# ID-One PIV 2.4 on Cosmo V8.2

## NPIVP & CIV
## Configurations

### FIPS 140-2 Non-Proprietary
### Cryptographic Module Security Policy

IDEMIA Identity & Security, N.A.
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*<br>ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts*<br>ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols*<br>ISO/IEC 7816-4:2013 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*<br>ISO/IEC 7816-5:2004 *Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers*<br>ISO/IEC 7816-6:2004 *Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange*<br>ISO/IEC 7816-8:2004 *Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations*<br>ISO/IEC 7816-9:2004 *Identification cards -- Integrated circuit cards -- Part 9: Commands for card management*<br>ISO/IEC 7816-11:2004 *Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods* |
| [ISO 14443] | ISO/IEC 14443-1: 2016 *Identification cards — Contactless integrated circuit cards — Proximity cards -- Part 1: Physical characteristics*<br>ISO/IEC 14443-2: 2016 *Identification cards — Contactless integrated circuit cards — Proximity cards -- Part 2: Radio frequency power and signal interface*<br>ISO/IEC 14443-3: 2016 *Identification cards — Contactless integrated circuit cards — Proximity cards -- Part 3: Initialization and anticollision*<br>ISO/IEC 14443-3/A1: 2016 *Identification cards — Contactless integrated circuit cards — Proximity cards -- Part 3: Initialization and anticollision, AMENDMENT 1: RFU handling rules*<br>ISO/IEC 14443-4: 2016 *Identification cards — Contactless integrated circuit cards — Proximity cards -- Part 4: Transmission protocol*<br>ISO/IEC 14443-4/A1: 2016 *Identification cards — Contactless integrated circuit cards — Proximity cards -- Part 4: Transmission protocol, AMENDMENT 1: RFU handling rules* |
| [ISO 24787] | ISO/IEC 24787: 2010 *Information technology -- Identification cards -- On-card biometric comparison* |
| [JavaCard] | *Java Card 3.0.4 Classic - Runtime Environment (JCRE) Specifications*<br>*Java Card 3.0.4 Classic - Virtual Machine (JCVM) Specifications*<br>*Java Card 3.0.4 Classic - Application Programming Interface (API)*<br>Published by Sun Microsystems, September 2011 |
| [GlobalPlatform] | *GlobalPlatform Card Specification 2.2.1 - January 2011,*<br>*GlobalPlatform Card Specification 2.2 – Amendment D – Secure Channel Protocol '03'– Version1.1.1 – July 2014,*<br>*GlobalPlatform Card Specification – Amendment E – Security Upgrade for card content management – Public Release November 2011 v1.0*<br>*GlobalPlatform Card Basic ID Configuration - Version 1.0 - December 2011*<br>*GlobalPlatform Card Technology Card Specification – ISO Framework Version 0.9.0.18 Public Review July 2013*<br>*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. |

| Reference | Full Specification Name |
|---|---|
| [ANSI 504-1] | INCITS 504-1-2013/AM1-2016 Information Technology - Generic Identity Command Set - Part 1: Card Application Command Set - Amendment 1 |
| [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 3 December 2019. |
| [FIPS 113] | NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985. |
| [FIPS 197] | 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 |
| [FIPS 202] | NIST, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, August 2015 |
| [SP800-38B] | NIST, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005. |
| [SP800-38F] | NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012 |
| [SP800-56A] | NIST, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007 |
| [SP800-56A Rev3] | NIST, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, Revision 3, April 2018 |
| [SP800-56B] | NIST, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography,* August 2009 |
| [SP800-56B Rev2] | NIST, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, Revision 2,* July 2018 |
| [SP800-56CRev1] | NIST, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, Revision 1, April 2018 |
| [SP800-57] | NIST, *Recommendation for Key Management*<br>– Part 1: General, revision 4, January 2016<br>– Part 2: Best Practices for Key Management Organization, Revision 1, May 2019<br>– Part 3: Application-Specific Key Management Guidance, Revision 1, January 2015 |
| [SP800-67 Rev2] | NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, November 2017 |
| [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 Rev2] | NIST, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019 |
| [SP800-133 Rev1] | NIST, *Recommendation for Cryptographic Key Generation, Revision 1*, July 2019 |

**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 |
| IC | Integrated Circuit |
| ISD | Issuer Security Domain, see [GlobalPlatform] |
| KAT | Known Answer Tests |
| NVM | Non-Volatile Memory (e.g. EEPROM, Flash) |
| OP | Open Platform (predecessor to Global Platform) |
| PCT | Pairwise Consistency Test |
| PII | Personal Identification Information |
| PKI | Public Key Infrastructure |
| POST | Power-On Self Tests |
| 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 2.4 on Cosmo V8.2 NPIVP & CIV Configurations cryptographic module from IDEMIA, 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 (NIST Personal Identity Verification Program), aka "PIV Government", is the COTS configuration for US Government Federal Employees and Contractors and targets PIV and PIV-I cards.
2. CIV, aka PIV-Civilian or PIV-C, is the COTS configuration for Commercial uses. It is fully backward compatible with NPIVP from an APDU perspective but offers enhanced functionality and additional access conditions.

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

| Security Requirement | Security Level |
|---|---|
| Cryptographic Module Specification | 2 |
| 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 version:** '30'
**OS Firmware version:** '6F01' for ID-One Cosmo v8.2
**Application Firmware version:** ID-One PIV Applet version 2.4.2

- Factory Configurations of ID-One PIV Instance:
  - NPIVP (SP800-73-4)
  - CIV (aka PIV-C)

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

- Contact Only
- Contactless Only
- Dual Interface

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 IDEMIA during manufacturing and cannot be changed.

The NPIVP and CIV instances of the ID-One PIV application run in FIPS 140-2 Level 2 Mode of Operation when the following conditions are met:

- Module shall return "FIPS140-2 Level 2" when the READ BINARY command (PIV Info (Unauthenticated) service) on its Elementary file (EF) with SFI=01 is called.
- The procedural methods provided in Section 9 are applied.

The NPIVP and CIV instances of the ID-One PIV application will run in the non-Approved mode of Operation if one of the above conditions is not met.

## 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.

When the chip is configured to support MIFARE DESFIRE EV1 emulation on a locked-out part of the EEPROM memory, such memory area as well as the MIFARE DESFIRE EV1 communication protocol is excluded from the cryptographic boundary of the module; the MIFARE DESFIRE EV1 emulation was not tested and is not a FIPS compliant component.

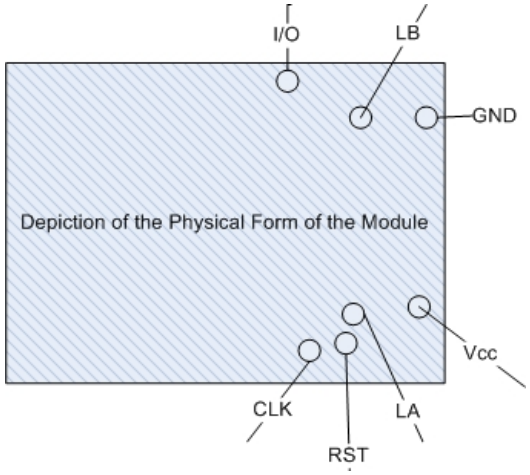


Figure 1 –Physical Form

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) |

| Port | Description | Logical Interface Type |
|---|---|---|
| LA, LB | ISO 14443: Antenna | Power, Control in, Data in, Data out, Status out<br>(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.

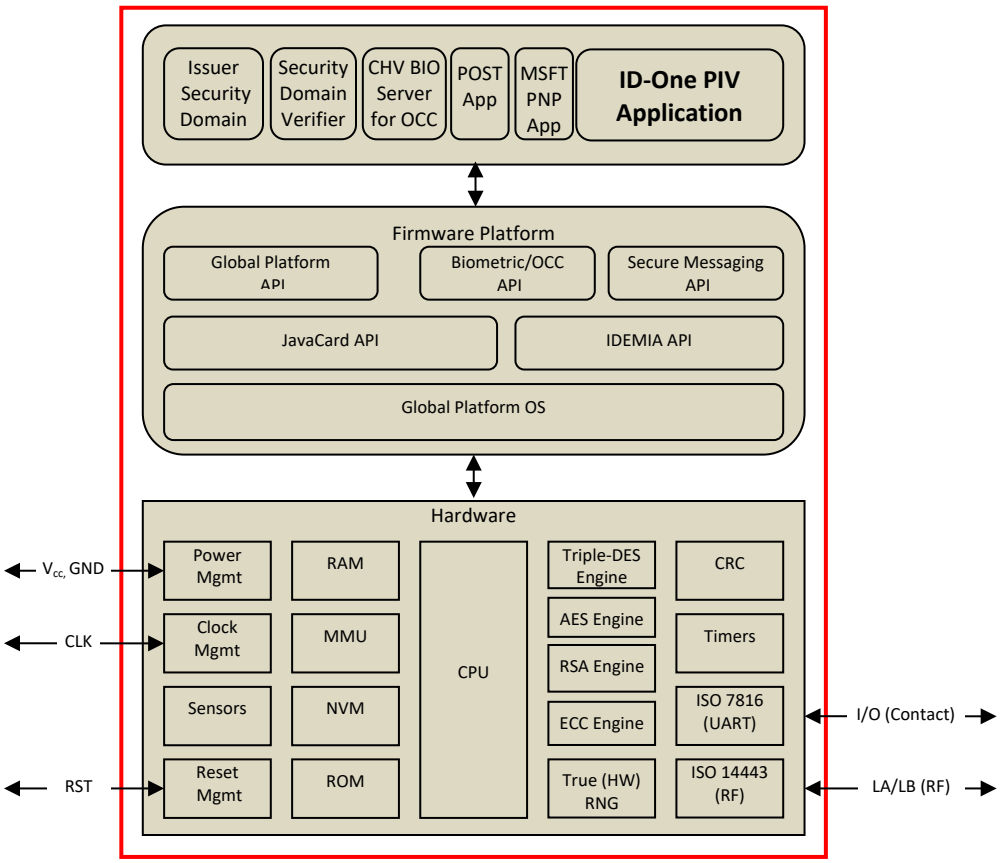


**Figure 2 - Module Block Diagram**
**(Cryptographic Boundary Outlined in Red)**

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.

The POST application provides on-demand POSTs and the MSFT PNP application provides identification of the associated mini-driver for Microsoft Windows to load to communicate with the module. 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 NDRNG. 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, non-Approved but allowed, and non-Approved and non-allowed security functions listed in Table 5, Table 6, and Table 7 below. Note that the full cryptographic algorithm implementation capabilities were tested for the Approved cryptographic functions but only algorithms/mode of operations/key sizes/ functionalities identified in Table 5 are implemented by the module.

| CAVP Cert.# | Security Function | Standard | Mode / Method | Strength[1] | Use |
|---|---|---|---|---|---|
| C982 | AES | [FIPS 197], [SP800-38A] | CBC, ECB | 128<br>192<br>256 | Data Encryption/ Decryption |
| C989 | AES CMAC | [SP800-38B] | CMAC | 128<br>192<br>256 | Message Authentication;<br>SP800-108 KDF |
| C1286 | AES KW | [SP800- 38F] | KW decryption with AES-128 inverse cipher | 128 | KW is not used by the module, only a self-test is performed. |
| Vendor Affirmed | Cryptographic Key Generation | [SP800-133 Rev1] | ¶5.1: Digital signature (seed is the direct output of the DRBG)<br>¶6.3: KAS generation<br>¶6.4: Derived from a Pre-Shared Key | 128<br>256 | Asymmetric key generation and symmetric key derivation |
| C991 | ECC CDH CVL | [SP800-56A] | ECC CDH Primitive | P-224<br>P-256<br>P-384<br>P-521 | Key Pair Generation<br>Shared Secret Computation |
| C984 | RSADP CVL | [SP800-56B] | RSA (CRT) key decryption primitive | RSA 2048 | Key decryption |
| C983 | RSADP CVL | [SP800-56B] | RSA (STD) key encryption primitive | RSA 2048 | Key encryption<br>(Not used by the module, only self-test is performed.) |
| C986 | RSASP1 CVL | [FIPS 186-4] | RSA (CRT) signature generation primitive | RSA 2048 | Signature generation primitive (off card hash). |
| C985 | RSASP1 CVL | [FIPS 186-4] | RSA (STD) signature verification primitive | RSA 2048 | Signature verification primitive (off card hash).<br>(Not used by the module, only self-test is performed.) |
| C987 | DRBG | [SP800-90A Rev1] | CTR | 128 | Deterministic Random Bit Generation<br>Derivation function is enabled |

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

| CAVP Cert.# | Security Function | Standard | Mode / Method | Strength[1] | Use |
|---|---|---|---|---|---|
| C990 | ECDSA | [FIPS 186-4] | The Hash is either provided by off-card entity or computed by the card depending on the digital signature key being called. | P-224<br>P-256<br>P-384<br>P-521 | Digital Signature Generation, Signature Verification, Key Generation, and Key Verification. |
| C988 | HMAC | [FIPS 198-1] | HMAC | SHA-256 | Message Authentication;<br>SP800-108 KDF<br>HMAC is not used by the module, only a self-test is performed. |
| Vendor Affirmed | KAS-SSC | [SP800-56ARev3] | OnePass EC Diffie-Hellman | P-256<br>P-384<br>P-521 | Secure Messaging Key Agreement |
| C995 | KBKDF | [SP800-108] | AES CMAC | 128<br>256 | Deriving keys from existing keys. |
| Vendor Affirmed | KDA | [SP800-56CRev1] | One-step key-derivation functions option 1 with SHA-256, SHA-384, or SHA-512 | ⩾ 256 | Secure Messaging Key Agreement |
| C982<br>C989 | KTS | [SP800-38F] | AES CBC/AES CMAC | 128<br>256 | SP800-38F §3.1 ¶3 Key transport (Uses AES Cert. #C982 and AES CMAC Cert. #C989);<br>Key establishment methodology provides 128 or 256 bits of encryption strength. |
| C994 | RSA CRT | [FIPS 186-4] | PSS | RSA 2048 | RSA key generation, digital signature generation and verification. |
| C979 | SHA-3 | [FIPS 202] | SHA3-512 | | SHA-3 is not used by the module, only a self-test is performed. |
| C978 | SHS | [FIPS 180-4] | SHA-224<br>SHA-256 | | Message Digest |
| C980 | SHS | [FIPS 180-4] | SHA-384<br>SHA-512 | | Message Digest |
| C981 | Triple-DES | [SP800-67 Rev2] | TCBC, TECB | 3-Key | Data Encryption/ Decryption / PIV. A procedural method described in section 9 ensure compliance with IG A.13 (maximum of $2^{16}$ 3-key Triple-DES encryptions with the same key). |

**Table 5 –Approved Security Functions**

| Security Function | Description |
|---|---|
| NDRNG | Hardware True RNG used to seed the FIPS approved DRBG. The NDRNG provides 128 bits of minimum entropy to the DRBG. |
| CSPs obfuscation (no security claimed) | CSPs obfuscation with a non-Approved algorithm. |

**Table 6 – Non-Approved but Allowed Security Functions**

| Security Function | Description |
|---|---|
| RSA CRT | 1024-bit RSA CRT signature generation primitive (off card hash). |
| 2-key TDEA | Two-Key Triple DES encryption and decryption (ECB and CBC modes). |
| 3-key TDEA | Three-Key Triple DES encryption (ECB and CBC modes) when the procedural method described in Section 9 ensuring compliance with IG A.13 is not met. |

**Table 7 – Non-Approved and non-allowed Security 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.

| CSP | Description / Usage |
|---|---|
| OS-DRBG-SEED | Entropy input and nonce provided by the NDRNG, used to seed the Approved DRBG. |
| OS-DRBG-STATE | The current AES-128 CTR_DRBG state. |
| 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 CMAC key used to verify inbound secure channel data integrity |
| SD-RMAC | AES-256 Session CMAC key used to generate response secure channel data MAC. |
| DAP-AES | AES-128 CMAC new firmware signature verification key. |

**Table 8 – OS Critical Security Parameters**

| CSP | Description / Usage |
|---|---|
| PIV-SENC | AES-128 and AES-256, PIV Secure Messaging (SM) session encryption key. |
| PIV-SMAC | AES-128 and AES-256, PIV Secure Messaging (SM) session Command CMAC key. |
| PIV-SRMAC | AES-128 and AES-256, PIV Secure Messaging (SM) session Response CMAC key. |
| PIV-SCFRM | AES-128 and AES-256, PIV Secure Messaging (SM) session key confirmation key. |
| PIV-SM | PIV Secure Messaging Key Establishment Key (04) as described in [SP800-73-4] or [ANSI 504-1].<br>All key types specified by [SP800-78-4] are supported: ECC P-256, and P-384 curves as well as P-521 for cipher suite ID CS6 specified in [ANSI 504-1]. |
| PIV-AUTH | Eight (8) bytes PIV authentication datum, with six (6) instances (3 Local and 3 Global) used for card holder PIN verification, PIN unblocking and Application Administrator authentication. |

| CSP | Description / Usage |
|---|---|
| PIV-PA | PIV Authentication Key (9A) as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384, and P-521 curves. |
| PIV-AA | Application Administrative Key (9B) as described in [SP800-78-4].<br>All key types specified by [SP800-78-4] are supported: 3-key Triple-DES, AES-128, AES-192, AES-256. |
| PIV-DS | PIV Digital Signature Key (9C) as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P-521 curves. |
| PIV-KM | Key Management Key (9D) as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P-521 curves. |
| PIV-RKM | Retired Key Management Keys (‘82’to ‘95’). Up to 20 instances as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P-521 curves. |
| PIV-SCA | Symmetric Card Authentication Key (9E) as described in [SP800-78-4]. All key types specified by [SP800-78-4] are supported: 3-key Triple-DES, AES-128, AES-192, AES-256 |
| PIV-ACA | Asymmetric Card Authentication Key (9E mandatory) as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P-521 curves. |
| PIV-MA | PIV Mutual Authentication Key; key type is identical to [SP800-78-4] 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-224, SHA-256, SHA-384 & SHA-512), and RSA PSS or ECDSA. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, P-224, P-256, P-384 and P-521 curves. |
| PIV-SAM-CMAC | Symmetric key (‘96’ optional) for generic CMAC computation (SAM functionality). AES-128, AES-192, AES-256 |
| PIV-SAM-KDF | Symmetric key (‘97’ optional) used to return the diversified key of a target card (SAM functionality): AES-128, AES-192, AES-256 |
| PIV-SAM-KDF-ENC | Symmetric key (‘98’ optional) used for Administrator to unlock a child PIV card. AES-128, AES-192, AES-256 |

**Table 9 –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 [SP800-78-4] is supported: P-256, P-384 and P-521 curves. |
| PIV-PA-PUB | PIV Authentication Key (9A) public component as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P-521 curves. |
| PIV-DS-PUB | PIV Digital Signature Key (9C) public component as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P-521 curves. |
| PIV-KM-PUB | Key Management Key (9D) public component as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P-521 curves. |
| PIV-ACA-PUB | Asymmetric Card Authentication Key (9E mandatory) public component as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P521 curves. |
| PIV-RKM-PUB | Retired Key Management Key (‘82’to ‘95’) public component as described in [SP800-78-4]. A superset of key types specified by [SP800-78-4] is supported: 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 [SP800-78-4] is supported: RSA-2048, ECC P-224, P-256, P-384 and P-521 curves. |

**Table 10 – 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 (PIV Verify service) 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 is encrypted during entry (by SD-SDEK or PIV-SENC) on both contact and contactless interfaces.

Table 11 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 11 - Roles Supported by the Module**

## 3.1 GP Secure Channel Protocol Authentication Methods

### 3.1.1 GP Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method is provided by the Secure Channel service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The off-card entity participating in the mutual authentication sent a 64-bit challenge to the Smart Card. The Smart Card generates its own challenge and computes a 64-bit cryptogram with SD-SMAC key and both challenges. The Smart Card cryptogram and challenge are sent to the off-card entity which checks the Smart Card cryptogram and creates its own 64-bit cryptogram with both challenges. A 64-bit message authentication code (MAC) is also computed on the command containing the off-card entity cryptogram with AES-CMAC and SD-SMAC key, the MAC is concatenated to the command, and the command is sent to the Smart Card. The Smart Card checks the message authentication code and compares the received cryptogram to the calculated cryptogram. If all of this succeeds, the two participants are mutually authenticated (the 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 (MAC||cryptogram, using a 128-bit block for authentication)

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/(2^128) = 2.6E-38 (MAC||cryptogram, using a 128-bit block for authentication)

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.

### 3.1.2 GP Secure Channel Protocol Authentication Method using Pseudo Random

The module supports Global Platform Authentication using an optional Pseudo Random method, described in [GlobalPlatform] Amendment D. The CO can determine the challenge which will be generated by the module. The use of a pseudo-random card challenge allows the offline preparation of personalization scripts while the module is not present and the processing of these scripts on the module without an online connection to the entity that prepared the scripts. When this option is called, the card challenge mentioned in the above section is the result of an AES-CMAC computed on a 24-bit counter value, a constant AID value, and a host challenge. The counter is initialized to 0 when the key is created or replaced, and the module returns an error when the counter reached $2^{24}$-1.

The use of the optional pseudo random card challenge does not impact the probabilities listed above.

## 3.2 PIV Symmetric Key Authentication Method

The external entity obtains a 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 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 = 4.8E-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, Alphanumeric (ASCII Printable), Numeric in BCD, HEX value, and minimum number of characters 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 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.

For configurations where only numeric PIN are supported, 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 two (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 can be configured up to 15, so the probability that a random attempt will succeed over a one-minute interval is:

- 15/(10^6 * 11^2) = 1.2E-7

For configurations where alphanumeric PIN are supported, the worst-case scenario permitted by the module is achieved with a minimum length of four (4) printable ASCII characters with at least one upper case, one lower case, one digit and one special character. The character space for the first four (4) bytes in this scenario is 94 (the values '20' through '7E' are permitted) and in the last four (4) characters is 95 (the values '20' through '7E' and 'FF' are permitted). The probability that a random attempt will succeed using this authentication method is:

- 1/(94^4 * 95^4) =1.5E-16

The maximum number of consecutive failed authentication attempts can be configured up to 15, so the probability that a random attempt will succeed over a one-minute interval is:

- 15/(94^4 * 95^4) = 2.3E-15

## 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 (FMR) at or below the respective values defined by NIST in Table 16 of [SP800-76-2], i.e., an 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 False Non-Match Rate (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. These services are available in both the Approved mode of operation and non-Approved mode of operation (when use with the non-Approved and non-allowed security functions listed in Table 7).

| Service | Description |
|---|---|
| Context | Select an application or manage logical channels. The selection of the POST application executes the Power-On Self-tests on demand. |
| Module Info (Unauthenticated) | Read unprivileged data objects, e.g., module configuration or status information. |
| Module Reset | Power cycle or reset the module. |
| PIV Info (Unauthenticated) | Read unprivileged data objects, e.g., application configuration or status information. Equivalent to FIPS 140-2 Show Status service. |
| Card Authentication | Authenticate in accordance with the [SP800-73-4] Card Authentication process. |
| PIV Authentication | System level authentication of the PIV Application/card in accordance with [SP800-73-4]. |
| PIV Digital Signature | Sign an externally generated hash in accordance with [SP800-73-4]. |
| PIV Secure Messaging | Establish and use a PIV Secure Messaging communications channel. |
| PIV System Key Services | Decrypt a key or generate a shared secret in accordance with [SP800-73-4]. Key decryption is the use of [SP800-56B] Section 7.1.2 RSADP key decryption primitive. Shared secret generation is the use of [SP800-56A] Section 5.7.1.2 |

**Table 12 - 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. All the CSPs are zeroized when the life cycle status is set to TERMINATED. | 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 [SP800-73-4]. | | X | |
| PIV Digital Signature (Authenticated) | Digital signature of SHA digest provided by the off-card entity. | | | X |
| PIV Info (Authenticated) | Read PIV Application privileged data objects. | | | X |
| PIV Manage Content | 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 on-card Hash | Same as PIV Digital Signature but with message hashing and formatting performed within the module. | | | X |
| PIV-SAM | Use the PIV card as a SAM to compute CMAC, KDF or authentication cryptogram to unlock a target card. | | | X |

**Table 13 –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] and [ANSI 504-1] establishes a secure channel to protect confidentiality and integrity of transmitted information and allows the off-card entity initiating the PIV Secure Messaging to authenticate the module. Unlike GP Secure Channel, the PIV Secure Messaging does not allow the module to authenticate the off-card entity.

The PIV Secure Messaging protocol conforms to [SP800-56A] or [ANSI 504-1] for the establishment of a shared secret and key derivation for session keys.

## 3.7 CSP Access Type

| Service | CSPs | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | OS-DRBG-SEED | OS-DRBG-STATE | SD-KENC | SD-KMAC | SD-KDEK | SD-SENC | SD-SMAC | SD-RMAC | DAP-AES | PIV-SENC | PIV-SMAC | PIV-SRMAC | PIV-SCFRM | PIV-SM | PIV-AUTH | PIV-PA | PIV-AA | PIV-DS | PIV-KM/PIV-RKM | PIV-SCA | PIV-ACA | PIV-MA | PIV-DS-HASH | PIV-SAM-CMAC | PIV-SAM-DKF | PIV-SAM-KDF-ENC |
| Context | -- | -- | -- | -- | -- | E | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Module Info (Unauthenticated) | -- | -- | -- | -- | -- | E | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Module Reset | G E Z | G E Z | -- | -- | -- | Z | Z | Z | -- | Z | Z | Z | Z | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV Info (Unauthenticated) | -- | -- | -- | -- | -- | -- | -- | -- | -- | E | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Card Authentication | -- | -- | -- | -- | -- | -- | -- | -- | -- | E | E | E | -- | -- | -- | -- | -- | -- | -- | 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 | -- | G E | G E | G E | G E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV System Key Services | -- | -- | -- | -- | E | E | E | E | -- | E | E | E | -- | -- | -- | -- | -- | -- | E | -- | -- | -- | -- | -- | -- | -- |
| | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GP Secure Channel | -- | G E | E | E | -- | G E | G E | G E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Lifecycle | Z | Z | Z | Z | Z | E | E | E | Z | -- | -- | -- | -- | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z |
| Manage Content | -- | -- | I | I | I | E | E | E | E | -- | -- | -- | -- | I | I | I | I | I | I | I | I | I | I | I | I | I |
| Module Info (Authenticated) | -- | -- | -- | -- | -- | E | E | E | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV Administrator Authentication | -- | -- | -- | -- | E | E | E | E | -- | E | E | E | -- | -- | E | -- | E | -- | -- | -- | -- | E | -- | -- | -- | -- |
| PIV Digital Signature (Authenticated) | -- | -- | -- | -- | 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 | -- | G I Z | I | G E I Z | E I Z | G E I Z | G E I Z | I Z | G E I Z | E I Z | G E I Z | E I Z | E I Z | E I Z |
| 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 14 – Access to CSPs by Service**

| Service | Public Keys | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | DAP-PUB | PIV-SM-PUB | PIV-PA-PUB | PIV-DS-PUB | PIV-KM-PUB | PIV-ACA-PUB | PIV-RKM-PUB | PIV-DS-HASH-PUB |
| Context | -- | -- | -- | -- | -- | -- | -- | -- |
| Module Info (Unauthenticated) | -- | -- | -- | -- | -- | -- | -- | -- |
| Module Reset | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV Info (Unauthenticated) | -- | -- | -- | -- | -- | -- | -- | -- |
| Card Authentication | -- | -- | -- | -- | -- | O | -- | -- |
| PIV Authentication | -- | -- | O | -- | -- | -- | -- | -- |
| PIV Digital Signature | -- | -- | -- | O | -- | -- | -- | O |
| PIV Secure Messaging | -- | O | -- | -- | -- | -- | -- | -- |
| PIV System Key Services | -- | -- | -- | -- | O | -- | O | -- |
| | | | | | | | | |
| GP Secure Channel | -- | -- | -- | -- | -- | -- | -- | -- |
| Lifecycle | Z | Z | Z | Z | Z | Z | Z | Z |
| Manage Content | E I O Z | -- | -- | -- | -- | -- | -- | -- |
| Module Info (Authenticated) | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV Administrator Authentication | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV Digital Signature (Authenticated) | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV Info (Authenticated) | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV Manage Content | -- | G I O Z | G I O Z | G I O Z | G I O Z | G I O Z | G I O Z | G I O Z |
| PIV Verify | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV Digital Signature with on card Hash | -- | -- | -- | -- | -- | -- | -- | -- |
| PIV-SAM | -- | -- | -- | -- | -- | -- | -- | -- |

**Table 15 – Access to Public Keys by Service**

The tables are organized to correspond to the set of unauthenticated services, then authenticated services.

- G = Generate: The module generates or derives the CSP.
- E = Execute: The module executes the CSP.
- I = Input: The CSP is imported into the module.
- O = Output: The CSP is output from 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-Tests

## 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 16 below.

During every subsequent power-on (both contact and contactless) the POSTs highlighted in bold are run; the other POSTs are performed during manufacturing and on demand (conditional self-tests) as per IG 9.11.

At any stage of the module's lifecycle, the operator can request a manual run of all the POST listed in Table 16 below by selecting the POST applet instance.

| Test Target | Description |
|---|---|
| **NVM Integrity** | 16-bit CRC performed over all executable (JavaCard packages) in NVM. |
| **ROM Code Integrity** | 32-bit CRC performed over all ROM code. |
| AES | Self-test of AES forward cipher is performed by the KBKDF self-test. Self-test of AES inverse cipher is performed by the AES KW self-test. |
| CRC-16 | Computes CRC-16 from a fixed message and checks the result (a critical function test). |
| DRBG | Performs a fixed input KAT of CTR_DRBG instantiate and generate functions. |
| DRBG Reseed | Test the reseed function of the DRBG. |
| ECDSA | Performs ECDSA signature generation and verification KATs using the P-224 curve. This self-test is inclusive of the KAS-SSC ECC CDH function self-test. |
| HMAC | Performs a fixed input KAT of HMAC. |
| RSA STD | Performs RSA signature verify KAT followed by an RSA signature verify KAT using an RSA 2048-bit key in its modulus/exponent form. For RSA keys defined as Key Management Keys, the RSA STD KAT performs an RSA Encrypt followed by an RSA Decrypt using an RSA 2048-bit key in its modulus/exponent form. |
| RSA CRT | Performs RSA signature generate KAT followed by an RSA signature verify KAT using an RSA 2048-bit key in its Chinese Remainder Theorem (CRT) form. This test is inclusive of the RSADP and RSASP primitives. For RSA keys defined as Key Management Keys, the RSA CRT KAT performs an RSA Encrypt followed by an RSA Decrypt using an RSA 2048-bit key in its Chinese Remainder Theorem (CRT) form. |
| RSA PSS | Performs a 2048-bit RSA-CRT PSS signature generation and verification Pairwise Consistency Check with SHA-256. |

| Test Target | Description |
|---|---|
| SHA-256 | Performs a fixed input KAT of SHA-256. This self-test is inclusive of the SHA-224 truncated variation and KDA component self-test. |
| SHA-512 | Performs a fixed input KAT of SHA-512. This self-test is inclusive of the SHA-384 truncated variation and KDA component self-test. |
| SHA-3 | Performs a fixed input KAT of SHA-3. |
| KBKDF | Performs a KAT of KBKDF. This self-test is inclusive of ECB and CBC AES encrypt function, AES CMAC, and KAS-SSC key confirmation self-test. |
| AES KW | Performs a KAT of SP800-38F key unwrapping. This self-test is inclusive of ECB and CBC AES decrypt function self-test. |
| Triple-DES | Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode. |

**Table 16 – Power-On Self-Tests**

## 4.2 Conditional Self-Tests

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

When an RSA or ECC key pair is generated or transported into the module, the module performs a pairwise consistency test, it is also inclusive to the assurances regarding KAS-SSC key generation and importation

When new firmware is loaded into the module using the *Manage Content* service, 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.

NOTE: If any self-test fails (POST or Conditional) other than the pairwise consistency during key loading and new firmware loading conditional self-test, the module will enter in the Kill Card state and emit an error code that identifies the type of test that failed. No further communication with the module is possible until the module is reset (Power-On). For pairwise consistency during key loading or key generation, and new firmware loading conditional self-test, the module returns a 6A80 error status code, if the self-test fails.

# 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 process (*Manage Content* 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: The chip includes sensors to detect light attacks. A hardware attack event triggers the KillCard behavior described below.
- Invasive fault attacks: The chip includes sensors for fault attacks. A hardware attack event triggers the KillCard 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 KillCard 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 KillCard 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.

The KillCard 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.

# 9 Security Rules and Guidance

The module implementation also enforces the following security rules:

1. The module provides three distinct operator roles: Cryptographic Officer, PIV Application Administrator and User.
2. The module provides identity-based authentication.
3. The module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The module allows the operator to initiate power-up self-tests by power cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output are inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not have any proprietary external input/output devices used for entry/output of data.
13. The module does not output intermediate key values or plaintext CSPs.
14. No additional interface or service is implemented by the module which would provide access to CSPs.

For the module to run in FIPS mode of operation, the following rules, that are not automatically enforced by the module, must be obeyed by a procedural method:

1. Only algorithms listed in Table 5 –Approved Cryptographic Functions or Table 6 – Non-Approved but Allowed Cryptographic Functions can be used in the approved mode of operation.
2. When a 3-key Triple-DES key is loaded into the module, the key Usage Counter that defines the maximum number of uses of the key shall be set to $2^{16}$ max.