ID-One PIV-C on Cosmo V8

FIPS 140-2 Cryptographic Module Security Policy

Oberthur Technologies of America

4250 Pleasant Valley Road

Chantilly, VA 20151

USA

Document Number: SP_Cosmo_V8_R2 *Version 1.1* ***Revision Date: March 6, 2018***

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 3.0.1 Classic - Runtime Environment (JCRE) Specifications* *Java Card 3.0.1 Classic - Virtual Machine (JCVM) Specifications* *Java Card 3.0.1 Classic - Application Programming Interface (API)* Published by Sun Microsystems, May 2009
[GlobalPlatform]	*GlobalPlatform Card Specification 2.2.1 - January 2011,* *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
[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*

Reference	Full Specification Name
	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*
[SP800-73-4]	*NIST, Interface for Personal Identity Verification*
[SP800-78-4]	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, December 2010
[SP800-108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[INCITS 504-1]	INCITS*, Information Technology -Generic Identity Command Set -Part 1: Card Application Command Set, 2013*

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
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-C on Cosmo V8 cryptographic module from Oberthur Technologies, hereafter denoted *the module*. The module, validated to FIPS 140-2 overall Level 3, is a single chip module implementing the Global Platform operational environment, with Card Manager and ID-One PIV-C Applet Suite. The PIV-C applet suite in the module is a commercial equivalent configuration of the PIV applet that while following the PIV suite of specifications (e.g. [SP800-73-4] and [SP800-78-4]) includes additional features and protections.

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

Table 3 – Security Level of Security Requirements

1.1 Versions, Configurations and Modes of operation

Hardware: '0F'
Firmware: '5601'
Firmware Extension: '082371' with ID-One PIV Applet Suite 2.3.5

The module is available in 3 hardware configurations:

- Contact Only
- Contactless Only
- Dual Interface

The module is always in the Approved mode. The indicator of Approved mode is obtained using the Module Info (Unauthenticated) service to read the value of the FIPS Mode data object (tag '05') within the Card Identification data object (tag 'DF52'). The value read should be '01' (module set in FIPS 140-2 mode of operation during manufacturing).

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. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the figure.

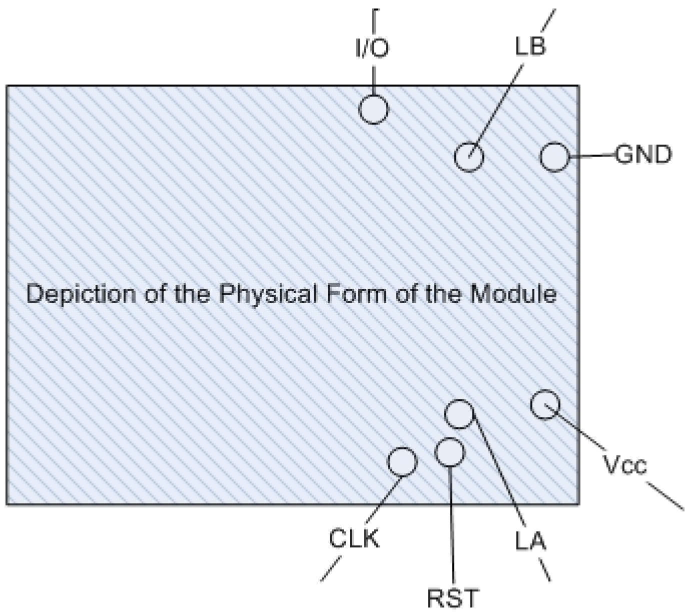

Figure 1 – Physical Form

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.

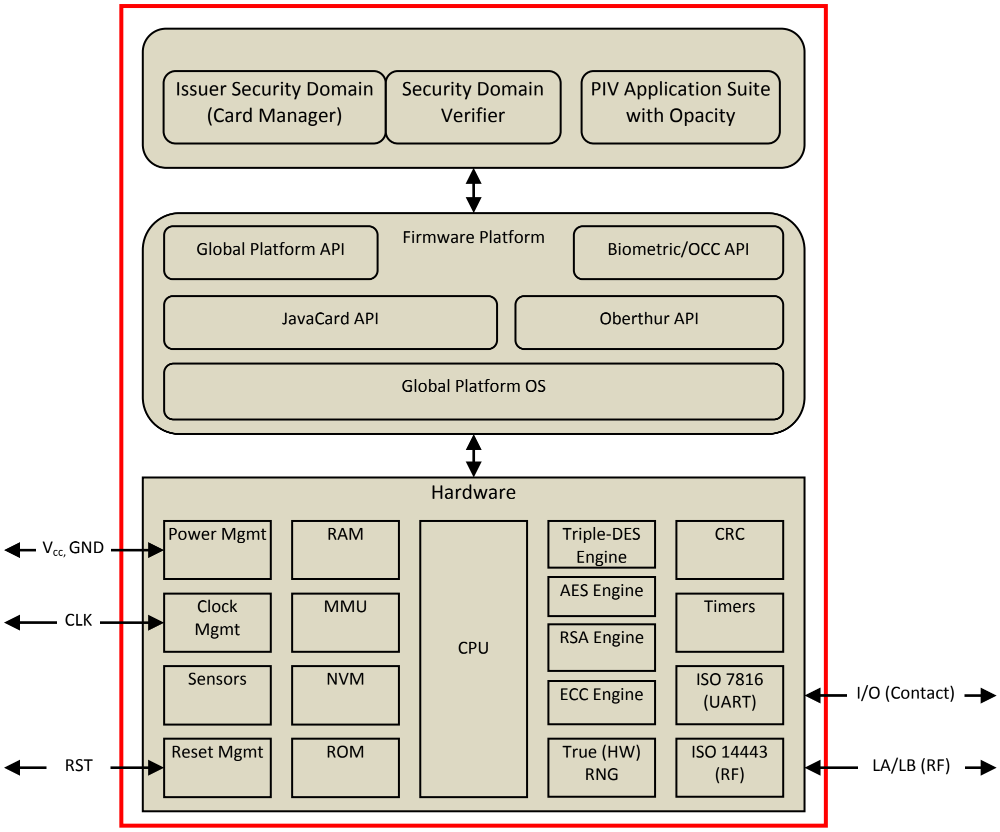

Figure 2 - Module Block Diagram
(Cryptographic Boundary Outlined in Red)

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.

Algorithm	Description	Cert #
DRBG	[SP 800-90A] AES-128 CTR_DRBG. Does not support prediction resistance, supports re-seed operation and concatenation to provide security strength greater than 128 bits.	537
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports 3-Key option only, and CBC and ECB modes.	1727
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports AES-128, AES-192- and AES-256 keys, and ECB and CBC modes.	2910
AES Key Wrap	[SP800-38F] AES Key Wrap (key establishment method provides 128-256 bits of encryption strength).	2910
KTS	AES Symmetric key wrap using AES 128, 192, 256 (key establishment method provides between 128 and 256 bits of encryption strength). Method compliant with SP 800-38F §3.1 ¶3, "combination" method based on AES and AES CMAC.	2910 2911
AES CMAC	[SP800-38B] AES CMAC. The module supports AES-128, AES-192 and AES-256 keys.	2911
SHA-256	[FIPS 180-2] Secure Hash Standard compliant one-way (hash) algorithms: SHA-224, SHA-256.	2449
SHA-512	[FIPS 180-2] Secure Hash Standard compliant one-way (hash) algorithms: SHA-384, SHA-512.	2450
RSA STD	[FIPS 186-4] RSA signature verification. The module supports 2048-bit RSA keys.	1531
RSA CRT	[FIPS 186-4] RSA key generation and signature generation. The module supports 2048-bit RSA keys.	1532
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-224, P-256, P-384, and P-521 curves for key pair generation, signature and signature verification.	526
KDF	[SP 800-108] AES CMAC-based KDF with AES-128, AES-192, AES-256.	33
RSADP	[SP 800-56B] SP 800-56B Section 7.1.2 RSA decryption primitive (as used by the PIV specification). The module supports the RSA-2048 key pair size, key decryption only.	336 (CVL)
SP 800-56A	[SP 800-56A] One-Pass Diffie-Hellman, C(1, 1, ECC CDH) scheme used by the Opacity protocol in [SP 800-73-4] PIV. This validated algorithm is inclusive of the Section 5.7.1.2 ECC CDH Primitive (as used by the PIV specification). The module supports the NIST defined P-224 and P-256 curves. Note: The module also supports parameter set ED (P-384 curve) without key confirmation, but this could not be tested through CAVS at the time of report submission. This issue has been raised with CAVP, and the additional testing will be performed when available.	48 (KAS)

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 usage 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-128, AES-192, AES-256 Master key used to generate SD-SENC.
SD-KMAC	AES-128, AES-192, AES-256 Master key used to generate SD-SMAC.
SD-KDEK	AES-128, AES-192, AES-256 Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES-128, AES-192, AES-256 Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES-128, AES-192, AES-256 Session MAC key used to verify inbound secure channel data integrity.
SD-RMAC	AES-128, AES-192, 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-192, AES-256 PIV Secure Channel (Opacity) session encryption key.
PIV-SMAC	AES-128, AES-192, AES-256 PIV Secure Channel (Opacity) session Command MAC key.
PIV-SRMAC	AES-128, AES-192, AES-256 PIV Secure Channel (Opacity) session Response MAC key.
PIV-SCFRM	AES-128, AES-192, AES-256 PIV Secure Channel (Opacity) session key confirmation key.
PIV-OSME	PIV Opacity Secure Messaging Establishment Key as described in [INCITS 504-1]. All crypto suites defined in [INCITS 504-1] table 91 are supported. A superset of key types specified by [SP 800-78-4] are supported: ECC P-224, P-256, and P-384 curves.
PIV-AUTH	8 byte PIV authentication datum, with 3 instances 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]. 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-AA	Application Administrative Key (9B) as described in [SP 800-78-4]. A superset of 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-SCA	Symmetric Card Authentication Key (9E optional) as described in [SP 800-78-4].A superset of 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.

Table 8 –PIV Critical Security Parameters

2.2 Public Keys

Key	Description / Usage
DAP-PUB	RSA 2048 new firmware signature verification key.
PIV-OSME-PUB	The public key component used by the PIV Secure Message (Opacity) protocol. A superset of key types specified by [SP 800-78-4] are supported: ECC P-224, P-256, and P-384curves.
PIV-OSME-ROOT	Root public key to verify the ECDSA signature of the host CVCs on the ICC.
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.

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 SCP 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. 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 SD-SDEK), and is only accessible by authenticated services.

Table 9 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* below.
AA	Application Administrator – a role that manages PIV application-related content and configuration. Authenticated as described in *PIV Application Administrator Authentication* below.
User	User – role for use in PIV-C applet suite. Authenticated as described in *PIV-C User Authentication* below.

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:

- 1/2^128 = 2.9E-39 (for any of AES-128/192/256 SD-KENC/SD-SENC, 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 = 4.4E-38 (for any of AES-128/192/256 SD-KENC/SD-SENC, 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.

3.2 PIV-C Symmetric Key Authentication Method

The external entity obtains an 8-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 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

3.2.1 PIV-C 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 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 6 characters means secrets can be created from 6 to 8 characters, determined by the user.

The worst case scenario permitted by the module is a minimum length of 6 characters with the Numeric in ASCII character set. The character space for the first 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

3.2.2 PIV-C Opacity Mutual Authentication Method

The module verifies the certificate of the external entity using the PIV-SM-ROOT. It then generates an ephemeral ECC key pair in which the generated private key part together with the host public key extracted from the host's certificate is used to generate a shared secret (Z1). This shared secret is then used to derive two keys K1 and K2 as per SP800-56A.

Another shared secret is generated using the PIV-SM and the host ephemeral public key. This shared secret together with the host identifier extracted from the certificate is used to derive the session keys used for secure messaging (PIV-SENC, PIV-SCMAC and PIV-SRMAC). The previously generated public ECC key, the host identifier and the host ephemeral public ECC key is used to create a cryptogram which will then be verified by the external entity. This will authenticate the module to the external entity. The external entity is implicitly authenticated to the module as soon as the next APDU is received since this APDU will have been sent under secure messaging using the session keys generated.

3.3 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.

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 Authentication	System level authentication of the PIV Application/card in accordance with [SP 800-73-4].			X
PIV Digital Signature	Sign an externally generated hash in accordance with [SP 800-73-4].			X
PIV Info (Authenticated)	Read PIV Application privileged data objects.			X
PIV Manage Content	Load or generate PIV Application keys and data.		X	
PIV Secure Channel	Establish and use a PIV (Opacity) secure communications channel.		X	X
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			X
PIV Verify	Grant access control rights for objects or services.		X	X

Table 12 –Authenticated Services

3.4 Opacity Modes

The Opacity protocol is defined in [INCITS 504-1]. Two modes of Opacity operation are supported by this module: Zero Key Management (ZKM) and Full Secrecy (FS).

Opacity ZKM establishes a secure channel to protect confidentiality and integrity of transmitted information, but does not provide any authentication services.

Opacity FS provides authentication service as well as establishment of a secure channel to protect confidentiality and integrity of the transmitted data.

Both modes of Opacity conform 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-OSME	PIV-AUTH	PIV-PA	PIV-AA	PIV-DS	PIV-KM	PIV-SCA	PIV-ACA	PIV-MA
Card Authentication	--	--	--	--	--	--	--	--	--	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	--	--	--	--	--	--	--	--	--	--
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
Module Info (Authenticated)	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV Administrator Authentication	--	--	--	--	--	E	E	E	E	E	E	E	--	--	E	--	E	--	--	--	--	E
PIV Authentication	--	--	--	--	--	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	GeW Z	EW Z	GEW Z	GEW Z	WZ	GEW Z	EWZ
PIV Secure Channel	--	--	--	--	--	E	E	E	E	GE	GE	GE	GE	E	--	--	--	--	--	--	--	--
PIV System Key Services	--	--	--	--	--	E	E	E	E	E	E	E	--	--	--	--	--	--	E	--	--	--
PIV Verify	--	--	--	--	--	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

On power-on or reset, the module performs self-tests as described in Table 12 below. All KATs must be completed successfully prior to any other use of cryptography by the module.

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. This test is inclusive of the RSADP primitive.
RSA CRT	Performs RSA CRT signature generate KAT using an RSA 2048-bit key.
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).

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.