HID Global and Gemalto

HID Global ActivID Applet Suite v2.7.4 on Gemalto TOPDLV2.1

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 2.0

Date: April 8, 2021

Table of Contents

Table of Tables

Table of Figures

References

Ref	Full Specification Name (*References used in Table 6 Approved Algorithms)*
[38A]	NIST Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December 2001
[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 Rev. 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013
[56B]	NIST Special Publication 800-56B Rev. 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, September 2014
[67]	NIST Special Publication 800-67 Rev. 1, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, January 2012
[90A]	NIST Special Publication 800-90A Rev. 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2015
[108]	NIST Special Publication 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, October 2009
[133]	NIST Special Publication SP800-133, Recommendation for Cryptographic Key Generation, December 2012
[180]	NIST FIPS Publication 180-4, *Secure Hash Standard*, August 2015
[186]	NIST FIPS Publication 186-4, *Digital Signature Standard (DSS)*, July 2013
[197]	NIST FIPS Publication 197, Advanced Encryption Standard (AES), November 26, 2001

Ref	Full Specification Name (*Other References*)
[140]	NIST FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001
[504]	*INCITS 504-1, Information Technology - Generic Identity Command Set - Part 1: Card Application Command Set, Amendment*
[73]	*NIST , Interface for Personal Identity Verification (Revised Draft)*
[78]	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification (Revised Draft)*
[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*
[GP]	*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 10 May 2017.
[JC]	*Java Card 2.2_01 Runtime Environment (JCRE) Specification* *Java Card 2.2_01 Virtual Machine (JCVM) Specification* *Java Card 2.2_01 Application Programming Interface* Published by Sun Microsystems, September 2002
[RSA]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002

Table 1 – References

Acronyms and definitions

Acronym	Definition
ACA	Access Control Applet
API	Application Programming Interface
ATR	Answer To Reset
CM	Card Manager, see [GP]
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
PIV	Personal Identity Verification: FIPS 201-2, [73], [78]
PKI	Public Key Infrastructure
PUK	Pin Unblocking Key
RSA	Rivest Shamir and Adelman
SMA	Secure Messaging Anonymous
TPDU	Transaction Protocol Data Unit, see [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 Gemalto TOPDLV2.1 Platform 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 conformant to PIV specification [73] and validated in the NPIVP program (Cert. #42). 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	3
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 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: NXP P60D144P VA (MPH149)
OS Firmware: Gemalto TOPDLV2.1 (Filter04)
Application Firmware: HID Global ActivID Applet Suite v2.7.4, comprising:

- **ASCLIB:** 2.7.4.10
- **ACA:** 2.7.4.10
- **GC/PKI/SKI:** 2.7.4.39
- **PIV EP Wrapper:** 2.7.4.39
- **SMAv3 (ZKM) library:** 2.7.4.12
- **SMAv3:** 2.7.4.11

The Module provides only a FIPS 140-2 Approved mode, as shown in Table 4 below. The Module is provided in the packages in Figure 1 below.

Table 4 - Approved Mode Indicators

Command and associated elements	Expected Response
Card Manager Module Info Service (GET DATA tag 0103).	0xB0 0x84 0x49 0x53 0x81, where the high order bit of the 5th byte (1000 0001 - left most bit) indicates the platform FIPS 140-2 Approved mode.
ACA applet Module Info service (GET PROPERTIES command with tag 24).	0x24 0x02 ***01*** YY, where the 0x01 (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 plastic card bodies, with a contact plate and contactless antenna connections. The physical form of the Module is depicted in Figure 1. The red outline depicts the physical cryptographic boundary, representing the surface and edges of the chip and the bond pads. The cross-hatching indicates the presence of the hard opaque outer layer shielding. In production use, the Module is wire-bonded to a frame connected to a contact plate (pads CLK, RST, VDD, I/O and VSS) and to an RF antenna (pads LA and LB), enclosed in epoxy and mounted in a card body. The LA and LB bond pads require connection to an antenna.

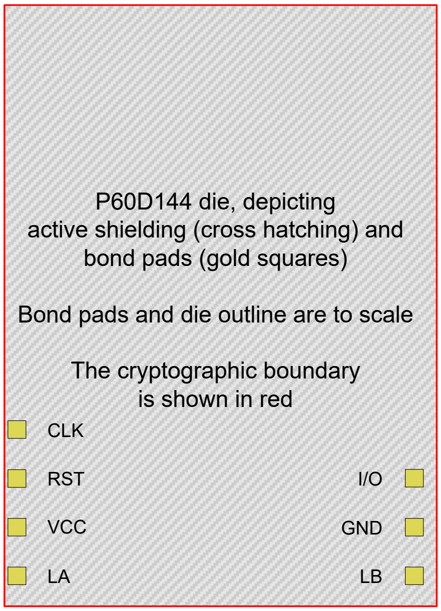
P60D144 die, depicting
active shielding (cross hatching) and
bond pads (gold squares)
Bond pads and die outline are to scale
The cryptographic boundary
is shown in red
CLK
RST
I/O
VCC
GND
LA
LB

Figure 1 – Physical Form and Cryptographic Boundary

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

Table 5 – Ports and Interfaces

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 (contact) and ISO 14443 (contactless) protocols.

2.1 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

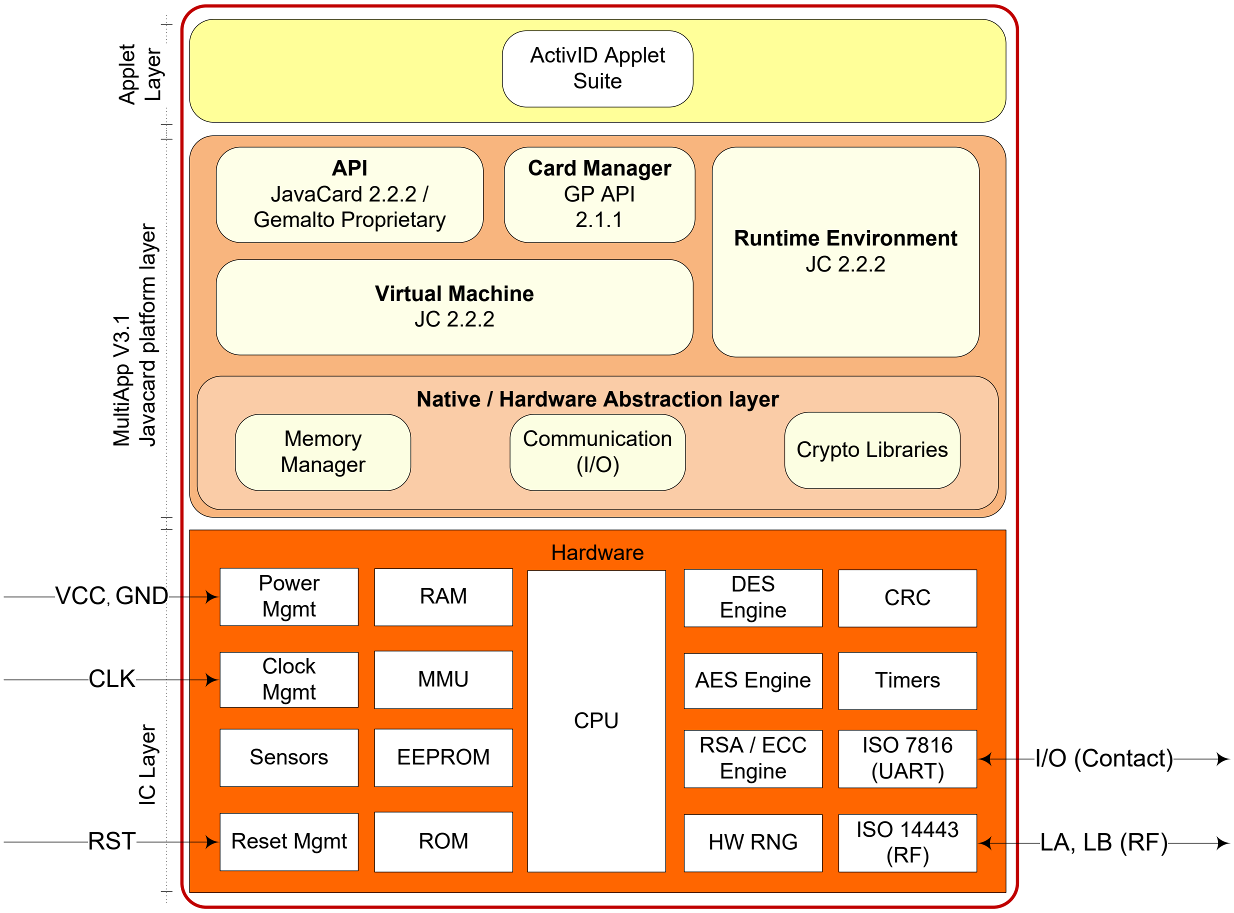

Figure 2 - Module Block Diagram

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). The *Cryptography Libraries* implement the algorithms listed in Section 2. The *Javacard Runtime Environment* implements the dispatcher, registry, loader, and logical channel functionalities. The *Virtual Machine* implements the byte code interpreter, firewall, exception management and byte code optimizer functionalities.

The *Card Manager* is the card administration entity, allowing authorized users to manage the card content, keys, and life cycle states. The Card Manager behaves similarly to an applet, but is properly represented as a constituent of the platform. The *Memory Manager* implements functions such as memory access, allocation, deletion and garbage collection.

The *Communication* handler implements the ISO 7816 and ISO 14443 communications protocols in contactless mode and dual mode.

Applets, such as the ActivID Applet Suite, access module functionalities via internal API entry points that are not exposed to external entities. External devices have access to CM services by sending APDU commands.

The HID Global ActivID Applet Suite 2.7.4 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 (ZKM) Library package** - 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** – This applet implements the OPACITY ZKM Secure Messaging protocol based on [504], as specified by [73]. 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 [73] (both at card-edge and data model levels). This Applet is a wrapper on top of the ActivID Applet Suite 2.7.4 (ASCLIB, ACA, GC/PKI/SKI and SMAv3/Lib 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 6 and Table 7 below. Items in curly brackets { } were CAVP validated but are not used by the module.

CAVP Cert	Algorithm List	Standard	Mode/ Method	Strength[1]	Use
3543	AES	[197], [38A]	CBC, ECB	128, {192}, 256	Data Encryption/ Decryption.
3543	AES	[197], [38A]	CMAC	128, {192, 256}	SP 800-108 KDF, PIV secure messaging
Vendor Affirmed	CKG	[133]	N/A		Key Generation
597	CVL	[56A]	ECC CDH Primitive	{P-224}, P-256, {P-384, P-521}	PIV system secret (non-CSP) computation
815	CVL	[186]	RSASP1 RSA signature generation primitive, 2048-bit modulus.		Signature generation primitive (off card hash).
834	CVL	[56B]	RSADP RSA key decryption primitive, 2048-bit modulus.		PIV system key (non-CSP) decryption.
900	DRBG	[90A]	CTR	128	Deterministic Random Bit Generation
721	ECDSA	[186]		P-256: (SHA-224, 256) {P-224: (SHA-224) P-384: (SHA-224, 256, 384) P-521: (SHA-224, 256, 384, 512) P-192: (SHA- 1)}	Digital Signature Generation, Verification and ECC Key Generation.
137	KAS	[56A]	ECC DH	P-256, SHA-256	PIV secure messaging key agreement
85	KBKDF	[108]	AES CMAC	128, 256, {192}	Symmetric key derivation
3543	KTS	[38F]	AES, CMAC	128, {192, 256}	SP 800-38F §3.1 ¶3 Key transport
1823	RSA	[186]	KeyGen, SigGen and SigVer (2048-bit modulus) with SHA-256, PKCS#1 {See footnote [2]}		RSA key generation, digital signature generation and verification.
2921	SHS	[180]	SHA-1, {SHA-224}, SHA-256, {SHA-384, SHA-512}		Message Digest. SHA-1 is used only to verify configuration data integrity.
1984	Triple-DES	[67]	TCBC, TECB	192	Data Encryption / Decryption

Table 6 –Approved Cryptographic Functions

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

[2] All other modes, methods and strengths listed on this cert are not used by this module

Algorithm	Description
NDRNG	Hardware TRNG, used only to provide entropy input (128 bits) to the Approved DRBG. Note: This entropy source is provided by Gemalto’s TOPDLv2.1 Platform

Table 7 – Non-Approved but Allowed Cryptographic Functions

RSA Cert. #1822 was also tested for the Gemalto TOPDLv2.1 Platform, but is not used by this module.

3.1 Critical Security Parameters

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

Key	Description / Usage
OS-RNG_EI	Entropy input used to instantiate the [SP800-90A] DRBG implementation.
OS-RNG_STATE	The current RNG state secret values (key and V).
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 Encapsulation 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 ephemeral public key, provided by the OPACITY host.

Table 9 – Public Keys

The PIV specifications [73] and [78] 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 ACA 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 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 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 (MAC||cryptogram, 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 2.7.4 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 eight (8) characters of the ACA-PIN or ACA-PUK value, and does not limit the character space. Based on this, the probability of false authentication of this authentication method is as follows:

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

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/(256^8) = 8.1E-19

Once the 15 failed authentication attempts are reached, the PIN is blocked; the Card Holder authenticated services will not be available. Only the Application Administrator would be able to unblock the PIN.

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.			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), secure messaging certificate (CVC), and associated properties.	X	X	X	X
Module Reset - Power cycle or reset; includes Power-On Self-Test.				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

Services	CSPs																						Public keys						
	OS-RNG_EI	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	PKI-RGPKPUB	PIV-RPAKPUB	PIV-RDSKPUB	PIV-RKDKPUB	PIV-RCAKPUB	SMA-CVC	SMA-HPUB
Authenticate	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--
Context	--	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Get OTP	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Lifecycle	Z	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	WZ	WE	WE	W	W GZ	WZ	GZ	GZ	WZ	GZ	G	--	--	--	--	W	W	W	W	W	W	--
Module Info	--	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Module Reset	GE W	GE W	--	--	--	Z	Z	--	--	--	--	--	--	--	--	--	--	--	Z	Z	Z	Z	--	--	--	--	--	--	--
Opacity Secure Messaging	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	GE Z	GZ	GZ	GZ	--	--	--	--	--	R	WE
PIV Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	E	E	E	--	R	--	--	--	--	--
PIV Card Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	E	E	E	--	--	--	--	R	--	--
PIV Digital Signature	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	E	E	E	--	--	R	--	--	--	--
PIV Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--
PIV System Key Services	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	E	E	E	--	--	--	R	--	--	--
Secure Channel	EW	EW	E	E	--	GE	GE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Sign	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	R	--	--	--	--	--	--

Table 12 - Access to CSPs and public key 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 described in Table 13. All KATs must be completed successfully prior to any other use of cryptography by the *Module*. If one of the KATs fails, the *Module* enters the *Card Is Mute* error state.

Test Target	Description
FW Integrity	16 bit CRC performed over all code located in EEPROM.
DRBG	Performs a fixed input KAT (SP 800-90A health monitoring tests).
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
AES	Performs a decrypt KAT using an AES-128 key in ECB mode.
AES CMAC	Performs an AES-CMAC Generate KAT using an AES 128 key. Note that AES-CMAC Verify is identical to a Generate KAT (perform Generate then compare to the input) hence a single KAT verifies both functions.
RSA CRT	Performs RSA CRT signature KAT using an RSA 2048 bit key. Inclusive of RSASP1, RSADP test (all 3 are the same implementation).
ECDSA	Performs separate ECDSA signature and verification KATs using P-224.
ECC CDH	Primitive "Z" Computation KAT for [SP 800-56A] Section 5.7.1.2 ECC CDH Primitive using the P-224 curve.
SHA-1, SHA-2	Performs separate KATs for SHA-1, SHA-256, and SHA-512

Table 13 – Power-On Self-Test

5.2 Conditional self-tests

On every call to the [90A] CTR DBRG, the Module performs a stuck fault test to assure that the output is different than the previous value.

When RSA or ECDSA key pair is generated, 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 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 modules depicted in Figure 1. 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 mechanism which is part of the Manage Content service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this Module is out of the scope of this validation and 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:

- Fault attacks
- Side channel analysis (Timing Analysis, SPA/DPA, Simple/Differential Electromagnetic Analysis)
- Probing attacks
- Card tearing

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.
- If the ACA applet is set to "PIN Numeric Only", then the applet verifies the new PIN is numeric only. In this scenario, PIV Applet administrators are required to procedurally enforce the PIN retry count to be less than 10.
- The same Triple-DES key shall not be used to perform more than 2^{28} block encryptions.

In addition, the guidance below 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 [140] validation.

- If the ACA applet is not set to "PIN Numeric Only ", the PIV applet always checks all 8 bytes and does not restrict character space in PIN values.

- However, an external system may impose rules which restrict character space or include padding schemes. PIV Applet administrators are required to procedurally enforce usage policy that ensures end users' PIV PIN values meet the conditions as described in [73] and that the selected PIN values also meet the [140] probability of false authentication. To ensure that the card application forces the PIN to be at least six digits long, the CO needs to do the following steps:
  1. Create a card policy based on the profile associated to the Gemalto TOP DL 2.1 with ActivID Applet 2.7.4
  2. The policy contains an application called PIN, click on "Configure" to define the details
  3. The default minimum PIN length is 6, verify that this is the case or increase it to a longer value if desired
  4. Save the changes in the PIN application
  5. Continue the configuration of the PKI applications in the cards to define the certificates to be loaded/updated
  6. Save the changes to the card policy in CMS.

  Thus, if the ACA applet is set to "PIN Numeric Only ", the PIN shall be at least 6 bytes long; the probability that a random attempt will succeed will be $1/10^6$ (= 1/1,000,000). Furthermore, in such cases, the maximum count of failed authentication shall be set to a value lower than 10 such that the probability that a random attempt will succeed in a one-minute period will be lower than $1/10^5$ (= 1/100,000).