G+D Mobile Security

StarSign PIV Applet V 1.0 on Giesecke+Devrient Sm@rtCafé Expert 7.0

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version **1.8**

Author : G+D Company Business Confidential
Status: **Final**
Rating : **Public**
File : SCE70 with PIV Applet Security Policy_v17.docx

Edition : October 11, 2018

Table of Contents

1 Introduction 8
2 PIV Applet 8
3 Security Level 8
3.1 Versions, Configurations and Modes of operation 9
4 Hardware and Physical Cryptographic Boundary 9
4.1 Firmware and Logical Cryptographic Boundary 11
5 Cryptographic Functionality 12
5.1 Critical Security Parameters and Public Keys 14
6 Roles, Authentication and Services 15
6.1 Secure Channel Protocol Authentication Method (CO) 16
6.2 PIV Application Administrator Method 17
6.3 PIV Applet Authentication Method 17
6.4 OCC Authentication Method 18
6.5 Services 19
7 Self-test 22
7.1 Power-On Self-tests 22
7.2 Conditional Self-tests 23
8 Physical Security Policy 24
9 Electromagnetic Interference and Compatibility (EMI/EMC) 24
10 Mitigation of Other Attacks Policy 24
11 Security Rules and Guidance 24

List of Tables

Table 1 – References 7
Table 2 – Acronyms and Definitions 7
Table 3 – Security Level of Security Requirements 9
Table 4 – Ports and Interfaces 11
Table 5 –Approved Cryptographic Functions 13
Table 6 – Non-Approved but Allowed Cryptographic Functions 13
Table 7 –Critical Security Parameters 15
Table 8 – Public Keys 15
Table 9 - Roles Supported by the Module 16
Table 10 - Unauthenticated Services 19
Table 11 –Authenticated Services 20
Table 12 –Access to CSPs by Service 21
Table 13 –Access to Public Keys by Service 22
Table 14 – Power-On Self-Test 23

List of Figures

Figure 1 – Contact only interface: P-M4.8-8-1 front and back 9
Figure 2 – Contact only interface: S-MFC6.8 front and back 10
Figure 3 – Dual interface: P-M8.4-8-3 front and back 10
Figure 4 – Dual interface: S-COM6.8 front and back 10
Figure 5 - Module Block Diagram 11

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1,* January 2011, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2* Amendment A, Confidential Card Content Management, Version 1.0, October 2007
[ISO 7816]	ISO/IEC 7816-1: 2011 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2013 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange* ISO/IEC 7816-6:2016 *Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange* ISO/IEC 7816-8:2016 *Identification cards -- Integrated circuit cards – Part 8: Commands and mechanisms for security operations* ISO/IEC 7816-12:2005 *Identification cards -- Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures* ISO/IEC 7816-15:2016 *Identification cards – Integrated circuit cards – Part 15: Cryptographic Information application*
[ISO 14443]	ISO/IEC 14443-1:2016 *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 Platform Runtime Environment (JCRE) Specification, Classic Edition. Version 3.0.4* *Java Card 3 Platform Virtual Machine (JCVM) Specification, Classic Edition. Version 3.0.4*

Acronym	Full Specification Name
	Java Card 3 Platform Application Programming Interface, Classic Edition. Version 3.0.4 Published by Oracle, September 2011
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[SP 800-56B]	NIST Special Publication 800-56B, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, September 2014
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[SP800-108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[SP800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 25 July 2013.
[RS]	Irving S. Reed, Gustave Solomon: *Polynomial codes over certain finite fields*. In: Journal of the Society for Industrial and Applied Mathematics, SIAM J. 8, 1960, ISSN 0036-1399, p. 300–304.
[SP 800-56A]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013*
[SP800-73-4]	NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation,* May 2015
[SP800-78-4]	NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* May 2015
[SP800-76-2]	NIST Special Publication 800-76-2, *Biometric Specifications for Personal*

Acronym	Full Specification Name
	Identity Verification, July 2013
[FIPS201-2]	NIST, *Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors,* August 2013
[SP800-133]	NIST, Special Publication 800-133, *Recommendation for Cryptographic Key Generation*, December 2012

Table 1 – References

Acronyms and definitions

Acronym	Definition
AA	Application Administrator
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
ATR	Answer To Reset
CM	Card Manager
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
DRBG	Deterministic Random Bit Generator
GP	GlobalPlatform
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
NVM	Non-volatile memory
PCH	PIV Card Holder
PCT	Pairwise Consistency Test
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis

Table 2 – Acronyms and Definitions

1 Introduction

This document defines the Security Policy for the **StarSign PIV Applet V 1.0 on 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 module implementing the GlobalPlatform operational environment, with Card Manager (CM) and a PIV Applet.

The module is a limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load function 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 requires a separate FIPS 140-2 validation.

2 PIV Applet

The **StarSign PIV Applet V 1.0** provides authentication, encryption, and digital signature cryptographic services and is intended for general use. The **StarSign PIV Applet V 1.0** is validated in the National PIV Program (Cert. #43) and is compliant with [SP800-73-4], [SP800-78-4], [SP800-76-2] and [FIPS201-2]. The term *platform* herein is used to describe the chip and operational environment, not inclusive of the PIV Applet.

3 Security Level

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

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

Security Requirement	Security Level
Design Assurance	3
Mitigation of Other Attacks	2

Table 3 – Security Level of Security Requirements

3.1 Versions, Configurations and Modes of operation

Hardware: SLE78CLFX4000P (M7892)

Firmware: Sm@rtCafé Expert 7.0, StarSign PIV Applet V 1.0

Packaging options (configurations):

Contact only: P-M4.8-8-1, S-MFC6.8

Dual-interface: P-M8.4-8-3, S-COM6.8

The chip and firmware are identical in all configurations. The chip design is a superset of all possible interface options; unused options are disabled during production.

The card is always in the Approved mode; the explicit indicator of Approved mode is given in the ATR: the value 0x46 ('F') in Historical Byte 9 indicates the Approved mode.

```
interface bytes             historical bytes
3B F9 96 00 00 80 31 FE 45  46 69 70 73 20 41 70 70 46 6E
                            F  i  p  s     A  p  p  F
```

4 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 Figures 1, 2, 3 and 4, the cryptographic boundary is outlined in red on these Figures.

The module relies on [ISO7816] and [ISO14443] card readers as input/output devices.

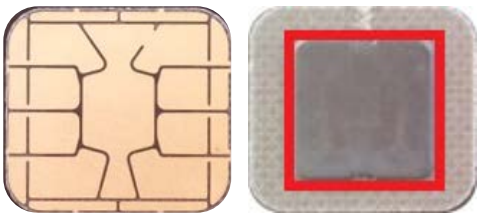

Figure 1 – Contact only interface: P-M4.8-8-1 front and back

Figure 2 – Contact only interface: S-MFC6.8 front and back

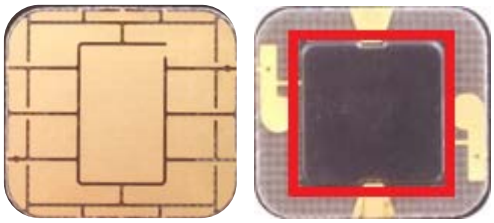

Figure 3 – Dual interface: P-M8.4-8-3 front and back

Figure 4 – Dual interface: S-COM6.8 front and back

The external circuitry appearing on the previous figures are related to the connection between the physical ports of the Module and the communication interfaces (contact plate or antenna).

For both contact only and dual interfaces, the position of the chip in configuration S-MFC6.8 (Figure 2) and S-COM6.8 (Figure 4) is flipped in comparison with its position in configuration P-M4.8-8-1 (Figure 1) and P-M8.4-8-3 (Figure 3). The contactless ports of the configuration P-M8.4-8-3 require connection to an antenna.

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 - Dual-interface configuration only
NC	Not connected	Not connected

Table 4 – Ports and Interfaces

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.

4.1 Firmware and Logical Cryptographic Boundary

Figure 3 depicts the module operational environment.

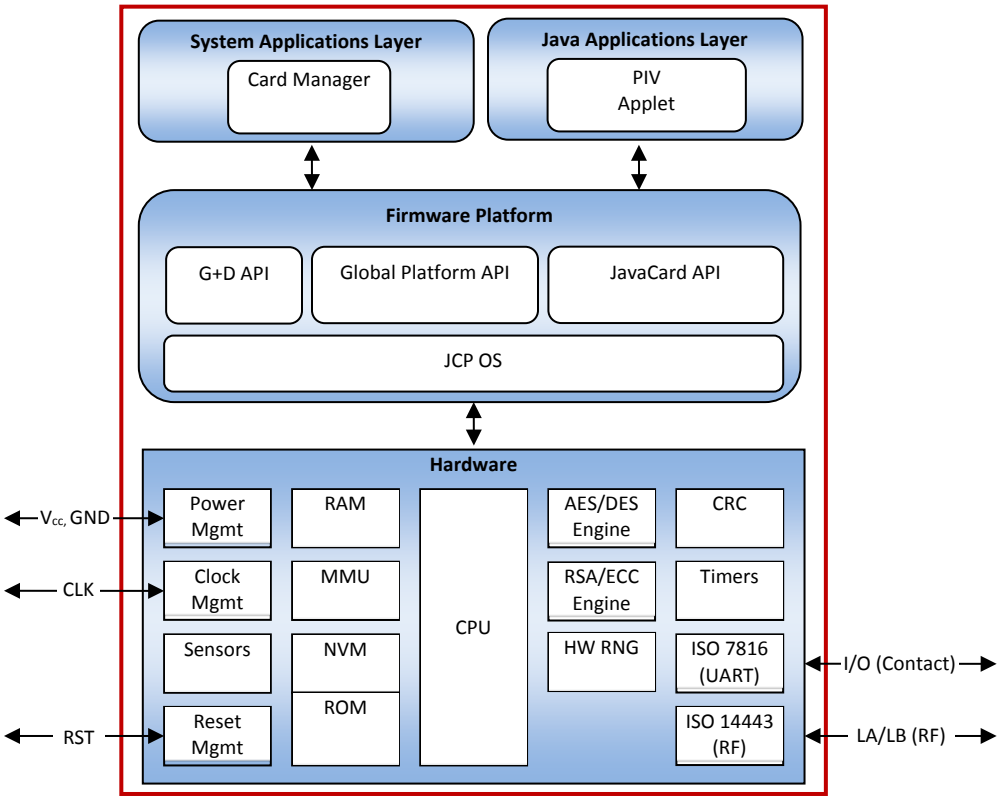

Figure 5 - Module Block Diagram

The JavaCard, GlobalPlatform and G+D APIs are internal interfaces available only to applets and security domains (i.e., Card Manager). Only PIV Applet services are available at the card edge (the interfaces that cross the cryptographic boundary). Section 3 describes applet functionality in greater detail.

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.

5 Cryptographic Functionality

The module implements the Approved and Non-Approved but Allowed cryptographic functions listed in Tables 5 and 6 below.

Algorithm	Description	FIPS 140-2 Module Cert. #2327[1]	Cert #
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports AES-128, AES-192- and AES-256 keys, and ECB and CBC modes.	X	2721
AES CMAC	[SP800-38B] AES CMAC. The module supports AES-128, AES-192 and AES-256 keys.	X	2720
CKG	[SP800-133] Cryptographic Key Generation compliant with sections 6.1, 6.2, 7.1 and 7.3.	X[2]	Vendor Affirmed
CVL (ECC CDH)	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive only (as used by the PIV specification). The module supports the NIST defined P-256, P-384 and P-521 curves. Note, curve P-521 is only used for self-test and curve P-224 is not available.	X	177
CVL (RSASP1)	[FIPS 186-4] RSASP1 Signature Primitive. The module supports 2048-bit RSA keys.	X	1192
CVL (RSADP)	[SP 800-56B] RSASDP Primitive. The module supports 2048-bit RSA keys.	X	1193
DRBG	[SP 800-90A] AES-256 CTR_DRBG. Does not support prediction resistance.	X	455
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-256, P-384 and P-521 curves for Key Pair Generation, Public Key Validation, Signature Generation and Signature Verification. Note, curve P-521 is only used for self-test and curve P-224 is not available.	X	476

[1] The algorithm is implemented by the Giesecke+Devrient Sm@rtCafé Expert 7.0 platform

[2] Implementation guidance was updated between both modules validation. The CKG was already implemented.

Algorithm	Description	FIPS 140-2 Module Cert. #2327[1]	Cert #
KAS	[SP800-56A] (Co-Factor) One-Pass Diffie-Hellman Scheme. The module supports the NIST defined P-256 curve, SHA256, and CMAC-AES128. The KAS algorithm calls CVL (ECC CDH), AES, AES CMAC, and ECDSA key generation algorithms APIs which are implemented by the platform.		166
KBKDF	[SP 800-108] CMAC-based KDF with AES-128, AES-192, AES-256.	X	18
KTS	AES Key Wrapping compliant with [SP800-38F] §3.1 ¶3 (Combination method using AES Cert. #2721 and AES CMAC Cert. #2720). Key establishment methodology provides between 128 to 256 bits of encryption strength.	X	2720 2721
RSA	[FIPS 186-4] RSA key generation, signature generation and verification. The module supports 2048-bit RSA keys.	X	1506
RSA CRT	[FIPS 186-4] RSA key generation and signature generation. The module supports 2048-bit RSA keys.	X	1507
SHA-1	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms: SHA-1	X	2290
SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms: SHA-224, SHA-256, SHA-384, SHA-512	X	2289
SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms: SHA-256	X	2288
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports 3-Key keys only, and CBC and ECB modes.[3]	X	1637

Table 5 –Approved Cryptographic Functions

Algorithm	Description
NDRNG	Hardware NDRNG provides at least 256 bits of entropy to the FIPS approved DRBG

Table 6 – Non-Approved but Allowed Cryptographic Functions

[3] The same Triple-DES key shall not be used to encrypt/decrypt more than 2^{16} 64-bit data blocks, see IG A.13

5.1 Critical Security Parameters and Public Keys

All CSPs and public keys used by the module are described in this section. In the tables below, the OS prefix denotes operating system, the SD prefix denotes the GlobalPlatform Security Domain, the DAP prefix denotes the GlobalPlatform Data Authentication Protocol, and the PIV prefix denotes a PIV Applet CSPs. All PIV Applet keys listed below correspond to those specified in NIST [SP800-73-4].

CSP	Description / Usage
OS-DRBG-STATE	Current DRBG state (value V and the Key).
SD-KENC	AES-128, AES-192, AES-256 Master key used to generate SD-SENC.
SD-KMAC	AES-128, AES-192, AES-256 Master key used to generate SD-SMAC.
SD-KDEK	AES-128, AES-192, AES-256 Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES-128, AES-192, AES-256 Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES-128, AES-192, AES-256 Session MAC key used to verify inbound secure channel data integrity.
SD-SRMAC	AES-128, AES-192, AES-256 Session MAC key used to verify response secure channel data integrity.
DAP-SYM	AES-128, AES-192, AES-256 authentication key used by the *Manage Content* service.
PIV-AUTH-PRIV	(9E asymmetric): 2048-bit private part of the RSA key pair or P-256 Private part of ECC key pair used for Internal authenticate of the card holder.
PIV-Local PIN	(Local PIN 80): An 8-byte PIN value used by the *PIN Authentication* service. The module always checks all 8 bytes of the PIN.
PIV-Global PIN	(00): An 8-byte PIN value allowing all digit values for each byte, used by the *PIN Authentication* service. The module always checks all 8 bytes of the PIN.
PIV-PUK	(00): 8-byte hexadecimal PIV Unblocking Key.
PIV-SC	(04): Cipher Suite 2 private components used by *PIV Secure Messaging Key* service.
SK_CFRM	AES-128 Key confirmation key used to compute authentication cryptogram
SK_MAC	AES-128 Secure messaging command authentication session keys
SK_ENC	AES-128 Secure messaging encryption session keys
SK_RMA	AES-128 Secure messaging response authentication session keys
PIV-KS	(82) up to (95) ECDSA (on P-256 or P-384) or RSA 2048 bits private key used by *Retired Key Management Keys* service.
PIV-KAP-PRI	(9A): ECDSA (on P-256) or RSA 2048 bits private key used by *PIV Authentication Key* service.
PIV-AD	(9B) 3DES, AES-128, AES-192, AES-256, used by *PIV Card Application Administration*

CSP	Description / Usage
	service.
PIV-SGV-PRIV	(9C): ECDSA (on P-256 or P-384) or RSA 2048 bit private key used by the *Digital Signature Key* service.
PIV-ADKM	(9D) ECDSA (on P-256 or P-384) or RSA-2048 private key used by *Key Management Key* service.
PIV-AUTH-SYM	(9E symmetric): 3DES, AES-128, AES-192, AES-256 used by *Card Authentication Keys* service.
PIV-AUTH-ASYM	(9E asymmetric): ECDSA (on P-256) or RSA 2048 bits private key used by *PIV Card Authentication Key* service.

Table 7 –Critical Security Parameters

Key	Description / Usage
DAP-PUB	RSA 2048 new firmware signature verification key.
PIV-SC-PUB	(04): Cipher Suite 2 public components used by PIV Secure Messaging Key service.
PIV-KAP-PUB	(9A): ECDSA (on P-256) or RSA 2048 bits public key used by the *Key Agreement Primitive* service.
PIV-SGV-PUB	(9C): ECDSA (on P-256 or P-384) or RSA 2048 bit public key used by the *Digital Signature Key* service.
PIV-ADKM-PUB	(9D): ECDSA (on P-256 or P-384) or RSA-2048 public key used by *Key Management Key* service.
PIV-AUTH-PUB	(9E): ECDSA (on P-256) or RSA 2048 bit public key used by *Card Authentication Keys* service.

Table 8 – Public Keys

6 Roles, Authentication and Services

The module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports GlobalPlatform 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. Authentication data is encrypted during entry (by SD-KDEK), and is only accessible by authenticated services.

Table 9 lists all operator roles supported by the module.

Role ID	Role Description
CO [Cryptographic Officer]	The CO manages module content and configuration, including issuance and management of module data via the ISD. *(Authenticated as described in Secure Channel Protocol Authentication in Section 6.1 below)*
Application Administrator [AA]	AA is a role for use in the PIV applet. The User is responsible for: • managing the content of the PIV application. • accessing data that is protected by the Secure Channel service. *(Authenticated as described in PIV Application Administrator authentication in Section 6.2 below)*
PIV Card Holder [PCH]	PCH is a role for use in the PIV applet. The PCH is responsible for: • ensuring the ownership of his CM, and for not communicating his PIN to other parties (the PIV Applet authenticates the User by verifying the local or Global PIN value) (PCH). • unblocking and/or changing the User PIN (PCH). The PIV Applet authenticates the User by verifying the PUK value. *(Authenticated as described in PIV Applet Authentication in Section 6.3 below or OCC Authentication in Section 6.4)*

Table 9 - Roles Supported by the Module

6.1 Secure Channel Protocol Authentication Method (CO)

The Secure Channel Protocol 03 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 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

The module enforces a maximum of fifteen (15) 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 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

6.2 PIV Application Administrator Method

This authentication method decrypts with PIV-AD 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 3-Key Triple DES; however, the limiting factor in this authentication method is the 64-bit block size.

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

6.3 PIV Applet Authentication Method

The PIV Applet Authentication method is provided by the *PIN authentication* service. In the worst case scenario, the module accepts a 6-byte PIN value coded on 8 bytes and compares all 6 bytes plus padding to a stored 8 byte 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 2 characters is 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) = 1.23E-7

6.4 OCC Authentication Method

The module performs a biometric person authentication On-Card-Comparison (OCC) of a live fingerprint template as defined by [FIPS 201-2]. Fingerprint minutiae are sent to the Module and compared with a value stored on the card.

The PIV OCC authentication method is a valid authentication method when the "OCC Authentication" security rule below is applied.

The False Match Rate (probability that the Module incorrectly accepts biometric data) is 0.0000001.

The probability that a random attempt will succeed using this authentication method is 10^{-7}.

The module enforces a maximum of ten (10) consecutive failed OCC authentication attempts. The probability that a random attempt will succeed over a one minute interval is $10*10^{-7}$ which is lower than 10^{-5}.

6.5 Services

All services implemented by the module are listed in the tables below.

Service	Description
Context	Selects an applet or manage logical channels.
Module Info (Unauthenticated)	Reads unprivileged data objects, e.g., module configuration or status information.
Module Reset	Power cycles or resets the module. Includes Power-On Self-Test.
PIN Authentication	PIN authentication with OwnerPIN of the User.
Opacity Secure Messaging	Establish OPACITY Secure Messaging.
Administrator authentication	Application Administrator authentication (EXTERNAL AUTHENTICATE or MUTUAL AUTHENTICATE)
Application card authentication	Card authentication to the client application (INTERNAL AUTHENTICATE or MUTUAL AUTHENTICATE)

Table 10 - Unauthenticated Services

Service	Description	CO	User	
			AA	PCH
Lifecycle	Modifies the card or applet life cycle status.	X		
Manage Content	Loads and installs application packages and associated keys and data. Firmware update.	X		
Module Info (Authenticated)	Reads module configuration or status information (privileged data objects)	X		
Secure Channel	Establishes and uses the Secure Channel Protocol 03.	X		
PIN Management	Unblocks and changes the value of a PIN		X	X
PIV info	Read PIV Application privileged data objects.		X	X
Manage Applet Content	Creates uninitialized key objects for use by the PIV Applet's cryptographic services. Deletes on-card key objects, arrays, signature objects.		X	
Asymmetric Key Management	Generates an RSA or ECDSA Asymmetric Key Pair.		X	
Digital Signature	RSA, and ECDSA digital signature of an external hash value.			X
Key	Generate a Shared Secret as specified in SP 800-78-04			X

Service	Description	CO	User	
Establishment	(ECDH). Keys are not established into or used by the module.			
Key Decryption	Unwrap a key provided by off-card entity with RSA. Keys are not established into or used by the module.			X

Table 11 –Authenticated Services

Services	CSPs																						
	OS-DRBG-STATE	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-SRMAC	DAP-SYM	PIV-AUTH-PRI	PIV-Local PIN	PIV-Global PIN	PIV-PUK	PIV-SC	SK_CFRM	SK_MAC	SK_ENC	SK_RMA	PIV-KS	PIV-KAP-PRI	PIV-AD	PIV-SGV-PRIV	PIV-ADKM	PIV-AUTH-SYM	PIV-AUTH-ASYM
Context	--	--	--	--	Z	Z	Z	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Module Info (Unauth.)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Module Reset	GEW	--	--	--	Z	Z	Z	--	--	--	--	--	--	Z	Z	Z	Z	--	--	--	--	--	--	--
Lifecycle	Z	Z	Z	Z	E	E	E	Z	Z	Z	Z	Z	Z	--	--	--	--	Z	Z	Z	Z	Z	Z	Z
Manage Content	--	W	W	W	E	E	E	EW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Module Info (Auth.)	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure Channel	EW	E	E	--	GE	GE	GE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
PIN Authentication	--	--	--	--	--	--	--	--	--	E	E	--	--	--	E	E	E	--	--	--	--	--	--	--
Opacity Secure Messaging	--	--	--	--	--	--	--	--	--	--	--	--	GEZ	GEZ	GZ	GZ	GZ	--	--	--	--	--	--	--
Administrator authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	E	--	--	E	--	--	--	--
Application card authentication	--	--	--	--	--	--	--	--	E	--	--	--	--	--	E	E	E	--	E	--	--	--	E	E
PIN Management	--	--	--	--	--	--	--	--	--	WZ	WZ	EWZ	--	--	E	E	E	--	--	--	--	--	--	--
PIV info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--
Manage Applet Content	--	--	--	--	--	--	--	--	WZ	WZ	WZ	WZ	WZ	--	--	--	--	WZ	WZ	WZ	WZ	WZ	WZ	WZ
Asymmetric Key Management	--	--	--	--	--	--	--	--	G	--	--	--	GW	--	E	E	E	G	G	--	G	G	--	G
Digital	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	E	--	--	--	E	--	--	--

Services	CSPs																							
	OS-DRBG-STATE	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-SRMAC	DAP-SYM	PIV-AUTH-PRI	PIV-Local PIN	PIV-Global PIN	PIV-PUK	PIV-SC	SK_CFRM	SK_MAC	SK_ENC	SK_RMA	PIV-KS	PIV-KAP-PRI	PIV-AD	PIV-SGV-PRIV	PIV-ADKM	PIV-AUTH-SYM	PIV-AUTH-ASYM
Signature																								
Key Establishment	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	E	E	--	--	--	E	--	--
Key Decryption	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	E	--	--	--	--	E	--	--

Table 12 –Access to CSPs by Service

Services	Public Keys					
	DAP-PUB	PIV-SC-PUB	PIV-KAP-PUB	PIV-SGV-PUB	PIV-ADKM-PUB	PIV-AUTH-PUB
Context	--	--	--	--	--	--
Module Info (Unauthenticated)	--	--	--	--	--	--
Module Reset	--	--	--	--	--	--
Lifecycle	Z	Z	Z	Z	Z	Z
Manage Content	EW	--	--	--	--	--
Module Info (Authenticated)	--	--	--	--	--	--
Secure Channel	--	--	--	--	--	--
PIN Authentication	--	--	--	--	--	--
Opacity Secure Messaging	--	--	--	--	--	--
Administrator authentication	--	--	--	--	--	--
Application card authentication	--	--	--	--	--	--
PIN Management	--	--	--	--	--	--
PIV info	--	R	R	R	R	R
Manage Applet Content	--	WZ	WZ	WZ	WZ	WZ
Asymmetric Key Management	--	G	G	G	G	G
Digital Signature	--	--	--	--	--	--
Key Establishment	--	--	--	--	--	--
Key Decryption	--	--	--	--	--	--

Table 13 –Access to Public Keys by Service

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP (read access to the CSP by an outside entity).
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure)
- -- = Not accessed by the service.

7 Self-test

7.1 Power-On Self-tests

On power-on or reset, the module performs self-tests as described in Table 14 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	Performs a fixed input KAT.
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.
SP 800-108 KDF	Performs a KAT of SP 800-108 KDF. This self-test is inclusive of AES CMAC and AES encrypt function self-test.
RSA	Performs separate RSA signature and verify KATs using an RSA 2048-bit key.
RSA CRT	Performs RSA CRT signature KAT using an RSA 2048-bit key.
ECDSA	Performs pairwise consistency test using the P-521 curve.
SHA-1	Performs a fixed input KAT.
SHA-256	Performs a fixed input KAT.
SHA-256(2)	Performs a fixed input KAT for the 2nd SHA-256 implementation.
SHA-512	Performs a fixed input KAT.
ECC CDH	Primitive "Z" Computation KAT for [SP 800-56A] Section 5.7.1.2 ECC CDH Primitive using the P-521 curve.

Table 14 – Power-On Self-Test

7.2 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 NDRNG hardware includes a continuous comparison test, such that each word formed is compared to the previous value; a duplicate value is discarded, and the NDRNG status indicates not ready.

When an RSA or ECDSA key pair is generated the module performs a pairwise consistency test. If the pairwise consistency test fails, the module enters the SELF-TEST ERROR state.

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 AES-CMAC algorithm (cert. #2720) and the SD-SMAC key. Optionally, the module may also verify a signature of the new firmware (applet) using the DAP-SV-PUB public key (RSA signature verification, cert. #1506) or the DAP-SYM key (AES CMAC, cert. #2720); the signature block in this scenario is generated by an external entity using the private key corresponding to DAP-SV-PUB or the symmetric DAP-SYM. Failure to verify the new firmware results in the BAD APDU error state; the module returns an error specific to the situation (MAC failure or DAP failure).

8 Physical Security Policy

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

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

9 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.

10 Mitigation of Other Attacks Policy

The module implements defenses against:

- Physical attacks
- Side-channel attacks (SPA/DPA and timing analysis)
- Differential fault analysis (DFA)

11 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.

This section documents the security rules imposed by the vendor:

- OCC authentication: the threshold applied to scores from the biometric comparison algorithms shall be set to achieve false match rates (FMR) at or below 0.0000001 for on-card fingerprint minutia matching.