Taglio
Taglio PIV Applet v2.1 on NXP JCOP 3 SecID P60 CS (OSB)

FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.0
Date: 8/18/2021

Table of Contents

List of Tables

List of Figures

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
[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
[56B]	NIST Special Publication 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1, September 2014
[67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July, 2011
[90A]	NIST, Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January, 2012
[108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, FIPS Publication 108, October, 2009
[133]	NIST, Special Publication 800-133, *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

Other References	
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS 201-2]	NIST, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.3,* October 2015, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card -- Confidential Card Content Management -- Card Specification 2.3 -- Amendment A*, November 2015 *GlobalPlatform Consortium: GlobalPlatform Card Technology -- Contactless Services -- Card Specification v2.3 -- Amendment C*, December 2015 GlobalPlatform Consortium: GlobalPlatform Card Technology -- Secure Channel Protocol '03' – Card Specification v2.2 – Amendment D, July 2014
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated August 28 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*

Other References	
	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 14443-1:2016 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics* ISO/IEC 14443-2:2016 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface* 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 3.0.5 Runtime Environment (JCRE) Specification*, *May 2015* *Java Card 3.0.5 Virtual Machine (JCVM) Specification*, *May 2015* *Java Card 3.0.5 Application Programming Interface* Published by Oracle
[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
[SP800-73-4]	NIST, *Interface for Personal Identity Verification,* May 2015 with updates 02-08-2016
[SP800-78-4]	NIST, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, December 2010
[SP800-85A-4]	NIST, *PIV Card Application and Middleware Interface Test Guidelines*, April 2016

Table 1: References

Acronyms and Definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CIV	Commercial Identity Verification
CM	Card Manager, see [GlobalPlatform]
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
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
PIN	Personal Identification Number
PIV	Personal Identification Verification
PUK	PIN Unblocking Key
PCT	Pairwise Consistency Test
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis
TPDU	Transaction Protocol Data Unit, see [ISO 7816]

Table 2: Acronyms and Definitions

1 Overview

This document defines the Security Policy for the Taglio PIV Applet v2.1 on NXP JCOP 3 SecID P60 CS (OSB) cryptographic module, hereafter denoted *the Module*. The Module, a single chip module embodiment validated to FIPS 140-2 overall Level 2, is the Taglio PIV applet running on NXP JCOP 3 SecID P60 CS (OSB) (denoted platform below). The Taglio PIV Applet is validated in the National PIV Program (Cert. #48) against [SP800-73-4] PIV Card Application.

The Module is bound to the platform of FIPS 140-2 Cert. #3175 NXP JCOP 3 SecID P60 CS (OSB) module, which provides a GlobalPlatform operational environment and Java Card Operating System. The Cert. #3175 module included a Demonstration Applet to demonstrate the operation of validated algorithms. In this Module:

- The hardware and operating system are unchanged from Cert. #3175.
- The Taglio PIV Applet v2.1 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.

The platform provides an operational environment for the PIV applet: all cryptographic algorithm implementations and associated self-tests, random number and key generation, card lifecycle management, and key storage and protection are provided by platform. The code for these functionalities is contained in the platform ROM. Unusable functionality is not discussed further in this document.

The Taglio PIV applet is available in two configurations:

- PIV configuration: The Module implements a configuration compliant with [SP800-85A-4] and [SP800-73-4].
- CIV configuration: The Module implements the previous PIV configuration and additional management functionality to personalize the card which it is not compliant with the NPIVP.

The PIV configuration is performed by Taglio during the initialization process and before delivering the Module.

The Module is a non-modifiable operational environment under the FIPS 140-2 definitions.

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

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

Table 3: Security Level of Security Requirements

1.1 Versions, Configurations and Modes of Operation

The Module is composed of a GlobalPlatform operational environment (platform) and a Java Card applet running on an NXP Semiconductors chip. The Module implements only Approved modes of operation once initialized and configured per Rule #14 of Section 8 of this Security Policy.

The platform component can be identified by using the IDENTIFY APDU command. This command returns the card identification data, which includes a Platform ID, a Patch ID and other information that allows to identify the content in ROM, EEPROM and loaded patches (if any). The Platform ID is a data string that allows to identify the platform component.

The platform is available in the following configuration:

Platform version and Identification	EEPROM	Interface	Hardware Version	Firmware version
J3H145C0019790400	144 kByte	Dual	P6022y VB	19790400

Table 4: Module Configurations and versions

The “identify” command is formatted as follow:

Code	Value	Parameter settings
CLA	‘80’	GlobalPlatform
INS	‘CA’	GET DATA (IDENTIFY) - ISD
P1	‘00’	High order tag value
P2	‘FE’	Low order tag value - proprietary data
Lc	‘02’	Length of data field
Data	‘DF28’	Module identification data
Le	‘00’	Length of response data

Table 5: APDU command

The command answers the content of the DF28 file. The firmware version is located at the tag ‘03’, the value is 4A784879797930303139373930343030 (JxHyyy0019790400 in ASCII, where “19790400” is the operating system version).

The PIV Applet version is Taglio PIV Applet v2.1.

To verify that the PIV Applet runs in the Approved mode of operation, the users will select the PIV applet and run the GET CONFIG APDU command.

Code	Value	Parameter settings
CLA	‘00’	PIV
INS	‘F2’	GET CONFIG
P1	‘00’	Default parameter
P2	‘00’	Default parameter
Lc	Absent	Non applicable
Data	Absent	Non applicable
Le	‘00’	Length of response data

Table 6: GET CONFIG APDU command

The command will return an 8-byte response. The users will verify that first byte is 02, the second byte is 01, the fourth byte is 11 and the eighth byte is 00. Additionally, the third byte shall be either 00 or 01 such that the response will look like 02010011XXXXXX00 or 02010111XXXXXX00 (XX fields are Module related value). The third byte indicates the applet configuration with 00 indicating the PIV configuration and 01 indicating the CIV configuration.

The personalized product shall have the applet identification:

- Package ID: A0 00 00 03 08 00 00 10
- Applet ID: A0 00 00 03 08 00 00 10 00 01 00

The validated configuration of the product identified here has exactly one applet instance: the Taglio PIV Applet instance. No other applet instance is allowed. The presence of another applet instance puts the product outside of the validated configuration.

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 wire bonded and encapsulated by epoxy with additional packaging (e.g., Dual Interface Modules)

The contactless ports of the Module require connection to an antenna. The Module relies on [ISO7816] and [ISO14443] card readers as input/output devices.

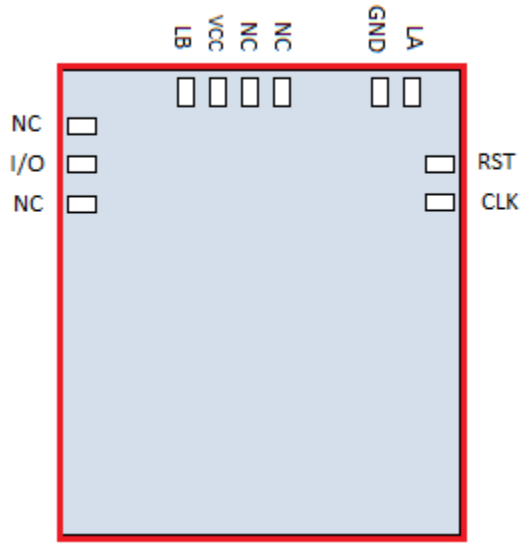

Figure 1: Taglio PIV Applet v2.1 on NXP JCOP 3 SecID P60 CS (OSB): Physical Form

Port	Description	Logical Interface Type	D
V_{CC}, GND	ISO 7816: Supply voltage	Power	X
RST	ISO 7816: Reset	Control in	X
CLK	ISO 7816: Clock	Control in	X
I/O	ISO 7816: Input/Output	Control in, Data in, Data out, Status out	X

Port	Description	Logical Interface Type	D
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out	X
NC	Not connected	Not connected	

Table 7: Ports and Interfaces

In the table above, 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.

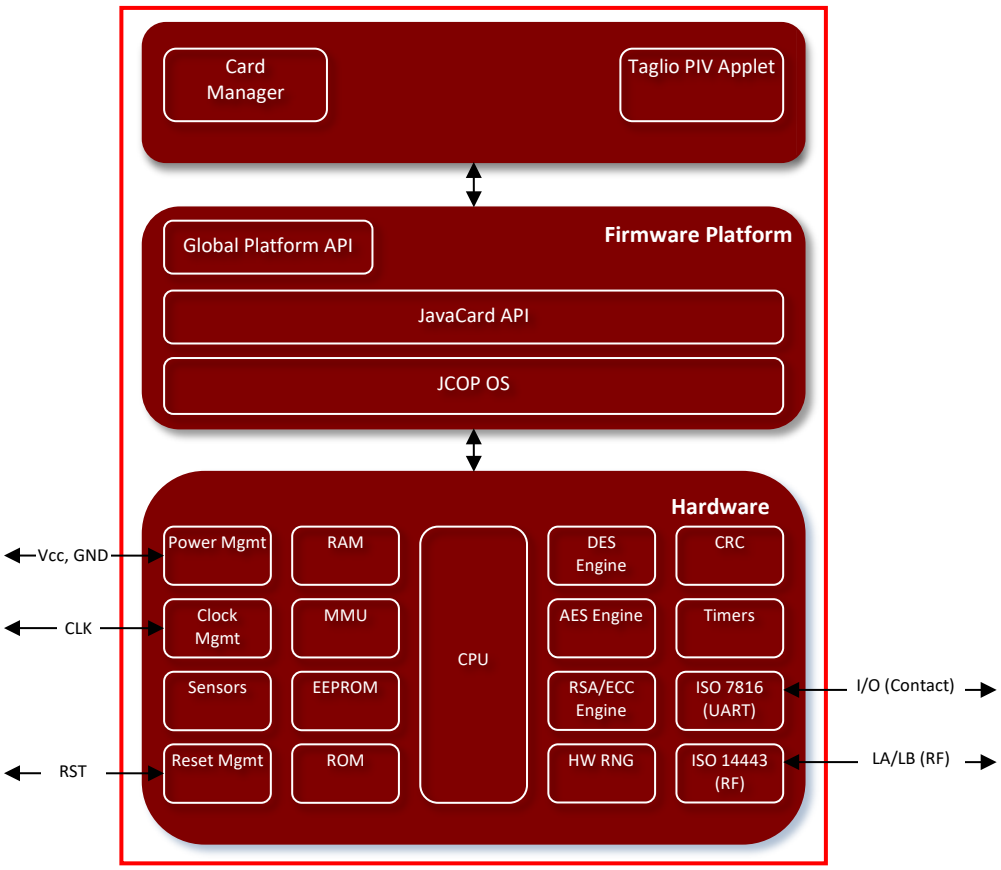

Figure 2: Module Block Diagram

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

2 Cryptographic Functionality

The Module implements the Approved and Allowed cryptographic functions listed below:

CAVP Cert	List	Standard	Mode/ Method	Strength[1]	Use	Boundary
4812	AES	[197], [38A]	CBC, ECB	128, 192, 256	Data Encryption/ Decryption	Cert. #3175
4812	AES CMAC	[197], [38B]	CMAC	128, 192, 256	Message Authentication; SP 800-108 KDF	Cert. #3175
824	CVL ECDH	[56A]	P-256 {, P-224, P-384, P-521}		Shared Secret Computation	Cert. #3175
C1667	CVL RSADP	[56B]	Decryption Primitive	n = 2048	Decryption of off-card-entity	Cert. #3175[2]
C1667	CVL RSASP1	[186]	Signature Primitive	n = 2048	Signature of off-card entity data	Cert. #3175[2]
1187	DRBG	[90A]	Hash_DRBG	256	Deterministic Random Bit Generation	Cert. #3175
890	ECDSA	[186]	P-256: (SHA-256), {P-192: (SHA-1)3, P-224: (SHA-224), P-384: (SHA-384), P-521: (SHA-512)}		Key Generation Digital Signature Generation Not used: Digital Signature Verification	Cert. #3175
91	KBKDF	[108]	CTR	128, 192, 256	Deriving keys from existing keys	Cert. #3175
4812	KTS	[IG] D.9	AES/CMAC	128, 192, 256	Symmetric key wrapping based on the combination of AES (Cert. #4812) and AES CMAC (Cert. #4812). Key establishment methodology provides between 128 and 256 bits of encryption strength.	Cert. #3175
2086	RSA	[186]	n=2048 {, 3072}		RSA key generation	Cert. #3175
2053	RSA	[186]	n=2048 {, 3072,} SHA-256, {SHA-(224, 384, 512)}		Digital signature generation.	Cert. #3175
			n=2048, {1024[2], 3072} SHA-256, {SHA-(1[3], 224, 384, 512[4])}		Digital signature verification Used by the self-test only.	Cert. #3175
3299	SHS	[180]	SHA-256, {SHA-1, SHA-224, SHA-384, SHA-512}		Message Digest generation	Cert. #3175
2547	Triple-DES[5]	[67]	CBC, ECB	3-Key (112)	Self-test only.	Cert. #3175

Table 8: Approved Algorithms

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

[2] This algorithm implementation is part Cert. #3175 module but was not tested at the time of this validation as it was not reachable.

[3] These algorithms are Approved for legacy use

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

[5] The Triple-DES is used for the self-test only. The Module does not support the Triple-DES in the FIPS configuration.

Note that Items in curly brackets { } are CAVP tested but not used by the Module.
Note that the module uses scenario 1, Section 4 of SP 800-133 rev2 to generate the seed that is used for the asymmetric key generation.

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.
RSA	RSA (CVL Cert. #C1667, key unwrapping; key establishment methodology provides 112 bits of encryption strength)

Table 9: Non-Approved but Allowed Cryptographic Functions

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 4. In the tables below, the following prefixes are used:

- OS prefix denotes operating system.
- SD prefix denotes a GlobalPlatform Security Domain.
- PIV prefix denotes an Applet CSP or a Public Key.

CSP	Description/Usage
	Card Manager
OS-DRBG-EI	384-bit NDRNG entropy input to Hash_DRBG.
OS-DRBG-V	880-bit value; the current DRBG state.
OS-DRBG-C	880-bit value; the current DRBG state.
OS-MKEK	AES-128- 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.
	Applet
PIV-AUK-PRI	PIV Card Application Authentication Key (9A): 2048-bit RSA or P-256 EC private key for signature generation
PIV-ADM	PIV Card Application Administration Key (9B): AES-128, AES-192, or AES-256 key for encryption/decryption
PIV-DSK-PRI	PIV Card Application Digital Signature Key (9C): 2048-bit RSA or P-256 EC private key for signature generation

CSP	Description/Usage
	Card Manager
PIV-KEK-PRI	PIV Card Application Key Management Key (9D): 2048-bit RSA or P-256 EC private key for key transport decryption
PIV-R-KEK-PRI	PIV Card Application Retired Key Management Keys (80-95): 2048-bit RSA or P-256 EC private key for key transport decryption.
PIV-KEK-SS	PIV Card Application ECDH Shared Secret: A 32-byte ECC-CDH computed shared secret.
PIV-A-CAK-PRI	PIV Card Application Asymmetric Card Authentication Key (9E): 2048-bit RSA or P-256 EC private key for signature generation
PIV-S-CAK	PIV Card Application Symmetric Card Authentication Key (9E): AES-128, AES-192, or AES-256 key for encryption/decryption
PIV-KL-ENC	AES-256 encryption key used to decrypt inbound data during loading of PIV CSPs
PIV-KL-MAC	AES-256 MAC key used to verify inbound data during loading of PIV CSPs
PIV-L-PIN	PIV Card Application Authentication Local PIN: between 6-byte and 8-byte decimal value
PIV-PUK	PIV Card Application PIN Unblocking Key: 8-byte hexadecimal values

Table 10: Critical Security Parameters

Public Key	Description/Usage
	Applet
PIV-AUK-PUB	PIV Card Application Authentication Key (9A): 2048-bit RSA or P-256 EC public key for signature verification
PIV-DSK-PUB	PIV Card Application Digital Signature Key (9C): 2048-bit RSA or P-256 EC public key for signature verification
PIV-KEK-PUB	PIV Card Application Key Management Key (9D): 2048-bit RSA or P-256 EC public key for key transport encryption
PIV-R-KEK-PUB	PIV Card Application Retired Key Management Keys (80-95): 2048-bit RSA or P-256 EC public key for signature verification
PIV-A-CAK-PUB	PIV Card Application Asymmetric Card Authentication Key (9E): 2048-bit RSA or P-256 EC public key for signature verification

Table 11: Public Keys

3 Roles, Authentication and Services

The Module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage.

- Only one operator at a time is permitted on a channel.

- Applet de-selection (including Card Manager), card reset, or power down terminates the current authentication. Re-authentication is required after any of these events for access to authenticated services.

Table 12 lists all operator 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 – manages the PIV Applet content and configuration. Authenticated as described in *Application Administrator* below.
CH	Card Holder (User) – performs PIV Applet cryptographic operations. Authenticated as described in *PIV Card Holder authentication* method.

Table 12: Roles Supported by the Module

3.1 Secure Channel Protocol Authentication Method

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, SD-SMAC, and SD-RMAC session keys. These sessions keys are used with AES-CBC and AES-CMAC to provide an end-to-end confidential and authenticated protected channel (Approved KTS) between the external entity (User) and the Module.
The external entity participating in the mutual authentication sent a 64-bit challenge to the Secure Element. The Secure Element generates its own challenge and computes a 64-bit cryptogram with SD-SMAC key and both challenges. The Secure Element cryptogram and challenge are sent to the external entity which checks the Secure Element 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 external entity cryptogram with AES-CMAC and SD-SMAC key, the MAC is concatenated to the command, and the command is sent to the Secure Element. The Secure Element 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 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

This authentication method includes a counter of failed authentication called “velocity checking” by GlobalPlatform. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication.

The Module enforces a maximum of 80 failed SCP authentication attempts before blocking the card. The probability that a random attempt will succeed over a one-minute interval is:

- 80/(2^128) = 2.4E-37 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

3.2 PIV Application Administrator Authentication Method

The PIV Application Administrator Authentication method is provided by *PIV AA Authentication* service. This authentication method decrypts with PIV-ADM an encrypted 64-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; the limiting factor in this authentication method is the 128-bloc 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 PIV Card Holder Authentication Method

The PIV Applet Authentication method is provided by the *PIV CH Authentication* service. The PIN value is set during pre-personalization of the product, before product delivery.

In the worst-case scenario, the Module accepts a 6-byte PIN value coded on 8 bytes and compares all 6 bytes to a stored reference (each character can be any value from 0-9 in ASCII). The character space for the first six bytes in this scenario 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 that a random attempt will succeed using this authentication method is:

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

The Module enforces a maximum of 15 consecutive failed authentication attempts. The probability that a random attempt will succeed over a one-minute interval is:

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

If the user fails to authenticate, the pin is blocked.

4 Services

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

Service	Description
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.
PIV AA Authentication	Application Administrator authentication (EXTERNAL AUTHENTICATE or MUTUAL AUTHENTICATE).
PIV AC Authentication	PIV Application Card authentication to the client application (INTERNAL AUTHENTICATE).

Service	Description
PIV Info	Read the PIV data content of the single data object. Also reads PIV applet configuration information.
PIV CH Authentication	Card Holder authentication by presenting the PIN.

Table 13: Unauthenticated Services

Service	Description	CO	AA	CH
	ISD (OS/Card Manager) Services			
Lifecycle	Modify the card or applet life cycle status.	X		
Manage Content	Load keys and data.	X		
Privileged Info	Read Module data (privileged data objects, but no CSPs).	X		
Secure Channel	Establish and use a secure communications channel.	X		
	PIV Applet Services			
PIV Privileged Info	Read the PIV data content of the single data object being authenticated		X	X
PIV CH Authentication Management	Change or unblock the Card Holder PIN of the PIV Applet. Change the PUK of the PIV Applet.		X	X
PIV Manage Content	Load PIV Applet cryptographic keys and data objects.		X	X
PIV External Key Establishment	Generate a shared secret in accordance with [SP800-73-4]. Shared secret generation is the use of [SP800-56A] Section 5.7.1.2			X
PIV Asymmetric Key Management	Generate an RSA or ECDSA Asymmetric Key Pair		X	X
PIV Digital Signature	Generate RSA and ECDSA signature of an external hash value.			X
PIV External Key Decryption	Decrypt a key in accordance with [SP800-73-4]. Key decryption is the use of [SP800-56B] Section 7.1.2 RSADP key decryption primitive.			X
PIV Auth Authentication	PIV Application Card Holder authentication to the client application (INTERNAL AUTHENTICATE) with the authenticated Card Holder.			X

Table 14: Authenticated Services

The red cross (X) indicates the Card Holder can also be authenticated to operate the corresponding services in CIV configuration only.

Table 15 below describes the access to CSPs by service with brief descriptions, which are intended to help readers understand the patterns of access. Explanations are provided in groups of services and/or keys (as best suited to explain the pattern of access), describing those aspects that have commonality across services or keys/CSPs.

Lifecycle: must be used with Secure Channel active (hence SD Session keys are 'E'); zeroizes all keys except session keys when Lifecycle is used for card termination.

OS-MKEK: generated on first power-up of the Module in a manufacturing setting; used whenever any private or secret key is accessed; zeroized on Lifecycle card termination.

OS-DRBG CSPs: OS-DRBG-EI is the NDRNG entropy input to the DRBG instantiation at power-on (Module Reset), zeroized after use. OS-DRBG-STATE is generated at startup (Module Reset), zeroized at shutdown as part of Module Reset, or by LifeCycle card termination. Each 'EI' in the OS-DRBG-STATE column indicates the use of the DRBG to generate keys (or nonce), as the value is used, and the state is updated.

Secure Channel Master Keys (SD-KENC, SD-KMAC): 'E' when a secure channel is initialized (GP Secure Channel). May be updated ('I') using the Manage Content service; zeroized by Lifecycle card termination.

SD-KDEK: is used to decrypt CSPs entered into the Module during the applet personalization.

Secure Channel Session Keys (SD-SENC, SD-SMAC, SD-RMAC): 'E' for any service that can be used with secure channel active. 'GE' on GP Secure Channel as a consequence of secure channel initialization and usage; however, while the SD-RMAC key is generated by default. 'Z' on Module Reset is a consequence of RAM clearing/garbage collection.

The PIV AA Authentication service authenticate the Host Application to the card application with symmetric keys. The PIV AC Authentication service authenticate the card application to the Host Application with either symmetric or asymmetric keys. The PIV Asymmetric Key Management service is used for RSA or ECC key generation; public keys are output in the service response. The PIV External Key Decryption is used to decrypt with RSA an encrypted key of the off-card entity; the decrypted key is not stored on the Module, but it is sent back to the off-card entity. The PIV External Establishment Key Service can be used to perform ECDH and send the result to the off-card entity. The PIV Digital Signature service provides RSA signature generation or ECDSA. The PIV Auth Authentication service authenticates the card application to the Host Application with asymmetric keys requiring authentication of the Card Holder. The applet keys can be imported with the PIV Manage Content service.

The modes of access shown in the tables below are defined as:

- G = Generate: The Module generates the CSP.
- O = Output: The Module outputs the CSP.
- E = Execute: The Module executes using the CSP.
- I = Input: The Module inputs(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. The red (I) indicates the Module inputs the CSP in the CIV configuration only.
- Z = Zeroize: The Module zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure). For the PIV External Key Establishment service, the shared secret (PIV-KEK-SS) is destroyed on applet deselect.
- -- = Not accessed by the service.

Services	OS-DRBG-EI	OS-DRBG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	PIV-AUK-PRI	PIV-ADM	PIV-DSK-PRI	PIV-KEK-PRI	PIV-R-KEK-PRI	PIV-KEK-SS	PIV-A-CAK-PRI	PIV-S-CAK	PIV-KL-ENC	PIV-KL-MAC	PIV-L-PIN	PIV-PUK
Unauthenticated	Card manager																				
Card Reset	G EZ	G EI Z	--	--	--	--	Z	Z	Z	--	--	--	--	--	Z	--	--	--	--	--	--
Context	--	--	--	--	--	--	EZ	EZ	EZ	--	--	--	--	--	Z	--	--	--	--	--	--
Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV AA Authentication	--	--	E	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--
PIV AC Authentication	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	E	E	--	--	--	--
PIV Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV CH Authentication	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--
Authenticated	Card manager																				
Lifecycle	Z	Z	Z	Z	Z	Z	E	E	E	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Manage Content	Z	Z	EZ	EI Z	EI Z	EI Z	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--
Privileged Info	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--
Secure Channel	--	--	E	E	E	--	G E	G E	G E	--	--	--	--	--	--	--	--	--	--	--	--
PIV Manage Content	--	--	E	--	--	--	--	--	--	I	I	I	I	I	--	I	I	EI	EI	--	--
PIV Privileged Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIV CH Authentication Management	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	I	EI
PIV External Key Establishment	--	--	E	--	--	--	--	--	--	--	--	--	E	E	G O	--	--	--	--	--	--
PIV Asymmetric Key Management	--	--	E	--	--	--	--	--	--	G	--	G	G	G	--	G	--	--	--	--	--
PIV Digital Signature	--	--	E	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--
PIV External Key Decryption	--	--	E	--	--	--	--	--	--	--	--	--	E	E	--	--	--	--	--	--	--
PIV Auth Authentication	--	--	E	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--

Table 15: CSPs Access within Services

Services	Public Keys				
	PIV-AUK-PUB	PIV-DSK-PUB	PIV-KEK-PUB	PIV-R-KEK-PUB	PIV-A-CAK-PUB
Unauthenticated	**Taglio PIV applet**				
Card Reset	--	--	--	--	--
Context	--	--	--	--	--
Info	--	--	--	--	--
PIV AA Authentication	--	--	--	--	--
PIV AC Authentication	--	--	--	--	--
PIV Info	--	--	--	--	--
PIV CH Authentication	--	--	--	--	--
Authenticated	**Taglio PIV applet**				
Lifecycle	Z	Z	Z	Z	Z
Manage Content	--	--	--	--	--
Privileged Info	--	--	--	--	--
Secure Channel	--	--	--	--	--
PIV Manage Content	--	--	--	--	--
PIV Privileged Info	--	--	--	--	--
PIV CH Authentication Management	--	--	--	--	--
PIV External Key Establishment	--	--	--	--	--
PIV Asymmetric Key Management	GO	GO	GO	GO	GO
PIV Digital Signature	--	--	--	--	--
PIV External Key Decryption	--	--	--	--	--
PIV Auth Authentication	--	--	--	--	--

Table 16: Public Keys Access within Services

5 Self-test

5.1 Power-On Self-tests

On power-on or reset, the Module performs self-tests as described in Table 17 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 is halted and will start again after a reset.

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. Both implementations of AES CMAC are tested.
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.

Test Target	Description
ECDSA	Performs ECDSA signature and verify KAT 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.
KBKDF	Performs a fixed input KAT on SP 800-108 AES-CMAC based KBKDF.
RSA	Performs separate RSA signature generation and verification KATs using a 2048-bit RSA key; this self-test is inclusive of the RSASP1 and RSADP self-tests.
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.

Table 17: Power-On Self-Test

5.2 Conditional Self-Tests

The Module performs the conditional self-tests as described in Table 18 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.

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.
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.

Table 18: Conditional Self-Tests

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 uses standard passivation techniques, implements Environmental Failure Protection mechanisms (EFP) to detect out-of-range supply voltages or temperatures, 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° C, 68° F), at high temperature (120° C, 248° F), and at low temperature (-40° C, -40° F).

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

7 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. In addition to the EFP mechanisms, protection features include detection of out-of-range frequencies, 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.

8 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 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 does not output CSPs (plaintext or encrypted).
6. The Module does not support manual key entry.
7. The Module does not output intermediate key values.
8. No additional interface or service is implemented by the Module which would provide access to CSPs.
9. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
10. Power up self-tests do not require any operator action.
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.

The following rules are imposed by the Vendor:

14. The Profile shall be PIV or CIV, the 9B and 9E Keys shall be AES, and the Encrypted Key Import shall be Required