ID-One PIV on Cosmo V8.1

NPIVP & CIV Configurations

FIPS 140-2 Non Proprietary Cryptographic Module Security Policy

Oberthur Technologies of America

4250 Pleasant Valley Road

Chantilly, VA 20151

USA

Table of Contents

List of Tables

List of Figures

References

Reference	Full Specification Name
[ISO 7816]	ISO/IEC 7816-1: 2011 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2013 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange* ISO/IEC 7816-5:2004 *Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers* ISO/IEC 7816-6:2004 *Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange* ISO/IEC 7816-8:2004 *Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations* ISO/IEC 7816-9:2004 *Identification cards -- Integrated circuit cards -- Part 9: Commands for card management* ISO/IEC 7816-11:2004 *Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods* ISO/IEC 24787: 2010 *Information technology -- Identification cards -- On-card biometric comparison*
[JavaCard]	*Java Card 3.0.4 Classic - Runtime Environment (JCRE) Specifications* *Java Card 3.0.4 Classic - Virtual Machine (JCVM) Specifications* *Java Card 3.0.4 Classic - Application Programming Interface (API)* Published by Sun Microsystems, September 2011
[GlobalPlatform]	*GlobalPlatform Card Specification 2.2.1 - January 2011,* *GlobalPlatform Card Specification 2.2 – Amendment D – Secure Channel Protocol '03'– Version1.1.1 – July 2014,* *GlobalPlatform Card Specification – Amendment E – Security Upgrade for card content management – Public Release November 2011 v1.0* *GlobalPlatform Card Basic ID Configuration - Version 1.0 - December 2011* *GlobalPlatform Card Technology Card Specification – ISO Framework Version 0.9.0.18 Public Review July 2013* *GlobalPlatform Consortium: http://www.globalplatform.org*
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[ANS X9.31]	American Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1998 - Appendix A.2.4.
[FIPS201-2]	NIST, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 25 July 2013.
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[FIPS 198-1]	NIST, *The Keyed-Hash Message Authentication Code (HMAC),* FIPS Publication 198-1, July 2008

Reference	Full Specification Name
[SP800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[SP800-76-2]	*NIST, Biometric Specifications for Personal Identity Verification, July 2013*
[SP800-73-4]	*NIST, Interface for Personal Identity Verification, May 2015 with updates 02-08-2016*
[SP800-78-4]	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, December 2010
[SP800-85A-4]	*PIV Card Application and Middleware Interface Test Guidelines, April 2016*
[SP800-90A-rev1]	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Revision 1, June 2015*
[SP800-108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[SP800-131A Rev1]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, November 2015
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions – August 2015

Table 1 – References

Acronyms and definitions

Acronym	Definition
AIS 31	A German acronym referring to standard for functionality and evaluation of random number generation.
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CHV	Card Holder Verification
CM	Card Manager, see [GlobalPlatform]
CRT	Chinese Remainder Theorem
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	Global Platform
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
NVM	Non-Volatile Memory (e.g. EEPROM, Flash)
OP	Open Platform (predecessor to Global Platform)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SAM	Secure Authentication Module
SCP	Secure Channel Protocol, see [GlobalPlatform]
STD	Standard, as in Standard (non-CRT) RSA
SPA	Simple Power Analysis
TPDU	Transport Protocol Data Unit, see [ISO 7816]

Table 2 – Acronyms and Definitions

Notation

Hexadecimal numbers in this document are indicated by placing them in single quotation mark (‘ ’). The numbers without the quotes around them represent decimal notation.

Example:

‘16’ – Represents 0x16, or 16h

16 – Represents decimal number 16

1 Introduction

This document defines the Security Policy for the ID-One PIV on Cosmo V8.1 cryptographic module from Oberthur Technologies, hereafter denoted *the module*. The module, validated to FIPS 140-2 overall Level 2, is a single-chip module implementing the Global Platform operational environment, with Card Manager and ID-One PIV Applet. The PIV applet in the module can be set in manufacturing in one of the following two configurations:

1. NPIVP configuration for US Federal Agencies and Contractors. This configuration has been validated by NIST to comply with SP800-85A-4 and SP800-73-4 (NPIVP Cert. #39).
2. CIV configuration, for Commercial and Enterprises. The CIV configuration is fully backward compatible with the NPIVP configuration from a command (APDU) perspective but offers additional functionalities for card management and operations to address the non-US Federal market.

The FIPS 140-2 security levels for the module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 3 – Security Level of Security Requirements

1.1 Versions, Configurations and Modes of Operation

- Hardware:
  - '**30-5F01**' with Firmware Extension: '**086294'+'086683'** (ID-One PIV 2.4.0 on Cosmo V8.1 LARGE)
  - '**30-5F02**' with Firmware Extension: '**090191'** (ID-One PIV 2.4.1 on Cosmo V8.1 LARGE)
  - '**40-6001**' with Firmware Extension: '**086294'+'086693'** (ID-One PIV 2.4.0 on Cosmo V8.1 STD)
  - '**40-6002**' with Firmware Extension: '**090211'** (ID-One PIV 2.4.1 on Cosmo V8.1 STD)

- Factory Configurations of ID-One PIV Instance:
  - NPIVP
  - CIV

The module is available in three (3) hardware configurations:

- Contact Only
- Contactless Only
- Dual Interface

And two (2) non volatile memory sizes for Application Data:

- ID-One PIV on Cosmo V8.1 LARGE: 128KB of non volatile memory available for application data and keys

- ID-One PIV on Cosmo V8.1 STD: 64KB of non volatile memory available for application data and keys

The module can support multiple instances of the ID-One PIV application, each instance running in its own mode of operations.

The mode of operation under which a given instance is run is defined by Oberthur during manufacturing.

The NPIVP and CIV instances of the ID-One PIV application always run in FIPS 140-2 Level 2 Mode of Operation.

The indicator of mode of operations of a given ID-One PIV instance can be retrieved at anytime using the READ BINARY command on its Elementary file (EF) with SFI=01. The value returned is the mode of operation encoded in plain text (ASCII). Example: "FIPS140-2 Level 2"

1.2 Hardware and Physical 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, shown as circles in the figure.

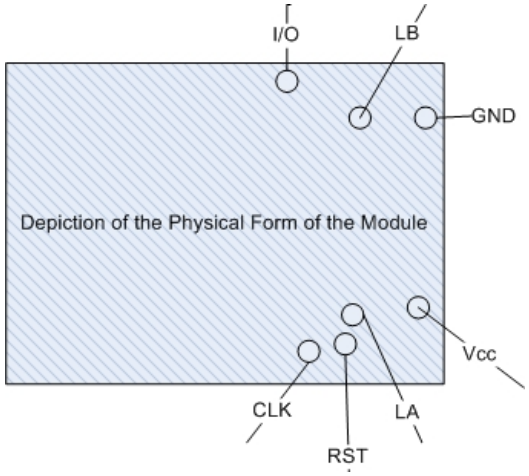

Figure 1 –Physical Form

The contactless ports (if supported) of the module require connection to an antenna. The module relies on [ISO7816] and [ISO14443] card readers and antenna connections as input/output devices.

Port	Description	Logical Interface Type
$V_{CC,}$ GND	ISO 7816: Supply voltage	Power (not available in contactless-only configurations)
RST	ISO 7816: Reset	Control in (not available in contactless-only configurations)
CLK	ISO 7816: Clock	Control in (not available in contactless-only configurations)
I/O	ISO 7816: Input/Output	Control in, Data in, Data out, Status out (not available in contactless-only configurations)
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out (Not available in Contact-only configurations)

Table 4 – Ports and Interfaces

1.3 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the module operational environment.

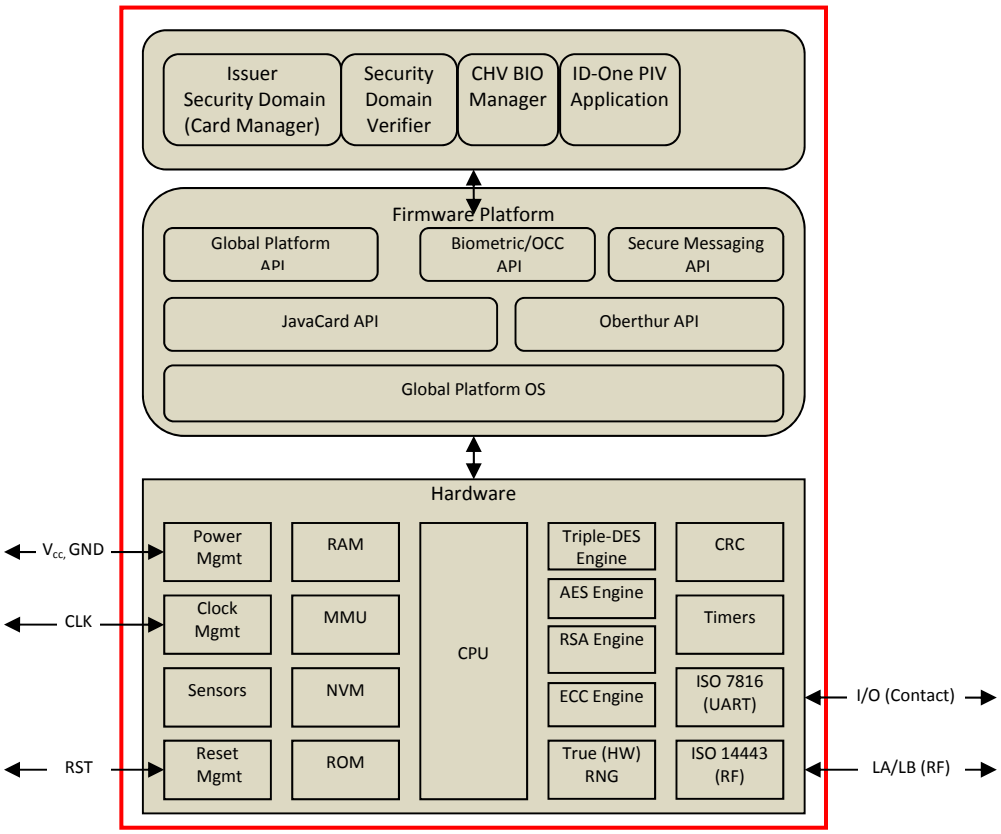

Figure 2 - Module Block Diagram
(Cryptographic Boundary Outlined in Red)

Section 3 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, Triple-DES, RSA, ECC, CRC and an AIS-31 P2 class tested True (HW) RNG. 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 Cryptographic Functionality

The module implements the Approved and Non-Approved but Allowed cryptographic functions listed in Table 5 and Table 6 below.

CAVP #	Algorithm	Standard	Mode / Method	Strength[1]	Use
AES Val#4107	AES	[FIPS 197], [SP800-38A]	CBC, ECB	128 192, 256	Data Encryption/ Decryption
AES Val#4108	CMAC	[SP800-38B]	CMAC	128 192 256	Message Authentication; SP 800-108 KDF (Uses AES Val#4107)
AES Val#4109	Key Wrap	[SP800-38F]	AES	128 192 256	SP 800-38F key transport
KTS	Key Wrap	[SP800-38F]	AES/CMAC	128 192 256	SP 800-38F §3.1 ¶3 Key transport (Uses AES Val#4107 and #4108)
CVL Val#921	RSADP	[SP 800-56B]	RSA key decryption primitive	RSA 2048	Key decryption
CVL Val#953	ECC CDH	[SP 800-56A]	ECC CDH Primitive	P-224 P-256 P-384 P-521	Shared Secret Computation
CVL Val#954	RSASP1	[FIPS 186] [SP 800-56B]	RSA signature generation primitive	RSA 2048	Signature decryption primitive (off card hash).
DRBG Val#1234	DRBG	[SP 800-90A]	CTR	128	Deterministic Random Bit Generation
ECDSA Val#933	ECDSA	[FIPS 186-4]		P-224 P-256 P-384 P-521 {P-192}	Digital Signature Generation, Verification and ECC Key Generation.
HMAC Val#2683	HMAC	[FIPS 198-1]	HMAC	SHA1 SHA-256 SHA-384 SHA-512	Message Authentication; SP 800-108 KDF (Uses SHS Val#3379)
KAS Val#48	EC Diffie-Hellman	[SP 800-56A]	OnePass DH	P-224 P-256	Key Agreement
KBKDF Val#106	KBKDF	[SP 800-108]	AES CMAC	128 192 256	Deriving keys from existing keys, (Uses KAS Val#953 & AES Val#4108)
RSA Val#2252	RSA	[FIPS 186-2] [FIPS 186-4]	PKCS1_V1_5 PSS KeyGen	RSA 2048 RSA 3072 RSA 4096	RSA key generation, digital signature generation and verification.

[1] Strength indicates DRBG Strength, Key Lengths, Curves or Moduli

CAVP #	Algorithm	Standard	Mode / Method	Strength[1]	Use
RSA Val#2253	RSA CRT	[FIPS 186-2] [FIPS 186-4]	PKCS1_V1_5 PSS KeyGen	RSA 2048 RSA 3072 RSA 4096	RSA key generation, digital signature generation and verification.
SHA-3 Val#6	SHA-3	[FIPS 202]	SHA3-224 SHA3-256 SHA3-384 SHA3-512		Message Digest
SHS Val#3379	SHS	[FIPS 180-4]	SHA-224 SHA-256 {SHA-1}		Message Digest
SHS Val#3380	SHS	[FIPS 180-4]	SHA-384 SHA-512.		Message Digest
Triple-DES Val#2245	3DES	[SP 800-67]	TCBC, TECB	3-Key	Data Encryption/ Decryption

Table 5 –Approved Cryptographic Functions

Algorithm	Description
True (HW) RNG	[AIS 31] Class P2 Hardware True RNG used to seed the FIPS approved DRBG.

Table 6 – Non-Approved but Allowed Cryptographic Functions

2.1 Critical Security Parameters

All CSPs used by the module are described in this section. All usages of these CSPs by the module are described in the services detailed in Section 4. In the tables below, the OS prefix denotes operating system, the SD prefix denotes the Global Platform Security Domain, the DAP prefix denotes the Global Platform Data Authentication Protocol, and the PIV prefix denotes a PIV Application CSP.

All CSPs, (keys and PINs) except OS-MKEK are store encrypted by OS-MKEK with a corresponding checksum.

CSP	Description / Usage
OS-DRBG-SEED	Entropy input provided by the True (HW) RNG, used to seed the Approved DRBG.
OS-DRBG-STATE	The current AES-128 CTR_DRBG state.
OS-MKEK	3-Key Triple-DES Key Encryption Key used for encrypted storage of CSPs.
SD-KENC	AES-256 Master key used to generate SD-SENC.
SD-KMAC	AES-256 Master key used to generate SD-SMAC.
SD-KDEK	AES-256 Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES-256 Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES-256 Session MAC key used to verify inbound secure channel data integrity.
SD-RMAC	AES-256 Session MAC key used to generate response secure channel data MAC.

Table 7 – OS Critical Security Parameters

CSP	Description / Usage
PIV-SENC	AES-128, AES-256 (192 bit channel strength), PIV Secure Messaging (SM) session encryption key.

CSP	Description / Usage
PIV-SMAC	AES-128, AES-256 (192 bit channel strength), PIV Secure Messaging (SM) session Command MAC key.
PIV-SRMAC	AES-128, AES-256 (192 bit channel strength), PIV Secure Messaging (SM) session Response MAC key.
PIV-SCFRM	AES-128, AES-256 (192 bit channel strength), PIV Secure Messaging (SM) session key confirmation key.
PIV-SM	PIV Secure Messaging Key Establishment Key (04) as described in [SP-800-73-4]. All key types specified by [SP 800-78-4] are supported: ECC P-256, and P-384 curves.
PIV-AUTH	Eight (8) byte PIV authentication datum, with six (6) instances (3 Local and 3 Global) used for card holder PIN verification, PIN unblocking and Application Administrator authentication.
PIV-PA	PIV Authentication Key (9A) as described in [SP 800-78-4]. All key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-AA	Application Administrative Key (9B) as described in [SP 800-78-4]. All key types specified by [SP 800-78-4] are supported: 3-Key Triple-DES, AES-128, AES-192, AES-256.
PIV-DS	PIV Digital Signature Key (9C) as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-KM	Key Management Key (9D) as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-RKM	Retired Key Management Keys (‘82’to ‘95’). Up to 20 instances as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-1024, RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-SCA	Symmetric Card Authentication Key (9E) as described in [SP 800-78-4]. All key types specified by [SP 800-78-4] are supported: 2-Key and 3-Key Triple-DES, AES-128, AES-192, AES-256
PIV-ACA	Asymmetric Card Authentication Key (9E mandatory) as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-MA	PIV Mutual Authentication Key; key type is identical to [SP 800-78-4] Application Administrative Key, except that the key is used to enforce mutual authentication access control rules.
PIV-DS-HASH	PIV Digital Signature Key (‘81’ optional) with built-in Hash (SHA-256 & SHA384) and padding (PSS). A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-SAM-CMAC	Symmetric key (‘96’ optional) for generic CMAC computation (SAM functionality). AES-128, AES-256
PIV-SAM-KDF	Symmetric key (‘97’ optional) used to return the diversified key of a target card (SAM functionality) AES-128, AES-256
PIV-SAM-KDF-ENC	Symmetric key (‘98’ optional) used for Administrator to unlock a child PIV card. AES-128, AES-256

Table 8 –PIV Critical Security Parameters

2.2 Public Keys

Key	Description / Usage
DAP-PUB	RSA 2048 new firmware signature verification key.
PIV-SM-PUB	The public key component used by the PIV Secure Message protocol. A superset of key types specified by [SP 800-78-4] are supported: ECC P-224, P-256, and P-384curves.
PIV-PA-PUB	PIV Authentication Key (9A) public component as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-DS-PUB	PIV Digital Signature Key (9C) public component as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-KM-PUB	Key Management Key (9D) public component as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-ACA-PUB	Asymmetric Card Authentication Key (9E mandatory) public component as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.

Key	Description / Usage
PIV-RKM-PUB	Retired Key Management Key ('82'to '95') public component as described in [SP 800-78-4]. A superset of key types specified by [SP 800-78-4] are supported: RSA-1024, RSA-2048, ECC P-224, P-256, and P-384 curves.
PIV-DS-HASH-PUB	PIV Digital Signature Key with built-in Hash public component. A superset of key types specified by [SP 800-78-4] are supported: RSA-2048, ECC P-224, P-256, and P-384 curves.

Table 9 – Public Keys

3 Roles, Authentication and Services

The module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports Global Platform logical channels, allowing concurrent operators in a limited fashion.

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. Card reset or power down terminates all current authentications. Applet de-selection (including ISD/Card Manager) terminates authentications with ISD and with PIV CSP declared as local. (for instance the Global PIN authentication status is not cleared). UNVERIFY command on a given reference data terminates authentication with that Reference Data (see [SP800-73-4]). Re-authentication is required after any of these events for access to authenticated services. Authentication data not used for User authentication is encrypted during entry (by SD-SDEK or PIV-SENC), and is only accessible by authenticated services. Authentication data for user authentication is encrypted during entry (by SD-SDEK or PIV-SENC) only when the entry is done over the contactless interface. Encryption of user authentication data during entry over the contact interface is supported but not mandatory to allow interoperability with PIN PAD without cryptographic capabilities.

Table 10 below lists all operator roles supported by the module.

Role ID	Role Description
CO	Cryptographic Officer – role that manages module configuration, including issuance and management of module data via the ISD. Authenticated as described in *GP Secure Channel Protocol Authentication Method* below.
AA	PIV Application Administrator – a role that manages PIV application-related content and configuration. Authenticated as described in *PIV Symmetric Key Authentication Method* below using the PIV-AA key, or the *PIV Secret Value Authentication Method* below, using a PIV-AUTH instance.
User	User – role for use in PIV applet. Authenticated as described in *PIV Secret Value Authentication Method* below using a PIV-AUTH instance.

Table 10 - Roles Supported by the Module

3.1 GP Secure Channel Protocol Authentication Method

The GP Secure Channel Protocol authentication method is provided by the GP *Secure Channel* service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The SD-SENC 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:

- 1/2^256 = 8.6E-78

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

- 9 /2^256 = 7.7E-77

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.

3.2 PIV Symmetric Key Authentication Method

The external entity obtains an 8-byte or 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 *PIV 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 3-Key Triple-DES, using 8 bytes (a single Triple-DES block).

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

- 1/2^64 = 5.4E-20

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

- 9/2^64 = 4.9E-19

3.3 PIV Secret Value Authentication Method

The external entity submits an identifier and corresponding secret value. The format of the secret value is checked for conformance to a defined format template (Numeric in ASCII, Numeric in BCD, HEX value, and minimum number of character before padding). If the format is valid, the module compares all eight (8) bytes to the appropriate stored reference instance (e.g. Cardholder PIN, Pin Unblocking Key or Administrator PIN). When the reference value is updated, the module enforces the defined template policy. 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 six (6) characters means secrets can be created from six (6) to eight (8) characters, determined by the user.

The worst case scenario permitted by the module is a minimum length of six (6) characters with the Numeric in ASCII character set. The character space for the first six (6) bytes in this scenario 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 that a random attempt will succeed using this authentication method is:

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

The maximum number of consecutive failed authentication attempts is 10, so the probability that a random attempt will succeed over a one minute interval is:

- 10/(10^6 * 11^2) = 8.3E-8

3.4 BIO Authentication method

The module performs a biometric person authentication On-Card-Comparison (OCC) of a live fingerprint template as defined by [FIPS 201-2].

The threshold applied to scores from the biometric comparison algorithms has been set to achieve false match rates at or below the respective values defined by NIST in Table 16 of [SP800-76-2], i.e., a FMR of 0.001 for on-card fingerprint minutia matching.

As required by [SP800-76-2] section 5.7.4.1, the on-card-matching algorithm matches single-finger native templates with FNMR less than or equal to 0.02 when the FMR is at or below 0.0001. As a result, the PIV OCC authentication method is not considered as a valid authentication method and services made available after successful PIV OCC authentication are classified as unauthenticated services from a FIPS 140-2 standpoint.

3.5 Services

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

Service	Description
Card Authentication	Authenticate in accordance with the [SP-8000-73-4] Card Authentication process.
Context	Select an application or manage logical channels.
Module Info (Unauthenticated)	Read unprivileged data objects, e.g. module configuration or status information.
Module Reset	Power cycle or reset the module. Includes Power-On Self-Test.
PIV Info (Unauthenticated)	Read unprivileged data objects, e.g. application configuration or status information.
PIV Authentication	System level authentication of the PIV Application/card in accordance with [SP 800-73-4].
PIV Digital Signature	Sign an externally generated hash in accordance with [SP 800-73-4].
PIV Secure Messaging	Establish and use a PIV Secure Messaging communications channel.
PIV Manage Content (Unauthenticated)	Load or generate PIV Application keys and data[2].
PIV System Key Services	Decrypt a key or generate a shared secret in accordance with [SP 800-73-4]. Key decryption is the use of [SP 800-56B] Section 7.1.2 RSADP key decryption primitive. Shared secret generation is the use of [SP 800-56A] Section 5.7.1.2

Table 11 - Unauthenticated Services

Service	Description	CO	AA	User
GP Secure Channel	Establish and use a Global Platform secure communications channel.	X		
Lifecycle	Modify the card or applet life cycle status.	X		
Manage Content	Load and install application packages and associated keys and data.	X		
Module Info (Authenticated)	Read module configuration or status information (privileged data objects)	X		
PIV Administrator Authentication	Authentication of AA role to the module in accordance with [SP 800-73-4].		X	
PIV Info (Authenticated)	Read PIV Application privileged data objects.			X
PIV Manage Content (Authenticated)	Load or generate PIV Application keys and data.		X	
PIV Verify	Grant access control rights for objects or services.		X	X
PIV Digital Signature with	Same as PIV Digital Signature but with message hashing and			X

[2] In CIV configuration, USER or BIO authentication also grants the rights for the Card Holder to update PKI keys and certificates inside the module.

Service	Description	CO	AA	User
on-card Hash	formatting performed within the module.			
PIV-SAM	Use the PIV card as a SAM to compute CMAC, KDF or authentication cryptogram to unlock a target card.			X

Table 12 –Authenticated Services

Note that PIV Digital Signature with on card Hash and PIV-SAM services require a two factor authentication (User + BIO).

3.6 PIV Secure Messaging

The PIV Secure Messaging protocol defined in [SP800-73-4] establishes a secure channel to protect confidentiality and integrity of transmitted information, but does not provide any authentication services.

The PIV Secure Messaging protocol conforms to [SP 800-56A] for the establishment of a shared secret and key derivation for session keys.

Service	CSPs																								
	OS-DRBG-SEED	OS-DRBG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-SRMAC	PIV-SENC	PIV-SMAC	PIV-SRMAC	PIV-SCFRM	PIV-SM	PIV-AUTH	PIV-PA	PIV-AA	PIV-DS	PIV-KM/RKM	PIV-SCA	PIV-ACA	PIV-MA	PIV-DS-HASH	PIV-SAM-CMAC	PIV-SAM-DKF	PIV-SAM-KDF-ENC
Card Authentication	--	--	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	E	E	E	--	--	--	--
Context	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Module Info (Unauthenticated)	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Module Reset	GE WZ	GE WZ	--	--	--	--	Z	Z	Z	Z	Z	Z	Z	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV Info (Unauthenticated)	--	--	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV Authentication	--	--	--	--	--	E	E	E	E	E	E	E	--	--	--	E	--	--	--	E	E	E	--	--	--	--
PIV Digital Signature	--	--	--	--	--	E	E	E	E	E	E	E	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--
PIV Secure Messaging	--	--	--	--	--	E	E	E	E	GE	GE	GE	GE	E	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV Manage Content (Unauthenticated)	--	--	--	--	--	E	E	E	E	E	E	E	--	WZ	W	GEWZ	EWZ	GEWZ	GEWZ	WZ	GEWZ	EWZ	--	--	--	--	--
PIV System Key Services	--	--	--	--	--	E	E	E	E	E	E	E	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--
GP Secure Channel	--	GE	--	E	E	--	GE	GE	GE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Lifecycle	Z	Z	Z	Z	Z	Z	E	E	E	--	--	--	--	Z	Z	Z	Z	Z	Z	Z	Z	Z	--	--	--	--	--
Manage Content	--	--	--	W	W	W	E	E	E	--	--	--	--	W	W	W	W	W	W	W	W	W	W	W	W	W	W
Module Info (Authenticated)	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV Administrator Authentication	--	--	--	--	--	E	E	E	E	E	E	E	--	--	E	--	E	--	--	--	--	E	--	--	--	--	--
PIV Digital Signature	--	--	--	--	--	E	E	E	E	E	E	E	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--
PIV Info (Authenticated)	--	--	--	--	--	E	E	E	E	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV Manage Content	--	--	--	--	--	E	E	E	E	E	E	E	--	WZ	W	GEWZ	EWZ	GEWZ	GEWZ	WZ	GEWZ	EWZ	GWZ	GWZ	GWZ	GWZ	
PIV Secure Messaging	--	--	--	--	--	E	E	E	E	GE	GE	GE	GE	E	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV Verify	--	--	--	--	--	E	E	E	E	E	E	E	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--
PIV Digital Signature with on card Hash	--	--	--	--	--	E	E	E	E	E	E	E	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--
PIV-SAM	--	--	--	--	--	E	E	E	E	E	E	E	--	--	--	--	--	--	--	--	--	--	--	E	E	E	

Table 13 – Access to CSPs by Service

The table is organized to correspond to the set of unauthenticated services, then authenticated services.

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP (read access to the CSP by an outside entity).
- E = Execute: The module executes using the CSP.

- W = Write: The CSP is imported into the module.
- Z = Zeroize: The module zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure)
- -- = Not accessed by the service.

4 Self-test

4.1 Power-On Self-tests

Integrity test and the KAT for all approved algorithms are run during module manufacturing. This includes all Power-On Self-Tests (POST) described in Table 14.

During every subsequent power-on (both contact and contactless) the Firmware Integrity Test is run.

At any stage of the module's lifecycle, the operator can request a manual run of all the POST listed in Table 14 by sending the "Run POST" command described in the module user guide.

Test Target	Description
CRC-16	Compute CRC 16 from a fixed message and check the result (a critical function test).
Firmware Integrity	16 bit CRC performed over all executable code in NVM.
DRBG	Performs a fixed input KAT.
AES	Self-test of AES forward cipher is performed by the SP 800-108 self-test. Self-test of AES inverse cipher is performed by the SP 800-38F self-test.
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
SP 800-108 KDF	Performs a KAT of SP 800-108 KDF. This self-test is inclusive of AES CMAC and AES encrypt function self-test.
SP 800-38F	Performs a KAT of SP 800-38F key unwrapping. This self-test is inclusive of AES decrypt function self-test.
RSA STD	Performs RSA signature verify KAT using an RSA 2048-bit key.
RSA CRT	Performs RSA CRT signature generate KAT using an RSA 2048-bit key. This test is inclusive of the RSADP primitive.
ECDSA	Performs known answer test using the P-224 curve. This self-test is inclusive of the ECC CDH function self-test.
SHA-256	Performs a fixed input KAT of SHA-256 (inclusive of the SHA-224 truncated variation).
SHA-512	Performs a fixed input KAT of SHA-512 (inclusive of the SHA-384 truncated variation).
SHA-3	Performs a fixed input KAT of SHA-3

Table 14 – Power-On Self-Test

4.2 Conditional self-tests

On every call to the DRBG or True (HW) RNG, the module performs the AS09.42 continuous RNG test to assure that the output is different than the previous value.

The module performs the SP 800-90A health monitoring tests for all DRBG functions.

When an RSA or ECC key pair is generated or loaded, the module performs a pairwise consistency test.

When new firmware is loaded into the module using the *Manage Content* service, the module verifies the integrity of each packet using AES CMAC. Optionally, the firmware load process can also verify the signature of

the new firmware (applet) using the DAP-PUB public key; the signature block in this scenario is generated by an external entity using the private key corresponding to DAP-PUB.

NOTE: If any self-test fails, the system emits an error code (0x6FXX) and enters the SELF-TEST ERROR state.

5 Physical Security Policy

The module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations.

The module is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging.

Module hardness testing was performed at the following temperatures:

- Nominal temperature: 20°C
- Low temperature: -40°C
- High temperature: 120°C

6 Operational Environment

The module is designated as a limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

7 Electromagnetic interference and compatibility (EMI/EMC)

The module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

8 Mitigation of Other Attacks Policy

The module implements defenses against:

- Light attacks
- Invasive fault attacks
- Side-channel attacks: SPA/DPA; Timing analysis;
- Electromagnetic attacks
- Differential fault analysis (DFA)
- Card tearing attacks

9 Security Rules and Guidance

The module implementation also enforces the following security rules:

- No additional interface or service is implemented by the module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the comprehensive zeroization mechanism.
- The module does not support manual key entry, output plaintext CSPs or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.