Chunghwa Telecom Co., Ltd.

HiCOS PKI Applet V4 on IDEMIA ID-One Cosmo X

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.1
Last update: 2026-07-22

Prepared by:

atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759
www.atsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document defines the Security Policy for the Chunghwa Telecom Co., Ltd. HiCOS PKI AppletV4 on IDEMIA ID-One Cosmo X cryptographic module and hereafter denoted the module. The module, validated to FIPS 140-3 overall Security Level 3, is a single chip module implementing the Global Platform operational environment, with Card Manager and HiCOS PKI AppletV4.

1.2 Security Levels

The FIPS 140-3 security levels for the module are as follows:

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module, a single chip embodiment validated to FIPS 140-3 Overall Security Level 3, is the combination of the HiCOS PKI Applet (denoted *PKI Applet* below) running on and bound to the IDEMIA ID-One Cosmo X (denoted *platform* below).

The *platform* provides an operational environment for the *PKI Applet*, all cryptographic algorithm implementations and random number and key generation, card lifecycle management, and key storage and protection are provided by the *platform*. The factory configuration of the module constrains the module to the set of services provided by the platform's Card Manager (implementing a standard set of GlobalPlatform services) and the PKI Applet.

The *PKI Applet* is a Java Card applet that provides security for stored user data and credentials and a set APDU commands of PKI services (e.g., for strong authentication, encryption and digital signatures).
Module Type: Hardware
Module Embodiment: Single Chip

Cryptographic Boundary:

The module is designed to be embedded into a plastic card body, with a contact plate and/or contactless antenna connections, or in a USB token or other standard IC packaging, such as SOIC, QFN or MicroSD.

The physical form of the module is depicted in Figure 1 below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads for the module's interfaces, shown as circles in the figure. See Table 12: Ports and Interfaces for the function of each interface.

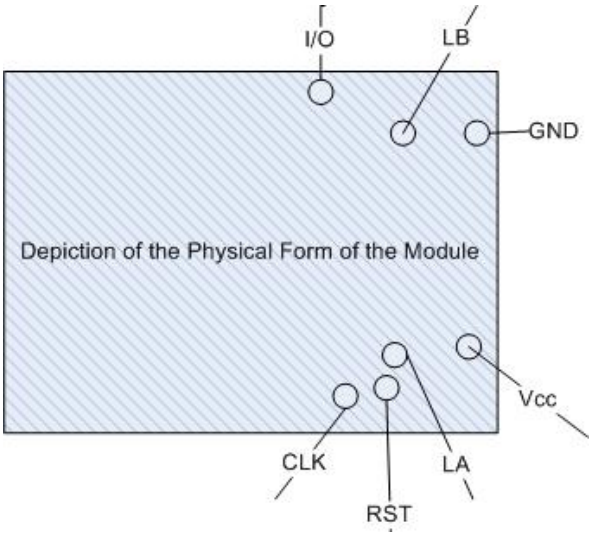

Figure 1: Depiction of Physical Form

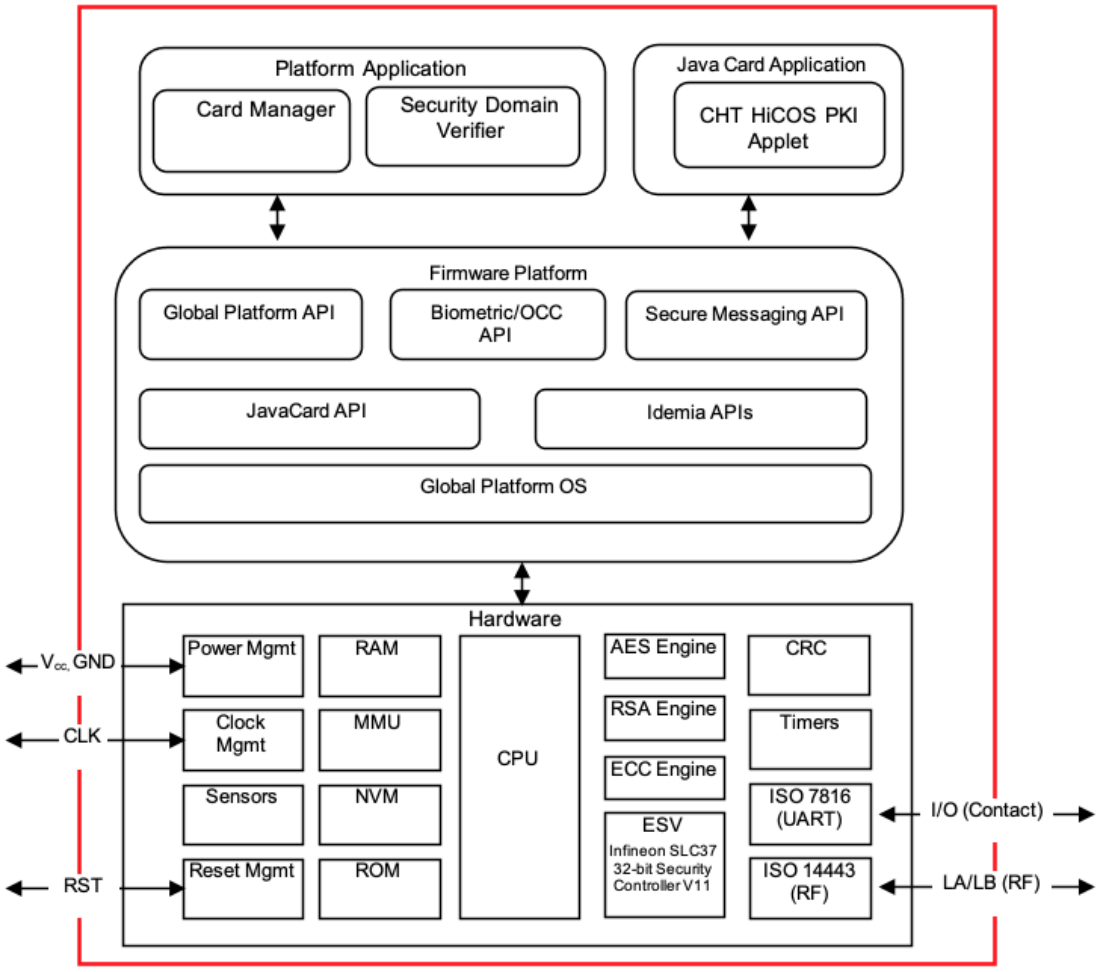

Figure 2: Block Diagram

Section 4 describes applet functionality in greater detail. The JavaCard and Global Platform APIs are internal interfaces available only to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary). In the figure above, the Security Domain Verifier prevents loading an unauthorized (unsigned) code package into the module and does not provide separate services.

All code is executed from ROM and NVM.

The chip family provides accelerators for AES, RSA, ECC, CRC and an SP800-90B ESV. The communications options for contact and contactless configurations are present in the physical circuitry of all members of the processor family but are selectively enabled during module manufacturing.

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
HiCOS PKI Applet v4 On Cosmo X	09A4D1	0400020E	32-bit Arm®	Contact-Only, Contactless-Only or Dual Interface

Table 2: Tested Module Identification – Hardware

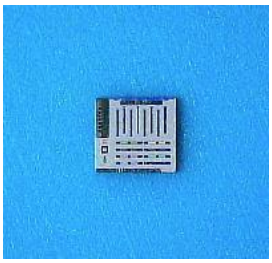

Figure 3: Bottom View

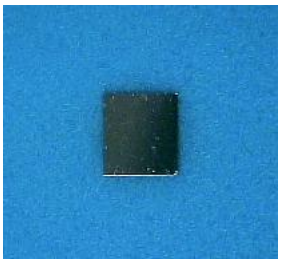

Figure 4: Top View

2.3 Excluded Components

There are no components within the cryptographic boundary excluded from the FIPS 140-3 requirements.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	The module only supports an Approved mode of operation.	Approved	The indicator of mode of operations of a given HiCOS PKI Applet instance can be retrieved at any time using the GET DATA (tag 'FE00') command (PKI Applet Info service). The module will return '01', the value of tag "FE00" to indicate execution in "FIPS140-3 Level 3 Mode of Operations"

Table 3: Modes List and Description

The module is always in the Approved mode.

2.5 Algorithms

Approved Algorithms:

The module only implements approved algorithms and does not implement any non-approved algorithms. Therefore, the module only has approved mode of operation.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4945	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A4945	Direction - Generation Key Length - 128, 192, 256	SP 800-38B
AES-ECB	A4945	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
Counter DRBG	A4945	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4945	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4945	Component - No, Yes Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4945	Component - No, Yes Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
KAS-ECC CDH-Component (CVL)	A4945	Function - Key Pair Generation Curve - P-224, P-256, P-384, P-521	SP 800-56A Rev. 3
KAS-ECC Sp800-56Ar3	A7823	Domain Parameter Generation Methods - P-384 Function - Key Pair Generation Scheme - ephemeralUnified - KAS Role - Responder KDF Methods - twoStepKdf - Key Length - 256	SP 800-56A Rev. 3
KDF SP800-108	A4945	KDF Mode - Counter Supported Lengths - Supported Lengths: 64, 256	SP 800-108 Rev. 1
RSA Decryption Primitive Sp800-56Br2 (CVL)	A4945	Modulo - 2048, 3072, 4096	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-4)	A4945	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.3 Private Key Format - Chinese Remainder Theorem	FIPS 186-4
RSA SigGen (FIPS186-4)	A4945	Signature Type - PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA Signature Primitive (CVL)	A4945	Private Key Format - crt	FIPS 186-4
RSA SigVer (FIPS186-4)	A4945	Signature Type - PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A4945	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-384	A4945	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-512	A4945	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Type:Symmetric and Asymmetric	N/A	CKG for asymmetric keys as per SP 800-133Rev2 section 4 example 1 with no post processing on the U value

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES-ECB	BC-UnAuth	Symmetric encryption and Decryption	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	AES-ECB: (A4945)
AES-CBC	BC-UnAuth	Symmetric encryption and Decryption	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	AES-CBC: (A4945)
AES-CMAC	MAC	Message Authentication Code	Key Size:128, 192, 256 bits	AES-CMAC: (A4945)

Name	Type	Description	Properties	Algorithms
			Key Strength:128, 192, 256 bits	
CTR DRBG	DRBG	CTR_DRBG using AES-256	Derivation Function:Enabled Prediction Resistance:No Key Size:256 bits Key Strength:256 bits	Counter DRBG: (A4945)
ECDSA keyGen	AsymKeyPair-KeyGen CKG	ECDSA key generation using Testing Candidates	Curves:P-256, P-384, P-521 Strength:128, 192, 256 bits	ECDSA KeyGen (FIPS186-4): (A4945) CKG: ()
ECDSA sigGen	DigSig-SigGen	ECDSA Digital Signature Generation	Message Digest:SHA2-256, SHA2-384, SHA2-512 Curves:P-256, P-384, P-521 Strength:128, 192, 256 bits	ECDSA SigGen (FIPS186-4): (A4945)
ECDSA sigGen component	DigSig-SigGen	ECDSA Digital Signature Generation Component	Curves:P-256, P-384, P-521 Strength:128, 192, 256 bits	ECDSA SigGen (FIPS186-4): (A4945)
ECDSA sigVer	DigSig-SigVer	ECDSA Digital Signature Verification	Message Digest:SHA2-256 Curves:P-256, P-384, P-521 Strength:128, 192, 256 bits	ECDSA SigVer (FIPS186-4): (A4945)
KAS-ECC	KAS-Full	ECDH Key Agreement Scheme	IG:IG D.F Scenario 2 path (2), <end-to-end> Key confirmation:No Key derivation:KDA (tested as part KAS certificate) Caveat:Key establishment methodology provides between 256 and 256 bits of security strength	KAS-ECC Sp800-56Ar3: (A7823)
KAS-ECC CDH Component	KAS-SSC	ECDH Component	Curves:P-256, P-384, P-521	KAS-ECC CDH-Component: (A4945)

Name	Type	Description	Properties	Algorithms
			Strength:128, 192, 256 bits	
RSA keyGen	AsymKeyPair-KeyGen CKG	RSA Key Generation	Generation Method:A.1.6 Probable Primes with conditions based on Auxiliary Probable Primes Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA KeyGen (FIPS186-4): (A4945) CKG: ()
RSA sigGen	DigSig-SigGen	RSA Digital Signature Generation	Scheme:PSS Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA SigGen (FIPS186-4): (A4945)
RSA sigPrim	DigSig-SigGen	RSA Digital Signature Generation primitive	Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA Signature Primitive: (A4945)
RSA sigVer	DigSig-SigVer	RSA Digital Signature Verification	Scheme:PSS using SHA2-256 Key Size:2048 bits Key Strength:112 bits	RSA SigVer (FIPS186-4): (A4945)
RSA Decryption Primitive	KTS-Wrap	RSA decryption primitive	Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA Decryption Primitive Sp800-56Br2: (A4945)
KBKDF SP 800-108	KBKDF	Key Based Key Derivation with Counter	Fixed Data Order:Middle Fixed Data Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	KDF SP800-108: (A4945)
SHA	SHA	Message Digest Generation using SHA2-256, SHA2-384, SHA2-512		SHA2-256: (A4945) SHA2-384: (A4945) SHA2-512: (A4945)
KTS (AES-CBC + AES-CMAC)	KTS-Unwrap KTS-Wrap	SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	Standard:SP 800-38F IG D.G:Approved key-wrapping technique "combination"	AES-CBC: (A4945) AES-CMAC: (A4945)

Name	Type	Description	Properties	Algorithms
			method (AES-CBC + AES-CMAC) Caveat:Key establishment methodology provides between 256 and 256 bits of security strength	

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

IG C.K: The module includes CAVP certificates using FIPS 186-4 tests done prior to the IG C.K transition date of Feb 5th, 2024, and are mathematically identical to FIPS 186-5 CAVP tests, hence the module claim FIPS 186-5 compliance for these tests.

The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS.

Compliance to SP 800-56ARev3 assurances

For KAS-ECC, the module satisfies IG D.F Scenario 2 path (2) (i.e., tested compliance with One Pass DH key agreement schemes followed by the derivation of the key as shown in Section 5.8 of SP 800-56Arev3). The key derivation function complies to SP 800-56C rev2 (i.e., One-Step KDF). Furthermore, the module obtained the appropriate assurances, as required in Sections 5.6.2 of SP 800-56A rev3.

5.6.2.1 Assurances Required by a Key Pair Owner:

5.6.2.1.1 Owner Assurance of Correct Generation: The module performs key generation for ephemeral keys. Using the key generation algorithm validated by the CAVP (ECDSA KeyGen Cert. #A4945). For static keys, a trusted third party (TTP) generates the key pair and securely enters the module using SP800-38F key wrapping (AES + CMAC). The module will perform a pairwise consistency check upon generating ECDH keys.

5.6.2.1.2 Owner Assurance of Private-Key Validity: For ephemeral key pair, the module provides the assurance since the module generates it. For static key pairs, after receiving the key pair, the module performs a separate check to determine that the private key is in the correct interval.

5.6.2.1.3 Owner Assurance of Public-Key Validity: For both static and ephemeral key pairs, the module performs a full public-key validation as a separate process from the key-pair generation process.

5.6.2.1.4 Owner Assurance of Pair-wise Consistency: The module performs a pair-wise consistency test when the module generates ephemeral key pairs and when static key-pairs are entered into the module.

5.6.2.1.5 Owner Assurance of Possession of the Private Key: For ephemeral key pairs, the owner generates the key pair as specified in Section 5.6.1 and for static key pairs, the module performs a pair-wise consistency test when the key pairs are entered.

5.6.2.2 Assurances Required by a Public Key Recipient

5.6.2.2.1 Recipient’s assurance Static Public-Key Validity: The module makes used of approved EC curves listed in SP800-140D and performs a successful full public-key validation of the received public key i.e., ECC Full Public-Key Validation Routine specified in SP800-56A rev3 section 5.6.2.3.3.

5.6.2.2.2 Recipient Assurance of Ephemeral Public-Key Validity: Not applicable. The module generates ephemeral keys and does not ever receive them.

5.6.2.2.3 Recipient's assurance of owner's possession of private key can be met via the use of a Trusted Third party that requires the key confirmation procedure. Both of which are handled by the entity outside of the module that requested the ECDH Key Agreement service from the module. That is, such checks are out of the module's scope.

5.6.2.2.4 Recipient Assurance of the Owner's Possession of an Ephemeral Private Key: Not applicable. The module generates ephemeral keys and does not ever receive them.

5.6.2.3 Public Key Validation Routines

The module performs the required public key validation before initiating the handshake following 5.6.2.3.3 ECC Full Public-Key Validation Routine.

2.8 RBG and Entropy

Cert Number	Vendor Name
E107	Infineon Technologies AG

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Infineon SLC37 32-bit Security Controller V11 Entropy Source	Physical	SLC37 32-bit Security Controller V11	1 bits	0.418445 bits	non-vetted conditioning function

Table 8: Entropy Sources

RNG Information: The module implements an approved SP 800-90Ar1 Deterministic Random Bit Generator in the form of CTR_DRBG. The DRBG seed is generated from the SP 800-90B entropy source.

2.9 Key Generation

The module implements key generation services for RSA, ECDSA, EC Diffie-Hellman, and AES keys in compliance to SP800-133rev2 Cryptographic Key Generation (CKG, vendor affirmed).

2.10 Key Establishment

The module provides an approved SP800-56Arev3 EC Diffie-Hellman Key Agreement Scheme that is fully compliant with IG D.F scenario 2 path (2).

The module provides an approved SP800-38F Key Transport that is fully compliant to IG D.G i.e., employing an approved key-wrapping technique using a "combination" method: AES-CBC together with an approved authentication method AES-CMAC.

2.11 Industry Protocols

The GP Secure Channel Protocol '03' establishment provides mutual authentication service as well as establishment of a secure channel to protect confidentiality and integrity of the transmitted data.

The ISO7816 Secure Messaging protocol is a Secure Channel Protocol based on ISO7816 Secure Messaging Format which establishes a secure channel to protect confidentiality and integrity of transmitted information.

The ISO7816 Secure Messaging protocol conforms to SP800-56A for the establishment of a shared secret and key derivation for session keys.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
RST [ISO 7816: Reset] Not available in contactless-only configurations	Control Input	Reset Signal
CLK [ISO 7816: Clock] Not available in contactless-only configurations	Control Input	Clock Signal
I/O [ISO 7816: Input/Output] Not available in contactless-only configurations	Data Input Data Output Control Input Status Output	APDU Command data field; ATR and APDU Response data field; APDU Header (CLA INS P1-P2); Status Word SW1-SW2
LA, LB [ISO 1443: Antenna] (Not available in contact-only configurations)	Data Input Data Output Control Input Status Output	APDU Command data field; ATR and APDU Response data field; APDU Header (CLA INS P1-P2); Status Word SW1-SW2
Vcc, GND [ISO 7816: Supply voltage] (Not available in contactless-only configurations)	Power	None

Table 9: Ports and Interfaces

The module does not implement any control output interface.

3.2 Trusted Channel Specification

The module does not transmit unprotected CSPs over any interface.

The module does not implement a trusted channel.

3.3 Control Interface Not Inhibited

The control interface is inhibited while in the error state without any exceptions.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
GP Secure Channel Protocol Authentication	Identity-based authentication using Global Platform Secure Channel Protocol '03' Authentication	AES-CMAC	1/2^128 = 2.9E39 (for any of AES128/192/256 SD-DAK/SC-ENC, assuming a 128bit block)	9 /2^128 = 2.6E38 (for any of AES128/192/256 SD-DAK/SC-ENC, assuming a 128bit block)
PKI Applet Symmetric Key Authentication (External Authentication)	It provides a challenge-response-based proof of the authenticity and the access rights of a terminal.	AES-CBC	1/2^128 = 2.9E-39	5/2^128 = 1.4E-38
PKI Applet Secret Value Authentication	This authentication method compares a PIN value sent to the Module over an encrypted channel to the stored PKI-PIN value; if the two values are equal, the operator is authenticated.	N/A	3.97E-67	5.96E-66

Table 10: Authentication Methods

GP Secure Channel Protocol Authentication Method

The GP Secure Channel Protocol Authentication method is provided by the *GP Secure Channel* service, the *PKI Applet Secure Channel* service. These services each invoke the same underlying library calls, but from the Card Manager and PKI Applet respectively.

The SD-DAK and SD-DMK keys are used to derive the SC-ENC and SC-C-MAC keys, respectively. The SC-C-MAC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the module in the CO role).

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

- 1/2^128 = 2.9E-39 (for any of AES-128/192/256 SD-DAK/SC-ENC, assuming a 128-bit block)

The module enforces a “slowdown mechanism” that increases the response time between two authentications attempts following a failed authentication, such that no more than 9 attempts are possible in a one-minute period. The probability that a random attempt will succeed over a one-minute interval is:

- 9 /2^128 = 2.6E-38 (for any of AES-128/192/256 SD-DAK/SC-ENC, assuming a 128-bit block)

GP Secure Channel Protocol establishment provides mutual authentication service as well as establishment of a secure channel to protect confidentiality and integrity of the transmitted data.

PIV Symmetric Key Authentication Method

The PKI Applet Symmetric Key Authentication method is provided by the PKI Applet Entity authentication with symmetric key service. The external entity obtains an 16-byte challenge from the module, encrypts the challenge and sends the cryptogram to the module. The module decrypts the cryptogram, and the external entity is authenticated if the decrypted

value matches the challenge. This method is used by the PKI Applet Authentication and Administrator Authentication services. The strength of authentication using this method is dependent on the algorithm, key size and challenge size used: the minimum strength key used for this method is AES-128, using 16 bytes (a single AES block).

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

- 1/2^128 = 2.9E-39

The maximum number of consecutive failed authentication attempts is 5, so the probability that a random attempt will succeed over a one minute interval is:

- 5/2^128 = 1.4E-38

PIV Secret Value Authentication Method

The PKI Applet Secret Value Authentication method is provided by the PKI Applet *Entity authentication with password* service. The external entity submits an identifier and corresponding secret value. The module compares all 64 bytes to the appropriate stored reference instance (e.g., Cardholder PIN). The enforcement of minimum number of characters before padding is not the same as a fixed minimum length for the secret. For example, a minimum of 6 characters means secrets can be created from 6 to 64 characters, determined by the user.

The worst-case scenario permitted by the module is a minimum length of 6 characters allowing only numeric ASCII characters. The character space for the first 6 bytes in this scenario is 10 (the values ‘30’ through ‘39’ are permitted) and in the last 58 characters is 11 (the values ‘30’ through ‘39’ and ‘FF’ are permitted). The probability that a random attempt will succeed using this authentication method is:

- 1/(10^6 *11^58) = 3.97E-67

The applet implements a failed attempt counter, can be configured up to 15, blocking after 15 failed attempts. The probability that a random attempt will succeed over a one-minute interval is:

- 15/(10^6 * 11^58) =5.96E-66

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	GP Secure Channel Protocol Authentication
User	Identity	User	GP Secure Channel Protocol Authentication PKI Applet Symmetric Key Authentication (External Authentication) PKI Applet Secret Value Authentication

Table 11: Roles

The module supports the following roles:

- Cryptographic Officer (CO): Manages module content and configuration, including management of module data via the Supplementary Security Domain (SSD).
- User (the device Holder (applet user): Performs Approved cryptographic operations.

Authentication of each operator and their access to roles and services is as described below.

The module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.

- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.
- Implement security conditions which must be satisfied to access specific features, not necessarily as a separate role.

Authentication of each operator and their access to roles and services is as described below. Only one operator at a time is permitted on a channel. Applet de-selection (including ISD/Card Manager), card reset, or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services. Authentication data is encrypted during entry (by SC-ENC) and is only accessible by authenticated services.

4.3 Approved Services

The following convention is used to specify access rights to SSPs:

- **Generate (G)**: The module generates or derives the SSP.
- **Read (R)**: The SSP is read from the module (e.g. the SSP is output).
- **Write (W)**: The SSP is updated, imported, or written to the module.
- **Execute (E)**: The module uses the SSP in performing a cryptographic operation.
- **Zeroize (Z)**: The module zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Reset	Power cycle or reset the module	Successful Execution Status '9000'	N/A	Module ATR (Contact) or ATS (Contactless) that contains configuration information	None	Unauthenticated
Select	Select an application instance	Successful Execution Status '9000'	AID of Application to Select	Successful execution status	None	Unauthenticated
GP Secure Channel Establish	Establish a Global Platform secure communications channel	Successful Execution Status '9000'	Key Identifier, Host Challenge, Security Level Host Cryptogram, MAC	Card Challenge, Card Cryptogram, diversification data, and key information, Status Word of the command	AES-ECB AES-CMAC KBKDF SP 800-108	Crypto Officer - SC-ENC: G,E - SC-C-MAC: G,E - SC-R-MAC: G,E - SD-DAK: E - SD-DMK: E - SD-DEK: E - OS-DRBG-SEED: G,E - OS-DRBG-STATE: G,E
GP Get Data (Cleartext)	Retrieve from the Module data objects transmitted over a plaintext channel	Successful Execution Status '9000'	Tag of the Data Object to Retrieve	Data Object Retrieved and Successful execution status	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Data (SC)	Retrieve from the Module data objects transmitted through a Global Platform Secure Channel	Successful Execution Status '9000'	Tag of the Data Object to Retrieve for which the AC are satisfied	Data Object Retrieved and Successful execution status	None	Unauthenticated
Global Platform Lock / Unlock	Temporarily lock & unlock the full module or one of its applications using Global Platform card life cycle status	Successful Execution Status '9000'	Global Platform card life cycle status to set, and AID of the application	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Module Termination	Set the card life cycle status to TERMINATED. All the CSPs are zeroized when the life cycle status is set to TERMINATED	Successful Execution Status '9000'	N/A	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SC-ENC: E,Z - SC-C-MAC: E,Z - SC-R-MAC: E,Z - OS-DRBG-SEED: Z - OS-DRBG-STATE: Z - SD-DAK: Z - SD-DMK: Z - SD-DEK: Z - DAP-AES: Z - DAP-PUB (including intermediate values): Z - PKI-KPK: Z - PKI-KXAUTH: Z - PKI-KIAUTH: Z - PKI-KRSA-PRI: Z - PKI-KECC-PRI: Z - PKI-PIN: Z - Shared-Secret-Z: Z - PKI-SENC: Z - PKI-SMAC: Z - PKI-KRSA-PUB: Z - PKI-KECC-PUB: Z - PKI-EPKECC-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PRI: Z - SHARED-SEC-SM: Z - PKI-EPKECC-PUB: Z - IFD-EPKECC-PUB: Z
Load FW with RSA DAP	Load and install application packages (FW)	Successful Execution Status '9000'	Signed Packages (FW)	Successful execution status	AES-CBC AES-CMAC RSA sigVer	Crypto Officer - DAP-PUB (including intermediate values): E
Load FW with AES DAP	Load and install application packages (FW)	Successful Execution Status '9000'	Signed Packages (FW)	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - DAP-AES: E
Manage SD Keys	Update SD keys	Successful Execution Status '9000'	SD keys	Successful execution status	AES-CBC AES-CMAC KTS (AES-CBC + AES-CMAC)	Crypto Officer - DAP-PUB (including intermediate values): W,E - DAP-AES: W - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - SD-DAK: W - SD-DMK: W - SD-DEK: W
Manage SD Data	Create or update Security Domain (SD) data	Successful Execution Status '9000'	SD Data	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SD-DEK: E - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Show Status	Retrieve the identification and status of all applications present in the module	Successful Execution Status '9000'	Level of details to retrieve	Requested application status and Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Global Platform DELETE APPLICATION	Remove an application and all its data and keys from the module	Successful Execution Status '9000'	AID of the application to remove	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - PKI-KPK: Z - PKI-KXAUTH: Z - PKI-KIAUTH: Z - PKI-KRSA-PRI: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PKI-KECC-PRI: Z - PKI-PIN: Z - Shared-Secret-Z: Z - PKI-SENC: Z - PKI-SMAC: Z - PKI-KRSA-PUB: Z - PKI-KECC-PUB: Z - PKI-EPKECC-PRI: Z - SHARED-SEC-SM: Z - PKI-EPKECC-PUB: Z - IFD-EPKECC-PUB: Z
PKI Applet Run Self-Tests	Run all pre-operational and conditional self-tests	Successful Execution Status '9000'	N/A	Successful execution status	AES-ECB CTR DRBG ECDSA sigGen ECDSA sigVer KAS-ECC RSA sigGen RSA sigVer KBKDF SP 800-108 SHA	
PKI Applet Run Self-Tests	Run all pre-operational and conditional self-tests	Successful Execution Status '9000'	N/A	Successful execution status	AES-ECB CTR DRBG ECDSA sigGen ECDSA sigVer KAS-ECC RSA sigGen RSA sigVer KBKDF SP 800-108 SHA	Unauthenticated
PKI Applet Get DRBG	Retrieve random numbers	Successful Execution Status '9000'	Number of bytes	Requested number of bytes from the	CTR DRBG	Unauthenticated - OS-DRBG-SEED: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				DRBG generator		- OS-DRBG-STATE: G,E
PKI Applet GP Secure Channel Establish	Establish a Global Platform secure communication channel of PKI Applet associated Security Domain	Successful Execution Status '9000'	Key Identifier, Host Challenge, Security Level Host Cryptogram, MAC	Card Challenge, Card Cryptogram, diversification data, and key information, Successful execution status	AES-ECB AES-CMAC KBKDF SP 800-108	User - OS-DRBG-SEED: G,E - OS-DRBG-STATE: G,E - SC-ENC: G,E - SC-C-MAC: G,E - SC-R-MAC: G,E - SD-DAK: E - SD-DMK: E - SD-DEK: E
PKI Applet Configuration	Manage PKI applet authentication data and PKI Applet lifecycle. It is only available in PKI Applet life cycle state SELECTABLE	Successful Execution Status '9000'	Authentication Key Configuration Data, PIN Configuration Data, Change default periodic counter	Successful execution status	AES-CBC	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - SD-DAK: E - PKI-KXAUTH: W - PKI-KIAUTH: W - PKI-PIN: W - PKI-KPK: W
PKI Applet Key Management (Symmetric key)	Symmetric key update	Successful Execution Status '9000'	Key ID, Wrapped key	Successful execution status	AES-CBC KTS (AES-CBC + AES-CMAC)	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KPK: W,E - PKI-KXAUTH: W - PKI-KIAUTH: W
PKI Applet Key Management (Asymmetric key)	Asymmetric key pair import	Successful Execution Status '9000'	Key ID, Wrapped key components	Successful execution status	AES-CBC KTS (AES-CBC + AES-CMAC)	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KPK: E - PKI-KRSA-PRI: W - PKI-KRSA-PUB: W - PKI-KECC-PRI: W - PKI-KECC-PUB: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
PKI Applet Asymmetric Key Pair Generation	RSA or ECC key generation	Successful Execution Status '9000'	KeyID, Algorithm ID , Domain parameters for ECC	Successful execution status	ECDSA keyGen RSA keyGen	
PKI Applet Asymmetric key pair Generation	RSA or ECC key generation	Successful Execution Status '9000'	KeyID, Algorithm ID , Domain parameters for ECC	Successful execution status	ECDSA keyGen RSA keyGen	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KRSA-PRI: G,W - PKI-KECC-PRI: G,W - PKI-KRSA-PUB: G,W - PKI-KECC-PUB: G,W - OS-DRBG-SEED: G,E - OS-DRBG-STATE: G,E
Preparing Security Operation Environment	Specify the key to be used by the PSO command and its operation	Successful Execution Status '9000'	Key ID, Hash algorithm	Successful execution status	None	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Perform Security Operation (RSA digital signature generation)	RSA digital signature generation	Successful Execution Status '9000'	Input data (message) or /hashed message)	Signature and Successful execution status	RSA sigGen RSA sigPrim	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KRSA-PRI: E
Perform Security Operation (ECDSA generation)	ECDSA generation	Successful Execution Status '9000'	Input data (message) or /hashed message)	Signature and Successful execution status	ECDSA sigGen ECDSA sigGen component	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KECC-PRI: E
Perform Security Operation (ECC CDH)	ECC CDH Primitive Shared Secret Computation	Successful Execution Status '9000'	algorithm, Host ECC public key	shared secret and Successful execution status	KAS-ECC CDH Component	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KECC-PRI: E - PKI-KECC-PUB: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Shared-Secret-Z: G,R
Perform Security Operation (Compute Hash)	Compute the hash value	Successful Execution Status '9000'	Message	Hash and Successful execution status	SHA	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Perform Security Operation (RSADP)	RSADP operations	Successful Execution Status '9000'	Input data (ciphertext)	decryption data (plaintext) and Successful execution status	RSA Decryption Primitive	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KRSA-PRI: E
RSA Raw Operation	RSADP operations for RSA 2048 bits key only	Successful Execution Status '9000'	Key ID, Input data (ciphertext)	First 128 bytes of decryption data (plaintext) and Successful execution status	RSA Decryption Primitive	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KRSA-PRI: E
Get RSA Raw Operation Result	Retrieves the remaining 128 bytes RSA computation response of a prior RSA Raw Operation service	Successful Execution Status '9000'	the Offset of the buffer to be retrieved	The remaining 128 bytes decryption data (plaintext) and Successful execution status	None	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Change PIN	Allows the User to change their PIN	Successful Execution Status '9000'	PIN ID, old PIN value, new PIN value	Successful execution status	None	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-PIN: W
Unblock PIN	Mechanism to reset the retry counter when the card is blocked after too many failed PIN verify attempts	Successful Execution Status '9000'	PIN ID, new PIN value	Successful execution status	None	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-PIN: W
Read File Content (Cleartext)	Provides file content management (read)	Successful Execution Status '9000'	File ID, offset, length	Binary data and Successful execution status	None	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Read File Content (Transparent EF)	Provides file content management (read)	Successful Execution Status '9000'	File ID, offset, length	Binary data and Successful execution status	None	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Read File Content (Public Key EF)	Provides file content management (read)	Successful Execution Status '9000'	KeyID, Key Component index	Public Key Component data and Successful execution status	None	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KRSA-PUB: R - PKI-KECC-PUB: R
Write File Content	Provides file content management (update)	Successful Execution Status '9000'	File ID, offset, length, data	Successful execution status	None	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Entity authentication with PIN	PKI Applet Secret Value Authentication Method for User role Authentication	Successful Execution Status '9000'	PIN ID, PIN value	Successful execution status	None	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-PIN: E
Entity authentication with symmetric key (EXT-AUTH)	PKI Applet Symmetric Key Authentication Method for User role Authentication	Successful Execution Status '9000'	Key ID, data (host cryptogram)	Card challenge and Successful execution status	AES-CBC	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KXAUTH: E
Entity authentication with symmetric key (INTER-AUTH)	Internal Authentication for a device authentication	Successful Execution Status '9000'	Key ID, host challenge	Card cryptogram and Successful execution status	AES-CBC	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PKI-KIAUTH: E
GP Security Domain Secure Messaging	Unwraps command APDU or Wraps Response APDU by using GP Secure Channel Protocol	Successful Execution Status '9000'	Protected Command APDU or plain text Response APDU	Unprotected Command APDU or Protected Response APDU	AES-CBC AES-CMAC	User - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
ISO7816 Secure Messaging	Unwraps command APDU or Wraps Response APDU	Successful Execution Status '9000'	Protected Command APDU or plain	Unprotected Command APDU or Protected	AES-CBC AES-CMAC	User - PKI-SENC: E - PKI-SMAC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	by using PKI Applet ISO7816 Secure Messaging Protocol		text Response APDU	Response APDU		
PKI Applet Info (Show Version)	Read unprivileged PKI applet data objects	Successful Execution Status '9000'	Command parameters	PKI applet version or Data Object Retrieved and Successful execution status	None	Unauthenticated
File Selecting	Select a File by supplying its file ID	Successful Execution Status '9000'	File ID	Empty or File Control Information of selected file and Successful execution status	None	Unauthenticated
ISO7816 Secure Messaging Establish	Establish a secure communication channel according to ISO7816-4 Secure Message format	Successful Execution Status '9000'	IFD Ephemeral Public Key, IFD Nonce	ICC Ephemeral Public Key, ICC Authentication Token and Successful execution status	KAS-ECC	Unauthenticated - PKI-EPKECC-PRI: G,E - PKI-EPKECC-PUB: G,R - SHARED-SEC-SM: G,E - PKI-SENC: G - PKI-SMAC: G,E

Table 12: Approved Services

The module supports unauthenticated services which perform cryptographic operations which are compliant to exceptions provided in IG 4.1.A.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

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

When new firmware is loaded into the module using the "Load FW with RSA DAP" and "Load FW with AES DAP" services, the Module verifies the SHA-256 digest computed over the all firmware, and the AES-CMAC authentication code computed with SD-SMAC on each block of the firmware and the SHA-256 digest. In addition to the previous method, the firmware load process verifies an RSA PSS signature computed with DAP-PUB or an AES-CMAC authentication code computed with DAP-AES key on the firmware SHA-256 digest.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs an integrity test over the executable firmware loaded in non-volatile memory (NVM) (i.e. Javacard Packages) and over the ROM Code (i.e. Operating System). The integrity test uses a 16-bit CRC.

The module does not provide any services via the HMI, SFMI, HFMI, or HSMI interface that allow the operator to examine the executable code.

5.2 Initiate on Demand

The pre-operational integrity test can be performed on demand by power cycling or resetting the module. The module may perform conditional cryptographic algorithm self-tests on demand through the "Run Self-Tests" service.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

The module is classified as a single chip hardware module running on limited modifiable firmware, the requirements of this section are not applicable.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Hard tamper-evident coating	Determined by the operator	Observe the coating surroundings of the chip for any signs of damage

Table 13: Mechanisms and Actions Required

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-25C	EFP	Module stops all operations and shuts down
HighTemperature	112C	EFP	Module stops all operations and shuts down
LowVoltage	1.5V	EFP	Module stops all operations and shuts down
HighVoltage	6.6V	EFP	Module stops all operations and shuts down

Table 14: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-25°C
HighTemperature	115°C

Table 15: Hardness Testing Temperatures

8 Non-Invasive Security

This module implements non-invasive security techniques that are not listed in SP800-140F. These techniques are mentioned in Section 12.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Volatile memory is used to temporarily store Generated or Established SSPs.	Dynamic
NVM	Non-Volatile memory (FLASH)	Static

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Global Platform Secure Channel (SC) [Import]	Outside entity	NVM	Encrypted	Manual	Electronic	KTS (AES-CBC + AES-CMAC)
Global Platform Secure Channel (SC) [Export]	NVM	Outside entity	Encrypted	Manual	Electronic	KTS (AES-CBC + AES-CMAC)
OU_PUB	NVM	Outside entity	Encrypted	Automated	Electronic	KTS (AES-CBC + AES-CMAC)
OU_APDU01	RAM	Outside entity	Encrypted	Automated	Electronic	KTS (AES-CBC + AES-CMAC)
OU_APDU02	RAM	Outside entity	Plaintext	Automated	Electronic	
IN_SSP01	Outside entity	NVM	Encrypted	Automated	Electronic	KTS (AES-CBC + AES-CMAC)
IN_SSP02	Outside entity	NVM	Encrypted	Automated	Electronic	KTS (AES-CBC + AES-CMAC)
IN_SSP03	Outside entity	NVM	Encrypted	Automated	Electronic	KTS (AES-CBC + AES-CMAC)
IN_SSP04	Outside entity	NVM	Encrypted	Automated	Electronic	KTS (AES-CBC + AES-CMAC)
IN_SSP05	Outside entity	RAM	Plaintext	Automated	Electronic	

Table 17: SSP Input-Output Methods

OU_PUB: Output to outside through Read File content service for public key components with Secure Messaging protection.

OU_APDU01: Output to outside through Perform Security Operation (ECC CDH) service Response APDU within Secure Messaging.

OU_APDU02: Output to outside through PKI Applet ISO7816 Secure Messaging Establish service.

IN_SSP01: Input from outside through PKI Applet Configuration service with Secure Messaging protection.

IN_SSP02: Input from outside through PKI Applet Key Management service with Secure Messaging protection (When PKI-KPK does not exist).

IN_SSP03: Input from outside through PKI Applet Key Management service with Secure Messaging protection (When PKI-KPK exists).

IN_SSP04: Input from outside through PKI Applet Change PIN service with Secure Messaging protection.

IN_SSP05: Input from outside through PKI Applet ISO7816 Secure Messaging Establish service.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Global Platform TERMINATED STATE	Securely zeroizes all stored SSPs within the module. Zeroisation operation takes less than 1 second to erase all plaintext SSPs	All stored keys zeroized	By setting the module in the GLOBAL PLATFORM TERMINATED STATE
Global Platform DELETE KEY	Securely zeroizes global platform keys	Key values are zeroized, this is also followed by garbage collection to clear any values in memory	Global Platform DELETE KEY Command
Global Platform DELETE APPLICATION	Remove an application and all its data and keys from the module	Key values are zeroized, this is also followed by garbage collection to clear any values in memory	Global Platform DELETE APPLICATION Command
M_CLEAR_APDU	Zeroizes the APDU buffer memory which is used as temporary memory buffer	Values in memory overwritten with zeros	Automatically upon completing the processing of a service
SELECT Context	Clears global platform session keys from memory	Values in memory overwritten with zeros	SELECT Context Command
New key generation	Overwrites the previous key before replacing with newly generated value	Previous key overwritten with zeros prior to generating the new key	Automatically upon generation of a new key
Error handling	Secure messaging keys are zeroized once an error occurs	Values in memory are overwritten with zeros	Automatically upon error detection
Module Reset	Power cycles the module	The module resets clearing the contents of SSPs stored in RAM memory	By invoking Module Reset service, or by removing power from the module

Table 18: SSP Zeroization Methods

9.4 SSPs

The table below summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
OS-DRBG-SEED	Entropy input and nonce provided by the Entropy Source used to seed the Approved DRBG	256 - 256	CSP - CSP			CTR DRBG
OS-DRBG-STATE	The current AES-128 CTR_DRBG Internal State (V, Key)	128 - 128	CSP - CSP	CTR DRBG		CTR DRBG
SD-DAK	Security Domain Data Authentication Key (DAK) used to generate SC-ENC	256 - 256	CSP - CSP			AES-CMAC KBKDF SP 800-108
SD-DMK	Security Domain Data MAC Key (DMK) used to generate SC-C-MAC/SC-R-MAC	256 - 256	CSP - CSP			AES-CMAC KBKDF SP 800-108
SD-DEK	Security Domain Data Encryption Key (DEK) used to decrypt CSPs	256 - 256	CSP - CSP			AES-CBC
SC-ENC	Session key used to encrypt / decrypt Secure Channel (SC) data once Mutual Authentication is successful	256 - 256	CSP - CSP	KBKDF SP 800-108		AES-CBC
SC-C-MAC	Session key used to verify inbound (Command) Secure Channel (SC) data integrity	256 - 256	CSP - CSP	KBKDF SP 800-108		AES-CMAC
SC-R-MAC	Session key used to verify outbound (Response) Secure Channel (SC) data integrity	256 - 256	CSP - CSP	KBKDF SP 800-108		AES-CMAC
DAP-AES	Data Authentication Pattern AES Key. New	256 - 256	CSP - CSP			AES-CMAC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	firmware signature verification key					
DAP-PUB (including intermediate values)	RSA 2048 new firmware signature verification key.	2048 - 112	CSP - PSP			RSA sigVer
PKI-KPK	PKI Applet KEY Protection Key	256 - 256	CSP Symmetric Key - CSP			AES-CBC
PKI-KXAUTH	PKI applet External Authentication key	128, 192, 256 - 128, 192, 256	CSP Symmetric Key - CSP			AES-CBC
PKI-KIAUTH	PKI applet Internal Authentication key	128, 192, 256 - 128, 192, 256	CSP Symmetric Key - CSP			AES-CBC
PKI-KRSA-PRI	PKI applet signature generation private keys	2048, 3072, 4096 - 112, 128, 150	CSP Private Key - CSP	RSA keyGen		RSA sigGen RSA sigPrim RSA Decryption Primitive
PKI-KECC-PRI	PKI applet ECDSA private keys for digital signature generation or ECCDH share secret establishment.	P256, P384, P521 - 128, 192, 256	CSP Private Key - CSP	ECDSA keyGen		ECDSA sigGen ECDSA sigGen component KAS-ECC CDH Component
PKI-PIN	User Credential for PKI Applet Secret Value Authentication.	N/A - N/A	CSP Plaintext - CSP			
Shared-Secret-Z	Shared Secret generated with ECC CDH	256, 384, 521 - 128, 192, 256	CSP Plaintext - CSP		KAS-ECC CDH Component	
PKI-SENC	ISO 7816 Secure Messaging (SM) session encryption key	256 - 256	CSP Derived Symmetric Key - CSP		KAS-ECC	
PKI-SMAC	ISO 7816 Secure Messaging (SM) session encryption key	256 - 256	CSP Derived Symmetric Key - CSP		KAS-ECC	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PKI-KRSA-PUB	RSA public keys held in the module for retrieval by external users through the PKI applet.	2048, 3072, 4096 - 112, 128, 150	PSP Public Key - PSP		RSA keyGen	
PKI-KECC-PUB	ECC public keys held in the module for retrieval by external users through the PKI applet.	P256, P384, P521 - 128, 192, 256	PSP Public Key - PSP			
PKI-EPKECC-PRI	Ephemeral key generated by the module, used for shared secret (SHARED-SEC-SM) calculation	P384 - 192	CSP Private Key - CSP	ECDSA keyGen		KAS-ECC CDH Component
SHARED-SEC-SM	Used to derive ISO 7816 Secure Messaging session keys	384 - 192	CSP Plaintext - CSP		KAS-ECC CDH-Component (A4945)	KAS-ECC
PKI-EPKECC-PUB	Ephemeral key generated by the module	P384 - 192	PSP Public Key - PSP	ECDSA keyGen		
IFD-EPKECC-PUB	External users's Ephemeral Public Key	P384 - 192	PSP Public Key - PSP			KAS-ECC KAS-ECC CDH Component

Table 19: SSP Table 1

The following table continues to summarize the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
OS-DRBG-SEED		RAM:Plaintext	Until zeroized	Module Reset	OS-DRBG-STATE:Derives
OS-DRBG-STATE		RAM:Plaintext	Until zeroized	Module Reset	OS-DRBG-SEED:Derived From
SD-DAK	Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE	SC-ENC:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SD-DMK	Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE	SC-C-MAC:Derives SC-R-MAC:Derives
SD-DEK	Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE	
SC-ENC		RAM:Plaintext	Until Secure Channel closed	SELECT Context Module Reset	SD-DAK:Derived From
SC-C-MAC		RAM:Plaintext	Until Secure Channel closed	SELECT Context Module Reset	SD-DMK:Derived From
SC-R-MAC		RAM:Plaintext	Until Secure Channel closed	SELECT Context Module Reset	SD-DMK:Derived From
DAP-AES	Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE KEY	
DAP-PUB (including intermediate values)	Global Platform Secure Channel (SC) [Import] Global Platform Secure Channel (SC) [Export]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION New key generation	
PKI-KPK	IN_SSP01 IN_SSP02 IN_SSP03	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	SD-DEK:Decrypts SC-ENC:Wrapped By PKI-SENC:Wrapped By
PKI-KXAUTH	IN_SSP01 IN_SSP02 IN_SSP03	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	SD-DEK:Decrypts SC-ENC:Wrapped By PKI-SENC:Wrapped By
PKI-KIAUTH	IN_SSP01 IN_SSP02 IN_SSP03	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE	SD-DEK:Decrypts SC-ENC:Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Global Platform DELETE APPLICATION	PKI-SENC:Wrapped By
PKI-KRSA-PRI	IN_SSP02 IN_SSP03	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	PKI-KRSA-PUB:Paired With SC-ENC:Wrapped By PKI-SENC:Wrapped By SD-DAK:Decrypts PKI-KPK:Decrypts
PKI-KECC-PRI	IN_SSP02 IN_SSP03	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	PKI-KECC-PUB:Paired With SC-ENC:Wrapped By PKI-SENC:Wrapped By SD-DEK:Decrypts PKI-KPK:Decrypts
PKI-PIN	IN_SSP01 IN_SSP04	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	SC-ENC:Wrapped By PKI-SENC:Wrapped By
Shared-Secret-Z	OU_APDU01	RAM:Plaintext	Until end of command life cycle	M_CLEAR_APDU	PKI-KECC-PRI:Derived From IFD-EPKECC-PUB:Derived From PKI-SENC:Wrapped By SC-ENC:Wrapped By
PKI-SENC		RAM:Plaintext	Until Secure Channel closed	SELECT Context Module Reset	SHARED-SEC-SM:Derived From
PKI-SMAC		RAM:Plaintext	Until Secure Channel closed	SELECT Context Module Reset	SHARED-SEC-SM:Derived From
PKI-KRSA-PUB	OU_PUB IN_SSP02 IN_SSP03	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform	PKI-KRSA-PRI:Paired With SC-ENC:Wrapped By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				DELETE APPLICATION	PKI-SENC:Wrapped By
PKI-KECC-PUB	OU_PUB IN_SSP02 IN_SSP03	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	PKI-KECC-PRI:Paired With SC-ENC:Wrapped By PKI-SENC:Wrapped By
PKI-EPKECC-PRI		RAM:Plaintext	Until end of command life cycle	M_CLEAR_APDU Module Reset	PKI-EPKECC-PUB:Paired With
SHARED-SEC-SM		RAM:Plaintext	Until end of command life cycle	M_CLEAR_APDU Module Reset	PKI-EPKECC-PRI:Established By IFD-EPKECC-PUB:Established By PKI-SENC:Derives PKI-SMAC:Derives
PKI-EPKECC-PUB	OU_APDU02	RAM:Plaintext	Until end of command life cycle	M_CLEAR_APDU Module Reset	PKI-EPKECC-PRI:Paired With SHARED-SEC-SM:Establishes
IFD-EPKECC-PUB	IN_SSP05	RAM:Plaintext	Until end of command life cycle	M_CLEAR_APDU Module Reset	PKI-EPKECC-PRI:Paired With SHARED-SEC-SM:Establishes

Table 20: SSP Table 2

9.5 Transitions

The use of cryptographic keys with a security strength ≥112 but <128 bits for key generation, RSA digital signature generation, RSA digital signature verification, and RSA Decryption Primitive are deprecated after December 31, 2030. The use of HMAC Generation using keys ≥112 but <128 bits is acceptable through December 31, 2030, and disallowed thereafter.

10 Self-Tests

The module has the capability to perform pre-operational and conditional self-tests periodically by an internal counter and an associated maximum value. The periodic counter is set to its maximum value on power on and it is decremented when receiving an APDU. When the counter reaches zero, triggers a Periodic Self-Tests.

The periodic counter depends on the factory configuration (default is 32767) and can be adjusted from 1 to 32767 at PKI Applet Personalization.

10.1 Pre-Operational Self-Tests

The module performs pre-operational firmware integrity test automatically as a first action at power on. The module first performs a CAST on the cryptographic algorithm test used to perform the approved integrity technique. The module will enter the error state if either the conditional CAST or integrity test fails or proceed to test the conditional CASTs listed in Table 25 if both passes.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
CRC (ROM)	16-bit CRC	EDC	SW/FW Integrity	1	Performed over all ROM code
CRC (NVM)	16-bit CRC	EDC	SW/FW Integrity	1	Performed over all executable code in NVM

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The module performs conditional CAST prior to the algorithm’s first use. The module performs Conditional Pair-wise Consistency Tests upon generating RSA, ECDSA or ECDH asymmetric key pairs. The test is implemented by calculating a signature on predetermined data and subsequently performing a verification of the signature. If the signature cannot be verified, the generated key-pair is discarded. The module performs a conditional firmware load test when the module loads new firmware.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
CRC	16-bit CRC	KAT	CAST	1	CAST performed prior to use of algorithm for firmware integrity test	Device power-on or reset
AES-ECB (A4945)	128-bit key	KAT	CAST	1	Decrypt	Boot Up or "Context" service
KDF SP800-108 (A4945)	CTR mode KDF using AES-CMAC with 128-bit key	KAT	CAST	1	Key Derivation	Boot Up or "Context" service
Counter DRBG (A4945)	256-bit key	KAT	CAST	1	Instantiate, Generate, Reseed	Boot Up or "Context" service

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA KeyGen (FIPS186-4) (A4945)	signature generation followed by signature verification using curve P-256	PCT	CAST	1	Sign/Verify	On ECDSA Key Generation
ECDSA SigGen (FIPS186-4) (A4945)	ECDSA Signature Generation using curve P-256	KAT	CAST	1	Sign generation comparison	First Use or "Context" service
ECDSA SigVer (FIPS186-4) (A4945)	ECDSA Signature Generation using curve P-256	KAT	CAST	1	Sign verification comparison	First Use or "Context" service
KAS-ECC Sp800-56Ar3 (A7823)	KAS-ECC using curve P-384 followed by Two-step KDF	KAT	CAST	1	KAS comparison	First Use or "Context" service
SHA2-256 (A4945)	N/A	KAT	CAST	1	SHA2	Boot Up or "Context" service
SHA2-512 (A4945)	N/A	KAT	CAST	1	SHA2	Boot Up or "Context" service
RSA KeyGen (FIPS186-4) (A4945)	N/A	PCT	CAST	1	Using both Sign/Verify operations	On RSA Key Generation
RSA SigGen (FIPS186-4) (A4945)	N/A	KAT	CAST	1	Sign	Boot Up or "Context" service
RSA SigVer (FIPS186-4) (A4945)	Signature Verification using PKCS1-PSS with 2048-bit key	KAT	CAST	1	Verify	First Use or "Context" service
RSA SigVer (FIPS186-4) SW/FW Load test	Verification using PKCS1-PSS with 2048-bit key	Firmware load test	SW/FW Load	1	Using RSA signature verification	Firmware integrity test
AES-CMAC (A4945) SW/FW Load test	AES-CMAC message authentication code using 128 bit key	Integrity Test	SW/FW Load	1	Using CMAC	Firmware integrity test
SHA2-256 (A4945) SW/FW Load test	SHA-256 performed over loaded firmware	Integrity Test	SW/FW Load	1	Message Digest	Firmware integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Entropy - Adaptive Proportion Test (Continuous)	Cutoff value = 451	APT	Critical Function	1	Entropy Health Test	Upon seeding or reseeding the SP 800-90A DRBG
Entropy - Adaptive Proportion Test (Startup)	Startup test with 1024 samples; Cutoff value = 451	APT	Critical Function	1	Entropy Health Test	Boot Up
Entropy - Repetition Count Test (Continuous)	Cutoff value = 64	RCT	Critical Function	1	Entropy Health Test	Upon seeding or reseeding the SP 800-90A DRBG
Entropy - Repetition Count Test (Startup)	Startup test with 1024 samples; Cutoff value = 64	RCT	Critical Function	1	Entropy Health Test	Boot Up

Table 22: Conditional Self-Tests

10.3 Periodic Self-Test Information

The module has the capability to perform the pre-operational and conditional self-tests periodically. This may occur after a predefined number of -minutes passes, or, depending on the factory configuration, after invoking a predefined number of commands (APDUs).

The default configuration triggers a Periodic Self-Tests every 2 weeks of uninterrupted power. That time can be adjusted by the Application Administrator from 1 to 32767 minutes.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
CRC (ROM)	EDC	SW/FW Integrity	After invoking 1 to 32767 APDUs	Counter
CRC (NVM)	EDC	SW/FW Integrity	After invoking 1 to 32767 APDUs	Counter

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
CRC	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
AES-ECB (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
KDF SP800-108 (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
ECDSA KeyGen (FIPS186-4) (A4945)	PCT	CAST	After invoking 1 to 32767 APDUs	Counter
ECDSA SigGen (FIPS186-4) (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
ECDSA SigVer (FIPS186-4) (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
KAS-ECC Sp800-56Ar3 (A7823)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
SHA2-256 (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
SHA2-512 (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
RSA KeyGen (FIPS186-4) (A4945)	PCT	CAST	After invoking 1 to 32767 APDUs	Counter
RSA SigGen (FIPS186-4) (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
RSA SigVer (FIPS186-4) (A4945)	KAT	CAST	After invoking 1 to 32767 APDUs	Counter
RSA SigVer (FIPS186-4) SW/FW Load test	Firmware load test	SW/FW Load	Upon loading of new firmware	N/A
AES-CMAC (A4945) SW/FW Load test	Integrity Test	SW/FW Load	Upon loading of new firmware	N/A
SHA2-256 (A4945) SW/FW Load test	Integrity Test	SW/FW Load	Upon loading of new firmware	N/A
Entropy - Adaptive Proportion Test (Continuous)	APT	Critical Function	Prior to entropy generation	Automatically
Entropy - Adaptive Proportion Test (Startup)	APT	Critical Function	Prior to entropy generation	Automatically
Entropy - Repetition Count Test (Continuous)	RCT	Critical Function	Prior to entropy generation	Automatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Entropy - Repetition Count Test (Startup)	RCT	Critical Function	Prior to entropy generation	Automatically

Table 24: Conditional Periodic Information

10.4 Error States

The module enters an error state upon failing any self-test. When the test fails, a special memory zone called the “Kill Card Zone” records the reason for the failure. All cryptographic functions are inhibited while the module is in an error state. The table below describes the error states in detail:

Name	Description	Conditions	Recovery Method	Indicator
Kill Card State	No further communication is possible with the module until the module is reset.	Pre-operational firmware integrity test fail Any conditional self-test failure	Resetting the module	An error code is provided through the status interface
BAD APDU	Entered when an incorrectly formatted or unknown command is received.	The module outputs a status word indicating the error condition and returns to the Idle state, clearing the error. This state includes Manage Content service firmware load attempts that fail the firmware load test; i.e., an attempt to load new firmware that fails the firmware load test will result in rejection of the command, and the new firmware will not be accepted by the module.	Recovers automatically after reporting the error	An error code is provided through the status interface

Table 25: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Platform and the PKI Applet are configured at factory, to comply with and maintain the FIPS 140-3 validation, it would be the CO's responsibility to enable the Approved mode of operation as Administrator Guidance.

11.2 Administrator Guidance

To comply with and maintain the FIPS 140-3 validation, it would be the Crypto Officer's responsibility for PKI Applet installation and initialization to enable the Approved mode of operation as follows procedures.

1. Creating and Personalization a Security Domain for PKI Applet GP Secure Messaging.
2. Installation of the PKI Applet to the created Security Domain as associated Security Domain.
3. Personalization (initialization) of the PKI Applet.
4. Replace the default ISD keys with customer specific keys.
5. Change Card Life Cycle State to SECURED.

Detailed information about steps is described in document [GPC_SPE_014] for Security Domain operation and [PKI_APP_PM01] for PKI Applet Personalization.

11.3 Non-Administrator Guidance

The approved and non-approved security functions, physical ports, and logical interfaces available to the users are defined in this SP section 3.

Only approved mode of operation is available for users. In this mode of operation, only approved services in section 4.3.2 are available for users.

11.4 End of Life

The *Module Termination* service can be used to set the module's status to TERMINATED. All SSPs will be zeroized upon module reset.

12 Mitigation of Other Attacks

12.1 Attack List

The Module implements defenses against:

- Light attacks: The chip includes sensors to detect light attacks. A hardware attack event triggers the Kill Card behavior described below.
- Invasive fault attacks: The chip includes sensors for fault attacks. A hardware attack event triggers the Kill Card behavior described below.
- Side-channel attacks (SPA/DPA, timing analysis): The chip implements hardware countermeasures, such as induced clock jitter. The operating system enables the hardware counter measures and implements independent countermeasures in code, such as constant time execution.
- Electromagnetic attacks: This includes the defenses against side-channel attacks described above, where the detection mechanism is monitoring chip emissions rather than physical power connections. In addition, the hardware includes sensors to detect electromagnetic attacks, invoking Kill Card behavior if detected.
- Differential fault analysis (DFA): The operating system provides checks of expected conditions in areas of code deemed sensitive. If the check detects an error, the Kill Card behavior is initiated.
- Card tearing attacks: The operating system implements methods to assure protective measures are completed in the next cycle if the module loses power (i.e., is removed from the reader) before completion of the protective function.

12.3 Guidance and Constraints

The Kill Card function logs the detected attack type in a table. The table has a preset limit; when the limit is reached, the module initiates card termination, including overwrite of the CSPs, and the module is no longer operable.

References

ANS X9.63-2001	**Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography** 2001 https://webstore.ansi.org/standards/ascx9/ansix9632001
ANSI X9.62	**Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)** September 1999 https://webstore.ansi.org/standards/ascx9/ansix9621998
ANSI 504-1	**Information Technology - Generic Identity Command Set - Part 1: Card Application Command Set - Amendment 1** May 2016 https://webstore.ansi.org/standards/incits/incits5042013am12016
FIPS 140-3	**FIPS PUB 140-3 - Security Requirements for Cryptographic Modules** **November 2023** https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
FIPS 140-3 IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 180-4	**Secure Hash Standard (SHS)** March 2012 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS 186-4	**Digital Signature Standard (DSS)** July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS 197	**Advanced Encryption Standard** November 2001 https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 201-3	**Personal Identity Verification (PIV) of Federal Employees and Contractors** January 2022 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf

FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
GPC_SPE_014	**GlobalPlatform Card Technology Secure Channel Protocol '03' Card Specification v2.2 – Amendment D Version 1.1.1** July 2014 https://globalplatform.org/wp-content/uploads/2014/07/GPC_2.2_D_SCP03_v1.1.1.pdf
GPC_SPE_034	**GlobalPlatform Card Technology - Card Specification v2.3.1** March 2018 https://globalplatform.org/specs-library/card-specification-v2-3-1/
PKI_APP_PM01	**HiCOS PKI Applet V4 Personalization Manual, version 1.1** **October 2025**
ISO 7816	**Identification cards -- Integrated circuit cards** 2004
ISO 14443	**Identification cards — Contactless integrated circuit cards** 2016
JavaCard	**JAVA CARD CLASSIC PLATFORM SPECIFICATION 3.1 CE** February 2021 https://www.oracle.com/java/technologies/javacard-downloads.html
PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** February 2003 https://www.ietf.org/rfc/rfc3447.txt
SP 800-38A	**Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38B	**Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
SP 800-38F	**Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** December 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

SP 800-56Ar3	**Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
SP800-56B Rev2	**Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography** March 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf
SP 800-56Cr2	**Recommendation for Key-Derivation Methods in Key-Establishment Schemes** August 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf
SP 800-73-4	**Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation** May 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf
SP 800-78-4	**Cryptographic Algorithms and Key Sizes for Personal Identity Verification** May 2015 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-78-4.pdf
SP 800-85A-4	**PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)** April 2016 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-85A-4.pdf
SP 800-90Ar1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP 800-90B	**Recommendation for the Entropy Sources Used for Random Bit Generation** January 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
SP 800-108r1	**NIST Special Publication 800-108 - Recommendation for Key Derivation Using Pseudorandom Functions** August 2022 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-108r1.pdf
SP 800-131Ar2	**Transitioning the Use of Cryptographic Algorithms and Key Lengths** March 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

SP 800-133r2 **Recommendation for Cryptographic Key Generation**
June 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf

SP 800-140Br1 **CMVP Security Policy Requirements**
October 2022
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.2pd.pdf