypts PIV-SM-ECC:Encrypts PIV-SM-ECC-PUB:Encrypts OS-MKDK:Encrypts
SD-KENC	PutKey command protected	FLASH:Plaintext		Module entering TERMINATED state	SD-SENC:Derives SD-KDEK:Encrypted by
SD-KMAC	PutKey command protected	FLASH:Plaintext		Module entering TERMINATED state	SD-SMAC:Derives SD-KDEK:Encrypted by
SD-MDAP-KDEK	PutKey command protected	FLASH:Plaintext		Module entering	SD-MDAP-KDEK:Encrypted

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				TERMINATED state	d by SD-MDAP-KDEK:Encrypts SD-MDAP-KENC:Encrypts DAP-SYM:Encrypts SD-MDAP-KMAC:Encrypts
SD-SENC		RAM:Plaintext	Duration of SCP secure channel	Power-cycling the module Closing secure channel Module entering TERMINATED state	SD-KENC:Derived From
SD-SMAC		RAM:Plaintext	Duration of SCP secure channel	Power-cycling the module Closing secure channel Module entering TERMINATED state	SD-KMAC:Derived From

Table 20: SSP Table 2

9.5 Transitions

Per Table 4: Security strength time frames in Section 5.6.3 Projected Security Strength Time Frames and Current Approval Status of SP 800-57 Part 1 Revision 5 all key sizes less than 128-bits will be disallowed on January 1, 2031.

10 Self-Tests

The module maintains a flag in RAM memory that stores the state (self-test passed or not) for each Cryptographic algorithm that is approved.

- Each algorithm is self-tested, and has a specific flag
- This flag indicates if self-test has been correctly executed or not
- This information is stored into a global bitfield in RAM

Default value of this bitfield after power up may correspond to the state “self-test not executed.

10.1 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).

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Integrity Test	N/A	EDC (16-bit CRC)	SW/FW Integrity	Bit 32 of flag set to 1	Comparison with known value

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

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.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SP 800-90B APT	Statistic error event	Fault-Detection test	CAST	IND_2	TRNG error	N/A
AES ECB Decrypt	Decrypt KAT using an AES 128-bit key in ECB mode.	KAT	CAST	Bit 18 of flag set to 1	Decrypt	COND_1
Counter DRBG	Gets a random value with specific nonce (48 bytes) and entropy (128 bytes) and compares the	KAT	CAST	Bit 3 of flag set to 1	none	COND_1

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	generated random value with the value stored in ROM. Performs DRBG Instantiate and DRBG Generate per SP 800-90Ar1 Section 11.3 including health test .					
ECDSA KeyGen	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
ECDSA Signature Generation	ECDSA signature generation using an ECC P-224 key	KAT	CAST	Bit 30 of flag set to 1	Sign	COND_1
Firmware Load	Signature verification with AES CMAC (256 bits key)	Signature	SW/FW Load	IND_4	Signature verification with AES CMAC	COND_3
HMAC-SHA2-256	Compute HMAC with key 16 bytes message 24 bytes	KAT	CAST	Bit 10 of flag set to 1	HMAC	COND_1
KAS-ECC Sp800-56Ar3 OnePassDH C2	Performs OnePassDH algorithm relying on Crypto Suite2	KAT	CAST	Bit 6 of flag set to 1	AES 128, ECDSA (Curve P-256) with SHA2-256	COND_1
KAS-ECC Sp800-56Ar3 OnePassDH C7	Performs OnePassDH algorithm relying on Crypto Suite 7	KAT	CAST	Bit 7 of flag set to 1	(AES 256, ECDSA (Curve P-384) with SHA2-384)	COND_1
KAS-ECC-SSC	Generate standalone shared secret (SP800-56Ar3)	KAT	CAST	Bit 29 of flag set to 1	KAS-ECC-SSC Sp800-56Ar3 (ECDH P224)	COND_1
KDA HKDF	Performs a Key derivation (RFC5869) and verifies result	KAT	CAST	Bit 7 of flag set to 1	Key derivation	COND_1

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDA OneStep SP800-56Cr2	Performs a Key derivation and verifies result.	KAT	CAST	Bit 2 of flag set to 1	Key derivation	COND_1
KDF SP 800-108r1 Encrypt/Sign	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
IFC-Encrypt	Performs an RSA decrypt using an RSA 2048-bit public key implementation	KAT	CAST	Bit 26 of flag set to 1	Decrypt	COND_1
RSA Key Generation	Performs Signature Generation and Signature Verification using the key pair	PCT	PCT	IND_3	Signature Generation and Verification	COND_2
RSA Signature Generation (CRT)	Performs an RSA PKCS#1 v1.5 signature generation using an RSA 2048-bit private CRT key implementation	KAT	CAST	Bit 28 of flag set to 1	RSA Signature generation	COND_1
RSA Signature Generation (STD)	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	RSA SigGen STD, RSA encrypt	COND_1
SHA2-256	SHA2-256: hashes a 24-bytes message	KAT	CAST	Bit 22 of flag set to 1	Hash	COND_1
SHA2-512	SHA2-512: hashes a 24-bytes message	KAT	CAST	Bit 23 of flag set to 1	Hash	COND_1
SP 800-90B RCT	Entropy error event	Fault-Detection test	CAST	IND_2	TRNG error	N/A

Table 22: Conditional Self-Tests

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

The cryptographic KATs are executed automatically, in a mode named “on demand”, when a cryptographic service is requested.

Self-tests can be also played by any operator using the “autotests management” APDU command, corresponding to the “Request for autotest” service. The operator can choose the list of self-test execution giving in data of the APDU the self-test flag.

10.3 Periodic Self-Test Information

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 its zero, the integrity test is executed (see 10.1), the counter is reset to its maximum value again and the flag for on-demand tests is also reset so that at next cryptographic algorithm usage, the self-tests are executed again (see 10.2). No interruption to the module’s operation is expected while the self-tests are executed.

The periodic counter is stored in RAM and defined during the init flow.

The KATs may be run on demand by restarting the module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Integrity Test	EDC (16-bit CRC)	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
SP 800-90B APT	Fault-Detection test	CAST	N/A	N/A
AES ECB Decrypt	KAT	CAST	Periodic counter value	Count of APDU received by the CM
Counter DRBG	KAT	CAST	Periodic counter value	Count of APDU received by the CM
ECDSA KeyGen	PCT	PCT	N/A	N/A
ECDSA Signature Generation	KAT	CAST	Periodic counter value	Count of APDU received by the CM
Firmware Load	Signature	SW/FW Load	N/A	N/A
HMAC-SHA2-256	KAT	CAST	Periodic counter value	Count of APDU received by the CM
KAS-ECC Sp800-56Ar3 OnePassDH C2	KAT	CAST	Periodic counter value	Count of APDU received by the CM
KAS-ECC Sp800-56Ar3 OnePassDH C7	KAT	CAST	Periodic counter value	Count of APDU received by the CM

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC	KAT	CAST	Periodic counter value	Count of APDU received by the CM
KDA HKDF	KAT	CAST	Periodic counter value	Count of APDU received by the CM
KDA OneStep SP800-56Cr2	KAT	CAST	Periodic counter value	Count of APDU received by the CM
KDF SP 800-108r1 Encrypt/Sign	KAT	CAST	Periodic counter value	Count of APDU received by the CM
IFC-Encrypt	KAT	CAST	Periodic counter value	Count of APDU received by the CM
RSA Key Generation	PCT	PCT	N/A	N/A
RSA Signature Generation (CRT)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
RSA Signature Generation (STD)	KAT	CAST	Periodic counter value	Count of APDU received by the CM
SHA2-256	KAT	CAST	Periodic counter value	Count of APDU received by the CM
SHA2-512	KAT	CAST	Periodic counter value	Count of APDU received by the CM
SP 800-90B RCT	Fault-Detection test	CAST	N/A	N/A

Table 24: Conditional Periodic Information

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

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
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
Card is Mute	The module Resource Manager has shut down	Fault Detected	Reset card	Error log is stored

Table 25: Error States

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.

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.

In case of 8 failures, the module irreversibly enters a “Card Is Killed” state

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_HMAC_SHA2_256 **[0xA7]** - This error code is used when HMAC SHA2 256 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_ECDSA (SigGen) (FIPS186-5) **[0xAD]** - This error code is used when ECDSA CAST result is not matching with expecting pattern
- AT_LOG_CAST_ECDH1 (KAS-ECC Key Agreement) **[0xAE]** - This error code is used when ECDH 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_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_KDF_RF5869 (KDF-HKDF or KDA HKDF) **[0xB4]** - This error code is used when HKDF (based on RFC5869) CAST result is not matching with expecting pattern
- AT_LOG_CAST_CS2 (OnePassDH algorithm relying on Crypto Suite 2) **[0xB5]**
- AT_LOG_CAST_ECDH1 (KAS-ECC Key Agreement) **[0xAE]** - This error code is used when ECDH CAST result is not matching with expecting pattern
- AT_LOG_CAST_ECDH2 (KAS-ECC-SSC Sp800-56Ar3) **[0xAE]**: This error code is used when ECDH CAST result is not matching with expecting pattern

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.

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.thesesgroup.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.

11.4 Design and Rules

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 firmware throughout the development and validation cycle.

11.5 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.

11.6 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.
- Status information does not contain SSPs or sensitive data that if misused could lead to a compromise of the Module.

The Module by default is set in manufacturing to include PIV 4.0 and FIDO 2.1 applets.

At the time the card is issued, **the PIV Applet** shall be personalized with the appropriate data. Personalization includes PIV keys and PIN values. Personalization may be performed using a secure channel (ciphered) or in plaintext, as required by the operator.

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].

At the time the card is issued, the **FIDO Applet** shall be personalized with the appropriate data in order to be initialized in the Approved mode.

Personalization includes attestation certificate private key, wrap & mac keys, using approved algorithm and key lengths.

12 Mitigation of Other Attacks

No assured mitigations to 'other attacks' are covered in this security policy.