PKI BLADE Applet and

Protiva PIV DL Card

Security Policy

TITLE	**PKI BLADE Applet and Protiva PIV DL Card - Security Policy**
REF.	**TBD – 0.9**
DATE:	**26 April, 2011**

TABLE OF CONTENTS

References

[1] FIPS PUB 140-2 – Federal Information Processing Standard Publication – Security requirements for cryptographic modules – 2001, May the 25th, with change notice (12-03-2002).

[2] Derived Tests Requirements for FIPS PUB 140-2 - Federal Information Processing Standard Publication – Security requirements for cryptographic modules – 2004, March the 24th.

[3] NIST Web site, http://www.nist.gov

[4] Global Platform – Release 2.1.1

[5] Visa Global Platform – Release 2.1.1

[6] Java Card API Specification – (SUN) – Release 2.2.1

[7] Java Card Runtime Environment (JCRE) Specification (SUN) – 2.2.1

[8] Java Card Virtual Machine (VM) Specification – SUN – Release 2.2.1

[9] RSA PKCS#1: RSA Cryptographic Standard (RSA Laboratories) – 2.1

[10] ISO 7816 parts 1-6 (ISO / IEC)

[11] ISO X9.31

[12] ISO 14443 RF Interface (ISO / IEC)

[13] NIST Special Publication 800-73-2 Interfaces for Personal Identity Verification –Part 2: End-Point PIV Card Application Card Command Interface September 2008

[14] NIST Special Publication 800-73-2Interfaces for Personal Identity Verification –Part 1: End-Point PIV Card Application, Namespace, Data Model and Representation September 2008

1 Scope

This Security Policy specifies the security rules under which the PKI BLADE Applet and Protiva PIV DL Card, herein identified as the **Cryptographic Module or CM** must operate. These rules are derived from the security requirements of **FIPS 140-2 standard [1]**, from GEMALTO experience in embedded security software and from US Department of State security requirements.

These rules define the interrelationships between the:

- Module users and administrators,
- Module services,
- Critical Security Parameters.

The commercial name of the product is:

PKI BLADE Applet and Protiva PIV DL Card

Where:

- Protiva PIV DL card is a product including:
  - Java platform available in one memory configuration: the Dual Large (DL) 144K configuration. The platform may also be referred as “Protiva TPC DL” in this document.
  - Protiva PIV Applet 1.55 loaded on the Java Card platform “Protiva TPC DL”. This applet may also be referred as “PIV Applet” in this document.
- PKI BLADE Applet is an applet loaded on the Java Card platform.

2 Introduction

2.1 GEMALTO Smart Card Overview

GEMALTO aims to provide **FIPS140-2 Level 2** cryptographic smart cards. Together, the card and applets provide authentication, encryption, and digital signature cryptographic services. The present document is dedicated and focused on the security policy for the CM in its entirety, specifying the security rules under which all elements within the scope of the CM operate.

2.2 GEMALTO Smart Card Open Platform

The CM is a state of the art Java Open Platform-based smart card. This highly secure platform benefits from all the GEMALTO expertise in Java Card security, from the latest developments in cryptographic resistance against known attacks, and provides FIPS approved cryptographic algorithms and self-tests. Additional software countermeasures have also been added by GEMALTO.

All cryptographic functionality is implemented by the card platform. Applets such as the PIV Applet or PKI BLADE Applet perform applet specific services, calling the card platform to invoke the approved security functions as required. The platform ensures on-card applets safe coexistence thanks to its secure Virtual Machine (VM) and firewall. The Java VM is fully compliant with the **Java Card standard[8]**.

The card life cycle is managed according to the **Global Platform (GP) specification**. Issued cards have been loaded with a set of applets, cryptographic keys and PINs, and are moreover in the "SECURED" state. The security implementation is fully compliant with the **Global Platform (GP) specification**.

The CM integrates symmetric and asymmetric cryptographic algorithms as specified in the **JavaCard specification [6]** and offers RSA for Signature/Verification, SHA-1 hashing, on-board RSA Key generation, Triple-DES CBC and ECB and AES ECB and CBC algorithms.

2.3 Security Level

The product meets the overall requirements applicable to **FIPS140-2 Level 2**. The individual security requirements meet the level specifications as follows.

Security Requirements Section	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 1 – FIPS 140-2 Security Levels

2.4 PIV Applet

The PIV Applet is conformant to SP 800-73-2, Certificate #22 on the NPIVP website. The PIV Applet supports:

- All optional containers defined in SP 800-73-2
- Local PIN verification only
- 3 Key Triple-DES for card administrator authentication and card authentication
- RSA 1024 / 2048 key generation, PIV card authentication, key unwrap and signature

2.5 PKI BLADE Applet

The PKI Blade applet, designed for use on JavaCard 2.2.1 and Global Platform 2.1.1 compliant smart cards, provides security for stored user data and credentials and an easy to use interface to PKI services.

The PKI BLADE applet features:

- Multi-application secure storage and retrieval of objects and digital credentials.
- Authentication of the PKI BLADE User and the PKI BLADE Applet security officer
  - Supports PIN based authentication and / or on-token fingerprint authentication using the Precise BioMatch MOC algorithms.
- Execution of native platform cryptographic services integrated with managed objects:
  - 2 key Triple-DES encryption and decryption.
  - SHA1 secure hashing generation.
  - RSA 1024 / 2048 key unwrap and signature.

3 Cryptographic Module Specification

3.1 GEMALTO Crypto-Module Cryptographic Boundary

The Cryptographic Boundary is defined to be the 'ICC micro-module edge' of the **CM,** comprising a set of "embedded" hardware and firmware that implements cryptographic functions and processes, including cryptographic algorithms, key generation and applications services. The FIPS 140-2 embodiment of the **CM** is single chip. The micro-module is designed to be embedded in a plastic card body to provide an **ISO-7816 [10]** compliant smart card.

The CM provides dual interfaces (i.e. contact and contactless) where the same security level is achieved. The card is designed in the following configurations:

Protiva PIV DL Card identification:
The Protiva PIV DL (Dual Large memory) is based on **P5CD144** chip from NXP**.**
The hardware version: A1047808

The Firmware version for PKI BLADE Applet and Protiva PIV DL Card: EI08-M1004069, Softmask V01, PIV Applet V1.55, and PKI BLADE Applet V1.2.

The CM is a dual interface card providing both contact and contactless interfaces.
It is identified by three historical bytes that are present in ATS (TH8, TH9, TH10) and ATR (T6, T7, T8) having same respective values. These three bytes should be:

- 83h 11h 11h : for the configuration where RSA is supported in contactless mode
- 83h 11h 10h : for the configuration where RSA is not supported in contactless mode

Depending on the market and the end-customer requirements, either contact or contactless interfaces can be disabled during manufacturing. Moreover, for the contactless interface, Public Key (PK) support (i.e. PK enabled or PK disabled) can be also configured during the manufacturing depending on market and the end-customer requirements. This results in two configurations described below. Both configurations were FIPS 140-2 tested.

- **CONFIGURATION 1**: The product is initialized in dual interface mode; it means that both contact and contactless mode are supported, with RSA algorithm and corresponding self-test enabled in both contact and contactless modes.
- **CONFIGURATION 2**: The product is initialized in dual interface mode; it means that both contact and contactless mode are supported, with RSA algorithm and corresponding self-test enabled in contact mode and with RSA algorithm and corresponding self-test disabled in contactless mode.

During the GEMALTO manufacturing process, the chip (ICC) is wire-bonded on the inner side of a contact plate, then globe-topped with resin. **The resulting Micro-Module meets the physical security requirements of FIPS 140-2 Level 3.**

The figure below depicts all components within the cryptographic module boundary:

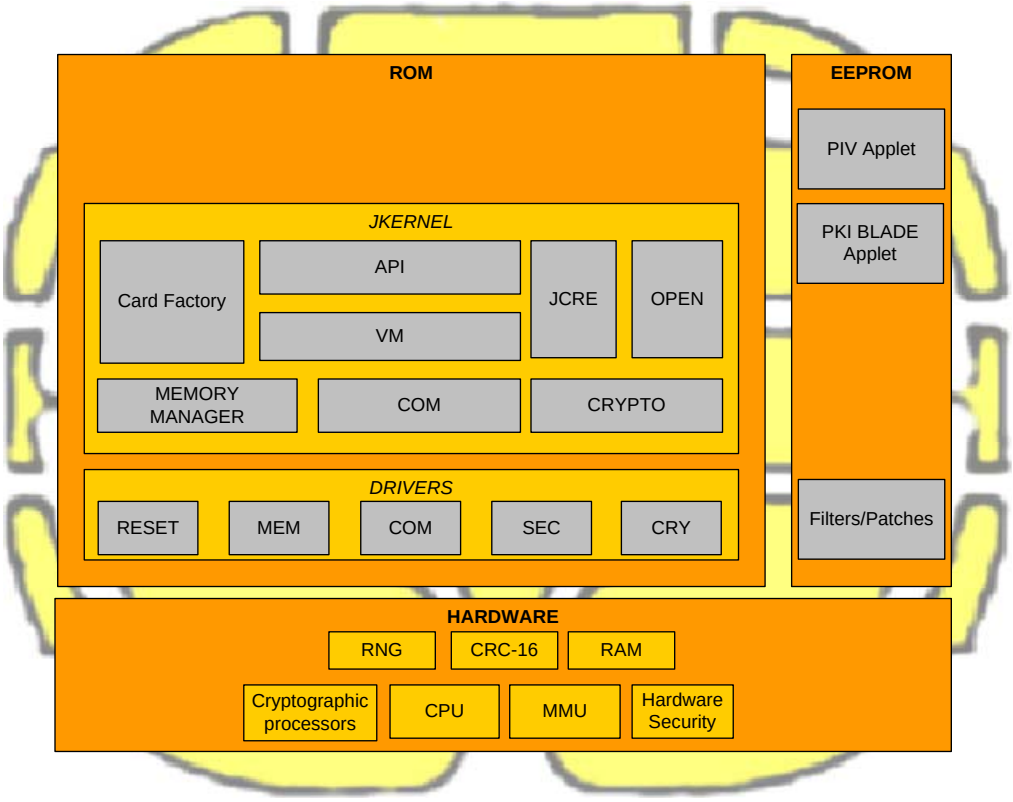

Figure 1 - Cryptographic Module Boundary

3.2 Language level

The CM operational environment is implemented using a high level language. A limited number of software modules have been written in assembler to optimize speed or size.

The PIV Applet and the PKI BLADE Applet are Java applets designed for the Java Card environment.

3.3 FIPS Approved and Allowed Security Functions

The following table gives the list of FIPS Approved security functions implemented by the **CM**.

SECURITY FUNCTION	DETAILS	FIPS APPROVED
Triple-DES	ECB mode in encryption	Cert. # 678
	ECB mode in decryption	
	CBC mode in encryption	
	CBC mode in decryption	
Triple-DES MAC	ECB and CBC modes	Cert. # 678 Vendor Affirmed
SHA-1	Hashing operation	Cert. # 786
RSA	Key generation following X9.31	Cert. # 372
	Signature following PKCS#1with SHA-1 hashing	
	Verification following PKCS#1with SHA-1 hashing	
P-RNG	Pseudo Random Number Generation	Cert. # 450
AES*	ECB mode in encryption	Cert. #782
	ECB mode in decryption	
	CBC mode in encryption	
	CBC mode in decryption	

Table 2 – FIPS Approved Security Functions

Triple-DES implements both 2Key and 3Key. The use of two-key Triple-DES for encryption is restricted: the total number of blocks of data encrypted with the same cryptographic key shall not be greater than 2^20. For the Card Manager, the design and implementation implement this restriction. For the PKI BLADE Applet, the CM must be configured and used in accordance with the guidelines given in Section 12 to operate in FIPS mode.

*The AES algorithm is uncallable functionality in the CM, available for future use. No service in the CM under validation uses AES.

The CM also implements the following Allowed algorithm:

- Triple-DES (Cert. #678, key wrapping; key establishment methodology provides 100 bits of encryption strength)

4 Cryptographic Module Ports and Interfaces

The **CM** restricts all information flow and physical access. Physical and logical interfaces define all entry and exit points to and from the micro module. The CM is intended to be used with ISO 7816 contact and ISO 14443 contactless readers external to the cryptographic boundary.

4.1 Physical Port – Contact mode

4.1.1 Contact assignments and dimensions:

Protiva PIV DL Card follows the standards **"ISO 7816-1 Physical characteristics" [10]** and **"ISO 7816-2 Dimensions and contact location" [10]**.

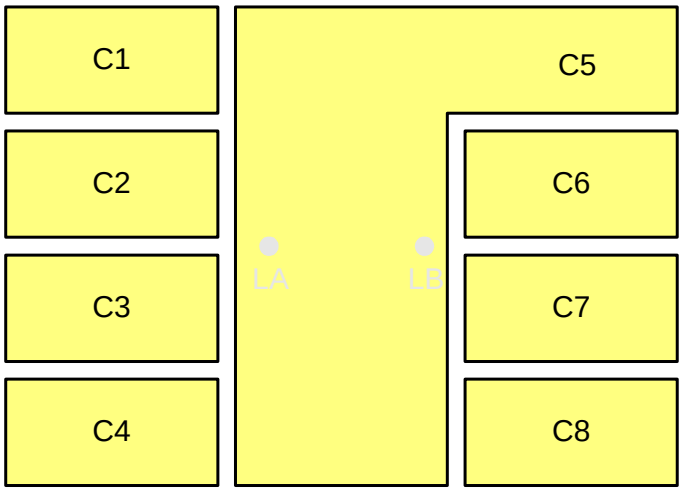

Figure 2 - Contact Plate

Contact No.	Assignments	Contact No.	Assignments
C1	VCC (Supply voltage)	C5	GND (Ground)
C2	RST (Reset signal)	C6	Not connected
C3	CLK (Clock signal)	C7	I/O (Data Input/Output)
C4	Not connected	C8	Not connected

Table 3 - Contact Connections

4.1.2 Conditions of use

The electrical signals and transmission protocols follow the **ISO 7816-3 [10]**. The conditions of use are the following:

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

Table 4 - Voltage and frequency ranges

4.2 Physical Port – Contactless mode

4.2.1 Contacts assignments

In the contactless mode the **CM** follows the standard **"ISO 14443 RF Interface" [12]** and only uses two connections that are physically different and distinct from the connections used in the contact mode. Those electrical connections, LA and LB, are placed on the module backside and are used to connect an external **antenna loop that is not within the cryptographic boundaries of the module.**

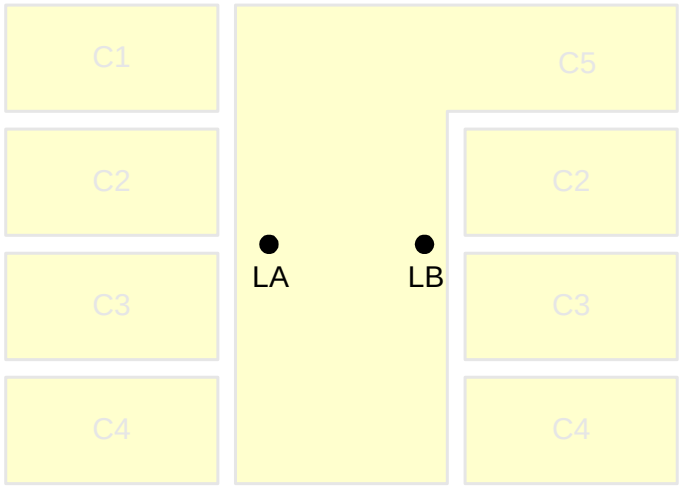

Figure 3 - Antenna Connections (Contactless)

Contact No.	Assignments	Contact No.	Assignments
LA	Antenna coil connection	LB	Antenna coil connection

Table 5- Antenna Connections (Contactless)

4.2.2 Condition of uses

The radio frequencies and transmission protocols follow **"ISO 14443 RF Interface" [12].** The conditions of use are the following:

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

Table 6 - Voltage and frequency ranges

4.2.3 CM Physical Encapsulation and External Connections

The figure below depicts the World Combi Thermal black resin process and the external connections made to the CM.

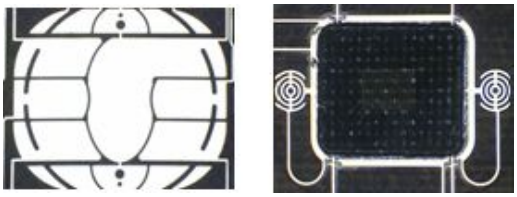

Figure 4 - CM Physical Encapsulation and External Connections

4.3 Logical Interface

The **Protiva TPC DL** platform provides services to both external devices and internal applets as the PKI BLADE Applet and the PIV and Card Manager applets.

External devices have access to services by sending APDU commands while internal applets such as the PIV Applet and PKI BLADE Applet have access to services through internal API entry points.

The CM provides an execution **sandbox for the PIV Applet and PKI BLADE Applet** and performs the requested services according to its roles and services security policy.

For security reasons, the **CM** inhibits all data output via the data output interface when an error state is reached and during self-tests.

5 Roles, Services and Authentication

This section specifies the roles, security rules, services, and CSPs of the CM. The Identification and Authentication Policy, and the Access Control Policy define the interrelationships between roles, identities, through the services and security rules.

The services that are provided by the CM are listed in the subsection labeled "SERVICES" in the Access Control Policy description.

5.1 Identification and Authentication Policy

5.1.1 Identity-based authentication policy

The module performs identity-based authentication using PIN and cryptographic keys. A unique index value is associated with the PIN or the cryptographic key to uniquely identify the off-card entity performing the authentication. The following table describes the roles associated to the CM:

Role ID	Description
CO	The Cryptographic Officer (CO) role is responsible for managing the security configuration of the card manager and security domains. The CO role authenticates to the CM by demonstrating to the Card Manager or PIV application knowledge of a GP secure channel TRIPLE-DES key set stored within the Card Manager. By successfully executing the GP secure channel mutual authentication protocol, the CO role establishes a secure channel to the Card Manager and execute services allowed to the CO role in a secure manner.
CAA	The PIV Card Application Administrator (CAA) role represents an external application requesting the services offered by the PIV Applet. An applet authenticates the CAA role by verifying possession of the Application External Authenticate (XAUT) TRIPLE-DES key
CH	The 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 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 PIN value.
PBU	The PKI BLADE User, authenticated by the PKI BLADE applet – see below for authentication mechanism.
PBSO	The PKI BLADE Security Officer (applet administrator), authenticated by the PKI BLADE applet – see below for authentication mechanism.

Table 7 - Role profile definitions

The CM does not implement a maintenance mode or role.

5.1.2 Mechanism Interfaces

The following tables describe the mechanisms for authentication of the roles:

Interface	Description
INITIALIZE UPDATE *APDU*	This APDU command initiates the setting up of a secure channel. The card generates the session keys and exchanges data with the host. Used in CO role authentication.
EXTERNAL AUTHENTICATE *APDU*	This APDU command is used by the card to authenticate the host and to determine the level of security required for all subsequent commands. A previous and successful execution of the INITIALIZE UPDATE command is necessary prior to processing this command. Used in CO role authentication.

Table 8 - Mechanism interfaces in personalization and applicative phase

Interface	Description
GENERAL AUTHENTICATE *APDU*	When used for PIV Applet CAA role authentication. The APDU command is used to perform a cryptographic operation such as an authentication protocol using the data provided in the data field of the command and returns the result of the cryptographic operation in the response data field. The GENERAL AUTHENTICATE command shall be used to authenticate the card or a card application to the client application (INTERNAL AUTHENTICATE), to authenticate an entity to the card (EXTERNAL AUTHENTICATE), and to perform a mutual authentication between the card and an entity external to the card (MUTUAL AUTHENTICATE). The GENERAL AUTHENTICATE command shall be used to realize the signing functionality on the PIV client-application programming interface.
VERIFY *APDU*	When used for PIV Applet CH and CHII role authentication. This APDU command initiates the comparison in the card of the reference data with data field of the command. The referenced PIN must be successfully verified

Table 9 - Mechanism interfaces in applicative phase

5.1.3 Security rules

The following table presents the security rules applied to these mechanisms:

Rule Identifier	Description
ia_pin_rule.1	It is not possible to get authenticated through the PIN authentication mechanism if the authorized number of successive unsuccessful attempts is reached.
ia_pin_rule.2	It is not possible to get authenticated through the PIN authentication mechanism if the referenced PIN is not found
ia_pin_rule.3	It is not possible to get authenticated through the PIN authentication mechanism if the submitted PIN is incorrect
ia_pin_rule.4	The pin must be re-authenticated if the card is reset
ia_pin_rule.5	The pin must be re-authenticated if a new application is selected on the same channel
ia_pin_rule.6	The pin remains active if another application is selected on another channel
ia_pin_rule.7	The PIN length must be 8 characters.
ia_co_rule.1	The Cryptographic Officer must be re-authenticated if the card is reset.
ia_co_rule.2	The Cryptographic Officer must be re-authenticated if the CM detects a secure messaging corruption.

Table 10 - Security rules

5.1.4 Strength of Platform Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
GP mutual authentication (CO Role authentication)	$1/2^{100}$
	The cryptogram sent is 8 bytes long and 2-Key Triple-DES is used. Strength is as described in SP 800-131A.
PIN verification (CH, CHII authentication)	$1/256^{8}$
	Pin verification is the responsibility of the PIV Applet that defines and maintains its own security policy regarding the PIN but uses the PIN management services provided by the platform. This authentication strength is the native strength implemented by the module. PIV identity systems external to the module impose further constraints on character set and length. Please see Section 12 for guidance.
Symmetric key External Authentication (CAA role authentication)	$1/2^{112}$
	CAA authentication is the responsibility of the PIV Applet using External Authenticate option of the GENERAL AUTHENTICATE command that involves verifying decryption of an 8-byte challenge using the secret 3-Key Triple-DES key. Strength for 3-Key Triple-DES is as described in SP 800-57.
PKI BLADE PIN verification (PBU, PBSO Authentication)	$1/255^{6}$
	See PKI BLADE PIN Authentication Mechanism and Authentication Strength.
PKI BLADE Biometric verification (PBU, PBSO Authentication)	$< 1/10^{6}$
	See PKI BLADE Biometric Authentication Mechanism and Strength below.

Table 11 – Strength of Platform Authentication Mechanisms

5.1.5 PKI BLADE Authentication Options

The enrollment station tools used to configure the PKI BLADE applet use the term Biometric, or Bio; the PKI BLADE Applet offers only the Fingerprint biometric. The terms Fingerprints, Biometric and Bio are equivalent.

The PKI BLADE Applet may be configured to authenticate in any of the following combinations:

- PIN only
- Bio only
- Bio-or-PIN – authentication strength is equivalent to Bio only
- Bio-and-PIN – authentication strength is greater than or equal to PIN only

See Section 12 for PKI BLADE Applet configuration and usage rules.

5.1.6 PKI BLADE PIN Authentication Mechanism and Authentication Strength

The PKI BLADE Applet Master File (MF) contains a User PIN and PBSO PIN file, and each Directory File (DF) can contain its own User PIN and SO PIN file. The appropriate MF or DF must be selected first prior to executing either VERIFY or CHANGE_REFERENCE_DATA command.

Each PIN instance has an associated non-volatile memory retry counter, with an initial value determined by a Configuration Data file value. A successful VERIFY resets the retry counter. Unsuccessful VERIFY or CHANGE_REFERENCE_DATA attempts decrement the associated retry count; the value persists across sessions. Exhausting the retry count disables the corresponding PIN and puts the applet in the Error state.

If allowed by the Configuration Data file, an authenticated SO may update the User PIN using the CHANGE REFERENCE DATA command in order to re-enable the User PIN and reset the associated retry counter. A limited number (default 10) of unsuccessful CHANGE_REFERENCE_DATA attempts are permitted.

SO PIN exhaustion results in either reversion of the associated PIN to the Backup SO PIN value, or reset of the SO PIN to an uninitialized state, based on a Configuration Data file setting.

Authentication strength for PIN authentication to the module is 1/255^6, (omitting the padding character in the input string, and with applet enforcement of a 6 byte minimum PIN), meeting the FIPS minimum requirement of 1/10^6. The number of failed attempts possible in one minute is 15/255^6, (based on a maximum of 15 retries) meeting the FIPs minimum requirement of 1/10^5.

The SO PIN can be reset to the default SO PIN by issuing the RECYCLE command.

5.1.7 PKI BLADE Biometric Authentication Mechanism and Strength

Prior to enrollment, the enrollment tools have been provided to authorized users and have been configured according to agency policies.

The strength of the biometric authentication is determined by the settings applied to the biometric algorithm by the enrollment software. The biometric algorithm provider has provided a Receiver Operating Curve (ROC) characteristic curve, achieved through a large statistical sampling process, for the algorithm for use with enrollment station configuration.

The operator must select the 1/1,000,000 FAR setting when the *Bio Only* or Bio-or-PIN settings are used. This setting achieves an authentication strength of just less than 1/10^6 as required by FIPS 140-2.If used as a second factor to the PIN (*Bio–and-PIN*), authentication strength is met by the PIN, and the FAR may be set to a lower level as determined by the operator.

The number of allowed bad fingerprint authentication attempts is set when the fingerprint template is enrolled on the smart card. The count of bad fingerprint authentication attempts is kept internally on the applet, independent of the PIN retry counters. It is incremented with every bad fingerprint logon attempt, regardless of which fingerprint is used. Switching fingers does not clear the count. The count of bad fingerprint authentication attempts is cleared with every successful fingerprint logon.

When the internal count of bad fingerprint authentication attempts exceeds the maximum value set at enrollment, logon via the fingerprint template is locked. Once locked, no fingerprint can be used to log on until a new fingerprint template is enrolled onto the smart card.

A flag can be set during enrollment to lock this parameter. If locked, the maximum bad fingerprint limit is fixed and cannot be changed during future enrollments. Once the lock flag is set, it cannot be cleared during re-enrollment.

See Section 12 for PKI BLADE Applet configuration and usage rules.

5.2 Access Control Policy

5.2.1 Introduction

This chapter is dedicated to access control security rules. Some services provided by the CM are subject to privileges. Privileges can be obtained by construction (for example at applet initialization) or by being identified as a privileged user.

List of the security related process or mechanisms specified for the PIV Applet during the applicative life cycle:

- **Secure messaging**: It is possible to open a secure channel during the personalization phase of the applet (between the personalization device and the card, when the applet is in the SELECTABLE state) by using the security domain of the java platform. Opening of this secure channel is necessary to perform the initial personalization (pre-personalization) of the PIV Applet. Once this initial PIV Applet pre-personalization is completed, the applet is in Application mode.
  In Application mode opening of a secure channel is optional. A secure channel may be part of access conditions to a particular object in which case it becomes necessary to access that object.

- **Access Conditions:** Each object stored in the card embeds its own access conditions. These conditions defines the minimum security required to access the object. As the access to the object is done through a command, a security condition is defined for each command accessing the object.

An **Access Rule** is encoded with an **Access Mode byte**, followed by one or more **Security Condition bytes.** The PIV Data objects Access management rules:

- **Free (always)**: No access condition.
- **Never**: No execution possible.
- **PIN**: The referenced PIN must be successfully verified. This flag is set until an incorrect PIN verification or an application selection or a reset.
- **PIN Always**: The referenced PIN must be successfully verified by the previous command.
- **Authentication**: The external authentication (using general authenticate command) must have been successfully performed with the referenced key. The authentication flag is set until a new successful authentication, an application selection or a reset.
- **Secure Channel (SM)**: A Secure Channel in MAC+ Encrypt mode must be opened.

Secure Messaging During Personalization phase :

- The Card Manager through the API used by PIV personalization provides the secure messaging.
  In a GP 2.1.1 card, the secure messaging is initiated after a mutual authentication. It means that **INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands have been successfully executed.**
  The secure channel can have the four following modes:
  - Mutual Authentication required before attempting any command: **AUTHENTICATION**.
  - All commands require a previous Mutual authentication and must be sent with Integrity (and/or Authentication): **MAC** mode.
  - All commands require a previous Mutual authentication and must be in **MAC** & **ENCRYPTION** mode.
- When in application mode only supports MAC & Encrypted mode is possible.

5.3 Services

The access control rules are applied to all of the following services. (The services have been grouped according to the role to which they provide a service.)

When the Card Manager applet is selected the following commands are available :

Interface	Service Description
DELETE – *APDU*	This APDU is used to delete a uniquely identifiable object such as an Executable Load File, an application, optionally an Executable Load File and its related Applications.
EXTERNAL AUTHENTICATE – *APDU*	This APDU command is used by the card to authenticate the host and to determine the level of security required for all subsequent commands. A previous and successful execution of the **INITIALIZE UPDATE** command is necessary prior to processing this command.
GET DATA – *APDU*	This APDU command is used to retrieve a single data object.
GET STATUS – *APDU*	This APDU command is used to retrieve the Card Manager, load file (package), and application life cycle data specific to the GP specification.
INITIALIZE UPDATE – *APDU*	This APDU command initiates the setting up of a secure channel. The card generates the session keys and exchanges data with the host.
INSTALL – *APDU*	This APDU command informs the card of the various steps required to load, install and make an applet selectable within the card.
LOAD – *APDU*	One or more LOAD commands are used to load the bytecode of the load file (package) defined in the previously issued **INSTALL** command to the card.
MANAGE CHANNEL - *APDU*	This command is used to open and close supplementary logical channels.
PUT DATA – *APDU*	This APDU command is used to set the value of the various data elements utilized and managed by the Card Manager (deprecated OP command)
PUT KEY – *APDU*	This APDU is used to: 1. Replace a single or multiple keys within an existing key set version; 2. Replace an existing key set version with a new key version; 3. Add a new key set version containing a single or multiple keys Key value is encrypted.
SELECT – *APDU*	This APDU command is used for selecting an application.
SET STATUS – *APDU*	This APDU command is used to change the state of the Card Manager or to change the life cycle state of an application.
STORE DATA – *APDU*	This APDU command is used to transfer data to an application or the security domain (card manager) processing the command.

Table 12 – System Applet Interfaces and Services

When PIV Applet is selected the following commands are available :

Interface	Service Description
EXTERNAL AUTHENTICATE* – *APDU*	This APDU command is used by the card to authenticate the host and to determine the level of security required for all subsequent commands. A previous and successful execution of the INITIALIZE UPDATE command is necessary prior to processing this command.
INITIALIZE UPDATE* – *APDU*	This APDU command initiates the setting up of a secure channel. The card generates the session keys and exchanges data with the host.
MANAGE CHANNEL - *APDU*	This command is used to open and close supplementary logical channels.
END PERSONALIZATION – *APDU*	The APDU command is used to end the personalization step.
VERIFY* – *APDU*	The APDU is used to initiate the comparison in the card of the reference data indicated with authentication data in the data field of the command.
GET DATA – *APDU*	This APDU command retrieves the data content of the single data object whose tag is given in the data field. The entire object is returned.
GENERAL AUTHENTICATE – *APDU*	The APDU command performs a cryptographic operation such as INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE. The GENERAL AUTHENTICATE command is also used to perform RSA signature (when using the PIV card application digital signature key with the RSA algorithm) and to perform key unwrap (when using the PIV card application key management key with the RSA algorithm).
GENERATE ASYMMETRIC KEY PAIR* – *APDU*	The APDU command initiates the generation and storing in the card of the reference data of an asymmetric key pair, i.e., a public key and a private key. The public key of the generated key pair is returned as the response to the command.
CHANGE REFERENCE DATA* – *APDU*	The APDU command initiates the comparison of the verification data with the current value of the reference data and if this comparison is successful replaces the reference data with new reference data.
RESET RETRY COUNTER* – *APDU*	The APDU command resets the retry counter of the key reference to its initial value and changes the reference data associated with the key reference. The command enables recovery of the PIN card application in the case that the cardholder has forgotten a PIV Card Application PIN. Note : Only retry counters associated with key references specific to the PIV Card Application; i.e. local key references may be reset by the PIV Card Application RESET RETRY COUNTER command [13].
PUT DATA* – *APDU*	During the personalization the APDU command is used to create and/or update Data Objects, PIN, Triple-DES secret keys, RSA private keys & property template.
SELECT – *APDU*	The ADPU command is used to select an application

Table 13 – PIV Applet Interfaces and Services

* APDU not available in contactless mode

When PKI BLADE Applet is selected the following commands are available :

Interface	Service Description
CHANGE_REFERENCE_DATA – Updates the PIN of the given type if the given current PIN is valid for the currently authenticated entity.	
CREATE_FILE – Creates an empty file of the given type.	
CRYPT – Performs Triple DES symmetric key encryption/decryption on the given data.	
DELETE_FILE – Deletes references to a given file. When used with a DF, DELETE_FILE will remove a whole sub-directory and the files it may contain.	
END_SESSION – Ends the current authenticated session, returning the card to the idle state.	
GENERATE_DES_KEY – Generates a 2 Key Triple DES key (DEK)	
GENERATE_PUBLIC_KEY_PAIR – Generates RSA 1024 or 2048 bit key pair (PSK/SVK or KUK/KWK)	
Generate_Random_Number –Creates a random number of the given size, using the Gemalto platform Approved DRNG.	
GETSTATUS – Returns the current status of the card. The remaining file space gives the number of bytes available for creating new files (16-bit number, MSB first). The Configuration Data format is described below.	
PB_CREATE_TEMPLATE – Creates the fingerprint template file on the token, and writes the initialized data to the file.	
PB_GET_PUBLIC_TEMPLATE – Returns the public template data structure from the requested fingerprint template file. The fingerprint template file must have been previously created with the PBCreateTemplate command.	
PB_VERIFY - Performs a match between a private fingerprint template and given fingerprint data.	
PERFORM_SECURITY_OPERATION - Dependent on the P1, P2 and data values, performs RSA key unwrap, or RSA signature operations: • RSA Key unwrap - Decrypts the given ciphertext key with the private KUK in the given file. • RSA Sign - Creates an RSA PKCS #1 v1.5 signature for the given data with the PSK in the given file.	
READ_BINARY - Returns the requested amount of data (at the given offset) from the active file.	
RECYCLE - Deletes all files and zeroes all allocated buffer space (applet zeroization).	
SELECT_FILE - Makes the given file the active file (sets the current file identifier) to be used by subsequent commands. Some commands will operate on the selected file if no file identifier is provided with the command.	
SHA1_DIGEST - Initiates, continues, or completes a SHA-1 hash of the given data.	
VERIFY - Hashes the given PIN and compares the result to the appropriate MF or DF hashed PIN value. successful comparison updates the applet security state for SO or User authentication.	
WRITE_BINARY - Writes the given data (at the given offset) to the active file.	

Table 14 – PKI BLADE Applet Services

Unauthenticated Platform / PIV Applet Services
EXTERNAL AUTHENTICATE
GENERAL AUTHENTICATE
GET DATA (Platform Specific) [1]
GET DATA (PIV Applet Specific)[1]
MANAGE CHANNEL
INITIALIZE UPDATE
SELECT
VERIFY (PIV Applet Specific)
Unauthenticated PKI BLADE Applet Services
GENERATE_RANDOM_NUMBER
GETSTATUS
PB_GET_PUBLIC_TEMPLATE
PB_VERIFY
READ_BINARY (only for files accessible to an unauthenticated operator)
RECYCLE
SELECT_FILE
SHA1_DIGEST
VERIFY (PKI BLADE Applet Specific)
WRITE_BINARY (only for files accessible to an unauthenticated operator)

Table 15 - Unauthenticated Services

Role ID	CO
DELETE	X
END PERSONALIZATION	X
GET STATUS	X
INSTALL	X
LOAD	X
PUT DATA (Platform Specific)	X
PUT KEY	X
SET STATUS	X
STORE DATA	X

Table 16 - CO Authenticated Services

[1] GET DATA does not require any authentication when used for access to containers with the READ ALWAYS security condition.

Role ID	CAA	CH	CHII
CHANGE REFERENCE DATA		X	
GENERAL AUTHENTICATE		X[2]	
GENERATE ASYMMETRIC KEY PAIR	X		
GET DATA (PIV Applet Specific)		X[3]	
PUT DATA (PIV Applet Specific)	X		
RESET RETRY COUNTER			X

Table 17 - CAA, CH, CHII Authenticated Services

Role ID	PBSO	PBU
CHANGE_REFERENCE_DATA	X	X
CREATE_FILE	X	X
CRYPT		X
DELETE_FILE	X	X
END_SESSION	X	X
GENERATE_DES_KEY		X
GENERATE_PUBLIC_KEY_PAIR		X
PB_CREATE_BIO_MATCH_J_TEMPLATE		X
PB_CREATE_TEMPLATE		X
PERFORM_SECURITY_OPERATION		X
READ_BINARY	X	X
WRITE_BINARY	X	X

Table 18 – PBSO, PBU Authenticated Services

5.4 Security rules

The following table presents the security rules applied:

Rule Identifier	Description
ac_co_rule.1	Administrative commands can only be used by the **Cryptographic Officer.**
ac_java_rule.1	**JCRE firewall** checks are enforced by the CM to ensure Java object protection.
ac_life_rule.1	The **Cryptographic Officer** is responsible for locking and terminating the Card Manager life cycle state.
ac_life_rule.2	An **applet** is responsible for managing its own life cycle state, in accordance with the GP specification.
ac_life_rule.3	The **Cryptographic Officer** is responsible for managing the life cycle state of any applet (including system applets), in accordance with the GP specification.

Table 19 - Security rules

[2] GENERAL AUTHENTICATE requires Card Holder authentication when used with PIV Authentication Key (9A), PIV digital Signature Key (9C) or PIV Key Management Key (9D).
[3] GET DATA requires Card Holder authentication when used to obtain containers with the PIN access condition.

5.5 Additional GEMALTO Security Rules

The following rules apply in addition to the FIPS140-2 requirements. The CM:

Rule Identifier	Description
AD_RULE.1	Does not support a multiple concurrent operators.
AD_RULE.2	Does not support a bypass mode.
AD_RULE.3	Does not provide a maintenance role/interface.
AD_RULE.4	Requires re-authentication when changing roles.
AD_RULE.5	Does not allow the loading of Software/Firmware - only applets.

Table 20 - GEMALTO additional security rules

5.6 Platform Critical Security Parameters

The CM uses the following CSPs:

- **Security Domain Key Sets**
- **Secure channel session keysets**
- **Card Holder PIN**
- **Card Holder II PIN (Also known as the PIN Unblocking Key or PUK)**
- **The PIV authentication key**
- **The PIV card application authentication key**
- **The PIV card application digital signature key**
- **The PIV card application key management key**
- **PRNG Seed and seed key**

See Section 9 for additional detail.

The following table defines an association between the services or authentication mechanisms (the interface name is provided) and the CSP they access. The access types are labeled as follows:

- W: write access
- U: the value is not explicitly read, but used within the scope of a comparison or computation process

Interface	CSP	Access type
DELETE	Secure channel session keys	U
EXTERNAL AUTHENTICATE	GP key set of the Card Manager Secure channel session leys	U U
GET STATUS	Secure channel session keys	U
INITIALIZE UPDATE	Secure channel session keys PRNG seed and seed key	U U
INSTALL	Secure channel session keys	U
LOAD	Secure channel session keys	U
PUT DATA	Secure channel session keys PIV card application authentication key PIV card application key management key	U
PUT KEY	GP key set of the Card Manager Secure channel session leys	W U
SET STATUS	Secure channel session keys	U
STORE DATA	Secure channel session keys	U
GENERAL AUTHENTICATE	PIV keys	U
VERIFY	Card Holder PIN	U
RESET RETRY COUNTER	Unblocking PIN (Card Holder II PIN) Card Holder PIN	U W
CHANGE REFERENCE DATA	Card Holder PIN	W U
GENERATE ASYMMETRIC KEY PAIR	PIV keys Card Holder PIN	W U

Table 21 - Platform Critical Security Parameter Usage

5.7 PKI BLADE Applet Critical Security Parameters

All PKI BLADE Applet CSPs, summarized in the table below, are stored in plaintext form in EEPROM. Keys are protected against unauthorized modification, substitution and disclosure by the PKI BLADE applet file access control system. Authenticated Users or the SO may enter or output keys in key files in plaintext form.

CSP	Length and type
SO PIN	6-20 byte data string for PBSO authentication. The reference value is stored hashed by SHA-1 in EEPROM. The PKI BLADE applet requires 1 instance in the MF and allows an additional instance in each possible DF.
Backup SO PIN	6-20 byte data string for PBSO authentication; the Backup SO PIN is an optional copy of the previous SO PIN value. See Section 5.1.6 for additional context. The reference value is stored hashed by SHA-1 in EEPROM. The PKI BLADE applet requires 1 instance in the MF and allows an additional instance in each possible DF.
User PIN	6- 20 byte data string for PBU authentication. The reference value is stored hashed by SHA-1 in EEPROM. The PKI BLADE applet requires 1 instance in the MF and allows an additional instance in each possible DF.
PBDEK	2-Key TDES (112 bit) PKI BLADE Data Encryption Key. The applet allows up to 64 instances, determined by available space and maximum number of files.
PSK	RSA 1024 or 2048 Private Signature Key. The applet allows up to 64 instances, determined by available space and maximum number of files.
PFT	Private portion of fingerprint template. Up to four fingerprint templates per user, stored under the MF or under any DF.
KUK	RSA 1024 or 2048 Key Unwrap Key, used by the PERFORM_SECURITY_OPERATION for RSA key transport. Up to 64 instances, determined by available space and maximum number of files.

Table 22 - PKI BLADE Applet Critical Security Parameters

A key file can be zeroized by issuing the DELETE_FILE command. Additionally, the RECYCLE command can be used to destroy all applet files including all key and PIN files.

Only an authenticated User can generate keys on the card. No internally generated secret or private keys can be read, written or updated. The PKI BLADE Applet uses the Protiva PIV TPC platform services to generate keys:

- 16 byte 2 Key Triple DES (using the Gemalto platform Approved DRNG)
- 1024 or 2048-bit RSA public and private key pairs (using the Gemalto platform Approved RSA key pair generation with conditional test)

The table below lists all services provided by the PKI BLADE Applet, the access control for the function by each PKI BLADE Applet role, and the relationship of each service to each CSP. The services are described further below the table. CSPs are defined in a later section. The PKI BLADE Applet has no access to platform CSPs.

Service	PINs			Bio	Symmetric		Asymmetric	
	SO	User	Backup SO	PFT	PBDEK	IV	PSK	KUK
CHANGE_REFERENCE_DATA	E,W	E, W	W	N	N	N	N	N
CREATE_FILE	N	N	N	N	N	N	N	N
CRYPT	N	N	N	N	E	E,W	N	N
DELETE_FILE	D	D	D	D	D	D	D	D
END_SESSION	N	N	N	N	N	N	N	N
GENERATE_DES_KEY	N	N	N	N	W	N	N	N
GENERATE_PUBLIC_KEY_PAIR	N	N	N	N	N	N	W	W
GENERATE_RANDOM_NUMBER	N	N	N	N	N	N	N	N
GETSTATUS	N	N	N	N	N	N	N	N
PB_CREATE_BIO_MATCH_J_TEMPLATE	N	N	N	W	N	N	N	N
PB_CREATE_TEMPLATE	N	N	N	W	N	N	N	N
PB_GET_PUBLIC_TEMPLATE	N	N	N	N	N	N	N	N
PB_VERIFY	N	N	N	E	N	N	N	N
PERFORM_SECURITY_OPERATION	N	N	N	N	E	E	E	E
READ_BINARY	N	N	N	N	R	R	R	R
RECYCLE	D	D	D	D	D	D	D	D
SELECT_FILE	N	N	N	N	N	N	N	N
SHA1_DIGEST	N	N	N	N	N	N	N	N
VERIFY	E	E	N	N	N	N	N	N
WRITE_BINARY	W	W	W	N	W	W	W	W

Table 23 – PKI BLADE Applet Services, Access Control and Relationship to CSPs

D = Destroy (zeroizes the CSP as a result of command execution)
E = Execute (uses the CSP in the execution of the command)
R = Read (the value of the CSP exits the module as a result of command execution)
W = Write (the value of the CSP is written into the module as a result of command execution)
U = Update
N = No access

5.8 PKI BLADE Applet Public Keys and Data

CSP Name	Length and type
SVK	RSA 1024 or 2048 Public Signature Verification Key (the public key associated with PSK). This public key is an output of key pair generation and is not used by the module.
KWK	RSA 1024 or 2048 Key Wrap Key, used by the PERFORM_SECURITY_OPERATION for RSA key transport. This public key is an output of key pair generation and is not used by the module.
PBFT	Public portion of fingerprint template. Up to four fingerprint templates per user, stored in the MF or any DF.

Table 24 - PKI BLADE Applet Public Keys and Data

5.9 Approved Mode of Operation

To maintain the module in an approved mode of operation, the operator must restrict the usage of the module as follows:

- The operator of the CM retrieves the ATR from the module to validate that the ATR bytes are the same as those listed in Section 3.1.
- The module operates in FIPS mode once the Card is issued and Applets are personalized.
- The module follows all security rules outlined in Section 5 to maintain in FIPS mode.

6 Finite State Model

The **CM** is designed using a finite state machine model that explicitly specifies every operational and error state.

The CM includes Power on/off states, Cryptographic Officer states, User services states, applet loading states, Key/PIN loading states, Self-test states, Error states, and the GP life cycle states.

An additional document (Finite State Machine document) identifies and describes all the states of the module including all corresponding state transitions for both platform and PIV Applet.

PKI BLADE Applet documentation includes the relevant PKI BLADE applet states and transitions.

7 Physical Security

The **CM** is designed to meet the **FIPS 140-2 level 3 Physical Security requirements**.

The manufacturing process consist of wire bonding the ICC over printed circuit plate providing ISO contacts and sealing the chip and wires in a 'glue globe':

- Opaque black epoxy coating polymerized with temperature

Any mechanical attack attempting to extract the chip from the micro-module results in damaging the chip so that it cannot work anymore. Furthermore, attempts to attack the chip or micro-module will result in signs of tampering such as scratches and deformation.

The module is designed for embedding in a plastic card body for Smart Card manufacturing.
Note: the chip is designed in such a way that no data can be collected by visual inspection.

8 Operational Environment

This section does not apply to **CM**. No code modifying the behavior of the CM operating system can be added after its manufacturing process.

Only authorized applets can be loaded at post-issuance under control of the Cryptographic Officer. Their execution is controlled by the CM operating system following its security policy rules.

9 Cryptographic Key Management

9.1 Card Manager Keys

The CM implements **GP[4]** specifications. The card issuer security domain includes key sets for card administration purposes. These key sets are used to establish a secure communication between the Card Manager applet and the Cryptographic Officer.

When the Card Manager is the selected applet, all commands besides those required to set up the secure channel must be performed within a secure channel. The one exception to this rule relates to the GET DATA APDU command that can be issued to the Card Manager without first setting up a secure channel.

The card life cycle state determines which modes are available for the secure channel. In the SECURED card life cycle state, all command data must be **secured by at least a MAC**. As specified in the GP specification, there exist earlier states (before card issuance) in which a MAC might not be necessary to send Card Manager commands. The key set associated with the secure channel is such that:

- All Triple-DES keys are double length keys (16 bytes),
- All Triple-DES operations are performed using Triple-DES encryption or decryption.
- All Triple-DES MAC generations result in an 8-byte field. These 8 bytes constitute the MAC.

Security Domain Keyset (each key is 16-bytes):
Key sets are identified by Key Version Numbers ('01' to '7F'). The keys within a key set version have the following different functionality:

- Secure Channel Encryption (K-Enc) is used for generation of keys used for secure channel encryption.
- Secure Channel Message Authentication Code Key (K-Mac) is used for generation of keys used for secure channel MAC verification.
- Data Encryption Key (DEK) is used for sensitive data encryption.

Secure Channel session keys (each key is 16-bytes):
The Secure Channel session keys are generated as per the GP specifications using random challenge values and Card Manager Key Set.

- S_{enc}: used to encrypt command and response APDU data encrypted mode of the secure channel to provide message confidentiality.
- S_{mac}: used to MAC command and response APDU data in MAC mode of the secure channel to provide message integrity.

DAP Public key: The RSA 1024-bit DAP public key used for verifying loading of applets is also managed by the Card Manager applet.

PRNG Seed and seed key: These are CSPs used in the ANSI X9.31 RNG. They are stored in EEPROM across power-cycles and in RAM during module execution.

9.2 PIV Application Keys

PIV Applet use keys of the following key types through the cryptographic services of the module: Triple-DES Keys, RSA public and private keys.

9.2.1 PIV Applet Key management:

The PIV Applet manages five types of keys through the platform cryptographic services:

- The ***PIV authentication key***: This key (asymmetric RSA) is generated on the card. This key is used to support card authentication for an interoperable environment, and it is a **mandatory non exportable key.**
  This key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the PIV authentication key. The PIV authentication key must be available only through the contact interface of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).

- The ***PIV card application administration key****:* This key is a symmetric Triple DES key. It may be used for personalization and post-issuance activities. The PIV Card shall not permit exporting the card authentication key. This key shall be imported to the card and allows authentication of the Card Application Administrator..

- The ***PIV card application digital signature key***: This key (asymmetric RSA) may support document signing.
  The PIV digital signature key shall be generated on the PIV Card. The PIV Card shall not permit exporting the digital signature key. If present, cryptographic operations using the digital signature key may only be performed using the contact interface of the PIV Card. Private key operations may not be performed without explicit user action.

- The ***PIV card application key management key***: This key (asymmetric RSA)may support key establishment and transport. This Key may be used as an encryption key. This key may be generated on the PIV Card or imported to the card. If present, the key management key must only be accessible using the contact interface of the PIV Card. This key is sometimes called an encryption key or a cipher key.

- The ***PIV card authentication key***: This key (asymmetric RSA) may be used for physical access control. The PIV card authentication key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the card authentication key.

9.2.2 PIV Applet security domain

It is possible to open a secure channel during the personalization phase and also application mode of the PIV Applet by using the security domain of the java platform. During the personalization, the applet restricts the use of authentication mechanism, defined in GP. Only the mode 3 is allowed when the Card Manager state is “SECURED”, and modes 1, 2 and 3 if Card Manager state is “INITIALIZED” or “OP_READY”.
During Application mode only mode 3 is allowed. In mode 3 the Secure Channel must be MAC+ ENCRYPT.

9.3 Key Generation

The CM on-board key generation is able to generate RSA key and RSA Chinese Remainder Keys. Strong prime numbers are generated in compliance with X9.31 standard.

For the **PIV Applet asymmetric keys**, the card stores a corresponding X.509 certificate.
The PIV Card imports and stores a corresponding X.509 certificate to support validation of the corresponding private key.

Keys are generated in the CM using the GENERATE ASYMMETRIC KEY PAIR command.

9.4 PIV Application Key Entry

Keys are entered in the CM using the PUT DATA APDU command of the PIV Applet and with the authentication of Card Holder, Card Application Administrator or Crypto Officer. The PIV Applet ensures that Secure Channel is MAC+ENCRYPT so that keys are entered in encrypted form.

The PIV Applets key set structure is presented to the card in plaintext. The key set structure includes a checksum for each key in order to ensure their integrity.

9.5 Card Manager Key Entry

The Card manager applet provides the PUT KEY APDU to replace the Card Manager keyset. This service is only available to the Crypto Officer. The Card Manager enforces entering cryptographic Triple-DES keys securely within a secure channel. The Card Manager keyset already present within the CM is the default. If this keyset version is replaced, the replacement becomes the default.

The Crypto Officer also uses the PUT KEY APDU command to enter a RSA public key for DAP verification.

9.6 Key Storage

Keys are protected against unauthorized disclosure, unauthorized modification, and unauthorized substitution.

Secret and private keys are Java objects. As a consequence, they are protected by the firewall from illegal access. An applet that owns a key is responsible for not sharing it.
Triple-DES keys are stored in the physical security of the NXP chip and are under the protection of the firewall that prevents the key from being accessed by unauthorized applets. Moreover, RSA keys are checksummed, Triple-DES keys are checksummed and masked. All keys are stored as plaintext in the module.

The Java inheritance mechanism ensures that a created Java object such as a key belongs to its owner, that is an applet with an execution context.

The CM stores key components according to the key type.

KEY TYPE	KEY COMPONENT
Triple-DES keys	Key value component
RSA Keys pair	Private portion in CRT (Chinese remainder theorem): Chinese Remainder **P** component (P, the prime factor p) Chinese Remainder **Q** component (Q, the prime factor q) Chinese Remainder **PQ** component (PQ = q^{-1} mod p) Chinese Remainder **DP1** component (DP1 = d mod (p - 1)) Chinese Remainder **DQ1** component (DQ1 = d mod (q - 1)) Public portion Public exponent e component Modulus N component

Table 25 - Key types and components mapping table

The PIN is a critical security parameter that implements the JavaCard OwnerPin class.

10 EMI/EMC

The **Protiva PIV DL** has been tested to meet the EMI/EMC requirements specified in FCC Part 15 Subpart J, Class B.

11 Self Tests

The **CM** performs the following self-tests to ensure that the module works properly. All the self tests are done by the **Protiva PIV TPC** platform.

SELF-TESTS	EXECUTION
Cryptographic algorithm test (Known-answer tests for Triple-DES, AES, SHA-1, RSA)	At Power-Up
EEPROM integrity test.	At Power-Up
Pseudo Random Number Generator test. (Known-Answer Test for P-RNG output)	At Power-Up
Security error test	At Power-UP
Sensors test	At Power-Up
Pair-wise consistency test.	Conditional
Firmware load test.	Conditional
Continuous random number generator test.	Conditional

Table 26 - Self-tests list

11.1 Self-Test Execution

After power up and on receipt of the first APDU command, the CM enters the self-test state and performs all of the cryptographic algorithm and software integrity self-tests as specified in FIPS 140-2 standard **[1]**. In addition to those tests, it also performs chip sensors verification and security status verification:

- **Sensors test:** at startup, the card detects if a hardware security error has been held during the previous session. If so, the card enters a mute state.
- **Security errors test:** at startup, if a pre-defined number of security errors is reached, the card is terminated as per Global Platform specifications. The GET DATA command is the only command that remains available.

These tests are conducted automatically as part of the normal functions of the CM. They do not require any additional operator intervention, nor applet specific functions.

Power-up self-tests are executed upon reset after the first APDU command is issued. The CM start-up process has been designed in such a way that it cannot be bypassed. This enforces the execution of the self-tests before allowing any use and administration of the module, thus guaranteeing a secure execution of the module's cryptographic services.

If these self-tests are passed successfully, the CM returns the status words relating to the requested APDU command via the status interface and incoming APDUs are processed.

All data output via the output interface are inhibited while any power-up and conditional self-test is running.

Resetting the CM, provides a means by which the operator can repeat the full sequence of power-up operating tests.

11.2 Self-Test Failure

No cryptographic operations can be processed and no data can be output via the data output interface while in the error state.

If an error occurs during the **SW load self-test**, an error code is returned via the status interface and the secure channel is closed (loading is aborted).

If an error occurs during another self-test, the card enters a state where no more commands can be performed. The behavior of the card depends on error:

- **Severity level 1 error:**
  - Integrity test, internal error counter is incremented, the card returns an error status before becoming mute.
- **Severity level 2 error:**
  - Cryptographic algorithms tests, internal error counter is incremented, the card returns an error status before becoming mute.
  - Conditional self-tests (PRNG continuous test and pair wise consistency test), internal error counter is incremented, the card returns an error status before becoming mute.

When the internal error counter reaches a certain value the card becomes mute.
An error while loading an applet closes the secure channel with the Card Manager. It shall be re-opened, to retry applet loading: the Cryptographic Officer has to be re-authenticated.

12 Guidance

12.1 PKI BLADE Applet User and SO Guidance

When or before the card is issued, the end-user should be made aware that the card is an extension of the user's ID and is capable of generating a digital signature for the user, which is as valid and legal as a written signature on a paper document. For this reason the user should also understand that he /she should keep the card on their person or under lock and key when not in use, and to protect their secret pass phrase from observation when logging on.

At the time the card is issued, an initial user pass phrase is in the card. The issuer should be urged to immediately change the initial pass phrase to one which the user can easily remember but one which others cannot easily guess.

Users must ensure RSA key transport services are used only for key wrap and unwrap; these operations limit use to data input of the appropriate size as a safeguard against usage for bulk encryption.

The PBSO is responsible for ensuring that cards are issued with a card configuration file as well as file permissions in accordance with organization security policy.

The following rules must be observed:

1. The 1/1,000,000 FAR setting must be selected when the *Bio Only* or *Bio-or-PIN* settings are used.
2. A value between 1 and 10 inclusive for the number of allowed bad fingerprint authentication attempts must be selected when the *Bio Only* or *Bio-or-PIN* settings are used.
3. The PBSO must change the default SO PIN as soon as the card is in possession of the PBSO and must not communicate his/her PIN to any entity.
4. When the Recycle command is issued the EXF file is deleted. This command must only be used when the card is destroyed.
5. The PBSO must unblock User PIN only for legitimate Users.
6. Use of PBDEK keys must be restricted to 2^20 encrypt or decrypt operations.

12.2 Card Manager and PIV Applet Guidance

In addition to the above guidance, the issuer and end-users must observe the following rules:

1. The PIV Applet Cardholder PIN value must use a length and character set combination that meets the FIPS 140-2 authentication strength requirement (probability of false acceptance 1/1,000,000).

13 Mitigation of Other Attacks

The CM has been designed to mitigate the following attacks:

- Timing Attacks,
- Differential Power Analysis,
- Simple Power Analysis,
- Electromagnetic Analysis,
- Fault Attack,
- Card Tearing

A separate and proprietary document describes the policy for mitigation of attacks implemented by the CM.

13.1 Hardware Security Mechanisms

Additionally, the embedded **P5CD144 chips from NXP** provide the CM with hardware security mechanisms such as probing detection, low frequency and supply voltage monitoring. The chip reacts to a low/high clock frequency, and low/high power supply voltage by resetting the CM. Any unprotected sensitive data are lost.

13.1.1 High/Low Frequency Sensor

The external clock frequency is monitored. If it is higher than the maximum value or lower than the minimum value, a security reset is generated.

13.1.2 High/Low Voltage Sensor

The supply voltage is monitored. If it is higher than the maximum value or lower than the minimum value, a security reset is generated.

13.1.3 High/Low Temperature Sensor

The temperature is monitored. If it is higher than the maximum value or lower than the minimum value, a security reset is generated.

13.1.4 Shields

Shields cover different chip areas.

13.1.5 Fault injection detection

Fault injection mechanisms are implemented such as redundancy checking (parity, duplication) on internal data and transmissions. When an error is detected a reset is generated.
Light sensors are implemented to detect light attacks commonly used when trying to inject faults.

13.1.6 Light sensor

Light sensors are spread in different parts of the chip. When light attack is detected a reset is generated.

13.1.7 Glitch sensor

A glitch sensor is present and monitors Vcc and Vss. When the sensor is triggered a reset is generated.

13.1.8 Filters

A filter is present on the RST (reset signal) and CLK (clock signal) lines.

13.1.9 BUS Scrambling

Physical and logical addresses have no correlation due to the use of ‘address scrambling’ at the BUS level.

13.1.10 Memory Scrambling

Some dedicated and NXP proprietary scrambling algorithms are implemented in order to protect data in the different memory areas such as EEPROM, ROM and RAM.

END OF DOCUMENT