HID Global ActivID Applet Suite v2.7.5 and v2.7.6 on Giesecke & Devrient Sm@rtCafé Expert 7.0

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Version: 1.7

Date: November 1, 2022

Table of Contents

References 3
Acronyms and definitions 4
1 Introduction 5
1.1 Versions, Configurations and Modes of operation 6
2 Hardware and Physical Cryptographic Boundary 6
2.1 Firmware and Logical Cryptographic Boundary 7
3 Cryptographic functionality 8
3.1 Critical Security Parameters 9
3.2 Public keys 10
4 Roles, authentication and services 10
4.1 Secure Channel Protocol Authentication 11
4.2 Secret Value Authentication 11
4.3 Symmetric Cryptographic Authentication 11
4.4 Services 12
5 Self-test 14
5.1 Power-on self-test 14
5.2 Conditional self-tests 14
6 Physical security policy 15
7 Operational environment 15
8 Electromagnetic interference and compatibility (EMI/EMC) 15
9 Mitigation of Other Attacks Policy 15
9.1 Physical Attacks 15
9.2 Side-channel attacks (SPA/DPA and timing analysis) 15
9.3 Differential fault analysis (DFA) 16
9.4 Physically induced faults (laser, light, clock glitching) 16
10 Security Rules and Guidance 16

Table of Tables

Table 1 – References 4
Table 2 – Acronyms and Definitions 4
Table 3 – Security Level of Security Requirements 5
Table 4 – Approved Mode Indicators 6
Table 5 – Ports and Interfaces 7
Table 6 – Approved Cryptographic Functions 9
Table 7 – Non-Approved but Allowed Cryptographic Functions 9
Table 8 – Non-Approved Cryptographic Functions 9
Table 9 – Critical Security Parameters 10
Table 10 – Public Keys 10
Table 11 – Roles 10

Table 12 – Applet Services (Approved Mode) 12
Table 13 – Applet Services (Non-Approved Mode) 12
Table 14 – Access to Public Keys and CSPs by services 13
Table 15 - Power-On Self-Test 14

Table of Figures

Figure 1 – P-M8.4-8-3 front and back (left); S-COM6.8 front and back (right) 6
Figure 2 – Module Block Diagram 7

References

Acronym	Full Specification Name
[FIPS 140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[FIPS 197]	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 14 March 2022.
[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]	*Javacard 3.0.4 Runtime Environment (JCRE) Specification* *Javacard 3.0.4 Virtual Machine (JCVM Specification* *Javacard 3.0.4 Application Programming Interface* *Published by Sun Microsystems,* August 2011
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[SP800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[SP800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[SP800-56B]	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, September 2014*
[SP800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011

Acronym	Full Specification Name
[SP800-73-4]	*NIST, Interface for Personal Identity Verification (Revised Draft),* February 2016
[SP800-78-4]	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* May 2015.
[SP800-90Ar1]	NIST Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators,* Revision 1, June 2015.
[SP800-108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011

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
G&D	Giesecke and Devrient
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, [SP800-73-4], [SP800-78-4]
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 Giesecke & Devrient Sm@rtCafé Expert 7.0 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 [SP800-73-4], validated in the NPIVP program (Cert. #40). 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 bound to the Cert. # 2327 Giesecke and Devrient Sm@rtCafé Expert 7.0 module, which provides a Global Platform JavaCard operational environment. The Cert. #2327 module included a Demonstration Applet to demonstrate the operation of validated algorithms.

In this Module:

- The hardware and operating system are unchanged from Cert. #2327
- The ActivID Applet Suite replaces the Demonstration Applet. 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 two of the six possible packaging options represented in Cert. #2327: the dual interface packages.
- In accordance with NPIVP [SP800-78-4] requirements, the RSA implementation has been tested for the RSADP and RSASP1 primitives. Note that the RSADP and RSASP1 are subsets of the RSA functionality; the PIV program requires CAVP testing of the primitives for requirements traceability.
- The PIV applet has been tested for NPIVP conformance.

1.1 Versions, Configurations and Modes of Operation

Hardware: SLE78CLFX4000P(M) M7892

OS Firmware: Sm@rtCafé Expert 7.0

Application Firmware: HID Global ActivID Applet Suite 2.7.5 and 2.7.6, comprising:

- **ASCLIB: 2.7.4.10**
- **ACA: 2.7.4.10**
- **GC/PKI/SKI: 2.7.4.11 / 2.7.6.1**
- **PIV EP Wrapper: 2.7.5.3 / 2.7.6.1**
- **SMAv3 (ZKM) library: 2.7.4.12**
- **SMAv3: 2.7.4.11**

The Module provides a FIPS 140-2 Approved mode, which must be maintained by adhering to the procedural controls outlined in Section 10. The platform and the ActivID Applet Suite provide indicators of the Approved mode but must be used in conjunction with the administrative guidance set forth in Section 10. The Module is provided in the packages in Figure 1 below.

Command and associated elements	Expected Response
Power-cycle or reset the Module to obtain ATR value.	0x46 ('F') in Historical Byte 9 indicates the 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.

Table 4 – Approved Mode Indicators

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 forms of the Module are depicted in Figure 1; the cryptographic boundary is the surface and edges of the packages (contact plate on the top side; epoxy, antenna connects (M8.4-8-3) and inductive coil (S-COM6.8) on the bottom side).

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.

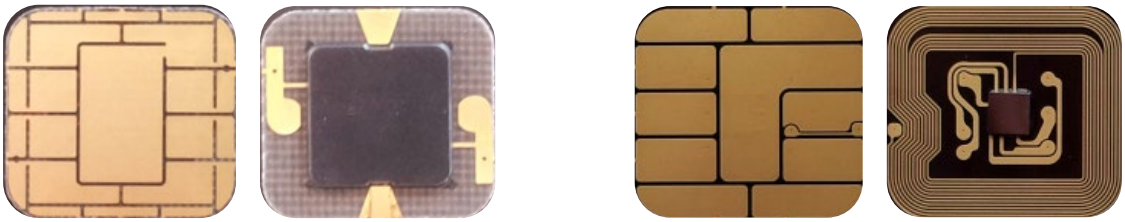

Figure 1 – P-M8.4-8-3 Front and Back (Left); S-COM6.8 Front and Back (Right)

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

Table 5 – Ports and Interfaces

2.1 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

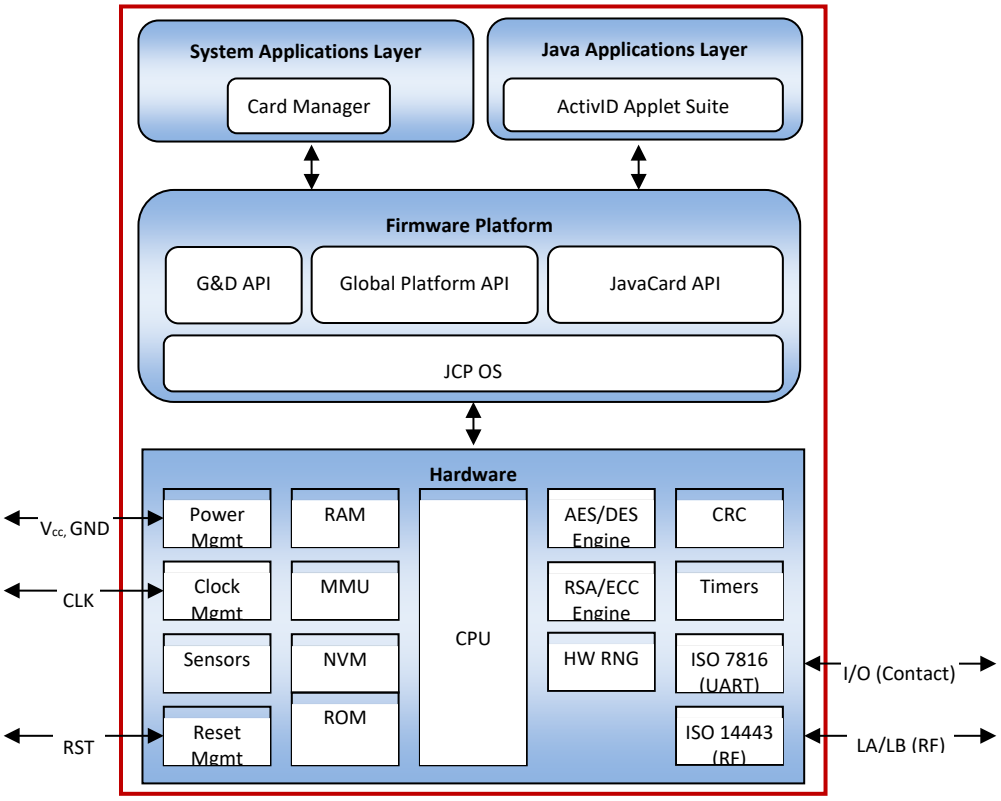

Figure 2 – Module Block Diagram

The JavaCard, GlobalPlatform and G&D 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 2.7.5 and 2.7.6 comprise:

- **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 [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 2.7.5 and 2.7.6 (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/Lib applets and libraries 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, Non-Approved but Allowed, and Non-Approved cryptographic functions listed in Table 6, Table 7 and Table 8 below.

Algorithm	Description	Cert #
DRBG	[SP 800-90A] AES-256 CTR_DRBG. Does not support prediction resistance.	455
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The Module supports 3-Key encrypt and decrypt in CBC or ECB modes.	1637
AES	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports AES-128 keys, and ECB and CBC modes.	2721
AES CMAC	[SP800-38B] AES CMAC. The Module supports AES-128 keys.	2720
KDF	[SP 800-108] CMAC-based KDF with AES-128.	18
SHA-1, SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms; SHA-1, SHA-256. SHA-1 is used only to verify integrity of the Module configuration table.	2290 2289

Algorithm	Description	Cert #
RSA CRT	[FIPS 186-4] RSA key generation and signature generation. The Module supports 2048-bit RSA keys.	1507
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-224, P-256, P-384, P-521 curves for key pair generation, signature and signature verification.	476
CVL	RSA signature generation primitive (RSASP1) using off card hash.	1192
CVL	[SP 800-56B] RSA decryption primitive	1193
KTS	[SP 800-38F] §3.1 ¶3 Key transport	AES 2720, AES 2721

Table 6 – Approved Cryptographic Functions

Algorithm	Description
NDRNG	Hardware TRNG, used only to provide entropy input (488 bits) to the Approved DRBG.

Table 7 – Non-Approved but Allowed Cryptographic Functions

Cert #	Algorithm	Standard	Mode/Method	Strength[1]	Use
177	ECC CDH (CVL)	[56A]	ECC CDH Primitive	{P-224}, P-256, {P-384, P-521}	PIV system secret (non-CSP) computation
91	KAS	[56A]	ECC DH	P-256, SHA-256	PIV secure messaging key agreement

Table 8 – Non-Approved 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.

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

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.

Table 9 – 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

Table 10 – 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.

4 Roles, Authentication and Services

Table 11 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 11 – 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 2.7.5 and 2.7.6 do 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 [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 12 (Approved Mode) and Table 13 (Non-Approved mode) below. The NR column in the tables indicate 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) 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.				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 12 – Applet Services (Approved Mode)

Service	Role			NR
	AA	CH	CO	
Opacity Secure Messaging - Establish OPACITY-ZKM Secure Messaging				X

Table 13 – Applet Services (Non-Approved Mode)

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
Authenticate	--	--	--	--	--	--	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
Logout	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Manage Configuration	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--
Manage Content	--	W	W	W	E	E	WZ	WE	WE	W	WGZ	WZ	GZ	GZ	WZ	GZ
Module Info	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--
Module Reset	GEW	--	--	--	Z	Z	--	--	--	--	--	--	--	--	--	--
PIV Authentication	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--
PIV Card Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E
PIV Digital Signature	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--
PIV Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV System Key Services	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--
Secure Channel	EW	E	E	--	GE	GE	--	--	--	--	--	--	--	--	--	--
Sign	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--

Table 14 – Access to Public Keys and 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-Tests

5.1 Power-on Self-Tests

On power-on or reset, the Module performs self-tests as described in Table 15 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the system emits an error code (0x6666) 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. #455)	Performs a fixed input KAT (SP 800-90A health monitoring tests).
Triple-DES (Cert. #1637)	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
AES (Cert. #2721)	Performs a decrypt KAT using an AES-128 key in ECB mode.
SP 800-108 KDF (Cert. # 18)	Performs a KAT of SP 800-108 KDF. This self-test is inclusive of AES CMAC and AES encrypt function self-test.
SHA-1 (Cert. #2290)	Performs a fixed input KAT.
SHA-256 (Cert. #2289)	Performs a fixed input KAT.
RSA CRT (Cert. #1507)	Performs RSA CRT signature KAT using an RSA 2048 bit key. Inclusive of RSASP1, RSADP test (all 3 are the same implementation).
ECC CDH (Cert. #177)	Primitive "Z" Computation KAT for [SP 800-56A] Section 5.7.1.2 ECC CDH Primitive using the P-521 curve.
ECDSA (Cert. #476)	Performs pairwise consistency test using the P-521 curve.

Table 15 – Power-On Self-Tests

5.2 Conditional Self-Tests

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. If the continuous RNG test fails, the Module enters the SELF-TEST ERROR state. The TRNG hardware includes a continuous comparison test, such that each word formed is compared to the previous value; a duplicate value is discarded, and the TRNG status indicates not ready.

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 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 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:

- Physical attacks
- Side-channel attacks (SPA/DPA and timing analysis)
- Differential fault analysis (DFA)
- Physically induced faults (laser, light, clock glitching)

9.1 Physical Attacks

This kind of attack is directed against the IC and is often independent of the embedded software (i.e., it could be applied to any embedded software and is independent of software countermeasures).

This module applies countermeasures against physical attacks, implemented on the chip hardware. Examples for mitigation of physical attacks are e.g., sensors to avoid exposure of e.g., light, high/low clock frequency, glitches, or high/low voltage. These measures are part of the hardware. In addition, the chip hardware applies also countermeasures against overcoming sensors and filters, e.g., deactivating or avoiding the different types of sensors that an IC may use to monitor the environmental conditions and to protect itself from conditions that would threaten normal operation.

9.2 Side-Channel Attacks (SPA/DPA and Timing Analysis)

In this type of attack an attacker uses power analysis to extract the secret key from power consumption traces taken during the execution of the crypto algorithm itself. The same can be achieved by using other information leaking with the analysis of time consumption in the calculation of crypto operations.

Countermeasures are implemented in software and hardware. The module uses the countermeasures of the crypto coprocessor which uses e.g., randomized and hiding methods of the key material and calculated (intermediate) results applied in the crypto operation, uses a noise generator for CPU and crypto unit, defines constant timing function for coprocessors and applies data and register masking.

Additionally, software countermeasures against timing attacks and SPA/DPA attacks are e.g., transient data arrays in RAM (clear on reset, clear on applet selection), mechanisms for sensitive data areas (creation,

access and clearing), data manipulation hiding, constant time code execution, randomized algorithm execution, randomized data initialization, erasure and comparison.

9.3 Differential Fault Analysis (DFA)

DFA can break cryptographic key systems, allowing retrieval of AES, RSA and ECC keys for example, by running the device under unusual physical circumstances. The attacker needs to inject an error at the right time and location to obtain exploitable erroneous cryptographic outputs.

The module uses and implements several countermeasures against DFA. The chip hardware controls and checks the physical circumstances by the chip hardware (sensors, filters, light detection) and detects data errors on the bus system in the hardware (bus controls, etc.). Additional measures are e.g., logical countermeasures like integrity checking, masking of data, active metal shield (complex implementation), frequency detection, voltage detection, temperature detection, constant timing for coprocessors, illegal address, and instruction detector.

The error detection in software are e.g., multiple (crypto) operations, secure data storage, secure data comparison, checksums and checksum management, flow control, timing control etc.

9.4 Physically Induced Faults (Laser, Light, Clock Glitching)

These type of faults are like the Physical Attacks, directed to the IC and independent of the embedded software. As mentioned in the Physical Attacks section above, the module implements in the chip hardware mitigations including sensors to avoid exposure to light, laser, high/low clock frequency, glitching or invalid voltage ranges.

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.
- Random seeds for asymmetric key generation are unmodified outputs from the DRBG.
- The user must ensure that the maximum number of encryptions operations performed with the same Triple-DES key does not exceed 2^16.

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 FIPS 140-2 validation.

- 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 user's PIV PIN values meet the conditions as described in [SP800-73-4] and that the selected PIN values also meet the FIPS 140-2 probability of false authentication of 1/1,000,000.
- Per [SP800-131], the KAS (Elliptic Curve Diffie-Hellman) functionality shall not be used in the Approved mode of operation; this includes all Opacity ZKM Secure Messaging services listed in Table 13, as provided by the SMA3v3 Library Package and SMAv3 Applet listed in Section 1.1.