HID Global ActivID Applet Suite v2.7.3 on Oberthur Technologies Cosmo V8

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.2

Date: January 19, 2016

Table of Contents

Table of Tables

Table of Figures

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1,* March 2003, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 25 July 2013.
[INCITS 504-1]	*INCITS, Information Technology - Generic Identity Command Set - Part 1: Card Application Command Set, Amendment*
[ISO 7816]	ISO/IEC 7816-1: 1998 *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 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification* *Java Card 2.2.2 Virtual Machine (JCVM) Specification* *Java Card 2.2.2 Application Programming Interface* Published by Sun Microsystems, March 2006
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[SP800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[SP800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[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
[SP800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[SP800-73-4]	*NIST, Interface for Personal Identity Verification (Revised Draft)*
[SP800-78-4]	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification (Revised Draft)*
[SP800-90Ar1]	NIST Special Publication 800-90A, *Recommendation for Random Number Generation Using* Deterministic Random Bit GeneratorsAmerican Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1998

Acronym	Full Specification Name
	- Appendix A.2.4., Revision 1, June 2015.
Acronym	**Full Specification Name**
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1,* March 2003, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004
[ISO 7816]	ISO/IEC 7816-1: 1998 *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 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification* *Java Card 2.2.2 Virtual Machine (JCVM) Specification* *Java Card 2.2.2 Application Programming Interface* Published by Sun Microsystems, March 2006
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[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.
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[SP800-108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[SP800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 25 July 2013.
[INCITS 504-1]	*INCITS, Information Technology - Generic Identity Command Set - Part 1: Card Application Command Set, Amendment*
[SP800-73-4]	*NIST, Interface for Personal Identity Verification (Revised Draft)*
[SP800-78-4]	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification (Revised Draft)*

Table 1 – References

Acronyms and definitions

Acronym	Definition
ACA	Access Control Applet
API	Application Programming Interface
ATR	Answer To Reset
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter, see [FIPS 140-2]
CVC	Card Verifiable Certificate
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
MMU	Memory Management Unit
NVM	Non-Volatile Memory
OP	Open Platform (predecessor to Global Platform)
OPACITY	Open Protocol for Access Control, Identification and Ticketing with privacY
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
PUK	Pin Unblocking Key
RSA	Rivest Shamir and Adelman
SMA	Secure Messaging Anonymous
TPDU	Transaction Protocol Data Unit, see [ISO 7816]
XAUT	External Authentication

Table 2 – Acronyms and Definitions

1 Introduction

This document defines the Security Policy for the HID Global ActivID Applet Suite on the Oberthur Technologies Cosmo V8 cryptographic module, hereafter denoted ***the Module***. The Module, validated to FIPS 140-2 overall Level 2, is a single chip smartcard module implementing the JavaCard platform, Global Platform operational environment, with Card Manager as well as the ActivID Applet Suite.

The HID Global ActivID Applet Suite is a commercial equivalent configuration of the PIV applet (PIV-C) that while following the PIV suite of specifications (e.g. [SP800-73-4] and [SP800-78-4]) is not intended for GSA FIPS 201 EP qualification. It is also compliant with the GSC-IS 2.1 standard.

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

Area	Description	Level
1	Module Specification	2
2	Ports and Interfaces	2
3	Roles and Services	3
4	Finite State Model	2
5	Physical Security	4
6	Operational Environment	N/A
7	Key Management	2
8	EMI/EMC	3
9	Self-test	2
10	Design Assurance	3
11	Mitigation of Other Attacks	2
	Overall	2

Table 3 – Security Level of Security Requirements

The Module is bound to the Cert. # 2303 Oberthur Technologies Cosmo V8 module, which provides a Global Platform JavaCard operational environment. The Cert. #2303 module included an Oberthur PIV applet suite, which is not available in this Module.

In this Module:

- The hardware and operating system are unchanged from Cert. #2303
- The ActivID Applet Suite replaces the Oberthur PIV Application Suite with Opacity. Cryptographic services and algorithms that are not available in this configuration have been removed from the security policy and validation process.
- This Module is available in one of the three possible packaging options represented in Cert. #2303: the dual interface package.

1.1 Versions, Configurations and Modes of operation

Hardware: Oberthur Technologies '0F'
OS Firmware: Oberthur Technologies firmware '5601'
Application Firmware: HID Global ActivID Applet Suite 2.7.3, comprising:

- **ASCLIB: 2.7.3.6**
- **ACA: 2.7.3.6**
- **GC/PKI/SKI: 2.7.3.6**
- **PIV EP Wrapper: 2.7.3.8**
- **SMAv3: 2.7.3.10**

The Module provides only a FIPS 140-2 Approved mode. The platform Answer To Reset (ATR) and the ActivID Applet Suite provide the indicators of the Approved mode.

Table 4 - Approved Mode Indicators

Command and associated elements	Expected Response
Use of Module Info service to read FIPS Mode data object (tag '05') within the Card Identification data object (tag 'DF52')	'01' (indicates FIPS mode; set in FIPS 140-2 mode of operation during manufacturing).
ACA applet Module Info service (GET PROPERTIES command with tag 24).	0x24 0x02 ***01*** YY, where the 01 (in bold italics) value indicates the FIPS 140-2 Approved mode.

2 Hardware and Physical Cryptographic Boundary

The Module is designed to be embedded into lead frames which are then built into plastic card bodies, with a contact plate and contactless antenna connections. The physical form of the Module is depicted in Figure 1; the cryptographic boundary is the surface and edges of the die, with the bond pads providing the physical port connection points.

The contactless ports of the Module require connection to an antenna. The Module relies on [ISO7816] and [ISO14443] card readers as input/output devices. Control/data input and status/data output share a common physical port, with the logical separation into interfaces determined by the ISO 7816 and ISO 14443 protocols.

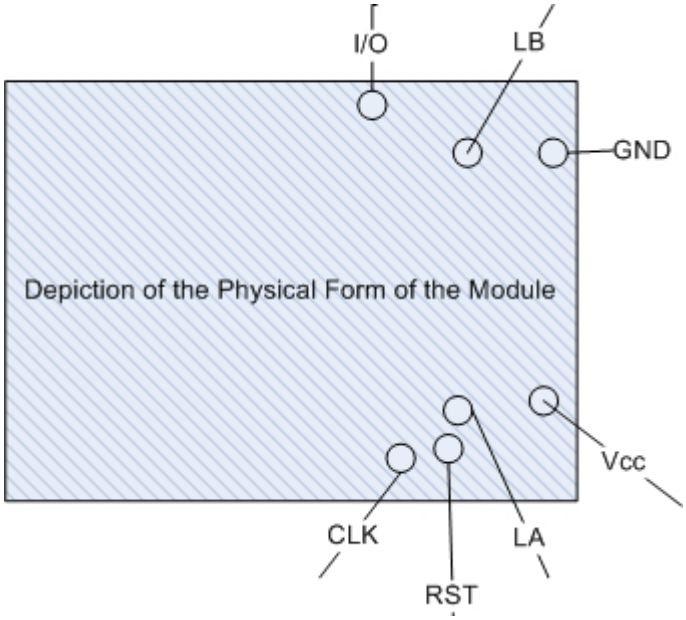

Figure 1 – To scale depiction of the Cosmo V8 Module (top, connection pads side)

Table 5 – Ports and Interfaces

Port	Description	Logical Interface Type
$V_{CC,}$ GND	ISO 7816: Supply voltage	Power
RST	ISO 7816: Reset	Control in
CLK	ISO 7816: Clock	Control in
I/O	ISO 7816: Input/Output	Control in, Data in, Data out, Status out
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out
NC	Not connected	Not connected

2.1 Firmware and Logical Cryptographic Boundary

Figure 4 depicts the Module operational environment.

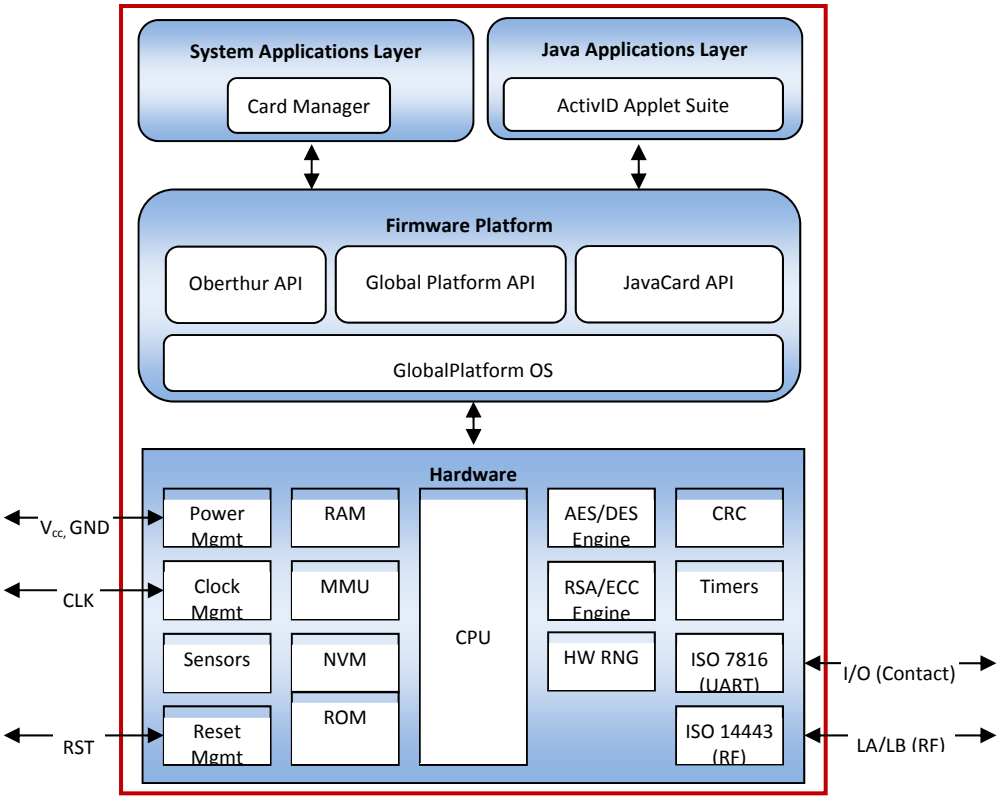

Figure 2 - Module Block Diagram

The JavaCard, GlobalPlatform and Oberthur APIs are internal interfaces available only to applets and security domains (i.e., Card Manager). Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

The NVM is separated into segments with different access rules, enforced by the hardware MMU. The MMU is initialized with the correct settings by startup code, and verified by the operating system each time the system starts. The MMU settings cannot be changed at run time. All code is executed from ROM and NVM.

The HID Global ActivID Applet Suite 2.7.3 comprises:

- **ASC Library package** – This is the library package that implements functions required by other applets. The library functions are not directly accessible via the cryptographic Module command interface.
- **Access Control Applet (ACA)** – This applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. Three off-card entity authentication methods – GP secure messaging, PIN, and External Authentication are included by default in the ACA applet.
- **SMAv3 Applet** – This applet implements the OPACITY ZKM Secure Messaging protocol based on [INCITS 504-1]. This Secure Messaging is initiated through the use of a key establishment protocol, based on a static ECC key pair stored in the applet and an ephemeral ECC key pair generated on the host application. This key establishment is a one-way authentication protocol that authenticates the card to the host application and establishes a set of AES session keys used to protect the communication channel between the two parties.
- **PKI/Generic Container/ SKI (PKI/GC/SKI) Applet** – The PKI/GC/SKI Applet provides secure storage for PKI credentials, and other data that are required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based

cryptographic operations using the RSA private key stored in the PKI buffers. The applet also exposes OTP (One Time Password) services for synchronous or asynchronous authentication. This applet is compliant with GSC-IS 2.1.

- **PIV EP Wrapper Applet** – This Applet aligns with [SP800-73-4] (both at card-edge and data model levels). This Applet is a wrapper on top of the ActivID Applet Suite 2.7.3 (ASCLIB, ACA, GC/PKI/SKI and SMAv3 above). Its purpose is to access the PIV card-edge and objects although objects are physically stored in the GC/PKI/SKI and SMAv3 applet instances. This Applet cannot operate in standalone mode and must interface with the ACA, GC/PKI/SKI and SMAv3 applets to operate properly.

The JavaCard API is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

3 Cryptographic functionality

The Module implements the Approved and Non-Approved but Allowed cryptographic functions listed in Tables 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 encrypt and decrypt in CBC or ECB modes.	1727
AES AES Key Wrap	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports AES-128 keys, and ECB and CBC modes. [SP800-38F] AES Key Wrap, denoted KW and KWP on the AES listing (key establishment method provides 128 bits of encryption strength).	2910
AES CMAC	[SP800-38B] AES CMAC. The Module supports AES-128 keys.	2911
KBKDF	[SP 800-108] CMAC-based KDF with AES-128.	33
SHA	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms: SHA-1, SHA-256.	2449
RSA CRT	[FIPS 186-4] RSA key generation and signature generation. The Module supports 2048-bit RSA keys.	1532
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 (KAS list)	[SP 800-56A] Inclusive of the Section 5.7.1.2 ECC CDH Primitive only (as used by the PIV specification for OPACITY). The Module supports the NIST defined P-256 curve.	48 (KAS)
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

Table 6 –Approved Cryptographic Functions

Algorithm	Description
NDRNG	Hardware NDRNG used to provide entropy input to the FIPS approved DRBG.
EC DH	EC Diffie-Hellman (key agreement; key establishment methodology provides 128 bits of encryption strength). Non-compliant SP 800-56A EC Diffie-Hellman in accordance with the OPACITY protocol. Listed as “non-compliant”, as it is not CAVP tested or power-on self-tested, with the exception of the ECC CDH primitive included in the KAS Cert. #48. Allowed in accordance with SP 800-131A and IG G.14.

Table 7 – Non-Approved but Allowed Cryptographic Functions

3.1 Critical Security Parameters

All CSPs used by the Module are described in this section.

Key	Description / Usage
OS-RNG_STATE	384 bit value; the current RNG state.
SD-KENC	AES-128 Master key used to generate SD-SENC.
SD-KMAC	AES-128 Master key used to generate SD-SMAC.
SD-KDEK	AES-128 Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES-128 Session encryption key used to decrypt secure channel data.
SD-SMAC	AES-128 Session MAC key used to verify inbound secure channel data integrity.
ACA-SPAK	3-Key TDEA key used by the ACA applet to authenticate the AA role (0-8 keys).
ACA-PIN	8 character string PIN used for local PIN verification.
ACA-PUK	8 character string PIN Unblocking Key used to confirm authorization to unblock a blocked PIN.
ACA-PC	8 character string Pairing Code used to associate a peer device for a virtual contact interface.
PKI-GPK	RSA 2048 general purpose key with usage determined outside the Module scope.
SKI-OTP	3-Key Triple-DES key used by the GC/PKI/SKI applet for one time password generation (0-n keys).
PIV-RPAK	RSA 2048 PIV Authentication (9A) RSA Authentication Key.
PIV-RDSK	RSA 2048 PIV Digital Signature (9C) RSA Private Signature Key.
PIV-RKDK	RSA 2048 PIV Key Management (9D) RSA Key Decryption Key. Up to 5 copies of this key may be stored in retired key locations ‘82’ though ‘86’.
PIV-RCAK	RSA 2048 PIV Card Authentication (9E) RSA Authentication Key.
SMA-OPRI	ECC P-256 static private key, used in the [INCITS 504-1] OPACITY protocol (ECC DH key agreement).
SMA-SCFRM	AES-128 session confirmation key used to compute the authentication data during SMA session establishment.
SMA-SENC	AES-128 session encryption key used to encrypt / decrypt secure channel data.
SMA-SCMAC	AES-128 session MAC key used to verify inbound (command) secure channel data integrity.
SMA-SRMAC	AES-128 session MAC key used to compute outbound (response) secure channel data integrity.

Table 8 – Critical Security Parameters

3.2 Public keys

Key	Description / Usage
PKI-RGPKPUB	RSA 2048 general purpose Key with usage determined outside the Module scope
PIV-RPAKPUB	RSA 2048 PIV Authentication (9A) RSA Authentication Public Key
PIV-RDSKPUB	RSA 2048 PIV Digital Signature (9C) RSA Signature Verification Key
PIV-RKDKPUB	RSA 2048 PIV Key Management (9D) RSA Key Decryption Key
PIV-RCAKPUB	RSA 2048 PIV Card Authentication (9E) RSA Authentication Public Key
SMA-CVC	ECC P-256 static public key (Card Verifiable Certificate), provided to the OPACITY host.
SMA-HPUB	ECC P-256 static public key, provided by the OPACITY host.

Table 9 – Public Keys

The PIV specifications [SP800-73-4, SP800-78-4] define the generation of asymmetric key pairs for PIV authentication (9A), digital signature (9C), key management (9D, with retired copies in 82-86) and card authentication (9E). When the Manage Content service is called to generate key pairs, the public keys listed above are returned by the PIV applet. An external entity (e.g., a card management system) is responsible for packaging the public key in an X509 certificate and storing it in the corresponding X509 certificate container in the PIV applet. The HID Global ActivID Applet Suite does not make use of the public keys after generation, and does not define any other usage of public keys.

Similarly, the SMA-CVC key is not used by the Module other than to provide to the host application in the OPACITY protocol.

4 Roles, authentication and services

Table 10 lists all operator roles supported by the Module. This Module does not support a maintenance role. The Module supports concurrent operators controlling access to restricted objects and services via the AC applet access control mechanism. The module clears previous authentications on power cycle.

Role ID	Role Description
AA	Application Administrator - responsible for configuration of the applet suite data. Authenticated using the Symmetric Cryptographic Authentication method.
CH	The Card Holder (user) uses the Module for an identity token. Authenticated in the PIV applet using the Secret Value authentication method.
CO	Cryptographic Officer - responsible for card issuance and management of card data via the Card Manager and ActivID Applet Suite. Authenticated using Secure Channel Protocol authentication.

Table 10 - Roles

4.1 Secure Channel Protocol Authentication

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 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 (SD-KENC/SD-SENC, using a 128-bit block for authentication)

The Module enforces a maximum of fifteen consecutive failed SCP authentication attempts. The probability that a random attempt will succeed over a one minute interval is:

- 15/(2^128) = 4.4E-38 (SD-KENC/SD-SENC, using a 128-bit block for authentication)

4.2 Secret Value Authentication

This authentication method compares a value sent to the Module to the stored ACA-PIN or ACA-PUK values; if the two values are equal, the operator is authenticated. This method is used to authenticate to the CH (User) role or to confirm authorization to unblock a blocked PIN.

The HID ActivID Applet Suite 2.7.3 does not support the FIPS 201 global PIN option.

The strength of authentication for this authentication method depends on both internal and external factors. The Module compares all 8 characters of the ACA-PIN or ACA-PUK value. Based on this, the probability of false authentication of this authentication method is as follows:

- 1/(256^8) = 5.4E-20

Based on the [SP800-73-4] defined maximum count of 15 for failed authentication attempts, the probability that a random attempt will succeed over a one minute period is

- 15/(256^8) = 8.1E-19

Please see Section 10 for guidance on required external security procedures associated with the PIV.

4.3 Symmetric Cryptographic Authentication

This authentication method decrypts (using ACA-SPAK) an encrypted challenge sent to the module by an external entity and compares the challenge to the expected value. This method is used to authenticate to the AA role.

The strength of authentication for this authentication method is based on the strength of ACA-SPAK; only 3-Key TRIPLE-DES are allowed for this key, but the limiting factor is the block size of 64 bits; hence the associated probability of false authentication of this authentication methods is:

- 1/(2^64) = 5.4E-20

The execution of this authentication mechanism is rate limited – the module can perform no more than 2^16 attempts per minute. Therefore, the probability that a random attempt will succeed over a one minute period is:

- (2^16)/(2^64) = 3.6E-15

4.4 Services

All services implemented by the Module are listed in the table below. The NR column in the table below indicates unauthenticated services available in the corresponding applet. Where NR and a role are checked, the service governs access to privileged objects based on access control rules and authentication status.

Service	Role			NR
	AA	CH	CO	
Authenticate – Authenticate an operator to a role.	X	X	X	
Context - Select an applet or manage logical channels.				X
Get OTP – Obtain a one-time password.		X		X
Lifecycle - Modify the card or applet life cycle status, inclusive of zeroization of all CSPs stored in non-volatile memory.			X	
Logout - Logout all previously authenticated roles (except Secure Messaging)				X
Manage Configuration – Register/unregister applet instances and related information for access control configuration. Set object identifiers associated with applet instances.			X	
Manage Content - Load and install application packages and associated keys and data. Applet Suite (Card Manager); manage applet properties, keys, PINs, pairing codes, secure messaging certificate, and other data associated with the applet.	X	X	X	
Module Info - Read module configuration or status information. Retrieve applet instance properties, public ACR (access control rule) and associated properties. Retrieve applet instance properties, public ACR (access control rule) and associated properties. Retrieve applet instance properties, secure messaging certificate (CVC).	X	X	X	X
Module Reset - Power cycle or reset; includes Power-On Self-Test and zeroization of all CSPs stored in volatile memory.				X
Opacity Secure Messaging - Establish OPACITY-ZKM Secure Messaging				X
PIV Authentication – Authentication of the PIV Application by an external system; requires cardholder consent via PIN verify.		X		
PIV Card Authentication – Authentication of the PIV Card by an external system.				X
PIV Digital Signature – Sign an externally generated hash value.		X		
PIV Info – Read PIV data objects and applet instance properties.		X		X
PIV System Key Services – Unwrap a key provided by the host. The key is not established into or used by the module.		X		
Secure Channel - Establish and use a secure communications channel.			X	
Sign - Sign an externally generated hash value.	X	X		

Table 11 - Applet Services

Service	OS-RNG_STATE	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	ACA-SPAK	ACA-PIN	ACA-PUK	ACA-PC	PKI-GPK	SKI-OTP	PIV-RPAK	PIV-RDSK	PIV-RKDK	PIV-RCAK	SMA-OPRI	SMA-SCFRM	SMA-SENC	SMA-SCMAC	SMA-SRMAC
Authenticate	--	--	--	--	--	--	E	E	--	E	--	--	--	--	--	--	--	--	E	E	E
Context	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Get OTP	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--
Lifecycle	Z	Z	Z	Z	E	E	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	--	--	--	--
Logout	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Manage Configuration	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Manage Content	--	W	W	W	E	E	W Z	W E	W E	W	W GZ	W Z	GZ	GZ	W Z	GZ	G	--	--	--	--
Module Info	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Module Reset	GE W	--	--	--	Z	Z	--	--	--	--	--	--	--	--	--	--	--	Z	Z	Z	Z
Opacity Secure Messaging	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	GE Z	GZ	GZ	GZ
PIV Authentication	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	E	E	E
PIV Card Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	E	E	E
PIV Digital Signature	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	E	E	E
PIV Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	E
PIV System Key Services	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	E	E	E
Secure Channel	E W	E	E	--	GE	GE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Sign	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--

Table 12 - Access to CSPs by 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 Module writes the CSP on import or update.
Z = Zeroize: The Module zeroizes the CSP.
-- = Not accessed by the service.
"E" in the secure channel / secure messaging session key columns indicates where secure channel or secure messaging may be used. "Z" in the Lifecycle row indicates key destruction as a consequence of card termination.

5 Self-test

5.1 Power-on self-test

On power-on or reset, the Module performs self-tests as described in Table 13 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If any self-test fails, the system emits an error code (0x6FXX) and enters the SELF-TEST ERROR state.

Test Target	Description
Firmware Integrity	16 bit Reed-Solomon EDC performed over all code in the cryptographic boundary.
DRBG (Cert. #537)	Performs a fixed input KAT (inclusive of SP 800-90A health monitoring tests).
Triple-DES (Cert. #1727)	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
AES (Cert. #2910)	Performs a decrypt KAT using an AES-128 key in ECB mode.
SP 800-108 KDF (Cert. # 33)	Performs a KAT of SP 800-108 KDF. This self-test is inclusive of AES CMAC (Cert. #2911) and AES encrypt (Cert. #2910) function self-test.
SHA-256 (Cert. #2449)	Performs a fixed input KAT.
RSA CRT (Cert. #1532)	Performs RSA CRT signature KAT using an RSA 2048 bit key.
ECC CDH (KAS Cert. #48)	Primitive "Z" Computation KAT for [SP 800-56A] Section 5.7.1.2 ECC CDH Primitive using the P-521 curve.
ECDSA (Cert. #526);	Performs known answer test using the P-224 curve. This self-test is inclusive of the ECC CDH function self-test.

Table 13 – Power-On Self-Test

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

When an ECC or RSA key pair is generated, the Module performs a pairwise consistency test. If the pairwise consistency test fails, the key is cleared, and a SW_CRYPTO_EXCEPTION exception is thrown. The PKI applet instance must be deleted and re-instantiated to be able to attempt a new key pair generation.

When new firmware is loaded into the Module using the Manage Content service, the Module verifies the integrity of the new firmware (applet) using MAC verification with the SD-SMAC key. Failure to verify the new firmware results in the BAD APDU error state; the Module returns an error specific to the situation (MAC failure).

6 Physical security policy

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module's physical hardness was tested at ambient temperature only.

The Module is intended to be mounted in additional packaging, the plastic card body, covering the back faces of the module. Physical inspection of the epoxied (back) face is typically not practical after packaging.

7 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 require a separate FIPS 140-2 validation.

8 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.

9 Mitigation of Other Attacks Policy

The Module implements defenses against:

- Light attacks: The NXP P60 chip includes sensors to detect light attacks. A hardware attack event triggers the KillCard behavior described below.
- Invasive fault attacks: The NXP P60 chip includes sensors for fault attacks. A hardware attack event triggers the KillCard behavior described below.
- Side-channel attacks (SPA/DPA, timing analysis): The NXP chip implements hardware countermeasures, such as induced clock jitter and address scrambling. 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. For example, a section of sensitive code will check for corresponding flags set by code that could have called the sensitive code. If the flags don't correspond, 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. For example, status of memory erasure is maintained, and on any reset, this activity must be completed before normal use can be resumed.

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

10 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 zeroization service.
- 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.

In addition, the following guidance must be followed to operate the Module within the conditions describes any further rules for using the Module in accordance with the conditions of the FIPS 140-2 validation.

- PIV Applet administrators are required to procedurally enforce usage policy that ensures end user's PIV PIN values meet the conditions as described in [SP80073-4] and that the selected PIN values also meet the FIPS 140-2 security strength of 1/1,000,000.