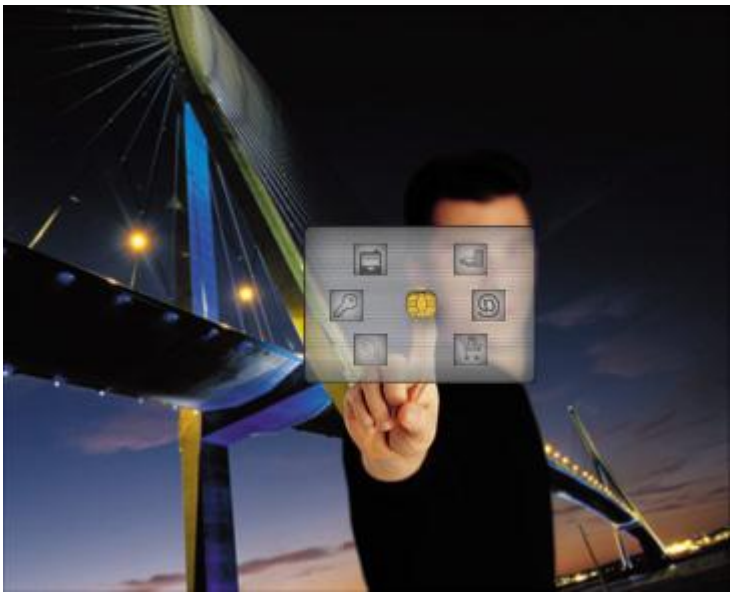
Protiva PIV Applet v1.55 on Protiva TOP DM Card

Security Policy



TITLE	**Protiva PIV Applet v1.55 on Protiva TOP DM Card - Security Policy**
REF.	**SP02R10610 – 05.02**
DATE:	**05/19/11**

TABLE OF CONTENTS

Table of figures:

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 800-73-3 - Interfaces for Personal Identity Verification - February 2010

1 Scope

This Security Policy specifies the security rules under which the Protiva™[1] PIV Applet v1.55 on Protiva PIV TOP DM platform, herein identified as the **"Protiva PIV DM"** product, must operate. Some of these rules are derived from the security requirements of **FIPS140-2' standard [1]**, others are derived from the GEMALTO' experience in embedded security software.

These rules define the interrelationships between the:

- Module users and administrators,
- Module services,
- Security Relevant Data Items (SRDIs).

The commercial name of the product is:

Gemalto Protiva PIV Applet v1.55 on Protiva TOP DM Card

Where:

- Protiva TOP DM is a Java platform available in the DM (Dual Medium) version.
- Protiva PIV Applet v1.55 is an applet loaded on the Java Card platform "Protiva TOP DM," This applet may also be referred as "PIV Applet" in this document.

[1] Protiva is a registered trademark of Gemalto.

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. This **whole product**, made up of the GEMALTO platform and the PIV Applet is aimed to reach FIPS 140-2 L2 compliance. The present document is dedicated and focused on both the GEMALTO Protiva TOP DM platform and the GEMALTO Protiva PIV Applet (PIV Applet).

This security policy specifies the security rules under which our Java Protiva TOP DM platform and the PIV Applet operate.

2.2 GEMALTO Smart Card Open Platform

The cryptographic module 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.

The PIV Applet doesn't implement any cryptographic services. But when needed the applet uses the cryptographic services provided by the card platform.
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 a PIN, and are moreover in the "SECURED" state. The security implementation is fully compliant with the **Global Platform (GP) specification**.
The cryptographic module 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	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 – FIPS 140-2 Security Levels

2.4 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 a single chip implementation of a cryptographic module. The micro-module is designed to be embedded in a plastic card body to provide an **ISO-7816 [10]** compliant smart card.

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

Protiva PIV DM identification:
The Protiva PIV DM (medium) is based on **P5CD072** chip from NXP.
The Firmware version for Protiva PIV TOP DM (72K): GCX4-FIPS EI07 (MPH051), GCX4-FIPS EI08, GXP4-FIPS EI07 (MPH052) and GXP4-FIPS EI08; Applet Versions: Protiva PIV Applet v1.55
The hardware version: GCX4-M2569420, GXP4-M2569430, GCX4-M2569422, GCX4-A1004155 and GCX4-A1026517.

Protiva PIV DM 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 the 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 the configurations described below. These 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 operated, with FIPS PK self-tests and PK service enabled.
- **CONFIGURATION 2**: The product is initialized in dual interface mode; it means that both contact and contactless mode are operated, with FIPS PK self-tests and PK service enabled in contact mode and without FIPS PK self-tests and so no PK services in contactless mode.

The following table gives an overview of thedifferent configurations regarding contactless and PK support.

	DUAL INTERFACE	PK SUPPORT IN CONTACTLESS MODE	PK SUPPORT IN CONTACT MODE
CONFIGURATION 1	Yes	Yes	Yes
CONFIGURATION 2	Yes	No	Yes

Table 1 –Interface and PK support configurations

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 FIPS140-2 Level 3.**

All the components of **Protiva PIV DM** that are included in the cryptographic module boundaries are those as shown in the following figure:

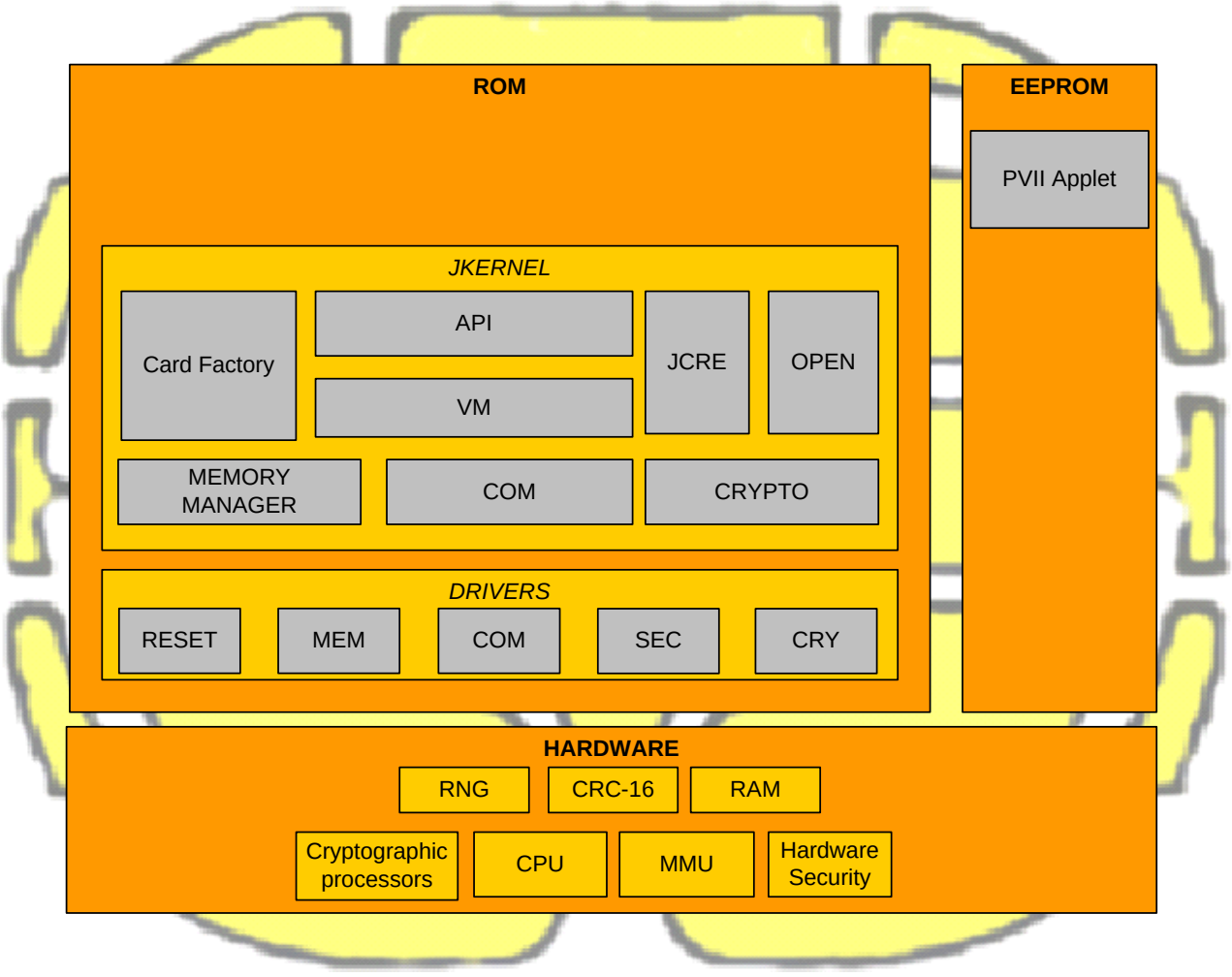


Figure 1- Cryptographic Module Boundary

2.5 Language level

The scope of this security policy is focused both on the Java Card Platform and on the PIV Applet (in EEPROM). The cryptographic module is implemented using a high level language, a limited number of software modules that require fast processing have been written in a low-level language.
The application code "Applet" is designed in the Java Card language that is a high level language. The applet code complies with the Java card code verifier to ensure compliance with language rules.

2.6 FIPS Approved Security Functions

The following table gives the list of FIPS approved security functions that are provided by the **Protiva PIV DM** Java Card API.

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#1 with SHA-1 hashing	
	Verification following PKCS#1 with 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

FIPS approved security functions used specifically by the **PIV Applet** are:

- **Triple-DES**
- **RSA**
- **P-RNG**

3 Cryptographic Module Ports and Interfaces

The **Protiva PIV DM** restricts all information flow and physical access.
Physical and logical interfaces define all entry and exit points to and from the micro module.

3.1 Physical Port – Contact mode

3.1.1 PIN assignments and contact dimensions:

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

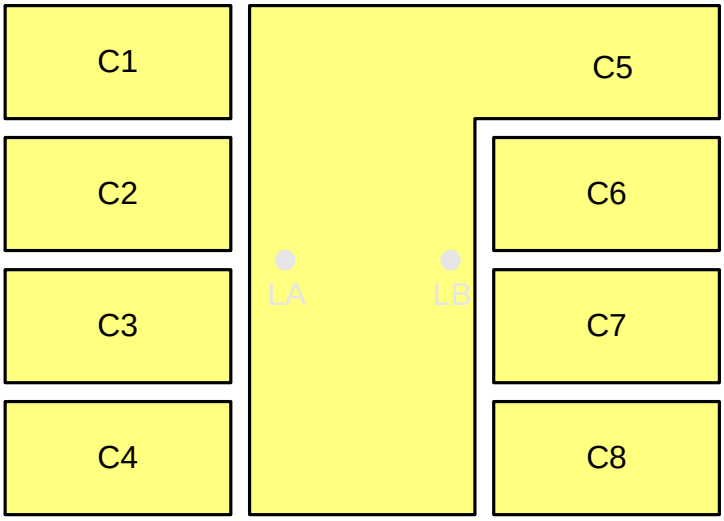


Figure 2 - Contact plate example – Contact physical interface

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

Table 3 - Contact plate pin list – Contact mode

3.1.2 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

3.2 Physical Port – Contactless mode

3.2.1 Contacts assignments

In the contactless mode the Protiva PIV DM cryptographic module 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.**

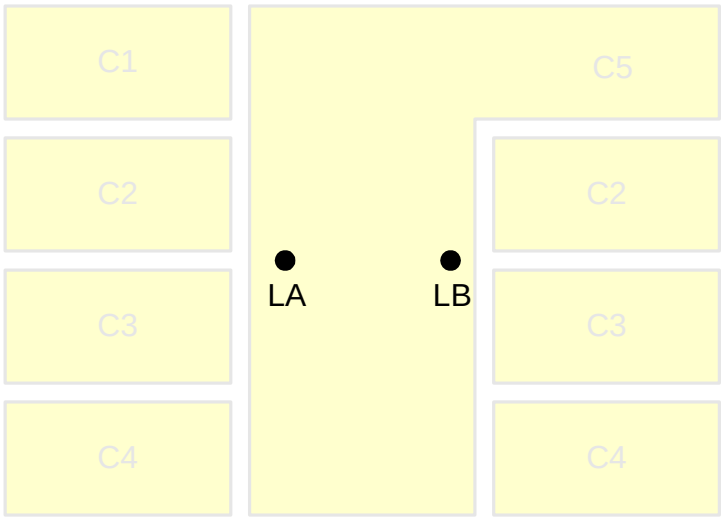


Figure 3 - Contact plate example - Contactless antenna contacts

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

Table 5- Contact plate pin list – Contactless mode

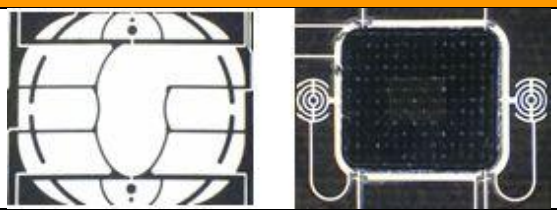
3.2.2 Condition of uses

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

Conditions	Range
Supported bit rate	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

3.2.3 Pictures – Dual Mode

World Combi Thermal black resin process, contact and contactless technology

Gem combi design and thermal black resin technology

3.3 Logical Interface

Protiva PIV DM provides services to both external devices and internal applets as the PIV and Card Manager applets.
External devices have access to services by sending APDU commands while internal applets as PIV Applets have access to services through internal API entry points.
The cryptographic module provides an execution **sandbox for PIV applets** and performs the requested services according to its roles and services security policy.

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

4 Roles, Services and Authentication

This section specifies the roles, security rules, services, and Security Relevant Data Items (SRDI) of the cryptographic module. 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 cryptographic module are listed in the subsection labeled "SERVICES" in the Access Control Policy description.

4.1 Identification and Authentication Policy

4.1.1 Introduction

This section is dedicated to our identity-based authentication policy, and the related security rules of the mechanism interfaces and SRDI.

4.1.2 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 Cryptographic Module:

Role ID	Description
Cryptographic Officer (CO)	This role is responsible for managing the security configuration of the card manager and security domains. The CO authenticates to the cryptographic module 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 establishes a secure channel to the Card Manager and execute services allowed by the CO role in a secure manner.
PIV Card Application Administrator (CAA)	The PIV Card Application Administrator role represents an external application requesting the services offered by the PIV Applet. An applet authenticates the Application Operator by verifying possession of the Application External Authenticate (XAUT) TRIPLE-DES key
Card Holder (CH)	The Card Holder role is responsible for ensuring the ownership of his cryptographic module, and for not communicating his PIN to other parties. The PIV Applet authenticates the Card Holder by verifying the PIN value.
Card Holder II (CHII)	The Card Holder II role is responsible for unblocking and/or changing the Card Holder PIN. The PIV authenticates the Card Holder II by verifying the PIN value.
Anonymous User (AU)	Anonymous User – the unauthenticated "role"
Maintenance	The CM does not implement a maintenance mode or role.

Table 7 - Role profile definitions

4.1.3 Mechanism Interfaces

The following tables describes 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.
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.

Table 8 - Mechanism interfaces in personalization and applicative phase

Interface	Description
GENERAL AUTHENTICATE *APDU*	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*	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

4.1.4 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 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 cryptographic module detects a secure messaging corruption.

Table 10 - Security rules

4.1.5 Strengths of Authentication Mechanisms:

Authentication Mechanism	Strength of Mechanism
GP mutual authentication	$\left(\frac{1}{2^{80}}\right)$
	The cryptogram sent is 8 bytes long and 2-Key Triple-DES is used is as described in SP 800-57
PIN verification	$\left(\frac{1}{256^{8}}\right)$
	Pin verification is the responsibility of the PIV Applet that defines and maintains its own security policy regarding PIN but uses the PIN management services provided by the platform.
Card Application Administrator 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.

Table 11 - Mechanism strengths

4.2 Access Control Policy

4.2.1 Introduction

This chapter is dedicated to access control security rules. Some services provided by the cryptographic module 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 to 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.

4.3 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 :

* APDU not available in contactless mode

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 setting up 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 shall be used to realize the signing functionality on the PIV client-application programming interface.
GENERATE ASYMETRIC 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

Platform		
Role ID	**CO**	**AU**
DELETE	X	
MUTUAL AUTHENTICATE (Initialize Update & External Authenticate)	X	X
GET DATA (Platform Specific)	X	X
GET STATUS	X	
INSTALL	X	
LOAD	X	
MANAGE CHANNEL	X	X
PUT DATA (Platform Specific)	X	
PUT KEY	X	
SELECT	X	X
SET STATUS	X	
STORE DATA	X	

Table 14 - Platform Services Access

PIV Applet				
Role ID	**CAA**	**CH**	**CHII**	**AU**
GET DATA (PIV Applet Specific)	X	X	X	X
PUT DATA (PIV Applet Specific)	X			
CHANGE REFERENCE DATA		X		
END PERSONALIZATION				
GENERAL AUTHENTICATE	X	X		
GENERATE ASYMETRIC KEY PAIR	X			
RESET RETRY COUNTER			X	
VERIFY		X		

Table 15 - PIV Applet Services Access

4.3.1 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 cryptographic module 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 16 - Security rules

4.4 Additional GEMALTO Security Rules

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

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 17 - GEMALTO additional security rules

4.5 Security Relevant Data Item

The Security Relevant Data Items (SRDIs) of the cryptographic module are the following:

- **GP key set of the Card Manager**
- **Secure channel session key**
- **Card Holder PIN**
- **Card Holder II PIN**
- **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 8 for additional detail.

The following table defines an association between the services or authentication mechanisms (the interface name is provided) and the SRDI 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	SRDI	Access type
DELETE	Secure channel session keys	
EXTERNAL AUTHENTICATE	GP key set of the Card Manager Secure channel session leys	 U
GET STATUS	Secure channel session keys	
INITIALIZE UPDATE	Secure channel session keys PRNG seed and seed key	 U
INSTALL	Secure channel session keys	
LOAD	Secure channel session keys	
PUT DATA	Secure channel session keys PIV card application authentication key PIV card application key management key	 U U
PUT KEY	GP key set of the Card Manager Secure channel session leys	 U
SET STATUS	Secure channel session keys	
STORE DATA	Secure channel session keys	
GENERAL AUTHENTICATE	PIV keys	
VERIFY	Card Holder PIN	
RESET RETRY COUNTER	unblocking PIN (Card Holder II PIN) Card Holder PIN	 W
CHANGE REFERENCE DATA	Card Holder PIN	 U
GENERATE ASYMMETRIC KEY PAIR	PIV keys Card Holder PIN	 U

Table 18 - Security Relevant Data Items

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

5 Finite State Model

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

The cryptographic module 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.

6 Physical Security

The CM single chip module is designed to meet the **FIPS140-2 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.

7 Operational Environment

This section does not apply to **CM**. No code modifying the behavior of the cryptographic module 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 cryptographic module operating system following its security policy rules.

8 Cryptographic Key Management

8.1 Card Manager Keys

The cryptographic module 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.

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

DAP Public key: The 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.

8.2 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

8.2.1 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 exporting 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.

8.2.2 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.
Retail MAC cannot be used as a Software Load Integrity mechanism to load applets on the card due to its use of DES algorithm

8.3 Key Generation

The cryptographic module 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 cryptographic module using the GENERATE ASSYMETRIC KEY PAIR command.

8.4 PIV Application Key Entry

Keys are entered in the cryptographic module 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 keyset structure is presented to the card in plaintext. The keyset structure includes a checksum for each key in order to ensure their integrity.

8.5 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 cryptographic module 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 an RSA public key for DAP verification.

8.6 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, a checksum is performed on the RSA keys, Triple-DES keys 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 cryptographic module stores key components according to the key type.

KEY TYPE	KEY COMPONENT
Triple-DES keys	Key value component
	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 = $q^{-1} \bmod p$) Chinese Remainder **DP1** component (DP1 = $d \bmod (p - 1)$) Chinese Remainder **DQ1** component (DQ1 = $d \bmod (q - 1)$) Public portion Public exponent e component Modulus N component

Table 19 - Key types and components mapping table

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

9 EMI/EMC

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

10 Self Tests

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

SELF-TESTS	EXECUTION
Cryptographic algorithm test (Known-answer tests for Triple-DES, AES, SHA-1, RSA)	At Power-Up
Software/firmware 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
Software load test.	Conditional
Continuous random number generator test.	Conditional

Table 20 - Self-tests list

10.1 Self-Test Execution

After **Protiva PIV** DM is powered up and before executing any APDU commands, the module 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 cryptographic module. 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 cryptographic module 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 cryptographic module 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 cryptographic module, provides a means by which the operator can repeat the full sequence of power-up operating tests.

10.2 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.

11 Design Assurance

The **CM** meets the Level 3 Design Assurance section requirements.

11.1 Configuration Management

The CM is designed and developed using a configuration management system that is operated with clear rules.

An additional document (Configuration Management Plan document) defines the methods, mechanisms and tools to identify and place under control all the data and information concerning the specification, design, implementation, generation, test and validation of the card software throughout the development and validation cycle.

11.2 Delivery and Operation

The CM is designed and developed using a configuration management system that is operated with clear rules.

Some additional documents ('Delivery and Operation', 'Reference Manual', 'Card Initialization Specification' and 'Applet Initialization Specification' documents) define and describe the steps necessary to deliver and operate the **CM** securely.

11.3 Guidance Documents

The Guidance document provided with CM is intended to be the 'Reference Manual'. This document is designed to allow a secure operation of the CM by its users as defined in the '**Roles, Services and Authentication'** chapter.

12 Mitigation of Other Attacks

The Protiva PIV DM 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 mitigating attacks implemented by the CM..

12.1 Hardware Security Mechanisms

Additionally, the embedded **P5CD072/P5CD144 chip from NXP** provides the cryptographic module 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 cryptographic module. Any unprotected sensitive data are lost.

12.1.1 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.

12.1.2 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.

12.1.3 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.

12.1.4 Shields

Shields cover different chip areas.

12.1.5 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.

12.1.6 Light sensor

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

12.1.7 Glitch sensor

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

12.1.8 Filters

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

12.1.9 BUS Scrambling

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

12.1.10 Memory Ciphering

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

END OF DOCUMENT