HID Global
Applets v3.0 on NXP JCOP 3 SecID P60 CS (OSB)

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

Document Version: 1.2
Date: 3/11/2021

Table of Contents

List of Tables

List of Figures

References

Table 1: References

Acronym	Full Specification Name
References used in Approved Algorithms Table	
[38A]	NIST, Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December, 2001
[38B]	NIST, Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May, 2005, updated on June 06 2016
[38F]	NIST, Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December, 2012
[56A]	NIST, Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March, 2007
[56Ar3]	NIST, Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, Revision 3, April, 2018
[56B]	NIST Special Publication 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1, September 2014
[56Crev1]	NIST, Special Publication 800-56C, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, Revision 1, April 2018
[67r2]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Revision 2, November, 2017
[90Ar1]	NIST, Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Revision 1, June, 2015
[108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, FIPS Publication 108, October, 2009
[133r2]	NIST Special Publication SP800-133, *Recommendation for Cryptographic Key Generation*, Revision 2, June, 2020
[180]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March, 2012
[186]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001
[198-1]	NIST, The Keyed-Hash Message Authentication Code (HMAC), July, 2008

Other References	
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[INCITS 504-1]	INCITS, *Information Technology - Generic Identity Command Set - Part 1: Card Application Command Set, Amendment*
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1,* January 2011, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card -- Confidential Card Content Management -- Card Specification 2.2 -- Amendment A*, January 2011 *GlobalPlatform Consortium: GlobalPlatform Card Technology -- Contactless Services -- Card Specification v2.2 -- Amendment C*, July 2014 GlobalPlatform Consortium: GlobalPlatform Card Technology -- Secure Channel Protocol '03' – Card Specification v2.2 – Amendment D, May 2009

Other References	
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated December 03, 2019
[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 7816-6:2016 *Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange* ISO/IEC 7816-8:2016 *Identification cards -- Integrated circuit cards – Part 8: Commands and mechanisms for security operations* ISO/IEC 7816-12:2005 *Identification cards -- Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures* ISO/IEC 7816-15:2016 *Identification cards – Integrated circuit cards – Part 15: Cryptographic Information application*
[ISO 14443]	ISO/IEC 14443-3:2016 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision* ISO/IEC 14443-4:2016 *Identification cards -- Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification, March 15, 2006* *Java Card 2.2.2 Virtual Machine (JCVM) Specification, March 15, 2006* *Java Card 2.2.2 Application Programming Interface, March 2006* *Java Card 3.0.4 Runtime Environment (JCRE) Specification, May 2015* *Java Card 3.0.4 Virtual Machine (JCVM) Specification, May 2015* *Java Card 3.0.4 Application Programming Interface* Published by Oracle
[SP800-73]	*SP 800-73-4, Interfaces for Personal Identity Verification, NIST, May 2015*
[SP800-78]	*SP 800-78-4, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST, May 2015*
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 2, March 2019
[DTR]	NIST, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, January 2011

Acronyms and Definitions

Table 2: Acronyms and Definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
BS	Block Size
CM	Card Manager, see [GlobalPlatform]
CNRNGT	Continuous random Number Generator Test, see [DTR] AS09.42
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	GlobalPlatform
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
KS	Key Size
MDS	Message Digest Size
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
OP	Open Platform (predecessor to GlobalPlatform)
PIN	Personal Identification Number
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis
TPDU	Transaction Protocol Data Unit, see [ISO 7816]

1 Overview

This document defines the Security Policy for the HID Global Applets v3.0 on NXP JCOP 3 SecID P60 CS (OSB) cryptographic module, 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 a Card Manager and the HID Global Applets v3.0.

The HID Global Applets v3.0 is conformant to PIV specification [SP800-73] and validated in the NPIVP program (Cert. #47).

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

Table 3: Security Level of Security Requirements

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

The Module is the physical boundary of the single chip, which provides a Global Platform JavaCard operational environment. The Module is a non-modifiable operational environment under the FIPS140-2 definitions.

1.1 Versions, Configurations and Modes of Operation

Hardware: P6022y VB
Product identifier: J3H145C
OS Firmware: 19790400
Application Firmware: HID Global ActivID Applet Suite v3.0, comprising:

- **ASCLIB:** 3.0.0.36
- **ACA:** 3.0.0.46
- **PIVExt:** 3.0.0.57
- **HMACLib:** 3.0.0.24
- **OATH:** 3.0.0.38 [1]
- **SMAv3 (ZKM) library:** 3.0.0.14 [1]
- **SMAv3:** 3.0.0.36 [1]

Factory configuration: FIPS 140-2-L2.

[1] This applet was tested but it is optional; the related services and CSPs will be annotated with this index.

HID Global ActivID Applet Suite v3.0 can be configured by HID Global with OATH applet or not. The OATH applet provides additional services which are independent of the services provided by the other applet. The module was tested with and without OATH applet.

HID Global ActivID Applet Suite v3.0 can be configured by HID Global with SMAv3 (applet and library) or not. The SMAv3 library provides OPACITY ZKM Secure Messaging protocol establishment service for PIV applet, when PIV Discovery Object is configured with VCI interface. The module was tested with and without SMA v3 applet/library.

After reception of the Module, the Module will be configured with HID Global Credential Management System and the profile of the end-user. To be in approved mode of operation, the profile of the Module shall meet security rule #16 of Section 7 below. At the end of the configuration, the Module state cannot be changed, and the Module will support an Approved mode of operation. The user will be able to know that the Module is configured in Approved mode of operation by sending the command of Table 4 below.

Table 4 - Approved Mode Indicators

Command and associated elements	Expected Response
ACA applet Module Info service (GET PROPERTIES command with tag 24). 80 56 02 00 01 24 00	0x24 0x02 0x***01*** YY, where 0x01 (in bold italics) value indicates the FIPS 140-2 Level 2 Approved mode.

1.2 Hardware and Physical Cryptographic Boundary

The Module is designed to be embedded into plastic card bodies, with a contact plate and contactless antenna connections. The physical form of the Module is depicted in Figure 1 (to scale); the red outline depicts the physical cryptographic boundary, representing the surface of the chip and the bond pads. In production use, the Module is delivered to either vendors or end user customers in various forms:

- As bare die in wafer form for direct chip assembly by wire bonding or flip chip assembly
- Wire bonded and encapsulated by epoxy with additional packaging (e.g., Dual Interface Modules; Contact only Modules; Contactless Modules; SMD packages)

The contactless ports of the module require connection to an antenna. The Module relies on [ISO 7816] and [ISO 14443] card readers as input/output devices.

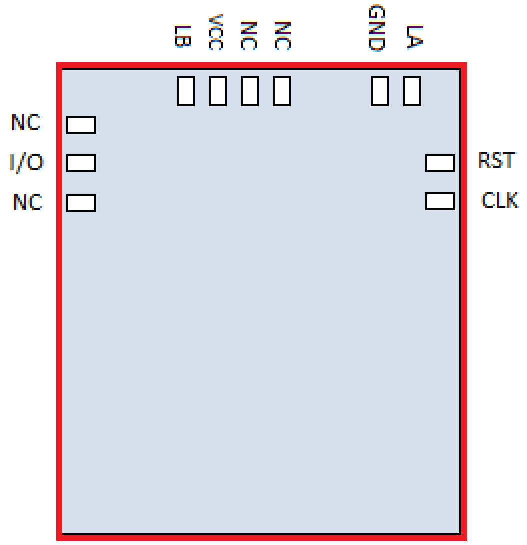

Figure 1: NXP Semiconductors JCOP 3 SecID P60 CS (OSB): Physical Form

Table 5: Ports and Interfaces

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

In the table above, an “X” in the C column indicates the port is active in the Contact mode; an “X” in the D column indicates the port is active in the Dual interface (Contact and contactless) mode.

1.3 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

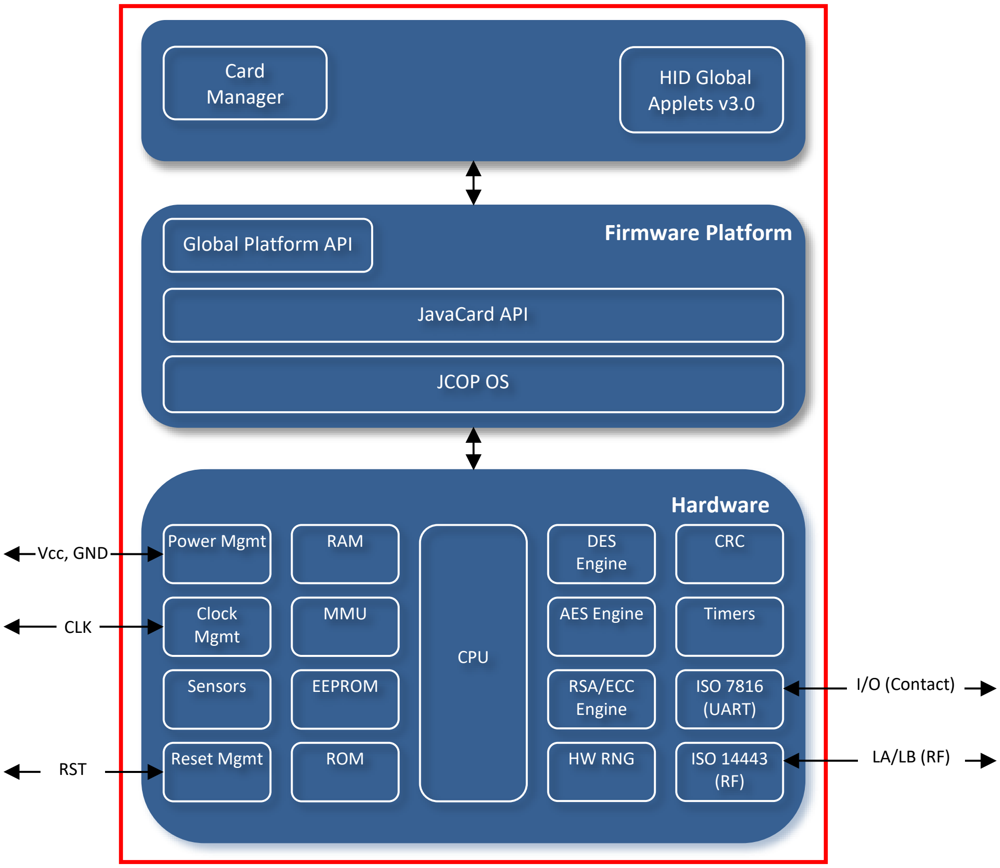

Figure 2: Module Block Diagram

The JavaCard and Global Platform APIs are internal interfaces available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

The HID Crescendo Applets v3.0 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.
- **SMAv3 (ZKM) Library package**[1] - This library implements ECC OnePassDH Key Agreement with Key Confirmation (Key Agreement Role Responder - Key Confirmation Role Provider and Type Unilateral). It is used by SMAv3 applet for OPACITY ZKM Secure Messaging protocol establishment.
- **SMAv3 Applet**[1] – 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.

- **PIVExt Applet** – This Applet implements [SP800-73](both at card-edge and data model levels) and is extended to support additional features on top of native PIV such as support of additional PKI RSA/ECC keys, etc. This applet can be instantiated in PIV EP mode (native PIV features) or in PIV Ext mode (extensions accessible through the 800-73-4 card edge.).
- **HMAC Library package** - This library implements Hash Message Authentication Code. It is used by ACA for HMAC Power-On Self-Test and by OATH applet[1] for authentication codes computation.
- **OATH Applet**[1] – The OATH Applet provides Open Authentication services that can be used by client application / embedded devices like the BLE Token to authenticate against an authentication server like ActivID Authentication Server. These authentication services consist in HMAC-Based One-Time password (HOTP), Time-Based One-Time password (TOTP), OATH Challenge-Response / Digital Signature Algorithm (OCRA)

2 Cryptographic Functionality

The module implements the Approved and Allowed cryptographic functions listed below.

Table 6: Approved Algorithms

CAVP Cert	List	Standard	Mode/Method	Strength[2]	Use
4812	AES	[197], [38A]	CBC, ECB	128, 256 Not Used: 192	Data Encryption/ Decryption
4812	AES CMAC	[197], [38B]	CMAC	128, 256 Not Used: 192	Message Authentication. SP 800-108 KDF
Vendor Affirmed	CKG	[133r2]	§4 Key Pairs for Digital Signature Schemes, generation uses the unmodified DRBG Cert. #1187 output	112, 128, 192	ECDSA and RSA Key Generations
824	CVL ECDH	[56B]	ECC CDH Primitive	P-256, P-384 Not used: P-224, P-521	Shared Secret Computation
C901	CVL RSADP	[56B]	n=2048		PIV system key (non-CSP) decryption
C901	CVL RSASP1	[186]	n=2048		Signature generation primitive (off card hash).
1187	DRBG	[90Ar1]	Hash_DRBG	256	Deterministic Random Bit Generation
890	ECDSA	[186]	P-256, P-384 Not Used: P-224, P-521		ECC Key Generation
			P-256: (SHA-256), P-384: (SHA-384) Not Used: P-224: (SHA-224), P-521: (SHA-512)		Digital Signature Generation
			Not Used: P-192: (SHA-1)[3], P-224: (SHA-224), P-256: (SHA-256), P-384: (SHA-384), P-521: (SHA-512)		Digital Signature Verification implementation is not reachable except for the Self-Test
C399	HMAC	[198-1]	HMAC-SHA-1, HMAC-SHA2-256 HMAC-SHA2-512 with: - KS < BS, KS > BS, KS = BS - λ > 32		OTP Generation
Vendor Affirmed	KAS-SSC	[56Ar3]	ECC DH	P-256, SHA-256 P-384, SHA-384	PIV Secure Messaging Key Agreement Key establishment methodology provides 128 or 192 bits of encryption strength
91	KBKDF	[108]	CTR	128, 256 Not Used: 192	Deriving keys from existing keys
Vendor Affirmed	KDA	[56Crev1]	One-step key-derivation functions option 1	SHA-256, SHA-384	Deriving keys KAS-SSC Shared Secret for Secure Messaging

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

[3] Legacy use only

CAVP Cert	List	Standard	Mode/Method	Strength[2]	Use
4812	KTS	[38F]	AES CBC/AES CMAC	128, 256 Not Used: 192	Meets the SP 800-38F §3.1 ¶3 requirements for symmetric key wrapping, using Cert. #4812 AES CBC and AES CMAC. Key establishment methodology provides 128 or 256 bits of encryption strength.
2086	RSA	[186]	n=2048 Not used: n = 3072		RSA key generation
2053	RSA	[186]	n=2048 SHA-256 Not used: n = 3072; SHA-(224, 384, 512)		Digital signature generation
			Not used: n = 1024[3], 2048, 3072; SHA-(1[4], 224, 256, 384, 512[5])		Digital signature verification implementation is not reachable except for the Self-Test
3299	SHS	[180]	SHA-1, SHA-256, SHA-384, SHA-512 Not used: SHA-224		Message Digest generation
2547	Triple-DES	[67r2]	CBC, ECB	3-Key (112)	This algorithm is implemented but it is never called except for the Self-Test

Table 7: Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	Hardware NDRNG; used as entropy input (384 bits) to the FIPS approved (Cert. #1187) DRBG. The non-deterministic hardware RNG outputs 8 bits per access, buffered by the device driver, which performs the continuous RNG test when a 32-bit value is available.

2.1 Critical Security Parameters and Public Keys

All CSPs used by the Module are described in this section. All usage of these CSPs is described in the services detailed in Section 3.4. In the tables below, the following prefixes are used:

- OS prefix denotes operating system.
- SD prefix denotes a GlobalPlatform Security Domain.
- ACA prefix denotes an ACA Applet CSP or Public Key
- PIV prefix denotes a PIV Applet CSP or Public Key
- SMA[1] prefix denotes an SMA V3 Applet CSP or Public Key
- OATH[1] prefix denotes an OATH Applet CSP or Public Key

Table 8: Critical Security Parameters

[4] This algorithm is Approved for legacy use

[5] The SHA-512 is not available for 1024-bit RSA signature verification

CSP	Description/Usage
	Card Manager
OS-DRBG-EI	384-bit NDRNG entropy input to Hash_DRBG.
OS-DRBG-STATE	880-bit value; the current hash_DRBG state (V, C, reseed_counter).
OS-MKEK	AES-128/192/256 key used to encrypt all secret and private key data stored in NVM.
SD-KENC	AES (128-bit, 192-bit, 256-bit) Master key used to derive SD-SENC.
SD-KMAC	AES (128-bit, 192-bit, 256-bit) Master key used to derive SD-SMAC.
SD-KDEK	AES (128-bit, 192-bit, 256-bit) Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES (128-bit, 192-bit, 256-bit) Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to verify inbound secure channel data integrity.
SD-RMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to generate response secure channel data MAC.
	Applets
ACA-SPAK	AES-128 key used by the ACA applet to authenticate the AA role (0-8 keys). One slot is used for PIV Card Application Administration Key (9B) storage.
ACA-PIN	8 characters string PIN used for local PIN verification
ACA-PUK	8 characters string PIN Unblocking Key used to confirm authorization to unblock a blocked PIN.
PIVX-GPK-Pr	General purpose key with usage determined outside the Module scope. The following key types are supported: RSA 2048, ECC P-256 and ECC P-384 curves.
PIV-AuK-Pr	PIV Card Application Authentication Key (9A): RSA (2048-bit) and ECDSA (P-256, P-384) private key for signature generation
PIV-DSK-Pr	PIV Card Application Digital Signature Key (9C): RSA (2048-bit) and ECDSA (P-256, P-384) private key for signature generation
PIV-KMK-Pr	PIV Card Application Key Management Key (9D): RSA (2048-bit) and ECDSA (P-256, P-384) private key for key establishment schemes realization
PIV-RKMK-Pr	PIV Card Application Key Management Key (82-90): RSA (2048-bit) and ECDSA (P-256, P-384) private key for key establishment schemes realization
PIV-CaK-Pr	PIV Card Application Authentication Key (9E): RSA (2048-bit) and ECDSA (P-256, P-384) private key for signature generation
SMA-OK-Pr[1]	PIV Card Application Opacity Secure Messaging keys (04): C(ipher) S(uite) 2 and CS 7 private components used by *PIV Secure Messaging Key* service.
SMA-SCFRM[1]	PIV Card Application Opacity Secure Messaging Key Confirmation Key: AES-128 key and AES-256 used to compute authentication cryptogram
SMA-SENC[1]	PIV Card Application Opacity Secure Messaging Encryption Session Key: AES-128 and AES-256 key
SMA-SCMAC[1]	PIV Card Application Opacity Secure Messaging Command Authentication Session Key: AES-128 and AES-256 key

CSP	Description/Usage
SMA-SRMAC[1]	PIV Card Application Opacity Secure Messaging Response Authentication Session Key: AES-128 and AES-256 key
OATH-OTP[1]	HMAC Key used by the OATH applet for one-time password generation. The following key lengths are supported: 160 bits, 256 bits and 512 bits

Table 9: Public Keys

Public Key	Description/Usage
	Applets
PIVX-GPK-Pu	General purpose key with usage determined outside the Module scope. The following key types are supported: RSA 2048, ECC P-256 and ECC P-384 curves.
PIV-AuK-Pu	PIV Card Application Authentication Key (9A): RSA (2048-bit) and ECDSA (P-256, P-384) public key for signature verification
PIV-DSK-Pu	PIV Card Application Digital Signature Key (9C): RSA (2048-bit) and ECDSA (P-256, P-384) public key for signature verification
PIV-KMK-Pu	PIV Card Application Key Management Key (9D): RSA (2048-bit) and ECDSA (P-256, P-384) public key for key establishment schemes realization
PIV-RKMK-Pu	PIV Card Application Key Management Key (82-90): RSA (2048-bit) and ECDSA (P-256, P-384) public key for key establishment schemes realization
PIV-CAK-Pu	PIV Card Application Authentication Key (9E): RSA (2048-bit) and ECDSA (P-256, P-384) public key for signature verification
SMA-OK-Pu[1]	PIV Card Application Opacity Secure Messaging keys (04): C(ipher) S(uite) 2 and CS 7 public components used by PIV Secure Messaging Key service.
ACA-PC	8 characters string Pairing Code used to associate a peer device for a virtual contact interface.

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, independent of logical channel usage. Concurrent operators are supported with limited fashion, controlling access to restricted objects and services via the ACA applet access control mechanism.

Table 10 lists all operator roles supported by the Module.

Table 10: Roles Supported by the Module

Role ID	Role Description
CO	Cryptographic Officer – manages Module content and configuration, including issuance and management of Module data via the ISD. Authenticated as described in *Secure Channel Protocol Authentication* below.
AA	Application Administrator - responsible for configuration of the applet suite data. Authenticated as described in *Application Administrator Authentication Method*.
CH	Card Holder (User) – uses the Module for an identity token. Authenticated as described in *Card Holder Authentication Method.*

3.1 Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method is provided by the Secure Channel service (Card Manager or Applets). 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 sends 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 this whole 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 maximum of eighty (80) consecutive failed SCP authentication attempts. The probability that a random attempt will succeed over a one-minute interval is:

- 80/2^128 = 2.4E-37 (MAC||cryptogram, using a 128-bit block for authentication)

3.2 Application Administrator Authentication Method

The Application Administrator Authentication method is provided by Authenticate service. This authentication method decrypts with ACA-SPAK an encrypted 128-bit challenge sent to the module by an off-card entity and compares the resulting challenge to the expected value. The authentication strength for this method depends on the algorithm, key size and challenge size used: the minimum strength key used for this method is AES-128 Key; however, the limiting factor in this authentication method is the 128-bit block size.

The associated probability of false authentication of this authentication methods is:

- 1/(2^128) = 2.9E -39

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/(2^128) = 1.9E -34

3.3 Card Holder Authentication Method

The Card Holder Authentication method is provided by Authenticate service. 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 3.0 does not support the FIPS 201 global PIN option.

The strength of this authentication method depends on both internal and external factors.

The Module supports numeric PIN values coded in ASCII with a length comprises between 6 and 8 bytes. The character space for the first 6 bytes is 10 (the values '30' through '39' are permitted) and in the last two (2) characters is eleven (11) (the values '30' through '39' and 'FF' are permitted). The probability of false authentication of this authentication method is as follows:

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

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

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

3.4 Services

All services implemented by the Module are listed in the tables below. The *ISD Services* are provided by the Card Manager and are available to off card entities. Such services are related to card content management (e.g., applet installation, deletion, card data access or storage) accessed via communication protocols like ISO7816 during the configuration of the module. The *Applets Services* are available to on card entities, i.e., Java Card applets. These services are typically cryptographic services available via the Java Card API.

Table 11: Unauthenticated Services

Service	Description
ISD (OS/Card Manager) Services	
Card Reset	Power cycle or reset the Module. Includes Power-On Self-Test.
Context	Select an applet or manage logical channels.
Info	Read unprivileged data objects, e.g., module configuration or status information.
	Applets Services
Logout	Logout all previously authenticated roles; if establish, the Secure Messaging stay opened.
PIV CA Authentication	PIV Application Card authentication to the client application (INTERNAL AUTHENTICATE).
VCI Establishment[1]	Open a Secure messaging from the Opacity Key Establishment protocol.
Applets Info	Read unprivileged data objects info.
ACA update properties (Unauthenticated)	ACA Update properties: Update Change Pin after first Use flag.

Table 12: Authenticated Services

Service	Description	CO	AA	CH
	ISD (OS/Card Manager) Services			
Secure Channel	Establish and use a secure communications channel.	X		
Lifecycle	Modify the card or applet life cycle status. This service can be used to zeroize the module.	X		
Manage Content	Install application packages and associated keys and data.	X		
Privileged Info	Read module data (privileged data objects, but no CSPs).	X		
	Applets Services			
Applets Secure Channel	Establish and use a secure communications channel.	X		
Applets Lifecycle	Modify the applet life cycle status.	X		
Applets Manage Content	Register/unregister applet instances and related information for access control configuration. Set object identifiers associated with applet instances. Manage applet properties, keys, PINs, pairing codes, secure messaging certificate, and other data associated with the applet.	X	X	
Authenticate	Application Administrator authentication, Card Holder authentication by presenting the PIN.		X	X*
Applets Privileged Info	Read the PIV data content of the single data object being authenticated.			X
CH Authentication Management	Change, unblock the Card Holder PIN of the PIV Applet.	X	X	X*
PIV AU Authentication	PIV Application authentication to the client application (INTERNAL AUTHENTICATE).			X
PIV Digital Signature	Generate RSA/ECDSA signature of an external hash value.			X
PIV Key Establishment	Realize key establishment schemes specified in SP 800-78 (RSA/ECDH).			X
PIVExt Sign	Sign an externally generated hash value (RSA/ECDSA).			X
OATH Authentication[1]	Obtain a One Time Password (HOTP, TOTP), Perform an OCRA challenge Response or Digital Signature[6].			X

*: Means may be sent through Opacity ZKM (Secure Messaging) session in contactless

Table 13 and Table 14 below describe the access to CSPs by service.

Table 13: CSP Accesses within Services of Card Manager, ACA applet, and PIVExt applet

Services	CSPs

[6] The Digital Signature is a HMAC computation; this terminology is defined in RFC 6287.

	OS-DRBG-EI	OS-DRBG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	ACA-SPAK	ACA-PIN	ACA-PUK	PIVX-GPK-Pr	PIV-AuK-Pr	PIV-DSK-Pr	PIV-KMK-Pr	PIV-RKMK-Pr	PIV-CaK-Pr
Unauthenticated	**Card Manager**									**ACA applet**			**PIVExt applet**					
Card Reset	GEZ	GEWZ	--	--	--	--	Z	Z	Z	--	--	--	--	--	--	--	--	--
Context	--	--	--	--	--	--	EZ	EZ	EZ	--	--	--	--	--	--	--	--	--
Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Logout	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV CA Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E
VCI Establishment	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Applets Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
ACA update properties (Unauthenticated)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Authenticated	**Card Manager**									**ACA applet**			**PIV applet**					
Secure Channel and Applets Secure Channel	--	--	--	--	--	--	GE	GE	GE	--	--	--	--	--	--	--	--	--
Lifecycle and Applets Lifecycle	Z	Z	Z	Z	Z	Z	E	E	E	Z	Z	Z	Z	Z	Z	Z	Z	Z
Manage Content and Applets Manage Content	Z	Z	Z	WZ	WZ	WZE	E	E	E	WZ	WZ	WZ	GWZ	GWZ	GWZ	GWZ	GWZ	GWZ
Authenticate	--	--	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--
Privileged Info and Applets Privileged Info	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--
CH Authentication Management	--	--	--	--	--	--	E	E	E	--	WZ	WZ	--	--	--	--	--	--
PIV AU Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--
PIV Digital Signature	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--
PIV Key Establishment	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	--
PIVExt Sign	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--
OATH Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Table 14: CSPs within Services of ZKM and OATH[1] applets, and Public Keys Access within Services

Services	CSPs						Public Key							
	SMA-OK-Pr	SMA-SCFRM	SMA-SENC	SMA-SCMAC	SMA-SRMAC	OATH-OTP	PIVX-GPK-Pu	PIV-AuK-Pu	PIV-DSK-Pu	PIV-KMK-Pu	PIV-RKMK-Pu	PIV-CaK-Pu	SMA-OK-Pu	ACA-PC
Unauthenticated	**ZKM applet**					**OATH**	**PIV applet**						**ZKM**	**ACA**
Card Reset	--	Z	Z	Z	Z	--	--	--	--	--	--	--	--	--
Context	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Logout	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV CA Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--
VCI Establishment	E	GEZ	G	G	G	--	--	--	--	--	--	--	--	E
Applets Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--
ACA update properties (Unauthenticated)	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Authenticated	**ZKM applet**					**OATH**	**PIV applet**						**ZKM**	**ACA**
Secure Channel and Applets Secure Channel	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Lifecycle and Applets Lifecycle	Z	--	--	--	--	Z	--	--	--	--	--	--	--	Z
Manage Content and Applets Manage Content	GZ	--	--	--	--	WZ	GR	GR	GR	GR	GR	GR	GR	WZ
Authenticate	--	--	E	E	E	--	--	--	--	--	--	--	--	--
Privileged Info and Applets Privileged Info	--	--	E	E	E	--	--	--	--	--	--	--	--	--
CH Authentication Management	--	--	E	E	E	--	--	--	--	--	--	--	--	WZ
PIV AU Authentication	--	--	E	E	E	--	--	--	--	--	--	--	--	--
PIV Digital Signature	--	--	E	E	E	--	--	--	--	--	--	--	--	--
PIV Key Establishment	--	--	E	E	E	--	--	--	--	--	--	--	--	--
PIVExt Sign	--	--	--	--	--	--	--	--	--	--	--	--	--	--
OATH Authentication	--	--	--	--	--	E	--	--	--	--	--	--	--	--

- 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. The write access is typically performed after a CSP is imported into the Module or when the module overwrites an existing CSP.
- 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 Table 15 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs other than HMAC fails, the system will not answer any services and the module will have to be restarted/reset. If the HMAC KAT fails, the module will return a SW_CRYPTO_EXCEPTION exception. In this state, the module will return a SW_CRYPTO_EXCEPTION exception to all services and the module will have to be restarted/reset.

Table 15: Power-On Self-Test

Test Target	Description
AES	Performs separate encrypt and decrypt KATs using an AES-128 key in CBC mode. Both the standard and fast implementations of AES encrypt and decrypt are separately tested.
AES CMAC	Performs AES CMAC generate and verify KATs using an AES-128 key.
DRBG	Performs a fixed input KAT and all SP 800-90A health test monitoring functions.
ECC CDH	Performs separate ECDSA signature and verify KATs using the P-256 curve.
ECDSA	Performs ECDSA signature and verify KATs using the P-256 curve; this self-test is inclusive of the ECC CDH self-test.
Firmware Integrity	16-bit CRC performed over all code located in EEPROM. This integrity test is not required or performed for code stored in masked ROM code memory.
HMAC[7]	Performs a fixed input KAT (HMAC SHA-1, inclusive of HMAC SHA-256, -512, per IG 9.4) on the first selection of whatever instance after a power-on.
KBKDF	Performs a fixed input KAT on SP 800-108 AES-CMAC based KBKDF.
RSA	Performs separate RSA signature and verify KATs using an RSA 2048-bit key.
SHA-1	Performs a fixed input KAT.
SHA-256	Performs a fixed input KAT (inclusive of SHA-224, per IG 9.4).
SHA-512	Performs a fixed input KAT (inclusive of SHA-384, per IG 9.4).
Triple-DES	Performs encrypt and decrypt KATs using 3-Key Triple-DES in CBC mode.

4.2 Conditional Self-Tests

The Module performs the conditional self-tests as described in Table 16 below. If one of the conditional self-tests fails, the system will not answer any services and the module will have to be restarted/reset.

Table 16: Conditional Self-Tests

Test Target	Description
DRBG CRNGT	On every call to the DRBG, the Module performs the AS09.42 continuous RNG test to assure that the output is different than the previous value.
Generate PCT	Pairwise consistency test performed when an asymmetric key pair is generated for RSA or ECC.

[7] POST HMAC is performed when OATH applet is loaded only.

Test Target	Description
NDRNG CRNGT	AS09.42 continuous RNG test performed on each 32 bits access from the NDRNG (buffered by the driver) to assure that the output is different than the previous value.
Signature PCT	Pairwise consistency test performed when a signature is generated for RSA or ECDSA.

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 uses standard passivation techniques and is protected by active shielding (a grid of top metal layer wires with tamper response). A tamper event detected by the active shield places the Module permanently into the *Tamper is detected* error state.

Hardness Testing was conducted at three (3) different temperatures; at nominal temperature (20^{o} C, 68^{o} F), at high temperature (120^{o} C, 248^{o} F), and at low temperature (-40^{o} C, -40^{o} F).

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

6 Mitigation of Other Attacks Policy

The module is protected against SPA, DPA, Timing Analysis and Fault Induction using a combination of firmware and hardware countermeasures. Protection features include detection of out-of-range supply voltages, frequencies or temperatures, and detection of illegal address or instruction. All cryptographic computations and sensitive operations such as PIN comparison provided by the module are designed to be resistant to timing and power analysis. Sensitive operations are performed in constant time, regardless of the execution context (parameters, keys, etc.), owing to a combination of hardware and firmware features.

7 Security Rules and Guidance

The Module implementation also enforces the following security rules:

1. The Module provides three distinct operator roles: Cryptographic Officer, Application Administrator, and the Card Holder (User).
2. The Module does not support a maintenance interface or role.
3. The Module provides identity-based authentication.
4. The Module clears previous authentications on power cycle.
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. The Module does not output CSPs (plaintext or encrypted).
8. The Module does not support manual key entry.
9. The Module does not output intermediate key values.
10. No additional interface or service is implemented by the Module which would provide access to CSPs.
11. Data output is inhibited during key generation, self-tests, zeroization, and error states.
12. There are no restrictions on which CSPs are zeroized by the zeroization service.
13. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
14. The Module does not provide bypass services

15. If the ACA applet is set to “PIN Numeric Only”, then the applet verifies the new PIN is numeric only.

The following rules are imposed by the Vendor:

16. FIPS Level 2 profiles shall be configured with an ACA applet with “PIN Numeric Only” configuration, with a Minimum / Maximum PIN Length set from 6 to 8. This ensures end-user’s PIV PIN value meets the conditions as described in [SP800 73] and that the selected PIN values also meet the [FIPS 140 2] probability of false authentication of 1 in 1,000,000.