HID Global

HID Applets v4.0 on NXP JCOP 4.5 P71D600

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document defines the Security Policy for the HID Applets v4.0 on NXP JCOP 4.5 P71D600 cryptographic Module, hereafter denoted the Module. The Module, validated to FIPS 140-3 overall Level 2, is a single chip Module implementing the Global Platform operational environment, with a Card Manager, Supplementary Security Domains and the HID Applets v4.0.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The HID Applets v4.0 on NXP JCOP 4.5 P71D600 is composed of a Global Platform operational environment and Java Card applets running on the P71D600 chip.

Module Type: Hardware

Module Embodiment: Single Chip

Cryptographic Boundary:

The JavaCard and Global Platform APIs are internal interfaces available to applets. Only HID applets and Card Manager, Supplementary Security Domain services are available at the card edge (the interfaces that cross the cryptographic boundary).

The product is delivered with HID v4.0 applets installed and configured before the module is delivered to the customer. The module is a non-modifiable operational environment under the FIPS 140-3 definitions. It always operates in an Approved mode of operation.

The HID Applets V4.0, also named Crescendo Applets later in the document, comprise:

- **ASCLib Library Package** – This is a library package that implements functions required by other applets. The library functions are not directly accessible via the cryptographic Module command interface.
- **CRYPTOLib Library Package** – This is a library implementing cryptographic algorithms like HMAC-SHAx. The library functions are not directly accessible via the cryptographic Module command interface.
- **Access Control Applet (ACA)** – This applet is responsible for Access Control verification for PIN, ADMIN key.
- **PIVExt Applet** – This applet implements SP800-73 at card-edge level for usage operations.
- **OATH Applet** – This applet provides Open Authentication services that can be used by client application / embedded devices like Crescendo Key to authenticate against and authentication server like ActivID Authentication Server. These authentication services consist in HMAC-Based One-Time password (HOTP), Time-Based One-Time password (TOTP), OATH Challenge-Response / Digital Signature Algorithm (OCRA).
- **FIDO Applet** – This applet provides FIDO enrollment and sign-in Services.

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

The following commands can be used to retrieve the module name and version:

- IDENTIFY APDU
- ACAAPPLET_SELECT_APDU_OK
- ACAAPPLET_GET_PROPERTIES_APDU_OK

The Module includes a firmware load function to support necessary updates. New firmware versions within the scope of this validation must be validated through the CMVP. Any other firmware loaded into this Module is out of the scope of this validation and requires separate FIPS 140-3 validation.

Tested Operational Environment's Physical Perimeter (TOEPP):

The Module is designed to be embedded into plastic card bodies, with a contact plate and contactless antenna connections, or as part of an embedded device like Crescendo Key. The physical form of the Module is depicted in Figure 2; the outline depicts the physical perimeter, representing the surface of the chip and the bond pads.

The contactless ports of the module require connection to an antenna. The Module relies on ISO 7816 and ISO 14443 card readers as input/output devices.

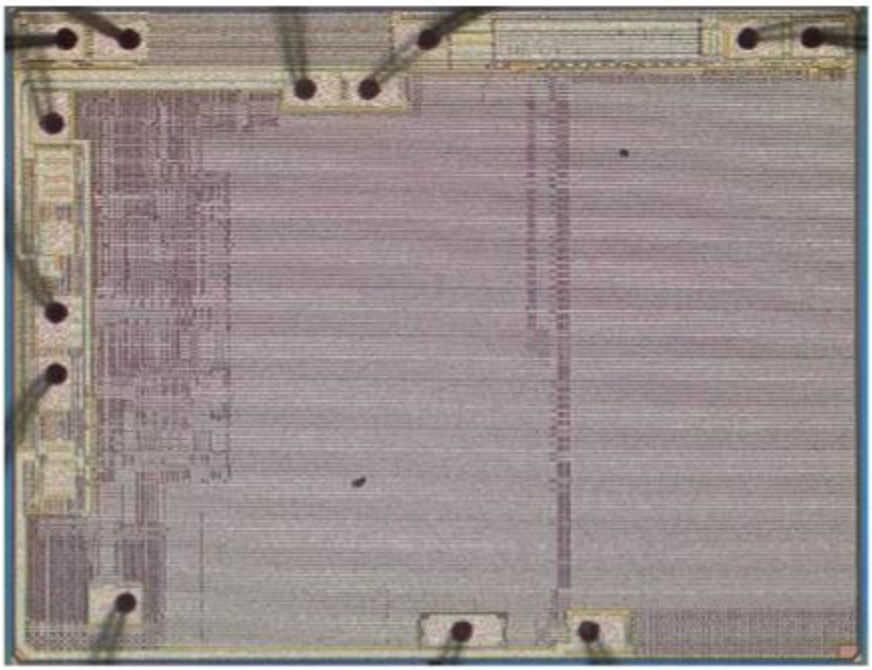

Figure 1: P71D600

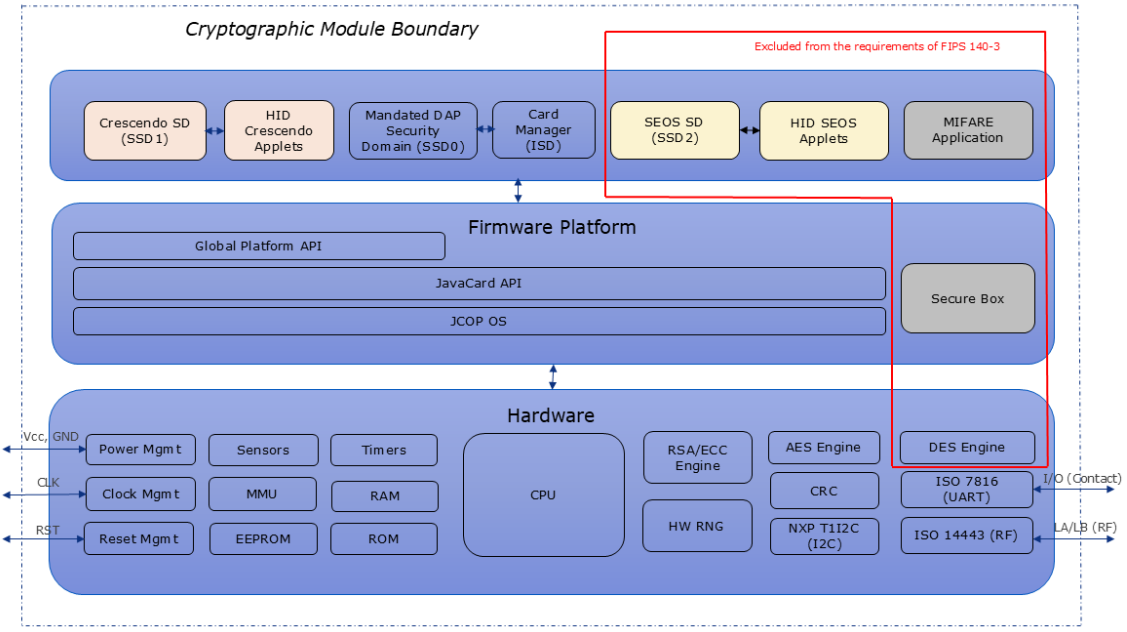

Figure 2: Block Diagram

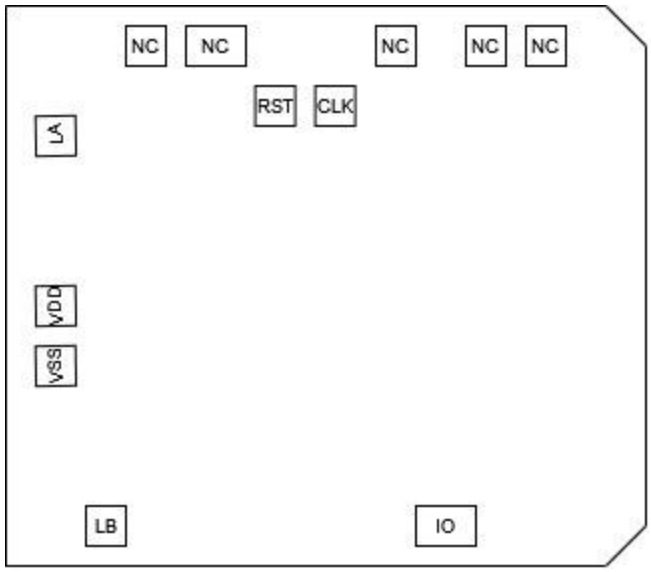

Figure 3: NXP Semiconductor JCOP 4.5 P71D600 Physical Form

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
P71D600	N7122 A1	HID Applets v4.0 on NXP JCOP 4.5 P71D600	MRK3-SC 16/32-bit RISC	ASCLib: 4.0.0.295 CRYPTOLib: 4.0.0.295 ACA: 4.0.0.295 PIVExt: 4.0.0.297 OATH: 4.0.0.295 FIDO: 4.0.0.296 ; ROM ID = B3375FE9B5508BC4 Patch ID = 0000000000000000 Platform ID = J3R6000373181200

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

The following components are excluded from the Evaluation:

- MIFARE applet
- DES Engine
- Secure Box
- SEOS SD and HID SEOS applet

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	In this mode, only approved security functions are accessible. (The module does not support a non-approved mode). The approved mode can be verified following the initialization instructions outlined in Section 11.1	Approved	2401A5

Table 3: Modes List and Description

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2713	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A2713	Key Length - 128, 192, 256	SP 800-38C
AES-CMAC	A2713	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A2713	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A2713	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-KWP	A6112	Direction - Decrypt Key Length - 128, 256	SP 800-38F
Counter DRBG	A2713	Prediction Resistance - No, Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6534	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigGen (FIPS186-5)	A6534	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6534	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA-1	A6112	Key Length - Key Length: 112-1024 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6112	Key Length - Key Length: 112-1024 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6112	Key Length - Key Length: 112-1024 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5910	Domain Parameter Generation Methods - P-384 Scheme - onePassDh - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF Sp800-56Cr1	A2713	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-4096 Increment 8 HMAC Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-56C Rev. 2
KDF SP800-108	A2713	KDF Mode - Counter, Feedback Supported Lengths - Supported Lengths: 112-4096 Increment 8, Supported Lengths: 128	SP 800-108 Rev. 1
KTS-IFC	A6139	Modulo - 3072 Key Generation Methods - rsakpg1-basic Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Key Length - 128	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A6140	Modulo - 2048, 3072, 4096	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A6535	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2pow100 Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A6535	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA Signature Primitive (CVL)	A2713	Private Key Format - crt	FIPS 186-4
RSA SigVer (FIPS186-5)	A6535	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
SHA-1	A2713	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A2713	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A2713	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG-DRBG	Key Type:Symmetric and Asymmetric	N/A	NIST SP800-133rev2 Section 4

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

Name	Properties	Implementation	Reference
AES-1	AES #A2713 (AES-CBC):key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength Per IG D.G. This unwrapping is only approved for legacy purposes per IG D.G.	Symmetric key unwrapping	According to RFC3394
AES-2	AES #2713 (AES-CBC):key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength Per IG D.G. This unwrapping is only approved for legacy purposes per IG D.G.	Symmetric key unwrapping	According to GlobalPlatform Amendment-I

Table 6: Non-Approved, Allowed Algorithms

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
CKG Symmetric Key Generation	CKG	NIST SP800-133rev2 Cryptographic Key Generation Section 4:		CKG-DRBG: ()

Name	Type	Description	Properties	Algorithms
		Symmetric keys are generated using methods described in Section 4 of SP800-133rev2		
ENT	ENT-ESV	Generate random data from hardware used as seed for DRBG		Counter DRBG: (A2713)
DRBG	DRBG	Deterministic random bit generator		Counter DRBG: (A2713)
BC-1-Auth	BC-Auth	AES-CCM Encryption/Decryption		AES-CCM: (A2713)
BC-2-UnAuth	BC-UnAuth	AES-128 CBC		AES-CBC: (A2713)
BC-3-UnAuth	BC-UnAuth	AES-128 ECB		AES-ECB: (A2713)
KTS-1	KTS-Decap	Unwraps session key data, RSA	Standard :SP 800-56Brev2 IG D.G:Approved method from D.G Key Confirmation:No Caveat:Key establishment methodology provides 3072 bits of security strength	KTS-IFC: (A6139)
KTS-2-Appletsv4	KTS-Unwrap	Unwraps key data, AES	Standard:SP 800-38F IG D.G:Approved method from IG D.G Caveat:Key establishment methodology provides 128 or 256 bits of security strength	AES-KWP: (A6112)
KTS-3	KTS-Unwrap	Unwraps AES CBC / AES CMAC	Standard:SP 800-38F IG D.G:Approved method from D.G Caveat:Key establishment methodology provides	AES-CMAC: (A2713) AES-CBC: (A2713)

Name	Type	Description	Properties	Algorithms
			between 128 and 256 bits of security strength	
ECDSA-DigSig-1	DigSig-SigGen	ECDSA Signature Generation		ECDSA SigGen (FIPS186-5): (A6534)
ECDSA-DigSig-2	DigSig-SigVer	ECDSA Signature Verification		ECDSA SigVer (FIPS186-5): (A6534)
RSA-AsymKeyPair	AsymKeyPair-KeyGen	RSA Key Generation		RSA KeyGen (FIPS186-5): (A6535) CKG-DRBG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A2713)
RSA-AsymKeyPairVerif	AsymKeyPair-KeyVer	RSA key Signature verification using PKCS1 v1.5 for padding		RSA SigVer (FIPS186-5): (A6535)
ECDSA-AsymKeyPair	AsymKeyPair-KeyGen	ECDSA Key Generation		ECDSA KeyGen (FIPS186-5): (A6534) CKG-DRBG: () Key Type: Symmetric and Asymmetric Counter DRBG: (A2713)
KAS-1	KAS-Full	Key Agreement	IG:IG D.F Scenario 2, Path 2 Key Conformation:No Key Derivation:KDA (separately	KAS-ECC-SSC Sp800-56Ar3: (A5910) KDA HKDF Sp800-56Cr1: (A2713)

Name	Type	Description	Properties	Algorithms
			tested) Caveat:Key establishment methodology provides 128 bits of security strength	CKG-DRBG: () Key Type: Symmetric and Asymmetric
KBKDF-2	KBKDF	Counter		KDF SP800-108: (A2713) AES-CTR: (A2713)
SHA	SHA	Message Length: 0-65536; Increment 8		SHA-1: (A2713) SHA2-256: (A2713) SHA2-512: (A2713)
MAC-Appletsv4	MAC	HMAC		HMAC-SHA-1: (A6112) HMAC-SHA2-256: (A6112) HMAC-SHA2-512: (A6112)
MAC-AES	MAC	AES-CMAC		AES-CMAC: (A2713)
RSA-DigSig -1-Appletsv4	DigSig-SigGen	RSA Signature Generation and Signature Primitive	Signature Generation:2048-bits, 3072-bits, 4096-bits	RSA Signature Primitive: (A2713) RSA SigGen (FIPS186-5): (A6535)
RSA-Decrypt-1-Appletsv4	KTS-Unwrap	RSA Decryption Primitive	RSA Decryption:3072-bits, 4096-bits	RSA Decryption Primitive Sp800-56Br2: (A6140)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

IG 2.4.B

RSADP (standard)
Usage Restriction: The RSA Decryption Primitive (CVL) shall only be used within the context of a SP 800-56Brev2 KTS.

IG D.H
Symmetric keys and seeds used for generating the asymmetric keys are generated using methods described in Section 4, Section 5.1, Section 6.2.1, Section 6.2.2, Section 6.3 and Section 6.4 of SP 800-133r2.

IG D.L
In the case of the CTR_DRBG, the test report shall indicate if a derivation function is used during the instantiation and reseeding: The CTR_DRBG implementation of the module does use a derivation function (CAVP Cert. #A2713).

In accordance with the Resolution in the IG, the V and Key values for the CTR_DRBG have been defined as CSPs as can be verified from the Section 9.4 SSP Table 1 Table 20.

IG D.M
Specific requirements for generating symmetric keys using SP 800-108 are found in Sec. 6.4 of SP 800-133rev1, “Symmetric Keys Derived from a Preshared Key.” SP 800-108 KDFs may not be used to generate asymmetric keys:

As can be verified from the Section 9.4 SSP Table 2 Table 21, the module only uses KBKDF to derive symmetric keys.

IG D.F:

KAS-1: Key Agreement i.e. KAS-ECC-SSC per NIST SP 800-56Arev3 combined with an HKDF per NIST SP 800-56Cr1 (KDA) used in the context of PIV ECDH Key Agreement service (Scenario 2 path (2) per IG D.F – KAS-ECC-SSC and KDA self-tested separately):

KAS (CAVP Cert. #A2713 KAS-ECC-SSC and CAVP Cert. #A2713 KDA HKDF NIST SP 800-56Cr1; P-256 curve providing 128 bits of encryption strength)

IG D.G:

KTS-1: Key wrapping (Using the approved AES modes CMAC and CBC) used to provide an end-to-end confidential and authenticated protected channel between the external entity (User) and the module (i.e. used in the context of the Secure Channel service). This is per Scenario 2 in IG D.G Approved methods for key transport i.e., a “combination” method: use any approved symmetric encryption mode, such as AES ECB, AES CBC, Triple-DES ECB, etc. together with an approved authentication method (for example, HMAC or AES CMAC, or KMAC):

KTS (CAVP Cert. #A2713 AES-CMAC and CAVP Cert. #A2713 AES-CBC; 128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength)

IG 9.6.A
An AES or a Triple-DES encryption using any approved mode of AES or the Triple-DES as defined in SP 800-140C CMVP Approved Security Functions: SSPs are stored encrypted using AES-CBC.

Additional Comment #1: The approved algorithm implementations used to protect stored SSPs shall be tested by the CAVP (or vendor affirmed if allowed by an IG): The AES-CBC has been tested per CAVP Cert. #A2713.

IG C.E:
The module generates RSA signature keys using an approved key generation procedure per RSA KeyGen validated for conformance to FIPS 186-5 Certs. #A6535 and #A6536.

IG C.F:
The RSA KeyGen, SigGen and SigVer implementations have been tested for all implemented RSA modulus lengths (moduli 2048, 3072 and 4096 bits). No untested moduli apply.

IG C.L:
Resolutions A and B: This requirement is inapplicable to the module since it does not support/implement any truncated hash functions.
Resolution C 1.-5.:
1. The HMAC key provides security strength between 112-256 bits and this meets the security requirements i.e. minimum required security strength at this time per NIST SP 800-131Ar2. The actual range is 112-320 bits per the following computation but capped at 256 bits (largest security strength that can be claimed):
For HMAC, NIST SP 800-107 Rev. 1 states that the effective security strength is:
"Security Strength"=min□("strength"(K)," " 2C) where:
Kis the HMAC key.
Cis the internal chaining value size of the hash function.
For SHA-1, C=160bits, so 2C=320bits.
Thus for HMAC-SHA-1, the key security strength is:
〖"Security Strength" 〗_(HMAC-SHA1)=min□("strength"(K)," " 320)
2. The HMAC key is stored in the JCOP OS' keystore to which no access is possible/provided by the module and is thus kept secret.
3. The module generates i.e. derives (using the NIST SP 800-108r1 KDF per SCP03/secure channel SFI) the keys (SD-SENC, SD-SMAC and SD-RMAC) per NIST SP 800-133r1 Section 6.2.2: Symmetric Keys Derived from a Pre-existing Key.
4. and 5. The module does not support a truncated HMAC and thus requirements per #4. and #5. do not apply to it.

Resolution D 1.:
The module derives the following keys with s i.e. security strengths as specified below:
For NIST SP 800-108r1 derived keys:
SD-SENC, SD-SMAC and SD-RMAC each with s 128 bits.
a. The security strength supported by the asymmetric keys, or key-derivation key: for each of the derived keys, the KDKs are the SD-KENC (used to derive SENC) and SD-KMAC (used to derive the SMAC and RMAC) keys each with a security strength of 128 bits.
b. The preimage strength of the hash function, or the hash function used in all HMAC constructions used to derive the key: 160-bits (for HMAC-SHA-1 used as a PRF for the NIST SP 800-108r1 KDF)
c. The length of the derived key in bits: 128 bits.

Resolution E: This requirement is inapplicable to the module since it implements a CTR-DRBG.

2.8 RBG and Entropy

Cert Number	Vendor Name
E148	NXP

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
JCOP 4.5 on P71D600	Physical	JCOP 4.5 on P71D600	8 bits	7.30359	N/A

Table 9: Entropy Sources

2.9 Key Generation

The module uses an approved NIST SP 800-90Ar1 DRBG for the generation of keys/SSPs.

2.10 Key Establishment

The module supports approved key establishment methods as specified in the Security Functions Implementations tables

2.11 Industry Protocols

N/A, this module does not implement industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
VSS, VDD	Power	These interfaces are used to supply power to the module in contact mode; The module starts when interface is powered
RST	Control Input	If a signal is sent on this interface in contact mode, the module will reboot (active low)
CLK	Control Input	The interface is used by an external device (ex: smartcard reader) to provide a clock signal to the IC in contact mode; The IC will derive its own clock from this signal
I/O	Data Input Data Output Control Input Status Output	This interface is used to communicate with an external entity (ex: SmartCard reader) in contact mode
LA, LB	Data Input Data Output	This interface is used to communicate with an external entity (ex: SmartCard reader) in contactless mode

Physical Port	Logical Interface(s)	Data That Passes
	Control Input Status Output	

Table 10: Ports and Interfaces

Control Output is not applicable for this module.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
SCP	Secure Channel Protocol	AES CMAC Mutual Authentication	2.9E39	5.2E-37
XAUTH	External Authentication	AES Encryption Challenge/Response	2.9E39	1.17E-35
PIN	PIN-based Authentication	PIN Comparison	8.3 E-9	1.24E-7

Table 11: Authentication Methods

- **SCP** - Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method is provided by the Secure Channel service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The off-card entity participating in the mutual authentication sends a 64-bit challenge to the Smart Card. The Smart Card generates its own challenge and computes a 64-bit cryptogram with SD-SMAC key and both challenges. The Smart Card cryptogram and challenge are sent to the off-card entity which checks the Smart Card cryptogram and creates its own 64-bit cryptogram with both challenges. A 64-bit message authentication code (MAC) is also computed on the command containing the off-card entity cryptogram with AES-CMAC and SD-SMAC key; the MAC is concatenated to the command, and this whole command is sent to the Smart Card. The Smart Card checks the message authentication code and compares the received cryptogram to the calculated cryptogram. If all of this succeeds, the two participants are mutually authenticated.

The probability that a random attempt will succeed using this authentication method is:

- 1/(2^128) = 2.9E-39 (MAC||cryptogram) using a 128-bit block for authentication).
  This authentication method includes a counter of failed authentication called “velocity checking” by Global Platform. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication.

The Module enforces a maximum of 60 failed Global Platform SCP03 authentication attempts before blocking permanently the card.

The probability that a random attempt will succeed over a one-minute interval is (with the assumption here that 3 attempts are possible per second)

- 60*3/2^128 = 5.2E-37 (MAC||cryptogram), using a 128-bit block for authentication.

Note: in the above paragraph, SD- stands for ISD, SD, i.e. Issuer Security Domain or Supplementary Security Domain.

- **XAUTH** - External Authentication Method

The External Authentication method is provided by Authenticate service. This authentication method decrypts with ACA-SPAK an encrypted 128-bit challenge sent to the module by an off-card entity and compares the resulting challenge to the expected value. The authentication strength for this method depends on the algorithm, key size and challenge size used: the minimum strength key used for this method is AES-128 Key; however, the limiting factor in this authentication method is the 128-bit block size.
The associated probability of false authentication of this authentication methods is:

- 1/(2^128) = 2.9E-39

The execution of this authentication mechanism is rate limited, the module can perform no more than (60/0.015) attempts per minute. Therefore, the probability that a random attempt will succeed over a one minute period is:

- 60/(0.015*(2^128)) = 1.17E -35

- **PIN** - PIN-Based Authentication Method

This PIN-Based authentication method compares a value sent to the Module to the stored ACA-PIN or ACA-PUK values; if the two values are equal, the operator is authenticated.

The strength of this authentication method depends on both internal and external factors.
The Module supports numeric PIN values coded in ASCII with a length comprises between 6 and 8 bytes. The character space for the first 6 bytes is 10 (the values ‘30’ through ‘39’ are permitted) and in the last 2 characters is 11 (the values ‘30’ through ‘39’ and ‘FF’ are permitted).
The probability of false authentication of this authentication method is as follows:

- 1/(10^6*11^2) = 8.3E-9

Based on the SP800-73 defined maximum count of 15 for failed authentication attempts, the probability that a random attempt will succeed over a one minute period is:

- 15/(10^6*11^2) = 1.24E-7

4.2 Roles

Name	Type	Operator Type	Authentication Methods
ICO- Issuer Cryptographic Officer	Identity	CO	SCP
CCO- Crescendo Applets Cryptographic Officer	Identity	CO	SCP
AA: Application Administrator	Identity	CO	XAUTH
HD: Help Desk Officer	Identity	CO	PIN
CH: Card Holder	Identity	CO	PIN
UU: Unauthenticated User	Role	Unauthenticated User	None

Table 12: Roles

- **ICO** - Issuer Cryptographic Officer:
  - Identity-based authentication using Global Platform Secure Channel Protocol Authentication Method with ISD and SSD0 keys.
  - Manages Module (Card Manager) and SSD0 Content.
- **CCO** - Crescendo Applets Cryptographic Officer:
  - Identity-based authentication using Global Platform Secure Channel Protocol Authentication Method with SSD1 keys.
  - Manages SSD1 content, as well as Crescendo (ACA, PIVEXT, OATH, FIDO) Applets content and configuration in managed mode.
- **AA** - Application Administrator:
  - Identity-based authentication using “External Authentication” Authentication Method with ACA-ADMK keys.
  - Manages Crescendo (ACA, PIVEXT, OATH, FIDO) Applets content and configuration in unmanaged mode and PIN Authenticator (unlock) in managed mode.
- **HD** - Help Desk Officer
  - Identity-based authentication using “PIN-based” Authentication Method with ACA-PUK.
  - Manages PIN Authenticator (unlock…) in unmanaged/managed.
- **CH** - Card Holder
  - Identity-based authentication using “PIN-based” Authentication Method with ACA-PIN.
  - Manages Crescendo (ACA, PIVEXT, OATH, FIDO) Applets content and configuration in unmanaged mode.
  - Uses Crescendo (ACA, PIVEXT, OATH, FIDO) Applets services and crypto operations in unmanaged/managed modes.
- **UU** - Unauthenticated User
  - No authentication needed
  - Accesses Module services where SSPs are not modified and CSPs are not disclosed.

Note:

Crescendo Applets are configurable in Managed or Unmanaged mode, each mode corresponding to a different Access Control Rules Definition.
In Managed mode, the Crescendo Applets content and configurations are done by CCO operator, while in Unmanaged mode they can be done by AA operator or CH user.
The recommended mode is the Managed mode involving a Credential Management System.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Card Reset	Power cycle or reset the Module. Includes Power-	Status Word	N/A	ATR	None	UU: Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	On Self-Test and Zeroization of SSPs.					User - OS-DRBG-EI: E - OS-DRBG-SEED: E - ISD-SENC: Z - ISD-SMAC: Z - ISD-RMAC: Z - ACA-SKISK: Z - FIDO-PINS: Z
Card Manager Context	Select the Card Manager; Card Manager Select and Manage Channel service	Status Word	Command Parameters	Card Manager Information, Channel Number	None	UU: Unauthenticated User - ISD-SENC: Z - ISD-SMAC: Z - ISD-RMAC: Z
Card Manager Secure Channel	Secure Channel Establishment; Initialize Update and External Authenticate Service	Status Word	Command Parameters	Secure Channel Parameters	CKG Symmetric Key Generation ENT DRBG KBKDF-2 MAC-AES	ICO-Issuer Cryptographic Officer - OS-DRBG-EI: E - OS-DRBG-SEED: E - OS-DRBG-KEY: E - OS-DRBG-V: E - OS-DRBG-OUTPUT: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- OS-DRBG-STATE: E - OS-MKEK: E - ISD-KENC: E - ISD-KMAC: E - ISD-SENC: G,E - ISD-SMAC: G,E - ISD-RMAC: G,E
Card Manager Info (Self-Test)	Read unprivileged data objects, e.g. module configuration or status information; Card Manager GET DATA unprivileged service	Status Word	Command Parameters	Requested Information	None	UU: Unauthenticated User
Card Manager Lifecycle	Modify the card or applet life cycle status; Card Manager SET STATUS service	Status Word	Command Parameters	N/A	None	ICO-Issuer Cryptographic Officer - ISD-SENC: E - ISD-SMAC: E - ISD-RMAC: E - OS-MKEK: Z
Card Manager Privileged Info (Show module's Status and Version)	Read privileged data objects and Read card or applet life cycle status; Card Manager GET DATA privileged	Status Word	Command Parameters	Requested Information	None	ICO-Issuer Cryptographic Officer - ISD-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and GET STATUS service					- ISD-SMAC: E - ISD-RMAC: E
Card Manager Manage Content	Delete a package or object, load, install and update application packages; Card Manager DELETE, LOAD, INSTALL and PUT KEY Service	Status Word	Command Parameters	N/A	BC-3-UnAuth KTS-3	ICO-Issuer Cryptographic Officer - ISD-SENC: E - ISD-SMAC: E - ISD-RMAC: E - ACA-ADMK: W - ACA-PIN: W - PIV-PWC-Pr: W - PIV-PWC-Pu: W - FIDO-IDENCK: G - FIDO-FAUTHK-Pr: G - FIDO-CREDRANDUVK: G - ISD-KENC: W - ISD-KMAC: W - ISD-KDEK: W,E - OS-MKEK: E,G - SD-DAPK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- OS-SKEK: W
SSD Context	Select the Security Domain and Manage Logical Channel; SSD SELECT and MANAGE CHANNEL service	Status Word	Command Parameters	N/A	None	UU: Unauthenticated User - SD-SENC: Z - SD-SMAC: Z - SD-RMAC: Z
SSD Secure Channel	Secure Channel Establishment; SSD INITIALIZE UPDATE and SSD EXTERNAL AUTHENTICATE service	Status Word	Command Parameters	Secure Channel Parameters	CKG Symmetric Key Generation ENT DRBG KBKDF-2 MAC-AES	ICO-Issuer Cryptographic Officer - OS-DRBG-EI: E - OS-DRBG-SEED: E - OS-DRBG-KEY: E - OS-DRBG-V: E - OS-DRBG-OUTPUT: E - OS-DRBG-STATE: E - OS-MKEK: E - SD-KENC: E - SD-KMAC: E - SD-SENC: G,E - SD-SMAC: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SD-RMAC: G,E CCO-Crescendo Applets Cryptographic Officer - OS-DRBG-EI: E - OS-DRBG-SEED: E - OS-DRBG-KEY: E - OS-DRBG-V: E - OS-DRBG-OUTPUT: E - OS-DRBG-STATE: E - OS-MKEK: E - SD-KENC: E - SD-KMAC: E - SD-SENC: G,E - SD-SMAC: G,E - SD-RMAC: G,E
SSD Info	Read unprivileged data objects, e.g. module configuration or status information;	Status Word	Command Parameters	Requested Information	None	UU: Unauthenticated User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	SSD GET DATA unprivileged service					
SSD Privileged Info	Read privileged data objects and Read Card or Applet life cycle status; SSD GET DATA privileged and GET STATUS service	Status Word	Command Parameters	Requested Information	None	ICO-Issuer Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E
SSD Manage Content	Update Security Domain Keys; SSD PUT KEY service	Status Word	Command Parameters (including SSPs)	N/A	KTS-3	ICO-Issuer Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - SD-KENC: W - SD-KMAC: W - SD-KDEK: W,E - SD-DAPK: W,Z - OS-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						MKEK: E CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - SD-KENC: W - SD-KMAC: W - SD-KDEK: W,E - SD-DAPK: W,Z - OS-MKEK: E
ACA Select Applet	Select Applet; ACA SELECT Service	Status Word	Command Parameters	Applets Information	None	UU: Unauthenticated User - SD-SENC: Z - SD-SMAC: Z - SD-RMAC: Z
ACA Secure Channel	Secure Channel Establishment; ACA INITIALIZE UPDATE and EXTERNAL AUTHENTICATE Service	Status Word	Command Parameters	Secure Channel Parameters	CKG Symmetric Key Generation ENT DRBG KBKDF-2 MAC-AES	CCO-Crescendo Applets Cryptographic Officer - OS-DRBG-EI: E - OS-DRBG-SEED: E - OS-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG-KEY: E - OS-DRBG-V: E - OS-DRBG-OUTPUT: E - OS-DRBG-STATE: E - OS-MKEK: E - SD-KENC: E - SD-KMAC: E - SD-SENC: G,E - SD-SMAC: G,E - SD-RMAC: G,E
ACA Logout	Logout ICO, CCO, CH, AA roles; ACA LOGOUT Service	Status Word	N/A	N/A	None	UU: Unauthenticated User - ACA-SKISK: Z - OS-MKEK: E
ACA Authenticate	Application Administrator Authentication and Card Holder Authentication by presenting the PIN; ACA GET CHALLENGE, EXTERNAL AUTHENTICATE and VERIFY Service	Status Word	Command Parameters (including Cryptogram and SSPs))	Challenge	None	AA: Application Administrator - ACA-ADMK: E - OS-MKEK: E CH: Card Holder - ACA-PIN: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- OS-MKEK: E
ACA PUT KEY	Put XAUTH Key (ACA Manage Content)	Status Word	Command Parameters (including SSPs)	N/A	KTS-2-Appletsv4 KTS-3	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - SD-KDEK: E - ACA-CAST-KWPK: E - ACA-ADMK: W,Z - OS-MKEK: E AA: Application Administrator - ACA-SKISK: E - ACA-CAST-KWPK: E - ACA-ADMK: W,Z - OS-MKEK: E CH: Card Holder - ACA-SKISK: E - ACA-CAST-KWPK: E - ACA-ADMK:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,Z - OS-MKEK: E
ACA CHANGE REFERENCE DATA (CREATE PIN)	Create PIN Value (ACA Manage Content)	Status Word	Command Parameters (including SSPs)	N/A	KTS-2-Appletsv4	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - SD-KDEK: E - ACA-PIN: W - ACA-CAST-KWPK: E - OS-MKEK: E
ACA CHANGE REFERENCE DATA (CREATE PUK)	Create/Update/Delete PUK value (ACA Manage Content)	Status Word	Command Parameters (including SSPs)	N/A	KTS-2-Appletsv4	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - SD-KDEK: E - ACA-PUK: W - ACA-CAST-KWPK: E - OS-MKEK: E AA: Application

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Administrator - ACA-PUK: W - OS-MKEK: E CH: Card Holder - ACA-PUK: W - OS-MKEK: E
ACA RESET CARD	Reset the card content (ACA Manage Content)	Status Word	N/A	N/A	None	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - ACA-ADMK: Z - ACA-SKISK: Z - ACA-PIN: W - ACA-PUK: Z - PIVX-GPK-Pr: Z - PIV-AuK-Pr: Z - PIV-DSK-Pr: Z - PIV-KMK-Pr: Z - PIV-RKMK-Pr: Z - PIV-CaK-Pr: Z - PIV-SKIKTK-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Pr: Z - PIVX-GPK-Pu: Z - PIV-AuK-Pu: Z - PIV-DSK-Pu: Z - PIV-KMK-Pu: Z - PIV-RKMK-Pu: Z - PIV-CaK-Pu: Z - PIV-SKIKTK-Pu: Z - OATH-OTP: Z - FIDO-PIN: Z - FIDO-ENTK-Pr: Z - FIDO-ENTK-Pu: Z - FIDO-IDENCK: G - FIDO-AUTHRK-Pr: Z - FIDO-AUTHRK-Pu: Z - OS-MKEK: E AA: Application Administrator - ACA-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ADMK: Z - ACA-SKISK: Z - ACA-PIN: W - ACA-PUK: Z - PIVX-GPK-Pr: Z - PIV-AuK-Pr: Z - PIV-DSK-Pr: Z - PIV-KMK-Pr: Z - PIV-RKMK-Pr: Z - PIV-CaK-Pr: Z - PIV-SKIKTK-Pr: Z - PIVX-GPK-Pu: Z - PIV-AuK-Pu: Z - PIV-DSK-Pu: Z - PIV-KMK-Pu: Z - PIV-RKMK-Pu: Z - PIV-CaK-Pu: Z - PIV-SKIKTK-Pu: Z - OATH-OTP: Z - FIDO-PIN: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- FIDO-ENTK-Pr: Z - FIDO-ENTK-Pu: Z - FIDO-IDENCK: G - FIDO-AUTHRK-Pr: Z - FIDO-AUTHRK-Pu: Z - OS-MKEK: E CH: Card Holder - ACA-ADMK: Z - ACA-SKISK: Z - ACA-PIN: W - ACA-PUK: Z - PIVX-GPK-Pr: Z - PIV-AuK-Pr: Z - PIV-DSK-Pr: Z - PIV-KMK-Pr: Z - PIV-RKMK-Pr: Z - PIV-CaK-Pr: Z - PIV-SKIKTK-Pr: Z - PIVX-GPK-Pu: Z - PIV-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						AuK-Pu: Z - PIV-DSK-Pu: Z - PIV-KMK-Pu: Z - PIV-RKMK-Pu: Z - PIV-CaK-Pu: Z - PIV-SKIKTK-Pu: Z - OATH-OTP: Z - FIDO-PIN: Z - FIDO-ENTK-Pr: Z - FIDO-ENTK-Pu: Z - FIDO-IDENCK: G - FIDO-AUTHRK-Pr: Z - FIDO-AUTHRK-Pu: Z - OS-MKEK: E
ACA UPDATE PROPERTIES (Shared PIN)	Update the shared/unshared PIN properties of the card (ACA Manage Content)	Status Word	Command Parameters	N/A	None	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						RMAC: E UU: Unauthenticated User
ACA UPDATE PROPERTIES (Others)	Update the applet properties (PIN Policy configurations, Managed Mode, Communication Media, Contactless Firewall, ForcePINChange) (ACA Manage Content)	Status Word	Command Parameters	N/A	None	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E AA: Application Administrator CH: Card Holder
ACA CHANGE REFERENCE DATA (CHANGE PIN)	Change the PIN value (ACA CH Authentication Management)	Status Word	Command Parameters	N/A	None	CH: Card Holder - ACA-PIN: W,E - OS-MKEK: E
ACA RESET RETRY COUNTER	Unblock and change the PIN value (ACA CH Authentication Management)	Status Word	Command Parameters (including SSPs)	N/A	KTS-2-Appletsv4	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - SD-KDEK: E - ACA-PIN: W - ACA-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						CAST-KWPK: E - OS-MKEK: E AA: Application Administrator - ACA-ADMK: E - ACA-PIN: W - OS-MKEK: E HD: Help Desk Officer - ACA-PIN: W - ACA-PUK: E - OS-MKEK: E
ACA Info	Retrieve FIPS Module Configuration, Trigger the Self-Tests, Retrieve the FIPS CAST execution status; ACA GET PROPERTIES service	Status Word	Command Parameters	FIPS Status	KTS-2-Appletsv4 MAC-Appletsv4	UU: Unauthenticated User - ACA-CAST-HMACK: E - ACA-CAST-KWPK: E - OS-MKEK: E
PIVEXT Select Applet	Select Applet; PIVEXT SELECT Service	Status Word	Command Parameters	Applets Information	None	UU: Unauthenticated User - SD-SENC: Z - SD-SMAC: Z - SD-RMAC: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
PIVEXT Secure Channel	Secure Channel Establishment; PIVEXT INITIALIZE UPDATE and EXTERNAL AUTHENTICATE Service	Status Word	Command Parameters	Secure Channel Parameters	CKG Symmetric Key Generation ENT DRBG KBKDF-2 MAC-AES	CCO-Crescendo Applets Cryptographic Officer - OS-DRBG-EI: E - OS-DRBG-SEED: E - OS-DRBG-KEY: E - OS-DRBG-V: E - OS-DRBG-OUTPUT: E - OS-DRBG-STATE: E - OS-MKEK: E - SD-KENC: E - SD-KMAC: E - SD-SENC: G,E - SD-SMAC: G,E - SD-RMAC: G,E
PIVEXT Manage Content	Update PIV Instance Type, Generate an asymmetric RSA or ECC Key Pair, Create, update, or delete PIV Data Object and/or	Status Word	Command Parameters	PSP	KTS-2-Appletsv4 KTS-3 RSA-AsymKey Pair RSA-AsymKey	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Inject or delete RSA/ECC private Key, update Security Configuration; PIVEXT UPDATE PROPERTIES, GENERATE ASYMMETRIC KEY PAIR(GENERATE KEY), PUT DATA and PUT KEY Service				PairVerif ECDSA-AsymKey Pair KAS-1 SHA	- SD-SMAC: E - SD-RMAC: E - SD-KDEK: E - PIVX-GPK-Pr: G,Z,W - PIV-AuK-Pr: G,Z,W - PIV-DSK-Pr: G,Z,W - PIV-KMK-Pr: G,Z,W - PIV-RKMK-Pr: G,Z,W - PIV-CaK-Pr: G,Z,W - PIV-SKIKTK-Pr: G,Z - PIVX-GPK-Pu: G,R,Z - PIV-AuK-Pu: G,R,Z - PIV-DSK-Pu: G,R,Z - PIV-KMK-Pu: G,R,Z - PIV-RKMK-Pu: G,R,Z - PIV-CaK-Pu: G,R,Z - PIV-SKIKTK-Pu: G,R,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PIV-PWC-Pr: E - PIV-PWC-Pu: E - ACA-CAST-KWPK: E - OS-MKEK: E AA: Application Administrator - PIVX-GPK-Pr: G,Z,W - PIV-AuK-Pr: G,Z,W - PIV-DSK-Pr: G,Z,W - PIV-KMK-Pr: G,Z,W - PIV-RKMK-Pr: G,Z,W - PIV-CaK-Pr: G,Z,W - PIV-SKIKTK-Pr: G,Z - PIVX-GPK-Pu: G,R,Z - PIV-AuK-Pu: G,R,Z - PIV-DSK-Pu: G,R,Z - PIV-KMK-Pu:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,R,Z - PIV-RKMK-Pu: G,R,Z - PIV-CaK-Pu: G,R,Z - PIV-SKIKTK-Pu: G,R,Z - PIV-PWC-Pr: E - PIV-PWC-Pu: E - ACA-CAST-KWPK: E - ACA-SKISK: E - OS-MKEK: E CH: Card Holder - PIVX-GPK-Pr: G,Z,W - PIV-AuK-Pr: G,Z,W - PIV-DSK-Pr: G,Z,W - PIV-KMK-Pr: G,Z,W - PIV-RKMK-Pr: G,Z,W - PIV-CaK-Pr: G,Z,W - PIV-SKIKTK-Pr: G,Z - PIVX-GPK-Pu:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,R,Z - PIV-AuK-Pu: G,R,Z - PIV-DSK-Pu: G,R,Z - PIV-KMK-Pu: G,R,Z - PIV-RKMK-Pu: G,R,Z - PIV-CaK-Pu: G,R,Z - PIV-SKIKTK-Pu: G,R,Z - PIV-PWC-Pr: E - PIV-PWC-Pu: E - ACA-CAST-KWPK: E - ACA-SKISK: E - OS-MKEK: E
PIVEXT Info	Retrieve the applet, Return the public key of the asymmetric key; PIVEXT GET PROPERTIES and GENERATE ASYMMETRIC KEY PAIR (GET MODULUS) Service	Status Word	Command Parameters	Requested Information, PSP	None	UU: Unauthenticated User - PIVX-GPK-Pu: R - PIV-AuK-Pu: R - PIV-DSK-Pu: R - PIV-KMK-Pu: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PIV-RKMK-Pu: R - PIV-CaK-Pu: R - PIV-SKIKTK-Pu: R - OS-MKEK: E
PIVEXT Privileged Info	Read the PIV Data Object content; PIVEXT GET DATA Service	Status Word	Command Parameters	Requested Information	None	CH: Card Holder UU: Unauthenticated User
PIVEXT Authenticate	Card Holder Authentication by presenting the PIN; PIVEXT VERIFY Service	Status Word	Command Parameters (including SSPs)	N/A	None	CH: Card Holder - ACA-PIN: E - OS-MKEK: E
PIVEXT CH Authentication Management	Change the PIN value, Unblock and change the value of the PIN; PIVEXT CHANGE REFERENCE DATA and RESET RETRY COUNTER Service	Status Word	Command Parameters (including SSPs)	N/A	None	CH: Card Holder - ACA-PIN: W,E - OS-MKEK: E AA: Application Administrator - ACA-PIN: W - ACA-PUK: E - OS-MKEK: E
PIVEXT RSA, ECC Crypto Operation	Perform a requested cryptographic operation with an RSA/ECC Asymmetric Key;	Status Word	Command Parameters (Data To be	Processed Value	KTS-1 ECDSA-DigSig-1 ECDSA-DigSig-2 KAS-1	CH: Card Holder - ACA-SKISK: W - PIVX-GPK-Pr:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	PIVEXT GENERAL AUTHENTICATE Service		Processed)		SHA RSA-DigSig -1-Appletsv4 RSA-Decrypt-1-Appletsv4	E - PIV-AuK-Pr: E - PIV-DSK-Pr: E - PIV-KMK-Pr: E - PIV-RKMK-Pr: E - PIV-SKIKTK-Pr: E - OS-MKEK: E UU: Unauthenticated User - PIV-CaK-Pr: E - OS-MKEK: E
PIVEXT Logout	Logout CH authentication; PIVEXT VERIFY (LOGOUT) Service	Status Word	N/A	N/A	None	UU: Unauthenticated User
OATH Select Applet	Select Applet; OATH SELECT Service	Status Word	Command Parameters	Applet Information	None	UU: Unauthenticated User - SD-SENC: Z - SD-SMAC: Z - SD-RMAC: Z
OATH Secure Channel	Secure Channel Establishment; OATH INITIALIZE UPDATE and EXTERNAL AUTHENTICATE Service	Status Word	Command Parameters	Secure Channel Parameters	CKG Symmetric Key Generation ENT DRBG	CCO-Crescendo Applets Cryptographic Officer - OS-DRBG-EI:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					KBKDF-2 MAC-AES	E - OS-DRBG-SEED: E - OS-DRBG-KEY: E - OS-DRBG-V: E - OS-DRBG-OUTPUT: E - OS-DRBG-STATE: E - OS-MKEK: E - SD-KENC: E - SD-KMAC: E - SD-SENC: G,E - SD-SMAC: G,E - SD-RMAC: G,E
OATH Info	Retrieve the applet properties; OATH GET PROPERTIES Service	Status Word	N/A	Requested Information	None	UU: Unauthenticated User
OATH GET CODE	Obtain a One Time Password (HOTP, TOTP), (Never to be used as a first factor for UU); (OATH Authentication)	Status Word	Command Parameter	HOTP, TOTP	MAC-Appletsv4	CH: Card Holder - ACA-CAST-HMACK: E - OATH-OTP: E UU: Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						User - ACA-CAST-HMACK: E - OATH-OTP: E
OATH OCRA AUTHENTICATE	Perform an OCRA challenge Response or Digital Signature (OATH Authentication)	Status Word	Data to be proceed	Processed Data	MAC-Appletsv4	CH: Card Holder - ACA-CAST-HMACK: E - OATH-OTP: E
OATH Manage Content	Inject or delete a new OATH key, or Security Configuration; OATH PUT KEY Service	Status Word	Command Parameters (including SSPs)	N/A	KTS-2-Appletsv4 KTS-3	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - SD-KDEK: E - ACA-CAST-KWPK: E - OATH-OTP: Z,W - OS-MKEK: E AA: Application Administrator - ACA-SKISK: E - ACA-CAST-KWPK: E - OATH-OTP: Z,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- OS-MKEK: E CH: Card Holder - ACA-SKISK: E - ACA-CAST-KWPK: E - OATH-OTP: Z,W - OS-MKEK: E
FIDO Select Applet	Select Applet; FIDO Select Service	Status Word	Command Parameters	Applets Information	KAS-1 SHA	UU: Unauthenticated User - SD-SENC: Z - SD-SMAC: Z - SD-RMAC: Z - FIDO-PWC-Pr: W - FIDO-AUTHKAK-Pr: G - FIDO-PINENCSK: Z - FIDO-PINAUTHSK: Z - FIDO-SALTENCSK: Z - FIDO-SALTAUTHSK: Z - FIDO-PWC-Pu: W - FIDO-AUTHKAK-Pu: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
FIDO Secure Channel	Secure Channel Establishment; FIDO INITIALIZE UPDATE and EXTERNAL AUTHENTICATE Service	Status Word	Command Parameters	Secure Channel Parameters	CKG Symmetric Key Generation ENT DRBG KBKDF-2 MAC-AES	CCO-Crescendo Applets Cryptographic Officer - OS-DRBG-EI: E - OS-DRBG-SEED: E - OS-DRBG-KEY: E - OS-DRBG-V: E - OS-DRBG-OUTPUT: E - OS-DRBG-STATE: E - OS-MKEK: E - SD-KENC: E - SD-KMAC: E - SD-SENC: G,E - SD-SMAC: G,E - SD-RMAC: G,E
FIDO Info	Retrieve the applet properties, Return the public key of the asymmetric key and Read the Data Object content; FIDO	Status Word	Command Parameters	Request Information Status	None	UU: Unauthenticated User - FIDO-ENTK-Pu: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	GET PROPERTIES, GENERATE ASYMMETRIC KEY PAIR (GET MODULUS) and GET DATA Service					- OS-MKEK: E
FIDO Manage Content	Inject attestation certificate, enterprise attestation certificate and RPID List, Inject Attestation Key, Generate Enterprise Attestation Ecc Key Pair, Update FIDO Applet Properties (AlwaysUv, MinPinLength,ForcePINChange, Communication Media, Enterprise Attestation configuration); FIDO PUT DATA, PUT KEY, GENERATE ASYMMETRIC KEY PAIR (GENERATE KEY) and UPDATE PROPERTIES Service	Status Word	Command Parameters (including SSPs)	PSP	KTS-2-Appletsv4 KTS-3 ECDSA-DigSig-1 ECDSA-DigSig-2 ECDSA-AsymKeyPair SHA	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-RMAC: E - SD-KDEK: E - ACA-CAST-KWPK: E - FIDO-ATTK-Pr: W - FIDO-ENTK-Pr: W,G - FIDO-ENTK-Pu: G,R
FIDO ECC Crypto Operation	Perform an ECDSA signature with an ECC Asymmetric Private Key; FIDO GENERAL AUTHENTICATE Service	Status Word	Command Parameters (Data to be Processed)	Processed Data	ECDSA-DigSig-1 SHA	CCO-Crescendo Applets Cryptographic Officer - SD-SENC: E - SD-SMAC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SD-RMAC: E - FIDO-ENTK-Pr: E
FIDO AuthenticatorMakeCredential	Create a new FIDO credential (discoverable or non-discoverable) (FIDO Services)	Status Word	Command Parameters	Response Data (including PSPs),	BC-1-Auth ECDSA-DigSig-1 ECDSA-DigSig-2 ECDSA-AsymKeyPair SHA MAC-Appletsv4	CH: Card Holder - ACA-CAST-HMACK: E - FIDO-PINS: Z,E - FIDO-ATTK-Pr: E - FIDO-ENTK-Pr: E - FIDO-IDENCK: E - FIDO-AUTHRK-Pr: G - FIDO-AUTHSK-Pr: G - FIDO-AUTHSK-Pu: G,R - FIDO-AUTHRK-Pu: G,R - OS-MKEK: E
FIDO AuthenticatorGetAssertion	Use FIDO Credential (FIDO Services)	Status Word	Command Parameters	Response Data	BC-1-Auth BC-2-UnAuth ECDSA-DigSig-1 SHA MAC-Appletsv4	CH: Card Holder - ACA-CAST-HMACK: E - FIDO-PINS: Z,E - FIDO-IDENCK: E - FIDO-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						AUTHRK-Pr: E - FIDO-AUTHKSK-Pr: E,R - FIDO-AUTHKSK-Pu: R - FIDO-FAUTHK-Pr: E - FIDO-SALTAUTHSK: W,E - FIDO-SALTENCSK: W,E - FIDO-CREDRANDUVK: E - OS-MKEK: E
FIDO AuthenticationGetNextAssertion	Use FIDO Credential (Next) (FIDO Services)	Status Word	Command Parameters	Response Data	BC-2-UnAuth ECDSA-DigSig-1 SHA MAC-Appletsv4	CH: Card Holder - FIDO-IDENCK: E - FIDO-FAUTHK-Pr: E - FIDO-AUTHRK-Pr: E - FIDO-SALTAUTHSK: E - FIDO-SALTENCSK: E - FIDO-CREDRANDUVK: E - OS-MKEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
FIDO AuthenticatorGetInfo	Get FIDO device information (FIDO Services)	Status Word	N/A	Requested Information	None	UU: Unauthenticated User
FIDO AuthenticatorClientPIN	Set, Change, authenticate PIN value (FIDO Services)	Status Word	Command Parameters (including SSPs)	N/A	BC-2-UnAuth KAS-1 SHA MAC-Appletsv4	CH: Card Holder - ACA-PIN: W,E - ACA-CAST-HMACK: E - FIDO-PIN: W,E - FIDO-PINS: G - PIV-PWC-Pr: E - PIV-PWC-Pu: E - FIDO-AUTHKAK-Pr: G - FIDO-PINENCSK: W,E - FIDO-PINAUTHSK: Z,W,E - FIDO-AUTHKAK-Pu: G,R - OS-MKEK: E
FIDO AuthenticatorReset	Reset FIDO credentials (FIDO Services)	Status Word	N/A	N/A	None	UU: Unauthenticated User - FIDO-PIN: Z - FIDO-PINS: Z - FIDO-IDENCK: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- FIDO-AUTHRK-Pr: Z - OS-MKEK: E
FIDO AuthenticatorCredentialManagement	List and Delete FIDO Credentials (command authenticated with pinUvAuthToken) (FIDO Services)	Status Word	Command Parameters	Response Data	MAC-Appletsv4	CH: Card Holder - ACA-CAST-HMACK: E - FIDO-PINS: Z,E
FIDO AuthenticatorConfig	Configure FIDO authenticator (enable Enterprise Attestation, set Min PIN Length) (FIDO Services)	Status Word	Command Parameters	N/A	MAC-Appletsv4	CH: Card Holder - FIDO-PINS: Z,E - ACA-CAST-HMACK: E

Table 13: Approved Services

The modes of access shown in the table above are defined as:

- G = Generate: The service generates or derives the CSP/Public Key.
- W = Write: The service inputs the CSP/Public Key.
- E = Execute: The Module executes using the CSP/Public Key.
- R = Read: The service outputs the CSP/Public Key.
- Z = Zeroize: The Module zeroizes the CSP/Public Key after usage.

4.4 Non-Approved Services

The module does not support Non-Approved Services

4.5 External Software/Firmware Loaded

A new FIPS140-3 CMVP validated HID signed applet (partial firmware loading) can be loaded through NXP platform Card Manager Manage Content service and Mandated DAP mechanism. The authenticity of the loaded firmware is verified by the module using DAP public key based on ECDSA P-256 with SHA2-256.

5 Software/Firmware Security

5.1 Integrity Techniques

Firmware Integrity: 32-bit CRC performed over all code located in Flash.

5.2 Initiate on Demand

Firmware Integrity can be done on Demand by performing a power up of the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Hard, tamper evident coating	N/A	N/A

Table 14: Mechanisms and Actions Required

The module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The module uses standard passivation techniques. The module includes Environmental Failure Protection features such as temperature and voltage sensors. Fault Induction mitigation techniques are light sensors and spike sensors on the supply voltage lines.
Identification of internal features such as sensitive components or interconnections is impeded by a fine mesh of metal shield lines that resides at the outermost layers of the chip.
Delivery forms of the module are QFN package, contactless chip card module, or sawn wafer. Therefore, the module does not rely on any physical security based on a package

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-45°C	EFP	Shutdown
HighTemperature	+125°C	EFP	Shutdown
LowVoltage	1.62V	EFP	Shutdown
HighVoltage	6.0V	EFP	Shutdown

Table 15: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-45°C
HighTemperature	+125°C

Table 16: Hardness Testing Temperatures

8 Non-Invasive Security

Please see Section 12 below for information regarding non-invasive security countermeasures.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Temporarily stored in RAM (COD)	plaintext cleared on Deselect (does not persist beyond a power cycle); object identifier to entity association	Dynamic
Temporarily stored in RAM (COR)	plaintext cleared on Reset (does not persist beyond a power cycle); object identifier to entity association	Dynamic
Stored in NVM	plaintext or encrypted with Approved AES CBC with OSMKEK; object identifier or key version to entity association	Static

Table 17: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Entered during manufacturing/ personalization	Vendor generated at manufacture/during personalization	Stored in NVM	Plaintext	N/A	N/A	
I0	External	Stored in NVM	Plaintext	Manual	Electronic	
I1	External	Stored in NVM	Encrypted	Automated	Electronic	KTS-3
I2	External	Stored in NVM	Encrypted	Automated	Electronic	KTS-2-Appletsv4
I3	External	Temporarily stored in RAM (COR)	Encrypted	Automated	Electronic	KTS-1
I4	External	Stored in NVM	Encrypted	Manual	Electronic	KTS-2-Appletsv4

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
I5	External	Stored in NVM	Plaintext	Automated	Electronic	
I6	External	Stored in NVM	Encrypted	Automated	Electronic	BC-1-Auth
I7	External	Stored in NVM	Encrypted	Manual	Electronic	BC-2-UnAuth
I8	External	Temporarily stored in RAM (COD)	Encrypted	Automated	Electronic	BC-2-UnAuth
O0	Stored in NVM	External	Plaintext	Automated	Electronic	
O1	Stored in NVM	External	Encrypted	Automated	Electronic	BC-1-Auth
O2	Temporarily stored in RAM (COR)	External	Encrypted	Automated	Electronic	BC-2-UnAuth

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power-off	Remove the power from the module. All the data in Transient Storage Area are reset	Overwrite with zeroes the RAM when power is removed	Operator initiation
Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	Modify the card or applet life cycle status. This service can be used to zeroize the module	Zeroize OS-MKEK, so all CSPs encrypted by OS-MKEK are destroyed	Operator initiation
Reset Device (ACA RESET CARD service)	The SSPs are cleared using the different objects clearKey() methods, PIN objects are randomized	Overwrite the keys with zeros, and randomization of PIN objects	Operator initiation

Table 19: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
OS-DRBG-EI	Random value from ENT (P) used to seed the AES-256 CTR_DRBG	384 bits - 384 bits	Entropy Input - Neither	ENT		CKG Symmetric Key Generation ENT DRBG
OS-DRBG-SEED	Seed provided to the CTR_DRBG. 3). Generated internally via SP800-90Ar1 DRBG process	384 bits - 384 bits	DRBG seed Value - Neither	DRBG		CKG Symmetric Key Generation ENT DRBG
OS-DRBG-KEY	Current DRBG state value (per IG D.L Resolution 3). Generated internally via SP800-90Ar1 DRBG process	256 bits - 256 bits	DRBG State Value - Neither	DRBG		CKG Symmetric Key Generation ENT DRBG
OS-DRBG-V	Current DRBG state value (per IG D.L Resolution 3). Generated internally via SP800-90Ar1 DRBG process	256 bits - 256 bits	DRBG State Value - Neither	DRBG		CKG Symmetric Key Generation ENT DRBG
OS-SKEK	Used to build OS-MKEK	128 bits - 128 bits	Symmetric key - CSP			BC-1-Auth BC-2-UnAuth BC-3-UnAuth MAC-AES
OS-MKEK	Used to encrypt all secret and private key data stored in NVM. Generated by OS-SKEK permutation (xor between OS-SKEK and a constant value)	128 bits - 128 bits	Symmetric key - CSP			BC-1-Auth BC-2-UnAuth BC-3-UnAuth MAC-AES
OS-DRBG-STATE	Current DRBG State Value	880 - 880	DRBG Internal State - Neither			KAS-1
OS-DRBG-OUTPUT	Unmodified output from the DRBG used for SSP generation. Generated internally via SP800-90Ar1 DRBG process	256 - 256	Entropy Output - Neither	DRBG		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ISD-KENC	AES (128-bit, 192-bit, 256-bit) Master key used to derive ISDSENC.	128-bits, 192-bits, 256-bits - 128-bits, 192-bits, 256-bits	Symmetric Key - CSP			KBKDF-2
ISD-KMAC	AES (128-bit, 192-bit, 256-bit) Master key used to derive ISDSMAC.	128-bits, 192-bits, 256-bits - 128-bits, 192-bits, 256-bits	Symmetric Key - CSP			KBKDF-2
ISD-KDEK	AES (128-bit, 192-bit, 256-bit) Sensitive data decryption key used to decrypt CSPs.	128-bits, 192-bits, 256-bits - 128-bits, 192-bits, 256-bits	Symmetric Key - CSP			KTS-3
ISD-SENC	AES (128-bit, 192-bit, 256-bit) Session encryption key used to encrypt / decrypt secure channel data.	128-bits, 192-bits, 256-bits - 128-bits, 192-bits,	Symmetric Key - CSP		KBKDF-2	BC-1-Auth BC-2-UnAuth BC-3-UnAuth MAC-AES

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		256-bits				
ISD-SMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to verify inbound secure channel data integrity.	128-bits, 192-bits, 256-bits - 128-bits, 192-bits, 256-bits	Symmetric Key - CSP		KBKDF-2	BC-1-Auth BC-2-UnAuth BC-3-UnAuth MAC-AES
ISD-RMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to generate response secure channel data MAC.	128-bits, 192-bits, 256-bits - 128-bits, 192-bits, 256-bits	Symmetric Key - CSP		KBKDF-2	BC-1-Auth BC-2-UnAuth BC-3-UnAuth MAC-AES
SD-KENC	AES (128-bit, 192-bit, 256-bit) Master key used to derive SD-SENC	128, 192, 256 bits - 128, 192, 256 bits	Symmetic key - CSP			KBKDF-2
SD-KMAC	AES (128-bit, 192-bit, 256-bit) Master key used to derive SD-SMAC	128, 192, 256 bits - 128, 192, 256 bits	Symmetric key - CSP			KBKDF-2
SD-KDEK	AES (128-bit, 192-bit, 256-bit) Sensitive data decryption key used to decrypt CSPs.	128, 192, 256 bits -	Symmetric key - CSP			KTS-2-Appletsv4 KTS-3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128, 192, 256 bits				
SD-SENC	AES (128-bit, 192-bit, 256-bit) Session encryption key used to encrypt / decrypt secure channel data.	128, 192, 256 bits - 128, 192, 256 bits	Symmetric key - CSP		KBKDF-2	BC-2-UnAuth
SD-SMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to verify inbound secure channel data integrity	128, 192, 256 bits - 128, 192, 256 bits	Symmetric key - CSP		KBKDF-2	MAC-AES
SD-RMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to generate response secure channel data MAC.	128, 192, 256 bits - 128, 192, 256 bits	Symmetric key - CSP		KBKDF-2	MAC-AES
SD-DAPK	ECC public key used for Mandated DAP	256 bits - 256 bits	Public key - PSP			ECDSA-DigSig-2
ACA-ADMK	AES 128-bits Administrator Key used to authenticate the AA role	128-bits - 128-bits	Symmetric Key - CSP			BC-3-UnAuth
ACA-SKISK	AES 128-bits Secure Key Injection Session Key used to download keys within Secure Key Injection protocol	128-bits - 128-bits	Symmetric Key - CSP			KTS-2-Appletsv4
ACA-PIN	6-63 characters string PIN used for local PIN verification	48-504 bits - N/A	Authentication PIN - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ACA-PUK	8-byte binary PIN Unlocking Key used to confirm authorization to unblock a blocked PIN.	8-bytes - N/A	N/A - CSP			
ACA-CAST-HMACK	HMAC 160-bits static key used for HMAC Cryptographic Algorithm Self-Tests	160-bits - 160-bits	Symmetric Key - CSP			MAC-Appletsv4
ACA-CAST-KWPK	AES 128-bits static key used for KWP Cryptographic Algorithm Self-Tests	128-bits - 128-bits	Symmetric Key - CSP			KTS-2-Appletsv4
PIVX-GPK-Pr	General purpose key with usage determined outside the Module scope. The following key types are supported: RSA (2048-bit, 3072-bit, 4096-bit), ECC P-256 and ECC P-384 curves.	2048-bits, 3072-bits, 4096-bits - 128, 192, 112, 128, 140	Private Key - CSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		ECDSA-DigSig-1 KAS-1 RSA-DigSig -1-Appletsv4 RSA-Decrypt-1-Appletsv4
PIV-AuK-Pr	PIV Card Application Authentication Key (9A): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256, P-384) private key for signature generation	256, 384, 2048, 3072, 4096 bits - 128, 192, 112, 128, 140	Private Key - CSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		ECDSA-DigSig-1 KAS-1 RSA-DigSig -1-Appletsv4 RSA-Decrypt-1-Appletsv4
PIV-DSK-Pr	PIV Card Application Digital Signature Key (9C): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256, P-384) private key for signature generation	256, 384, 2048, 3072, 4096 bits - 128, 192, 112, 128, 140	Private Key - CSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		ECDSA-DigSig-1 KAS-1 RSA-DigSig -1-Appletsv4 RSA-Decrypt-1-Appletsv4

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PIV-KMK-Pr	PIV Card Application Key Management Key (9D): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256, P-384) private key for key establishment schemes realization	256, 384, 2048, 3072, 4096 bits - 128, 192, 112, 128, 140	Private Key - CSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		ECDSA-DigSig-1 KAS-1 RSA-DigSig -1-Appletsv4 RSA-Decrypt-1-Appletsv4
PIV-RKMK-Pr	PIV Card Application Key Management Key (82-95): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256, P-384) private key for key establishment schemes realization	256, 384, 2048, 3072, 4096 bits - 128, 192, 112, 128, 140	Private Key - CSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		ECDSA-DigSig-1 KAS-1 RSA-DigSig -1-Appletsv4 RSA-Decrypt-1-Appletsv4
PIV-CaK-Pr	PIV Card ApplicationPIV Card Application Authentication Key (9E): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256, P-384) private key for signature generation Authentication Key (9E): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256, P-384) private key for signature generation	256, 384, 2048, 3072, 4096 bits - 128, 192, 112, 128, 140	Private Key - CSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		ECDSA-DigSig-1 KAS-1 RSA-DigSig -1-Appletsv4 RSA-Decrypt-1-Appletsv4
PIV-SKIKTK-Pr	Secure Key Injection Key Transport Key (F0): RSA (3072-bit): private key for transportation of the SKI Session Key.	3072-bits - 128-bits	Private Key - CSP	RSA-AsymKeyPair		KTS-1
PIV-PWC-Pr	Key used for the PairWise Consistency: ECDSA (P-256, P-384)	256, 384 bits - 128, 192	Private Key - CSP			KAS-1

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
OATH-OTP	HMAC Key (112-bits to 1024-bits) used by the OATH applet for one time password generation.	112-bits to 1024-bits - 112-bits to 1024-bits	Symmetric Key - CSP			MAC-Appletsv4
FIDO-PIN	6-63 characters PIN used for FIDO PIN verification	48bits to 504-bits - N/A	Authentication - Neither			
FIDO-PINS	32 bytes generated during the clientPIN getPINToken/getPINTokenwithPermissions operations and used to authenticate during other operations	128 bits - N/A	Authentication - Neither	CKG Symmetric Key Generation DRBG		MAC-Appletsv4
FIDO-ATTK-Pr	FIDO Attestation (ECDSA P-256) private key for attestation signature generation	256 bits - 128	Private Key - CSP			ECDSA-DigSig-1
FIDO-ENTK-Pr	FIDO Enterprise Attestation (ECDSA P-256) private key for enterprise attestation signature generation	256 bits - 128	Private Key - CSP	ECDSA - AsymKeyPair		ECDSA-DigSig-1
FIDO-PWC-Pr	Key used for the PairWise Consistency: ECDSA (P-256)	128 bits - 128	Private Key - CSP			KAS-1
FIDO-IDENCK	AES 128-bits Encryption Key used to wrap the FIDO-AUTHKSK-Pr to generate credential identifier	128-bits - 128-bits	Symmetric Key - CSP	CKG Symmetric Key Generation DRBG		BC-1-Auth
FIDO-FAUTHK-Pr	FIDO Private Fake Authentication Key (ECDSA P-256) used for fake signature generation in getAssertion operation	256 bits - 128	Private Key - CSP	ECDSA - AsymKeyPair		ECDSA-DigSig-1

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
FIDO-AUTHRK-Pr	FIDO Private Resident Key (ECDSA P-256) used for signature generation	256 bits - 128	Private Key - CSP	ECDSA - AsymKeyPair		ECDSA-DigSig-1
FIDO-AUTHKSK-Pr	FIDO Private Non-Resident Session Key (ECDSA P-256) used for signature generation	256 bits - 128	Private - CSP	ECDSA - AsymKeyPair		ECDSA-DigSig-1
FIDO-AUTHKAK-Pr	FIDO Private Key Agreement Key (ECDH P-256) used to establish a shared secret	256 bits - 128	Private Key - CSP	ECDSA - AsymKeyPair		KAS-1
FIDO-PINENCSK	AES 256-bits PIN Encryption Session key used to decrypt the PIN during clientPIN setPIN/changePIN operations	256-bits - 256-bits	Symmetric Key - CSP		MAC-Appletsv4	BC-2-UnAuth
FIDO-PINAUTHSK	FIDO HMAC (256-bits) PIN Authentication Session Key used to compute / verify authentication codes during clientPIN setPIN/changePIN operations	256-bits - 256-bits	Symmetric Key - CSP		MAC-Appletsv4	MAC-Appletsv4
FIDO-SALTENCSK	AES-256 Salt Encryption Session Key used to decrypt the salt during getAssertion operation	256-bits - 256-bits	Symmetric Key - CSP		MAC-Appletsv4	BC-2-UnAuth
FIDO-SALTAUTHSK	FIDO HMAC (256-bits) Salt Authentication Session Key used to compute / verify authentication codes during getAssertion operations	256-bits - 256-bits	Symmetric Key - CSP		MAC-Appletsv4	MAC-Appletsv4
FIDO-CREDRANDUVK	FIDO HMAC (256-bits) Credential Random with UV Key used to compute an hmac secret during getAssertion operations when UV is present	256-bits - 256-bits	Symmetric Key - CSP	CKG Symmetric Key Generation DRBG MAC-Appletsv4		MAC-Appletsv4

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PIVX-GPK-Pu	General purpose key with usage determined outside the Module scope. The following key types are supported: RSA (2048-bit, 3072-bit, 4096-bit), ECC P-256 and ECC P-384 curves.	2048-bits, 3072-bits, 4096-bits; P-256, P-384 - 128, 192, 112, 128, 140	Public Key - PSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		RSA-AsymKeyPairVerif ECDSA-DigSig-2 KAS-1
PIV-AuK-Pu	PIV Card Application Authentication Key (9A): RSA (2048-bit, 3072-bit, 4096-bit)and ECDSA (P-256, P-384) public key for signature verification	2048-bits, 3072-bits, 4096-bits; P-256, P-384 - 128, 192, 112, 128, 140	Public Key - PSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		RSA-AsymKeyPairVerif ECDSA-DigSig-2 KAS-1
PIV-DSK-Pu	PIV Card Application Digital Signature Key (9C): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256 , P-384) public key for signature verification	2048-bits, 3072-bits, 4096-bits; P-256, P-384 - 128, 192, 112, 128, 140	Public Key - PSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		RSA-AsymKeyPairVerif ECDSA-DigSig-2 KAS-1

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PIV-KMK-Pu	PIV Card Application Key Management Key (9D): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256 , P-384) public key for key establishment schemes realization	2048-bits, 3072-bits, 4096-bits; P-256, P-384 - 128, 192, 112, 128, 140	Public Key - PSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		RSA-AsymKeyPairVerif ECDSA-DigSig-2 KAS-1
PIV-RKMK-Pu	PIV Card Application Key Management Key (82-90): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256 , P-384) public key for key establishment schemes realization	2048-bits, 3072-bits, 4096-bits; P-256, P-384 - 128, 192, 112, 128, 140	Public Key - PSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		RSA-AsymKeyPairVerif ECDSA-DigSig-2 KAS-1
PIV-CaK-Pu	PIV Card Application Authentication Key (9E): RSA (2048-bit, 3072-bit, 4096-bit) and ECDSA (P-256, P-384) public key for signature verification	2048-bits, 3072-bits, 4096-bits; P-256, P-384 - 128, 192, 112, 128, 140	Public Key - PSP	RSA-AsymKeyPair ECDSA - AsymKeyPair		RSA-AsymKeyPairVerif ECDSA-DigSig-2 KAS-1

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PIV-SKIKTK-Pu	Secure Key Injection Key Transport Key (F0): RSA (3072-bit): public key for encryption of the SKI Session Key.	3072-bits - 128	Public Key - PSP	RSA-AsymKeyPair		
PIV-PWC-Pu	Key used for the PairWise Consistency: ECDSA (P-256, P-384)	256, 384 bits - 128, 192	Public Key - PSP			KAS-1
FIDO-ENTK-Pu	FIDO Enterprise Attestation (ECDSA P-256) public key for enterprise attestation signature verification	256-bits - 128	Public Key - PSP	ECDSA - AsymKeyPair		
FIDO-PWC-Pu	Key used for the PairWise Consistency: ECDSA (P-256, P-384)	256-bits - 128	Public Key - PSP			KAS-1
FIDO-AUTHRK-Pu	FIDO Public Resident Key (ECDSA P-256) used for signature verification	256 - 128	Public Key - PSP	ECDSA - AsymKeyPair		ECDSA-DigSig-2
FIDO-AUTHKSK-Pu	FIDO Public Non-Resident Session Key (ECDSA P-256) used for signature verification	256 - 128	Public Key - PSP	ECDSA - AsymKeyPair		
FIDO-AUTHKAK-Pu	FIDO Public Key Agreement Key (ECDH P-256) used to establish a shared secret	256 - 128	Public Key - PSP			

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
OS-DRBG-EI		Temporarily stored in RAM (COR):Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
OS-DRBG-SEED		Temporarily stored in RAM (COR):Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perfo	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				rm Zeroisation service)	
OS- DRBG-KEY		Stored in NVM:Plaintext	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
OS-DRBG-V		Stored in NVM:Plaintext	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
OS-SKEK	Entered during manufacturing/ personalization	Stored in NVM:Plaintext	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	OS-MKEK:Used to build
OS-MKEK		Stored in NVM:Plaintext	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
OS-DRBG-STATE		Stored in NVM:Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
OS-DRBG-OUTPUT		Stored in NVM:Plaintext	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
ISD-KENC	I1	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
ISD-KMAC	I1	Stored in NVM:Encrypted	Until terminati	Destroyed by termination of the module	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			on of module	(LifeCycle/Perform Zeroisation service)	
ISD-KDEK	I1	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	ISD-KMAC:Decrypts ISD-KDEK:Decrypts
ISD-SENC		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
ISD-SMAC		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
ISD-RMAC		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
SD-KENC	I1	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
SD-KMAC	I1	Stored in NVM:Encrypted	Until terminati	Destroyed by termination of the module	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			on of module	(LifeCycle/Perform Zeroisation service)	
SD-KDEK	I1	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
SD-SENC		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
SD-SMAC		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
SD-RMAC		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
SD-DAPK	I5	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
ACA-ADMK	I1 I2	Stored in NVM:Plaintext	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
ACA-SKISK	I3	Stored in NVM:Plaintext	Until terminati	Destroyed by termination of the module	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			on of module	(LifeCycle/Perform Zeroisation service)	
ACA-PIN	I0 I4	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
ACA-PUK	I2 I5	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
ACA-CAST-HMACK		Stored in NVM:Plaintext		N/A	
ACA-CAST-KWPK		Stored in NVM:Plaintext		N/A	
PIVX-GPK-Pr	I1 I2	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIVX-GPK-Pu:Paired With
PIV-AuK-Pr	I1 I2	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-AuK-Pr:Paired With
PIV-DSK-Pr	I1 I2	Stored in NVM:Encrypted	Until terminati	Destroyed by termination of the module	PIV-DSK-Pu:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			on of module	(LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
PIV-KMK-Pr	I1 I2	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-KMK-Pu:Paired With
PIV-RKMK-Pr	I1 I2	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-RKMK-Pu:Paired With
PIV-CaK-Pr	I1 I2	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-CaK-Pu:Paired With
PIV-SKIKTK-Pr		Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-SKIKTK-Pu:Paired With
PIV-PWC-Pr		Stored in NVM:Encrypted		N/A	FIDO-PWC-Pu:Paired With
OATH-OTP	I1 I2	Stored in NVM:Plaintext	Until terminati	Destroyed by termination of the module	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			on of module	(LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
FIDO-PIN	I7	Stored in NVM:Plaintext	Until "Reset Device" zeroization method is invoked	Reset Device (ACA RESET CARD service)	
FIDO-PINS	I8 O2	Temporarily stored in RAM (COR):Plaintext	Until power-cycle	Power-off Reset Device (ACA RESET CARD service)	
FIDO-ATTK-Pr	I1 I2	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
FIDO-ENTK-Pr	I1 I2	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	FIDO-ENTK-Pu:Paired With
FIDO-PWC-Pr		Stored in NVM:Encrypted		N/A	FIDO-PWC-Pu:Paired With
FIDO-IDENCK		Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
FIDO-FAUTHK-Pr		Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	
FIDO-AUTHRK-Pr		Stored in NVM:Encrypted	Until terminati	Destroyed by termination of the module	FIDO-AUTHRK-

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			on of module	(LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	Pr:Paired With
FIDO-AUTHKSK-Pr	O1 I6	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	FIDO-AUTHKSK-Pu:Paired With
FIDO-AUTHKAK-Pr		Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	FIDO-AUTHKAK-Pu:Paired With
FIDO-PINENCSK		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Reset Device (ACA RESET CARD service)	
FIDO-PINAUTHSK		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Reset Device (ACA RESET CARD service)	
FIDO-SALTENCSK		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Reset Device (ACA RESET CARD service)	
FIDO-SALTAUTHSK		Temporarily stored in RAM (COD):Plaintext	Until power-cycle	Power-off Reset Device (ACA RESET CARD service)	
FIDO-CREDRANDUVK		Stored in NVM:Plaintext	Until "Reset Device" zeroization method is invoked	Reset Device (ACA RESET CARD service)	
PIVX-GPK-Pu	O0	Stored in NVM:Encrypted	Until terminati	Destroyed by termination of the module	PIVX-GPK-Pr:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			on of module	(LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	
PIV-AuK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-AuK-Pr:Paired With
PIV-DSK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-DSK-Pr:Paired With
PIV-KMK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-KMK-Pr:Paired With
PIV-RKMK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-RKMK-Pr:Paired With
PIV-CaK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	PIV-CaK-Pr:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Reset Device (ACA RESET CARD service)	
PIV-SKIKTK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	PIV-SKIKTK-Pr:Paired With
PIV-PWC-Pu		Stored in NVM:Encrypted		N/A	PIV-PWC-Pr:Paired With
FIDO-ENTK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	FIDO-ENTK-Pr:Paired With
FIDO-PWC-Pu		Stored in NVM:Encrypted		N/A	FIDO-PWC-Pr:Paired With
FIDO-AUTHRK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service) Reset Device (ACA RESET CARD service)	FIDO-AUTHRK-Pr:Paired With
FIDO-AUTHKSK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	FIDO-AUTHKSK-Pr:Paired With
FIDO-AUTHKAK-Pu	O0	Stored in NVM:Encrypted	Until termination of module	Destroyed by termination of the module (LifeCycle/Perform Zeroisation service)	FIDO-PWC-Pr:Used With FIDO-AUTHKAK-Pr:Paired With

Table 21: SSP Table 2

9.5 Transitions

- NIST will transition away from the use of SHA-1 for applying cryptographic protection to all applications by December 31, 2030.
- The minimum key size will transition from 112-bits to 128-bits in 2030.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity	32-bit CRC performed over all code located in NVM	32-bit CRC	SW/FW Integrity	No switch to Mute state	If the integrity test fails at power on, the module enters the hard error (MUTE) state

Table 22: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt (A2713)	128-bit	KAT	CAST	No switch to Mute state	Encrypt	Performed automatically on every boot
AES-CBC (A2713)	128-bit	KAT	CAST	No switch to Mute state	Decrypt	Performed automatically on every boot
AES-CMAC Encrypt (A2713)	128-bit	KAT	CAST	No switch to Mute state	Encrypt	Performed automatically on every boot
AES-CMAC (A2713)	128-bit	KAT	CAST	No switch to Mute state	Decrypt	Performed automatically on every boot
Counter DRBG (A2713)	256-bit	KAT	CAST	No switch to Mute state	Health Tests: Generate, Reseed, Instantiate functions per Section 11 in NIST SP800-90Ar1	Performed automatically on every boot
ECDSA SigGen (FIPS186-5) (A6534)	P-521 SHA-256	KAT	CAST	No switch to Mute state	Signature Generation	Performed automatically on every boot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-5) (A6534)	P-521 SHA-256	KAT	CAST	No switch to Mute state	Signature Verification	Performed automatically on every boot
KDA HKDF Sp800-56Cr1 (A2713)	SHA-1, SHA2-256, SHA2-384, SHA2-512	KAT	CAST	No switch to Mute state	Key Derivation Function per NIST SP 800-56Cr1	Performed automatically on every boot
KDF SP800-108 (AES-128) (A2713)	Counter mode with AES-128	KAT	CAST	No switch to Mute state	Key Derivation Function per NIST SP 800-108r1 (Counter mode)	Performed automatically on every boot
KDF SP800-108 (A2713)	Feedback Mode with HMAC-SHA1	KAT	CAST	No switch to Mute state	Key Derivation Function per NIST SP 800-108r1 (Counter mode)	Performed automatically on every boot
RSA SigVer (FIPS186-5) (A6535)	2048-bit SHA2-256	KAT	CAST	No switch to Mute state	Signature Verification	Performed automatically on every boot
SHA-1 (A2713)	SHA-1	KAT	CAST	No switch to Mute state	Hash generation	Performed automatically on every boot
SHA2-256 (A2713)	SHA2-256	KAT	CAST	No switch to Mute state	Hash generation	Performed automatically on every boot
SHA2-512 (A2713)	SHA2-512	KAT	CAST	No switch to Mute state	Hash generation	Performed automatically on every boot
Firmware Load Test	ECDSA P-256 with SHA2-256	Load Test	SW/FW Load	No switch to Mute state	Signature Verification based on ECDSA P-256 with SHA2-256	Upon loading of firmware from an external source (e.g. the applet).
NIST SP800-90B ENT (P) Repetition Count Test (RCT)	-	NIST SP 800-90B Health Test	CAST	Implicit, based on output of entropy	-	Performed continuously by the entropy source

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
NIST SP800-90B ENT (P) Developer Defined Heath Test Transition Count Test	-	NIST SP 800-90B Health Test	CAST	Implicit, based on output of entropy	-	Performed continuously by the entropy source
NIST SP800-90B ENT (P) Developer Defined Heath Test ChiSquare Test	-	NIST SP 800-90B Health Test	CAST	Implicit, based on output of entropy	-	Performed continuously by the entropy source
NIST SP800-90B ENT (P) Developer Defined Heath Test Amplitude Limiter Analog Test	-	NIST SP 800-90B Health Test	CAST	Implicit, based on output of entropy	-	Performed continuously by the entropy source
AES-KWP (A6112)	128-bits	KAT	CAST	No switch to Mute state	Decrypt	Before first use
HMAC-SHA-1 (A6112)	HMAC-SHA-1 with a 160-bits key	KAT	CAST	No switch to Mute state	-	Before first use
Generate PCT RSA	Pairwise consistency test - 2048-bits / 3072-bits / 4096-bits	PCT	PCT	No switch to Mute state	Cipher decrypt / encrypt	On keypair generation
Generate PCT ECC	Pairwise consistency test - 256-bits / 384-bits	PCT	PCT	No switch to Mute state	ECDSA Sign/Verify ECDH Key Agreement	On keypair generation
Generate PCT ECC FIDO 1	Pairwise consistency test - 256-bits	PCT	PCT	No switch to Mute state	ECDSA Sign/Verify	On Signature key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Generate PCT ECC FIDO 2	Pairwise consistency test - 256-bits	PCT	PCT	No switch to Mute state	ECDH Key Agreement	On key Agreement pair generation
KAS-ECC-SSC Sp800-56Ar3 (A5910)	P-384 Scheme: onePassDh: KAS Role: initiator, responder	KAT	CAST	No switch to Mute state	Shared Secret Computation (Z)	Performed automatically on every boot
RSA SigGen (FIPS186-5) (A6535)	2048-bit SHA2-256	KAT	CAST	No switch to Mute state	Signature Generation	Performed automatically on every boot

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity	32-bit CRC	SW/FW Integrity	Repeated after every 500,000 CAPDUs/commands	Automatic execution per module design (the test is repeated after every 500,000 CAPDUs/commands)

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
AES-CMAC Encrypt (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
AES-CMAC (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
ECDSA SigGen (FIPS186-5) (A6534)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
ECDSA SigVer (FIPS186-5) (A6534)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDA HKDF Sp800-56Cr1 (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
KDF SP800-108 (AES-128) (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
KDF SP800-108 (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A6535)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
SHA-1 (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
SHA2-256 (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-512 (A2713)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
Firmware Load Test	Load Test	SW/FW Load	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
NIST SP800-90B ENT (P) Repetition Count Test (RCT)	NIST SP 800-90B Health Test	CAST	On Demand	Manually, by rebooting the module/resetting the entropy source
NIST SP800-90B ENT (P) Developer Defined Heath Test Transition Count Test	NIST SP 800-90B Health Test	CAST	On Demand	Manually, by rebooting the module/resetting the entropy source
NIST SP800-90B ENT (P) Developer Defined Heath	NIST SP 800-90B Health Test	CAST	On Demand	Manually, by rebooting the module/resetting the entropy source

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Test ChiSquare Test				
NIST SP800-90B ENT (P) Developer Defined Heath Test Amplitude Limiter Analog Test	NIST SP 800-90B Health Test	CAST	On Demand	Manually, by rebooting the module/resetting the entropy source
AES-KWP (A6112)	KAT	CAST	On Demand	Manually, by executing the following command after having selected the ACA (as per Table 28) CLA = 80, INS = 56, P1 = 02, P2 = 22, Le = 00
HMAC-SHA-1 (A6112)	KAT	CAST	On Demand	Manually, by executing the following command after having selected the ACA (as per Table 28) CLA = 80, INS = 56, P1 = 02, P2 = 44, Le = 00
Generate PCT RSA	PCT	PCT	Before first use	Manually, by rebooting the module
Generate PCT ECC	PCT	PCT	Before first use	Manually, by rebooting the module
Generate PCT ECC FIDO 1	PCT	PCT	Before first use	Manually, by rebooting the module
Generate PCT ECC FIDO 2	PCT	PCT	Before first use	Manually, by rebooting the module
KAS-ECC-SSC Sp800-56Ar3 (A5910)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service)

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.
RSA SigGen (FIPS186-5) (A6535)	KAT	CAST	On Demand	Manually, all the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120, and Le = 00.

Table 25: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
CRYPTO (Hard) error state	The module enters in CRYPTO error state when one of the AES KWP or HMAC-SHAx self test has failed. In that case, all module subsequent APDU's return 6600 status words until a power off is done	AES KWP Failure HMAC-SHAx Failure	Power Cycle; But in the event that the error persists, the module must be returned to the vendor	Return 6600 Status
MUTE (Hard) error state	All the Self-Tests can be performed on-demand with the GET DATA APDU command (Info service) with the following parameters: CLA = 80, INS = CA, P1 = 00, P2 = FE, Lc = 04, Incoming Data = DF4B0120,	In case of failure of a pre-operational, conditional self-test or NIST SP 800-90B compliant	A reset of the module can be attempted but in the event that the error persists, the module must	Return 66A7 (failure) status

Name	Description	Conditions	Recovery Method	Indicator
	and Le = 00. The expected result is FE04DF4B0120. The return code 9000 signifies success. In case of a failure, the module enters a hard error (MUTE) state and returns a code/status indicator	entropy source health test	be returned to the vendor	

Table 26: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

To verify the Cryptographic Module runs in Approved mode of operation, use the following commands:

- Select Applet (ACA) (Table 27)
- ACA Get FIPS Module Configuration (Table 28)

Code	Value	Description
CLA	'00'	ISO Cla Value
INS	'A4'	SELECT
P1	'04'	Select by name
P2	'00'	Reference Control Parameter P2
Lc	'07'	Length of data field
Data	'A0000000791000'	ACA AID
Le	'00'	Length of response data

Table 27: Select Applet (ACA)

Code	Value	Description
CLA	'80'	Proprietary Cla Value
INS	'56'	GET PROPERTIES
P1	'01'	Get Approved Configuration
P2	'00'	Reference Control Parameter P2
Lc	Empty	
Data	Empty	
Le	'00'	Length of response data

Table 28: ACA Get FIPS Module Configuration Command

Code	Value	Description
Data	'2401XX'	Approved mode configuration, where XX can have the following value: • 'A5': Approved mode
SW1/SW2	'9000'	Status Words

Table 29: ACA Get FIPS Module Configuration Response

11.2 Administrator Guidance

The cryptographic module is delivered with default ACA-ADM, ACA-PIN, SD-KENC, SD-KMAC and SD-KDEK authentication data for SSD1.
No authenticated operation is allowed with these authentication data until those default values are replaced.

- For Crescendo Applets Cryptographic Officer (CCO), SD keys need to be replaced via SSD PUT KEY service
- For Application Administrator, ACA-ADM key needs to be replaced via ACA PUT KEY service
- For Card Holder (CH), ACA-PIN needs to be replaced via ACA CHANGE REFERENCE DATA or PIVEXT CHANGE REFERENCE DATA service

11.3 Non-Administrator Guidance

To ensure that all modules reach their destination safely and in perfect condition, professional transportation services that specialize in secure and reliable deliveries are used.

Secure Handling: The modules are carefully packaged and handled to prevent damage during transit.
Trusted Carriers: Deliveries are managed by experienced logistics providers known for their secure and trackable shipping processes.
Tracking Information: Once the modules are shipped, a tracking number is issued to monitor its journey in real time.
Delivery Confirmation: A signature or confirmation is required upon delivery to ensure the modules reach the correct recipient.

11.4 Design and Rules

A Configuration Management system is used for the development of the cryptographic module, the module components, as well as the associated documentation. They are all tracked with their module name, as well as its version number.

The firmware is implemented using a high-level, non-proprietary language.

11.5 Maintenance Requirements

No specific maintenance requirements apply to the module.

11.6 End of Life

The module must be zeroised (using the Perform zeroisation service per Section 4.3 of this document) in order to perform secure sanitization of the module.

12 Mitigation of Other Attacks

12.1 Attack List

The module is protected against the following non-invasive attacks: SPA, DPA, Timing Analysis and Fault Induction using a combination of firmware and hardware countermeasures. Protection features include detection of out-of-range supply voltages, frequencies or temperatures, fault induction mitigations like light sensors, voltage glitch sensors and an active shield, and detection of illegal address or instruction.

12.2 Mitigation Effectiveness

All cryptographic computations and sensitive operations such as critical data comparison provided by the module are designed to be resistant to timing and power analysis. Sensitive operations are performed in constant time, regardless of the execution context (parameters, keys, etc.), owing to a combination of hardware and firmware features. In addition to the non-invasive attacks, the module also uses standard passivation techniques and is protected by active shielding (a grid of top metal layer wires with tamper response) which qualifies for classification under mitigation of other attacks.