Prime PIV v2.1 Applet on TOP DL V2.1 platform
FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Table of Contents

Table of Tables

Table of Figures

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 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 *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2* Amendment D, Sept 2009
[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*
[ISO 14443]	*Identification cards – Contactless integrated circuit cards – Proximity cards* ISO/IEC 14443-1:2008 Part 1*: Physical characteristics* ISO/IEC 14443-2:2010 Part 2: *Radio frequency power and signal interface* ISO/IEC 14443-3:2011 Part 3: *Initialization and anticollision* ISO/IEC 14443-4:2008 Part 4: *Transmission protocol*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification* *Java Card 2.2.2 Virtual Machine (JCVM) Specification* *Java Card 2.2.2 Application Programming Interface* *Java Card 3.0.1 Application Programming Interface [only for algos ECDSA, SHA2]* Published by Sun Microsystems, March 2006
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP 800-90A]	NIST Special Publication 800-90, *Recommendation for the Random Number Generation Using Deterministic Random Bit Generators (Revised)*, March 2007
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (Triple-DES) Block Cipher*, version 1.2, July 2011
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS 197]	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
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015

Acronym	Full Specification Name
[AESKeyWrap]	NIST, *AES Key Wrap Specification*, 16 November 2001. This document defines symmetric key wrapping, Use of 2-Key Triple-DES in lieu of AES is described in [IG] D.2.
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 1 August 2016.
[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 Identity Verification,* July 2013.
[FIPS201-2]	NIST, *Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors,* August 2013.

Table 1 – References

Acronyms and Definitions

Acronym	Definition
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter
DAP	Data Authentication Pattern, see [GlobalPlatform]
DF	Dedicated File
DPA	Differential Power Analysis
EF	Elementary File
GP	Global Platform
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
OP	Open Platform (predecessor to Global Platform)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
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 Gemalto Prime PIV v2.1 Applet on TOP DL V2.1 platform cryptographic module, herein denoted the *Module*. The *Module*, validated to FIPS 140-2 overall Level 2, is a single-chip "dual" module (P60D144) implementing the Global Platform operational environment, with Card Manager 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.

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

Security Requirement	Security Level
Cryptographic Module Specification	2
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
Design Assurance	3
Mitigation of Other Attacks	2

Table 3 – Security Level of Security Requirements

1.1 Cryptographic Module Ports and Interfaces

The *Module* is designed to be embedded into plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna. 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. The cross-hatching indicates the presence of the hard opaque outer layer shielding. In production use, the *Module* is wire-bonded to a frame connected to a contact plate (pads CLK, RST, VDD, I/O and VSS) and/or to an RF antenna (pads LA and LB), enclosed in epoxy and mounted in a card body. The *Module* relies on [ISO 7816] and/or [ISO 14443] card readers as input/output devices.

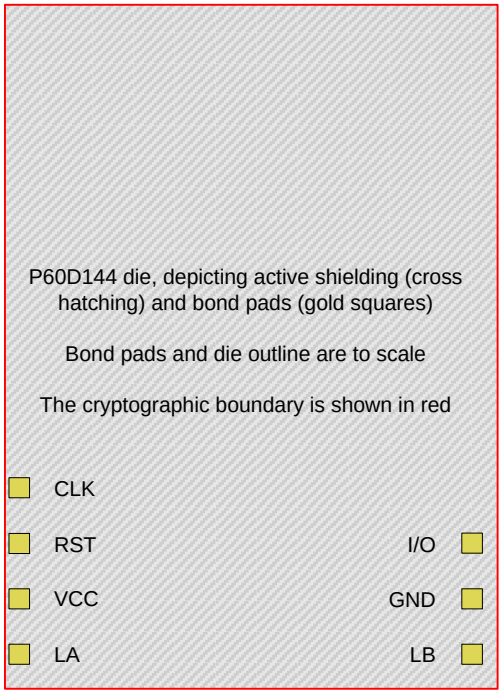

Figure 1 - Physical form and Cryptographic Boundary (P60D144)

Contact No.	Description	Logical interface type
VCC	Supply voltage	Power
RST	Reset signal	Control in
CLK	Clock signal	Control in
GND	Ground	Power
I/O	Input/output	Data in, data out, control in, status out
LA	LA (Antenna coil connection)	Power, Data in, Data out, Control in, Status out
LB	LB (Antenna coil connection)	Power, Data in, Data out, Control in, Status out

Table 4 – Module Physical Ports and Corresponding Logical Interfaces

For contact interface operation, the *Module* conforms to [ISO 7816] part 1 and part 2. The electrical signals and transmission protocols follow the [ISO 7816] part 3. The conditions of use are the following:

Conditions	Range
Voltage	3 V and 5.5 V
Frequency	1MHz to 10MHz

Table 5 - Voltage and Frequency Ranges

For contactless interface operation, the *Module* conforms to [ISO 14443] part 1 for physical connections, and to [ISO 14443] parts 2, 3 and 4 for radio frequencies and transmission protocols. The external antenna loop required for contactless operation is outside the module cryptographic boundary.

The conditions of use are the following:

Conditions	Range
Supported bit rate	106 Kbits/s, 212 Kbits/s, 424 Kbits/s, 848 Kbits/s
Operating field	Between 1.5 A/m and 7.5 A/m rms
Frequency	13.56 MHz +- 7kHz

Table 6 – Contactless voltage and Frequency Ranges

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment and applets.

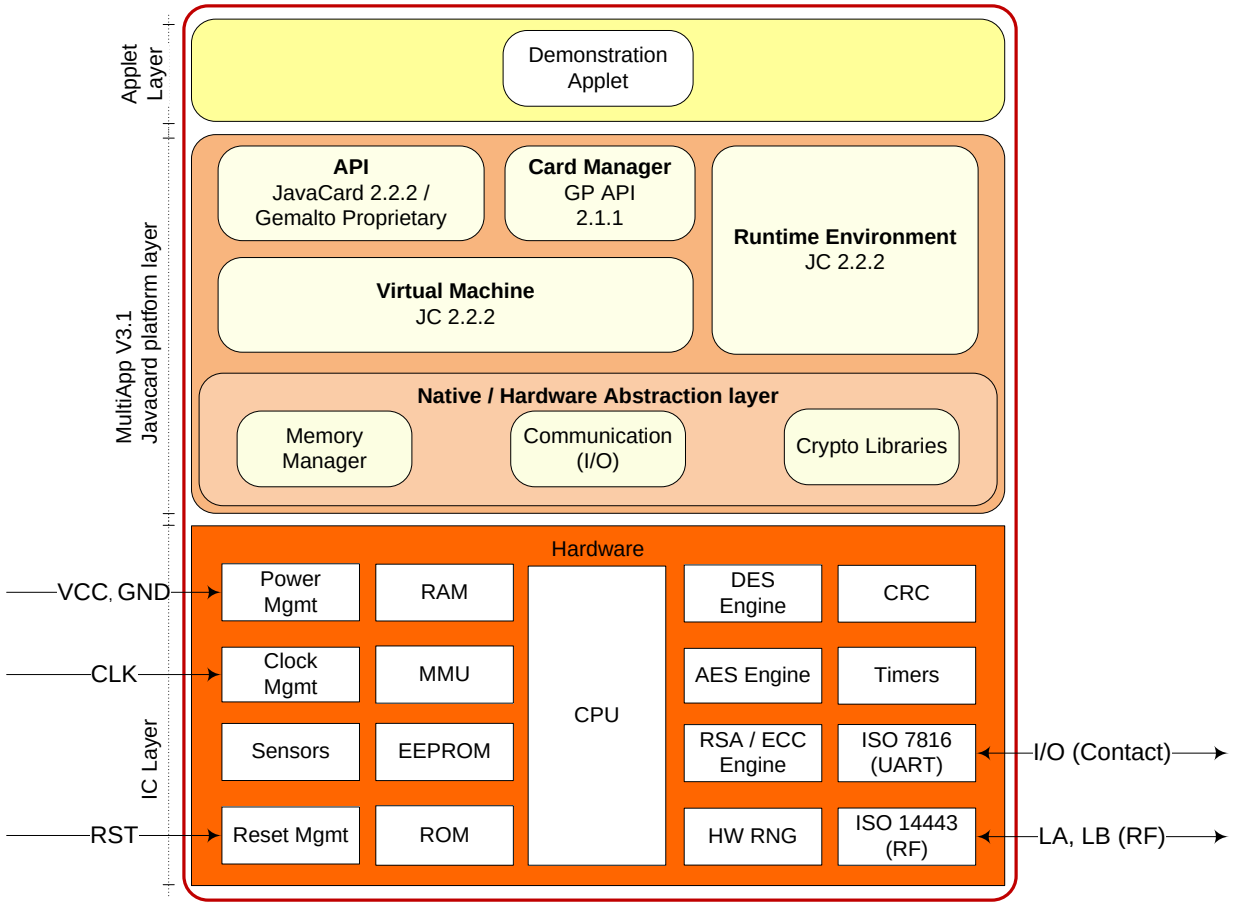

Figure 2 - Module Block Diagram

The *JavaCard API* is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary). The *Cryptography Libraries* implement the algorithms listed in Section 2. The *Javacard Runtime Environment* implements the dispatcher, registry, loader, and logical channel functionalities. The *Virtual Machine* implements the byte code interpreter, firewall, exception management and byte code optimizer functionalities.

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

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

Applets, such as PIVv2.1, access module functionalities via internal API entry points that are not exposed to external entities. External devices have access to CM services by sending APDU commands.

Section 3 describes applet functionality in greater detail.

1.3 Versions and Mode of Operation

Hardware: NXP P60D144P VA (MPH149)
Firmware: TOPDLV2.1 (Filter04), PIV Applet version V2.1

2. Cryptographic Functionality

The Module only implements an Approved Mode once configured as specified in Section 9 of this Security Policy. The cryptographic algorithms available once configured properly are listed in Table 7 and Table 8 below:

Algorithm	Description	Cert #
AES	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128-, 192- and 256-bit key lengths with ECB and CBC modes.	3543
AES CMAC	[SP 800-38D] The Module supports 128-, 192- and 256-bit key lengths.	3543
CVL (ECC CDH)	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive using the NIST defined curves: P-224, P-256, P-384 and P-521.	597
CVL (RSADP)	[SP 800-56B] RSA key decryption primitive using 2048-bit keys.	834
CVL (RSASP1)	[FIPS 186-4] [PKCS#1 v2.1] RSA signature generation primitive using 2048-bit keys.	815
DRBG	[SP 800-90A] Deterministic Random Bits Generator (CTR-DRBG based on AES)	900
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm using the NIST defined curves – Key pair generation: P-224, P-256, P-384 and P-521 curves – Signature generation: P-224, P-256, P-384 and P-521 curves with SHA-2 – Signature verification: P-192, P-224, P-256, P-384 and P-521 curves (with SHA-1 or SHA-2). Note: P-192, P-224 and P-521 were tested but are not used by this Module	721
KDF AES CMAC	[SP 800-108] KBKDF. The Module supports 128-, 192- and 256-bit key lengths	85
KTS (AES Key Wrap)	[SP 800-38F] Use of approved AES and AES CMAC for key wrapping, in accordance with SP 800-38F §3.1 ¶3.	3543
RSA	[FIPS 186-2] [PKCS#1 v1.5 and PSS] RSA algorithms. – Signature verification using 4096-bit key (any SHA size). [FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA algorithms – Key pair generation using 2048-bit keys – Signature generation using 2048-bit keys with SHA-2 – Signature verification using 1024, 2048-bit and 3072-bit keys (any SHA size) Note: RSA 3072 was tested but is not used by this Module	1822

RSA CRT	[FIPS 186-2] [PKCS#1 v1.5 and PSS] RSA CRT algorithm. – Signature verification using 4096-bit key with SHA-2. [FIPS 186-4] [PKCS#1 v1.5 and PSS] RSA CRT algorithm. – Key pair generation using 2048-bit keys; – Signature generation using 2048-and 3072-bit keys with SHA-2; – Signature verification using 1024-, 2048-and 3072-bit keys (any SHA size). Note: RSA CRT 3072 was tested but is not used by this Module	1823
SHA-1 SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms. The Module supports the SHA-1 (160 bits), SHA-2 (224- bit, 256-bit, 384-bit, 512-bit) variants. Note: SHA-224 and SHA-512 were tested but are not used by this Module	2921
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The Module supports the 3-Key options; CBC and ECB modes. Note that the Module does not support a mechanism that would allow collection of plaintext / ciphertext pairs aside from authentication, limited in use by a counter.	1984

Table 7 – FIPS Approved Cryptographic Functions

Algorithm	Description
NDRNG	True Random Number Generator; provides at least 128 bits of entropy

Table 8 – FIPS Non-Approved But Allowed Cryptographic Functions

If the Module is improperly configured, it is in a non-compliant state and can implement the *Non-Approved* cryptographic functions listed in Table 9 below:

Algorithm	Description
Triple-DES	The Module supports the 2-Key options, CBC and ECB modes.
RSA	The module supports: - Signature verification using 1024, 1280 and 1536-bit keys. - Key pair generation using 1024, 1280 and 1536-bit keys.
RSA CRT	The module supports: - Signature generation using 1024, 1280 and 1536-bit keys. - Key pair generation using 1024, 1280 and 1536-bit keys.

Table 9 – FIPS Non-Approved Cryptographic Functions

2.1 Platform Critical Security Parameters

All CSPs used by the Platform are described in this section. All usage of these CSPs by the Module are described in the services detailed in Section 4. In the tables below, the OS prefix denotes operating system, the SD prefix denotes the Global Platform Security Domain, the DAP prefix denotes the Global Platform Data Authentication Protocol.

Key	Description / Usage
OS-DRBG-EI-KEY	AES-128 random key generated by the card during startup is used as an entropy input for the [SP800-90A] DRBG implementation.
OS-DRBG-STATE	16-byte AES state V and 16-byte AES key used in the [SP800-90A] CTR DRBG implementation.
OS-GLOBALPIN	6 to 16 byte Global PIN value. Character space is not restricted by the module.
OS-MKDK	AES-128/192/256 (SCP03) key used to encrypt OS-GLOBALPIN value
SD-KENC	AES-128/192/256 (SCP03) master key used to derive SD-SENC
SD-KMAC	AES-128/192/256 (SCP03) Security Domain MAC master key, used to derive SD-SMAC
SD-KDEK	AES-128/192/256 (SCP03) Security Domain Sensitive data decryption key.
SD-SENC	AES-128/192/256 (SCP03) Security Domain Session decryption key used to decrypt secure channel messages.
SD-SMAC	AES-128/192/256 (SCP03) Security Domain Session MAC key, used to verify secure channel message integrity.
SD-SDEK	AES-128/192/256 (SCP03) Session DEK key used by the CO role to decrypt CSPs.
DAP-SYM	AES-128/192/256 (SCP03) key optionally loaded in the field and used to verify the MAC of packages loaded into the Module.

Table 10 – Platform Critical Security Parameters

2.2 PIV Critical Security Parameters

All CSPs used by the PIV applet are described in this section. All usage of these CSPs by the Module are described in the services detailed in Section 4. In the table below, the PIV prefix denotes PIV applet. All keys listed below correspond to those specified in NIST SP 800-73-4.

Key	Description / Usage
PIV-AUTH-TDES	PIV Card Application Administration Key (9B): Symmetric 3-Key TDES encryption / decryption key used by the PIV Applet. External authenticate using this key grants CAA rights. (application security status indicator)
PIV-AUTH-AES	PIV Card Application Administration Key (9B): Symmetric AES-128/192/256 encryption / decryption key used by the PIV Applet. External authenticate using this key grants CAA rights. (application security status indicator)
PIV-AUTH_CH-TDES	PIV Card Authentication Key (9E): Symmetric 3-Key TDES encryption / decryption key used by the PIV Applet. Internal authenticate using to authenticate the card holder (physical access rights)

PIV-AUTH_CH-AES	PIV Card Authentication Key (9E): Symmetric AES-128/192/256 encryption / decryption key used by the PIV Applet. Internal authenticate using to authenticate the card holder (physical access rights)
PIV-AUTH-RSA	PIV authentication Key (9A): 2048 bit private part of the RSA key pair used for Authentication.
PIV-AUTH-ECC	PIV authentication Key (9A): P-256 or P-384 Private part of ECC key pair used for Authentication.
PIV-AS-RSA	PIV Digital Signature Key (9C): 2048 bit private part of the RSA key pair used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).
PIV-AS-ECC	PIV Digital Signature Key (9C): P-256 or P-384 Private part of ECC key pair used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).
PIV-AKM-RSA	PIV Key Management Key (9D): 2048 bit private part of the RSA key pair used for Key Management.
PIV-AKM-ECC	PIV Key Management Key (9D): P-256 or P-384 Private part of ECC key pair used for Key Management.
PIV-AUTH_CH-RSA	PIV Card Authentication Key (9E): 2048 bit private part of the RSA key pair used for Internal authenticate using to authenticate the card holder (physical access rights).
PIV-AUTH_CH-ECC	PIV Card Authentication Key (9E): P-256 or P-384 Private part of ECC key pair used for Internal authenticate using to authenticate the card holder (physical access rights).
PIV-KS-RSA	Retired Key Management (82 up to 95): 2048 bit private part of the RSA key pair used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.
PIV-KS-ECC	Retired Key Management (82 up to 95): P-256 or P-384 Private part of ECC key pair used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.
PIV-Local PIN	Between 6 and 8 byte-long, PIV Card Application PIN (Local PIN 80), in numerical format. (application security status indicator)
PIV-Global PIN	Between 6 and 8 byte-long PIV Card Holder Global PIN (00), in numerical format. (global security status indicator)
PIV-PUK	8 byte-long PIV card PUK (81), in hexadecimal format (all characters allowed) (application security status indicator)

Table 11 – PIV Applet Critical Security Parameters

Key	Description / Usage
PIV-AUTH-RSA-PUB	PIV authentication Key (9A): 2048 bit public part of the RSA key pair used for Authentication.
PIV-AUTH-ECC-PUB	PIV authentication Key (9A): P-256 or P-384 public part of ECC key pair used for Authentication.
PIV-AS-RSA-PUB	PIV Digital Signature Key (9C): 2048 bit public part of the RSA key pair used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).
PIV-AS-ECC-PUB	PIV Digital Signature Key (9C): P-256 or P-384 public part of ECC key pair used for Asymmetric signature (Asymmetric key protected by PIN Always used for signature).
PIV-AKM-RSA-PUB	PIV Key Management Key (9D): 2048 bit public part of the RSA key pair used for Key Management.
PIV-AKM-ECC-PUB	PIV Key Management Key (9D): P-256 or P-384 public part of ECC key pair used for Key Management.
PIV-AUTH_CH-RSA-PUB	PIV Card Authentication Key (9E): 2048 bit public part of the RSA key pair used for Internal authenticate using to authenticate the card holder (physical access rights).
PIV-AUTH_CH-ECC-PUB	PIV Card Authentication Key (9E): P-256 or P-384 public part of ECC key pair used for Internal authenticate using to authenticate the card holder (physical access rights).
PIV-KS-RSA-PUB	Retired Key Management (82 up to 95): 2048 bit public part of the RSA key pair used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.
PIV-KS-ECC-PUB	Retired Key Management (82 up to 95): P-256 or P-384 public part of ECC key pair used for Key Storage, managed by PIV Card application Crypto Officer to store keys history.

Table 12 – PIV Applet 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 deselection (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-SDEK), is stored in plaintext and is only accessible by authenticated services.

Table 13 lists all operator roles supported by the Module.

Role ID	Role Description
CO	Cryptographic Officer - Role that manages Module content and configuration, including issuance and management of Module data via the ISD authenticated as described in *Secure Channel Protocol Authentication* below.
CAA	The PIV Card Application Administrator (CAA) role represents an external application requesting the services offered by the PIV Applet. An applet authenticates the Application Operator role by verifying possession of the Application External Authenticate TRIPLE-DES or AES key
CH	The PIV Card Holder (CH) role is responsible for ensuring the ownership of his CM, and for not communicating his PIN to other parties. The PIV Applet authenticates the Card Holder by verifying the PIN value.
CHII	The PIV Card Holder II (CHII) role is responsible for unblocking and/or changing the Card Holder PIN. The PIV authenticates the Card Holder II by verifying the PUK value.
UA	Unauthenticated role

Table 13 - Roles Supported by the Module

3.1 Secure Channel Protocol Authentication Method (CO)

The Secure Channel Protocol authentication method is provided by the *Secure Channel (Initialize Update, External Authenticate)* 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 255 failed SCP authentication attempts. The probability that a random attempt will succeed over a one minute interval is:

- 255/2^128 = 7.5E-37 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

3.2 PIV Application Administrator Authentication (CAA)

a) **The 3-Key Triple-DES** authentication provides 112 bits of security strength. The Module uses the PIV-AUTH-TDES to authenticate the CAA role.

- The probability that a random attempt at authentication will succeed is 1/2^64, assuming a 64-bit block length
- Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^64

b) **The AES** authentication provides 128/192/256 bits of security strength. The Module uses the PIV-AUTH-AES to authenticate the CAA role.

- The probability that a random attempt at authentication will succeed is 1/2^128 (for 128-bit length)
- Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^128

3.3 PIV Card Holders (CH & CHII)

a) **PIN Verification (CH)** This authentication method compares a PIN value sent to the Module to the stored PIN (or Global PIN) values. If the two values are equal, the Card Holder is authenticated. This method is used in the PIV Applet services to authenticate the CH role.

The module enforces string length of 6 bytes minimum (8 bytes maximum). The format supported is numerical (i.e. 0-9). The strength of this authentication method is as follows:

- The probability that a random attempt at authentication will succeed is 1/10^6
- Based on a maximum count of 3 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is lower than 3/10^6

b) **PUK Verification (CHII)** This authentication method compares a PUK value sent to the Module to the stored PUK value if the two values are equal, the Card Holder II is authenticated. This method is used in the PIV Applet services to authenticate the CHII role, and allows CHII to unblock and/or change the Card Holder PIN.

The module enforces string length of 8 bytes. The format supported is hexadecimal, meaning that all byte value from 00h to FFh are supported. Then the strength of this authentication method is as follow:

- The probability that a random attempt at authentication will succeed is lower than1/256^8
- Based on a maximum count of 15 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is lower than 15/256^8

3.4 Platform Services

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

Service	Description
Card Reset (Self-test)	Power cycle the Module by removing and reinserting it into the contact reader slot, or by reader assertion of the RST signal. The *Card Reset* service will invoke the power on self-tests described in Section §3. RAM is cleared on power cycle
EXTERNAL AUTHENTICATE	Secure channel protocol authentication method: Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. Uses SD-SENC and SD-SMAC.
INITIALIZE UPDATE	Secure channel protocol authentication method: Initializes the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. Uses the SD-KENC and SD-KMAC master keys to derive the SD-SENC and SD-SMAC session keys, respectively.
GET DATA	Retrieve a single data object. Optionally uses SD-SENC, SD-SMAC (SCP).
MANAGE CHANNEL	Open and close supplementary logical channels. Optionally uses SD-SENC, SD-SMAC (SCP).
SELECT	Select an applet. Does not use CSPs.

Table 14 - Unauthenticated Platform Services

Service	Description	CO
DELETE	Delete an applet from EEPROM. This service is provided for the situation where an applet exists on the card, and does not impact platform CSPs. Optionally uses SD-SENC, SD-SMAC (SCP).	X
GET STATUS	Retrieve information about the card. Does not use CSPs. Optionally uses SD-SENC, SD-SMAC (SCP).	X
INSTALL	Perform Card Content management. Optionally uses SD-SENC, SD-SMAC (SCP). Optionally, the Module uses the DAP-SYM key to verify the package signature.	X
LOAD	Load a load file (e.g. an applet). Optionally uses SD-SENC, SD-SMAC (SCP).	X
PUT DATA	Transfer data to an application during command processing. Optionally uses SD-SENC, SD-SMAC (SCP).	X
PUT KEY	Load Card Manager keys The Module uses the SD-KDEK key to decrypt the keys to be loaded. Optionally uses SD-SENC, SD-SMAC (SCP).	X
SET STATUS	Modify the card or applet life cycle status. Optionally uses SD-SENC, SD-SMAC (SCP).	X

Service	Description	CO
STORE DATA	Transfer data to an application or the security domain (ISD) processing the command. Optionally, updates OS-GLOBALPIN. Optionally uses SD-SENC, SD-SMAC (SCP).	X
GET MEMORY SPACE	Monitor the memory space available on the card. Optionally uses SD-SENC, SD-SMAC (SCP).	X
SET ATR	Change the card ATR. Optionally uses SD-SENC, SD-SMAC (SCP).	X

Table 15 – Authenticated Platform Services by Role

Service	OS-DRBG-EI-KEY	OS-DRBG-STATE	OS-GLOBALPIN	OS-MKDK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-SDEK	DAP-SYM
Card Reset	ZEW	ZEGW	--	--	--	--	--	Z	Z	Z	--
Get Data (Unauth)	--	--		--	--	--	--	E[1]	E[1]	E[1]	--
Select, Manage Channel	--	--		--	--	--	--	Z	Z	Z	--
Secure Channel: initialize update + external authenticate	--	EW		--	E	E	E	GE[1]	GE[1]	GE[1]	--
Manage Content: load, install, delete, Put data, Store data, Put key	--	--	W	--	W	W	W	E[1]	E[1]	E[1]	EW
Lifecycle: Set status	Z	Z	Z	Z	Z	Z	-Z-	--	--	--	Z
Module Info (Auth): Get Status	--	--	--	--	--	--	--	E[1]	E[1]	E[1]	

Table 16 – Platform CSP Access 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.

[1] "E" for Secure Channel keys is included for situations where a Secure Channel has been established and all traffic is received encrypted. The Secure Channel establishment includes authentication to the module.

3.5 PIV Services

All services implemented by the PIV applet are listed in the table below.

Service	Description	CAA	CH	CHII	UA
SELECT	Selects a DF or an EF by its file ID, path or name (in the case of DFs).	X	X	X	X
GENERAL AUTHENTICATE	Performs INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE.	X			
CHANGE REFERENCE DATA	Changes the value of a PIN. (Note : User Auth is always done within the command itself by providing previous PIN) Secure Messaging is enforced for this command.		X		
RESET RETRY COUNTER	Unblocks and changes the value of a PIN Secure Messaging is enforced for this command.	X		X	
PUT DATA	Creates, updates or deletes an object value in the data model.	X			
GET DATA	Retrieves the data content of the single data object whose tag is given in the data field.	X	X	X	X
GENERATE ASYMMETRIC KEY PAIR	Generates an RSA or ECDSA Asymmetric Key Pair	X			
VERIFY	Authenticates the user (CH) to the card by presenting the User PIN. The User Authenticated status is granted with a successful PIN verification.		X		

Table 17 – PIV Applet Services by Role

CSPs																
Service	**PIV-Local PIN**	**PIV-Global PIN**	**PIV-PUK**	**PIV-AUTH-TDES**	**PIV-AUTH-AES**	**PIV-AUTH_CH-AES**	**PIV-AUTH-RSA**	**PIV-AUTH-ECC**	**PIV-AS-RSA**	**PIV-AS-ECC**	**PIV-AKM-RSA**	**PIV-AKM-ECC**	**PIV-AUTH_CH-RSA**	**PIV-AUTH_CH-ECC**	**PIV-KS-RSA**	**PIV-KS-ECC**
Verify	EW	EW	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Change reference data	EWZ	EWZ	EWZ	--	--	--	--	--	--	--	--	--	--	--	--	--
Reset retry counter	W	W	--	--	--	--	--	--	--	--	--	--	--	--	--	--
General authenticate	--	--	--	E	E	E	E	E	E	E	E	E	E	E	E	E
Put data	--	--	--	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ
Generate asymmetric key pair	--	--	--	--	--	--	G	G	G	G	G	G	G	G	G	G
Get data	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Select	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Table 18 – PIV applet CSP Access 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.
- -- = Not accessed by the service.

4. Self-test

4.1 Power-on Self-test

On power on or reset, the *Module* performs self-tests described in Table 18. All KATs must be completed successfully prior to any other use of cryptography by the *Module*. If one of the KATs fails, the *Module* enters the *Card Is Mute* error state.

Test Target	Description
FW Integrity	16 bit CRC performed over all code located in EEPROM. This integrity test is not required or performed for code stored in masked ROM code memory.
DRBG	Performs SP800-90A Health tests with fixed inputs, inclusive of KAT
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key TDEA in ECB mode.
AES	Performs decrypt KAT using an AES 128 key in ECB mode. AES encrypt is self-tested as an embedded algorithm of AES-CMAC.
AES-CMAC	Performs an AES-CMAC Generate KAT using an AES 128 key. Note that AES-CMAC Verify is identical to a Generate KAT (perform Generate then compare to the input) hence a single KAT verifies both functions.
RSA	Performs separate RSA PKCS#1 signature and verification KATs using an RSA 2048 bit key.
RSA CRT	Performs RSA PKCS#1 signature KAT using an RSA 2048 bit key. RSA CRT signature verification is tested as part of the RSA signature verification KAT as described above.
ECDSA	Performs separate ECDSA signature and verification KATs using P-224.
ECC CDH	Performs a KAT for ECC CDH using P-224 keys constituents.
SHA-1, SHA-2	Performs separate KATs for SHA-1, SHA-256 and SHA-512.

Table 19 – Power-On Self-Test

4.2 Conditional Self-tests

On every call to the [SP800-90A] CTR DBRG, the *Module* performs a stuck fault test to assure that the output is different than the previous value.

When RSA or ECDSA key pair is generated the Module performs a pairwise consistency test.

When new firmware is loaded into the Module using the *Manage Content* service, the Module verifies the integrity of the new firmware (applet) using MAC verification with the SD-MAC key. Optionally, the Module may also verify a signature of the new firmware (applet) using the DAP-SYM key; the signature block in this scenario is generated by an external entity using the private key corresponding to the symmetric key DAP-SYM.

5. Physical Security Policy

The *Module* is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques.

The *Module* is designed to be mounted in a plastic smartcard or similar package; physical inspection of the epoxy side of the Module is not practical after mounting. The *Module* also provides a key to protect the *Module* from tamper during transport. and the additional physical protections listed in Section 7 below.

6. 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.

7. 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.

8. Mitigation of Other Attacks Policy

The *Module* implements defenses against:

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

9. 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 Mo*d*ule.

At the time the card is issued, **the PIV Applet** shall be personalized with the appropriate data. Personalization includes PIV keys and PIN values. Personalization may be performed using a secure channel (ciphered) or in plaintext, as required by the operator.

The following rules must be observed for conformance to SP800-73-4, FIPS 201-2 and FIPS 140-2:

- The PIN shall be at least 6 bytes composed of numeric characters.
- The PUK shall be 8 bytes, composed of hexadecimal characters in the range of [00h-FFh].
- The Key lengths shall be in the approved table (see section 2 - Table 7).

END OF DOCUMENT