Protiva™ PIV Card v2.0 using TOP DL v2 and TOP IL v2

Security Policy

TITLE	**Protiva™ PIV Card v2.0** using TOP DL v2 and TOP IL v2 **-** Security Policy
REF.	**R0R21576_PIVv2_001_SP - _10**
DATE:	**July 2011, the 20th**
AUTHOR	**FDefrance, SL, R&D, Gemalto**
	Frederic Garnier, OA R&D, Gemalto
APPROVED	**Michel Escalant, James McLaughlin, Gemalto**

1

REVISION HISTORY

Release (Xyy)	Date (dd/mm/yy)	Author	Modifications
01	20/07/11	F.Defrance, F.Garnier	Initial version.
02	03/08/11	F.Garnier	Update OATH Applet name and minor changes (review by PM, team, ...).
03	19/09/11	F.Defrance	Add contact only configuration
04	04/11/11	F. Garnier	Update with CMVP comments.
05	23/02/12	F.Defrance, F.Garnier	Update with CMVP comments: card terminated, keys zeroisation for ISD & PIV (as on v1.55). Add statement: re-use existing Cert. #1450.
06	28/03/12	J. McLaughlin	Added algorithm certificates
07	29/03/12	J. McLaughlin	Corrected cert for TDES
08	31/08/12	F.Defrance	Take into account SAIC remarks
09	23/10/12	F.Defrance	Following CMVP request add a description of the MOA
10	26/10/12	F.Defrance	Update the attack description and associated countermeasures

DISTRIBUTION LIST

N°	Name	Role	Society
1	F.Defrance	FIPS Coordinator	Gemalto
2	F.Garnier	Project Leader	Gemalto
3	E. Morris	FIPS Evaluator	SAIC Laboratories
4	W.Tung	FIPS Evaluator	SAIC Laboratories
5	M.Escalant	Sales technical consultant Manager	Gemalto
6	J.McLaughlin	Program Manager	Gemalto

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 Amdt A

[5] Java Card API Specification – (SUN) – Release 2.2.1, release 2.2.2 for SHA-2 & JC3.0.1 for ECDSA and ECDH;

[6] Java Card Runtime Environment (JCRE) Specification (SUN) – 2.2

[7] Java Card Virtual Machine (VM) Specification – SUN – Release 2.2

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

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

[10] ISO X9.31

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

[12] Global Platform – Release 2.2 Amdt D (Secure Channel Protocol 03)

[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 **Protiva™ PIV Card v2.00** using **TOP DL v2 (dual interface) and TOP IL V2 (contact only) platform.** Smart Card with the optional **OATH Applet v2.10** 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,
- Critical Security Parameters.

The commercial name of the product is:

Protiva™ PIV Card v2.0 using TOP DL v2 and TOP IL v2

Where **Protiva™ PIV Card v2.0 using TOP DL v2 and TOP IL v2 :**
- is a product that consists of:
    o Java platform available in one memory configuration: the Dual Large (DL) 128K configuration. The platform may also be referred to as "**TOP DL V2**" for dual interface and "**TOP IL V2**" for contact interface in this document
    o **Protiva™ PIV Applet v2.00** loaded on the Java Card platform "TOP DL/IL V2". This applet may also be referred as "PIV Applet" in this document.
- **OATH Applet V2.10** (in ROM) installed on the Java Card platform "TOP DL/IL V2". This applet may also be referred as "OATH Applet" in this document.

For simplicity the **Protiva™ PIV Card v2.0 using TOP DL v2 and TOP IL v2 is mostly referred to as PIV Card.**

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 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.

This cryptographic module uses a state of the art manufacturing flow in terms of security and provides applets with memory, cryptographic and I/O services.
The PIV Applet and the OATH Applet do not implement any cryptographic services. But when needed these applets use cryptographic services provided by the card platform. The cryptographic module ensures on-card applets safe coexistence thanks to its Virtual Machine (VM) and firewall. The Java VM is fully compliant with the **Java Card standard [7]**.

The card life cycle is managed according to the **Global Platform (GP) specification.** Issued cards have been loaded with applet, cryptographic keys, and a PIN, and are moreover in the "SECURED" state.
The security implementation is fully compliant with the **Global Platform (GP) specification [4][12]**.

The cryptographic module integrates symmetric and asymmetric cryptographic algorithms as specified in the **Java Card specification [5]** and platform offers RSA & ECDSA for Signature/Verification, SHA-1, SHA-256, SHA-384, SHA-512 hashing functions, on-board RSA Key generation, on-board ECC key generation, Triple-DES CBC and ECB , AES ECB and CBC and CMAC algorithms.

2.3 Security Level

The cryptographic module 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 OATH Applet

The OATH Applet, designed for use on JavaCard 2.2.1 and Global Platform 2.1.1 compliant smart cards, provides one time password (OTP) service generation that conforms to the OATH specification for hardware tokens.

The OATH Applet features:
- Authentication of the OATH Applet User and the OATH Applet security officer
  - Supports global PIN based authentication.
- Execution of native platform cryptographic services integrated with managed objects:
  - Two key Triple-DES encryption and decryption.
  - SHA1 secure hashing generation.
  - Pseudo-random number generation.

3 Cryptographic Module Specification

3.1 Gemalto Crypto-Module Cryptographic Boundary

The Cryptographic Boundary is defined to be the 'ICC module edge' of the **CM** , comprising a set of "embedded" hardware and software that implements cryptographic functions and processes, including cryptographic algorithms and 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 [9]** compliant smart card.

The Cryptographic Module provides dual interfaces (i.e. contact and contact-less) where the same security level is achieved.

 PIV Cardidentification:
The product is based on SLE66CLX1280PE(M) **chip from Infineon .**

The hardware and firmware versions : see in Appendix B – Identification and FIPS mode :
The TOP DL v2 Cryptographic Module has already achieved FIPS 140-2 Level 3 validation. NIST Certificate #1450 provides detail information on the FIPS validation:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1450

Depending on the market and the end-customer requirements, SCP support and applet set can be configured during the manufacturing in order to answer as precisely possible to the market and the end-customer requirements:

The product is initialized in dual interface mode or in contact only mode; In dual interface, both contact and contact-less modes are operated, with FIPS self-tests and associated services enabled.

The secure channel protocol (SCP) is based either on:
- AES keys for GP-SCP03-00 (option i=00) or GP-SCP03-10 (option i=10) or
- 3DES-2 keys GP-SCP01
  as per **GP specification [12]**.

The applet set is based either on:
- OATH Applet installed (not loaded because already present in ROM code) or
- PIV Applet loaded and installed or
- Both

The following table gives an overview of those 9 different configurations regarding SCP (Secure Channel Protocol) support and Applet set.

Applet / SCP	SCP03-00	SCP03-10	SCP01
OATH Applet	Config 1	Config 4	Config 7
PIV Applet	Config 2	Config 5	Config 8
OATH + PIV Applets	Config 3	Config 6	Config 9

Table 2 –SCP support and applet set configurations for TOP DL/IL V2

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.**

The contact-less antenna is not within the cryptographic boundaries of the module.
All the components of the **TOP DL/IL V2 – Micro-Module** that are included in the cryptographic module boundaries are those as shown in the following figure:

Figure 1- Cryptographic Module Boundary

The following sections provide a description of the different entities presented in this scheme.

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 OATH Applet are java applets designed for the Java Card environment.

3.3 FIPS Approved Security Functions

The following table gives the list of FIPS approved security functions that are provided by the TOP DL/IL v2 Card Java Card API.

SECURITY FUNCTION	DETAILS	FIPS APPROVED
Triple-DES	ECB mode in encryption ECB mode in decryption CBC mode in encryption CBC mode in decryption	Cert. #1280
Triple-DES MAC	Using MAC algorithm	Cert. #1280 (vendor affirmed)
SHA-1, SHA-256, SHA-384, SHA-512	Hashing operation	Cert. #1727
ECDSA (P-192, P-224, P-256, P-384, P-521)	EC Signature following X9.62 with SHA-1 hashing EC Verification following X9.62 with SHA-1 hashing EC Key pair generation following X9.62	Cert. #284
RSA	Key generation Signature following PKCS#1 with SHA-1 hashing Verification following PKCS#1 with SHA-1 hashing	Cert. #1019
P-RNG	Pseudo Random Number Generation following X9.31	Cert. #1038
AES	ECB mode in encryption ECB mode in decryption CBC mode in encryption CBC mode in decryption	Cert. #1973

Table 3 – FIPS Approved Security Functions

Additional cryptographic algorithms:
The following algorithms are part of the **JavaCard 3.0.1 specification:**

SECURITY FUNCTION	DETAILS	FIPS APPROVED
ECDSA (P-192, P-224, P-256, P-384, P-521)	Signature following X9.62 with SHA-256 / SHA-384 / SHA-512 hashing Verification following X9.62 with SHA-256 / SHA-384 / SHA-512 hashing	Cert. #284
ECC-CDH (P-192, P-224, P-256, P-384, P-	EC secret value derivation primitive, Diffie-Hellman version	Cert. #18

521)		

Table 4 – Additional Security Functions

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

- **Triple-DES**
- **AES**
- **RSA**
- **ECDSA**
- **ECC-CDH**
- **P-RNG**

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

- **Triple-DES**
- **SHA-1**
- **P-RNG**

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 PIN assignments and contact dimensions:

PIV Card– Micro-Module follows the standards **"ISO 7816-1 Physical characteristics" [9]** and **"ISO 7816-2 Dimensions and contact location" [9]**.

C1	C5
C2	C6
C3 LA LB	C7
C4	C8
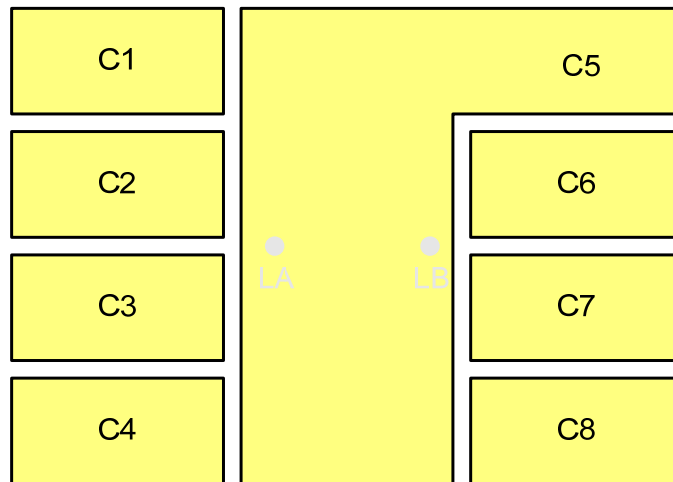
Figure 2 - Contact physical interfaces

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 5 - Contact plate pin list – Contact mode

4.1.2 Conditions of use

The electrical signals and transmission protocols follow the **ISO 7816-3 [9]**.

Conditions	Range
Voltage	1,62 V and 5.5 V
Frequency	1 MHz to 7,5 MHz

Table 6 - Voltage and frequency ranges

4.2 Physical Port – Contact-less mode

4.2.1 Contacts assignments

In the contactless mode the **CM** follows the standard **"ISO 14443 RF Interface" [11]** 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.**
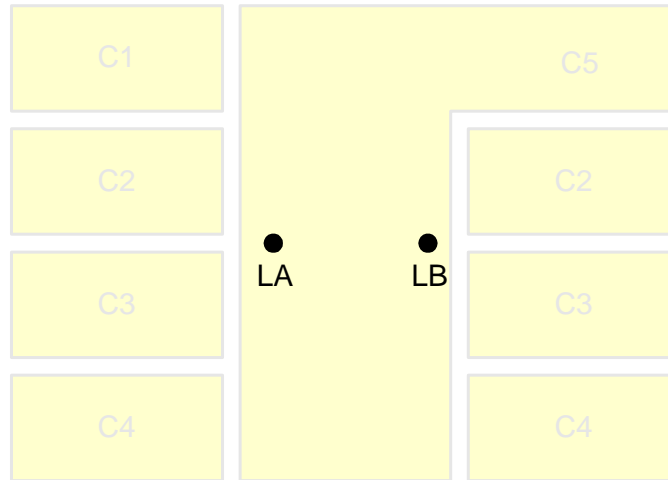
Figure 3 - Contact-less physical interfaces

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

Table 7- Contact-less plate pin list – Contact-less mode

4.2.2 Condition of uses

The radiofrequencies and transmission protocols follow the "ISO 14443 RF Interface" [11].

Conditions	Range
Supported bit rate	106 Kbits/s, 212 Kbits/s, 424 Kbits/s and 848 Kbits/s
Frequency	13.56 MHz

Table 8 - Voltage and frequency ranges

4.2.3 Picture

Thermal black resin process, contact and contactless technology
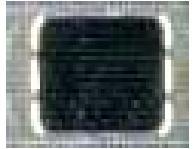
Dual : WORLD Combi module	
Design	**Thermal** black resin Technology
Contact : WORLD RLC module	
design	**Thermal** black resin Technology

Figure 4 - CM Physical Encapsulation and External Connections

4.3 Logical Interface

The **TOP DL/IL v2 platform** provides services to both external devices and internal applets as the PIV, OATH and Card Manager applets.

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

The CM provides an execution **sandbox for the PIV and OATH Applets** 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 Introduction

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

5.1.2 Identity based authentication policy

In order to describe our authentication policy we introduce the following diagram. It shows the links between the different roles, and helps rationalization of a complete trust chain. Both off-card and on-card entities are represented.

The following table describes the two roles associated to the Cryptographic Module:

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:

FIPS Role Type	Role ID	Description
Crypto Officer	**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 executes services allowed to the CO role in a secure manner.
Crypto Officer	**CAA**	The PIV Card Application Administrator (CAA) role represents an external application requesting the services offered by the PIV Applet. An applet authenticates the Application Operator role by verifying possession of the Application External Authenticate TRIPLE-DES key
User	**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.
User	**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 PUK value.
User	**OCH**	The OATH Card Holder (OCH) role is responsible for ensuring the ownership of his CM, and for not communicating his PIN to other parties. The OATH Applet authenticates the OATH Card Holder by verifying the PIN value.
Crypto Officer	**OCAA**	The OATH Card Application Administrator role represents an external application requesting the services offered by the OATH Applet. An applet authenticates the Application Administrator role by verifying possession of the OATH Card Application Administrator keys.
Unauthenticated	**AU**	Anonymous User – the unauthenticated "role"

Table 9 - Role profile definitions

The CM does not implement a maintenance mode or role.

5.1.3 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.
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 10 - 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 11 - Mechanism interfaces in applicative phase

5.1.4 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 CM detects a secure messaging corruption.
ia_co_rule.3	The Cryptographic Officer cannot get authenticated if the authorized number of attempts is reached.

Table 12 - Security rules

5.1.5   Mechanism strengths

Authentication Mechanism	Strength of Mechanism
GP mutual authentication	The strength of the mechanism used for GP authentication depends on the Secure Channel Protocol: SCP01 or SCP03.
	For Configuration with SCP03, the strength of GP mutual authentication relies on AES key length: - $\left(\dfrac{1}{2^{256}}\right)$ for AES 32-byte-long keys (default); - $\left(\dfrac{1}{2^{128}}\right)$ for AES 16-byte-long keys;
	For Configuration with SCP01, the strength of GP mutual authentication: $\left(\dfrac{1}{2^{80}}\right)$ The cryptogram sent is 8 bytes long and Triple-DES 2keys is used. Strength 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.
CAA authentication	On 3-Key Triple-DES key : $$\left(\frac{1}{2^{112}}\right)$$
	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.
	on AES key : $$\left(\frac{1}{2^{256}}\right)$$ for AES 32-byte-long keys;
OATH PIN Verification	$$\left(\frac{1}{256^{8}}\right)$$
	Pin verification is the responsibility of the OATH Applet that defines and maintains its own security policy regarding PIN but uses the PIN management services provided by the platform.

OCAA Authentication	$$\left(\dfrac{1}{2^{80}}\right)$$
	The cryptogram sent is 8 bytes long and Triple-DES 2keys is used. Strength is as described in SP 800-57.
	OCAA authentication is the responsibility of the OATH Applet using Mutual Authenticate command that involves verifying decryption of an 8-byte challenge using the secret 2-Key Triple-DES key.

Note: all authentication mechanisms above have a less than 1 in 1,000,000 random attempt success rate.

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 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 is possible.

5.2.2 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. 4. Zeroize keys of a key set: overwrite an existing key with random values.
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 (ISD) or to change the life cycle state of an application. For instance, the command can be used to set the card Manager (ISD) to "TERMINATED" state (with P1=80h, P2=FF). When this state is reached, no application can be selected – neither ISD nor PIV - and the P-RNG elements are zeroized automatically.
STORE DATA – *APDU*	This APDU command is used to transfer data to an application or the security domain (card manager) processing the command.

Table 13 – 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 or ECDSA signature (when using the PIV card application digital signature key with the RSA or ECDSA algorithm) and to perform key unwrap (when using the PIV card application key management key with the RSA or ECDSA algorithm).
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. After the personalization and before the card termination, the command can also be used to zeroize keys by overwriting existing values with new values.
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, 3DES or AES symmetric keys, RSA or ECC asymmetric keys & property template. After the personalization and before the card termination, the command can also be used to zeroize keys by overwriting existing values with random values.
SELECT – *APDU*	The ADPU command is used to select an application
CHANGE Global Pin – *APDU*	

	The ADPU command is used to reset the global pin retry counter or to change the global pin without any knowledge of the current value

Table 14 – PIV Applet Interfaces and Services

* APDU not available in contactless mode

When OATH Applet is selected the following commands are available :

Interface	Service Description
CHANGE PIN – Use this APDU to change the user PIN	
SELECT – used to select an application	
COMPUTE OTP – Use this APDU to generate an OTP value. The OTP value can be generated either in hexadecimal or in decimal format. If the applet is configured to require the PIN to be entered before each OTP computation, the successful execution of this command will invalidate the PIN. **(OTP:** One Time Password)	
GET DATA – Use this APDU to retrieve the data content of the single data object whose tag is given in the data field. The entire object is returned.	
VERIFY PIN - Use this APDU to verify the user pin. After the number of available Verify attempts has been exceeded, the PIN will be blocked.	
GET OTP - Use this APDU to retrieve OTP info (OTP counter, Token ID).	
GET MENU - Use this APDU to retrieve Menu info.	
IS MENU CHANGED - Use this APDU to retrieve Menu info (if changed).	
GET VERSION - Use this APDU to retrieve Applet info (applet version, battery counter).	
GET CHALLENGE - Use this APDU to generate a challenge for mutual authentication session keys.	
MUTUAL AUTHENTICATE - Use this APDU for the server and the card to authenticate each other with OCAA keys. **GET CHALLENGE** command is necessary prior to processing this command.	
PUT MENU - Use this APDU to set the Menu info (items and messages).	
PUT OTP - Use this APDU to create and/or update OTP info (OTP Data, Token ID).	
PUT DATA - During the personalization the APDU command is used to create and/or update Data Objects, such as: OTP counter, Token ID, PIN, PIN policy, Authentication keys, seed keys, server seed, ...	
UNBLOCK PIN - Use this APDU to unblock the user pin. It sets its ratification to the maximum one (defined during personalization).	
COMPUTE OCRA – One way challenge response - Use this APDU to generate an OTP with a server challenge and an applet counter. **(OCRA:** OATH Challenge Response Algorithm)	
COMPUTE OCRA – Response Only - Use this APDU to generate an OTP value using the OTP counter. The OTP value can be generated either in hexadecimal or in decimal format. If the applet is configured to require the PIN to be entered before each OTP computation, the successful execution of this command will invalidate the PIN flag	
GET CHALLENGE for OCRA - Use this APDU to generate a challenge for OCRA mutual authentication.	
COMPUTE OCRA – Mutual Challenge Response - Use this APDU to generate an OTP value using challenges and the OTP counter. The OTP value can be generated either in hexadecimal or in BCD format. If the applet is configured to require the PIN to be entered before each OTP computation, the successful execution of this command will invalidate the PIN flag. Mutual challenge-response is a variation of one-way challenge-response where both the card and server	

mutually authenticate each other. The card sends a random card-challenge to the server (through OCRA get challenge command). The server computes the server-response and sends it to the card along with a server-challenge.

The card verifies the server-response to authenticate the server. Then it computes the card-response and sends it to the server. The server verifies the card-response to complete the two-way authentication process.

Table 15 – OATH Applet Services

Platform		
Role ID	**CO**	**AU**
DELETE	X	
INITIALIZE UPDATE	X	X
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 16 - 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		
CHANGE Global PIN	X			
SELECT	X	X	X	X
INITIALIZE UPDATE	X	X	X	X
EXTERNAL AUTHENTICATE	X	X	X	X
MANAGE CHANNEL	X	X	X	X

Table 17 - PIV Applet Services Access

OATH Applet			
Role ID	**OCAA**	**OCH**	**AU**
SELECT	X	X	X
CHANGE PIN		X	
COMPUTE OTP		X	
GET DATA (OATH Applet Specific)	X	X	X
VERIFY PIN		X	
GET OTP	X	X	X
GET MENU	X	X	X
IS MENU CHANGED	X	X	X
GET VERSION	X	X	X
GET CHALLENGE	X	X	X
MUTUAL AUTHENTICATE	X		
PUT MENU	X		
PUT OTP	X		
PUT DATA (OATH Applet Specific)	X		
UNBLOCK PIN	X		
COMPUTE OCRA – One way challenge response		X	
COMPUTE OCRA – Response Only		X	
GET CHALLENGE for OCRA	X	X	X
COMPUTE OCRA – Mutual Challenge Response		X	

Table 18 – OATH Applet Services Access

5.2.3 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 **Card Life Cycle Manager** and the **Cryptographic Officer** are responsible for locking and terminating the Issuer Security Domain 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

5.3 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 input/output plain-text private/secret keys or other critical security parameters.
AD_RULE.2	Does not support a multiple concurrent operators.
AD_RULE.3	Does not support a bypass mode.
AD_RULE.4	Does not provide a maintenance role/interface.
AD_RULE.5	Requires re-authentication when changing roles.
AD_RULE.6	Does not allow the loading of Software/Firmware - only applets.

Table 20 - Gemalto additional security rules

5.4 Platform Critical Security Parameters

The CM uses the following CSPs:
- **GP key set of the Card Manager**
- **Secure channel session key**
- **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	U
	Secure channel session leys	U
GET STATUS	Secure channel session keys	U
INITIALIZE UPDATE	Secure channel session keys	U
	PRNG seed and seed key	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 [TRIPLE-DES, AES]	GP key set of a Security Domain (ISD/SD)	W
	Secure channel session leys	U
PUT KEY [RSA]	RSA public key for DAP verification	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)	U
	Card Holder PIN	W
CHANGE REFERENCE DATA	Card Holder PIN	W
		U
GENERATE ASYMMETRIC KEY PAIR	PIV keys	W
	Card Holder PIN	U

Table 21 - Platform Critical Security Parameters

5.5 OATH Applet Critical Security Parameters

The OATH Applet uses the following CSPs:

CSP	Length and type
OCH PIN	PIN value for OATH Card Holder authentication.
OCH PUK code	The PUK code is a 4 byte OTP number computed with the counter complementary value
OCAA Key	The 2-Key TDES OATH Card Application Authentication key used for Applet Mutual Authenticate (Kenc/Kmac).
OCAA service Key	The 2-Key TDES OATH Card Application Authentication key used for OTP service Mutual Authenticate (Kenc/Kmac).
OCAA session Key	The 2-Key TDES OATH Card Application Authentication session key used for Mutual Authenticate (SKenc/SKmac), and derived from either OCAA key or OCAA service key.
OATH Seed Key	This 2-Key TDES is used to compute and diversify the SEED.
OATH seed	The OATH SEED is used to generate the OTP.
Server seed Key	This 2-Key TDES is used to compute and diversify the server SEED.
Server seed	The server SEED is used to authenticate the server response during the OCRA mutual authentication process.

Table 22 - OATH Applet Critical Security Parameters

5.6 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 CM retrieves the ATR from the module to validate that the ATR bytes are the same as those listed in Appendix B.
- 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.

7 Physical Security

The **CM** single chip module is designed to meet the **FIPS140-2 level 3 Physical Security requirements**.

7.1 Manufacturing Process

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 hard 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.

7.2 Hardware Security Mechanisms

Though not tested as part of the module's FIPS 140-2 validation conformance testing, the embedded SLE66CLX1280PE(M) **chip from Infineon** provides the cryptographic module with hardware security mechanisms such as probing detection, low frequency, high temperature, light intensity and supply voltage monitoring. The chip reacts to a light attack, temperature range exceeded, low/high clock frequency, and low/high power supply voltage by resetting the cryptographic module. Any unprotected sensitive data are lost.
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 Issuer Security Domain Keys

When the Issuer Security Domain 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 Issuer Security Domain 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 Issuer Security Domain commands. The key set associated with the secure channel is such that:

Secure Channel Protocol is either SCP01 or SCP03 [4][12], depending on configuration (see Table 2 –SCP support and **applet set configurations**):

SCP01 uses Triple-DES keys 16 bytes:
- All Triple-DES keys are double length keys (16 bytes),
- All Triple-DES operations are performed using triple DES encryption or decryption.
- All MAC generations are computed on 8 bytes.

SCP03 uses AES keys 16 or 32 bytes
- All AES operations are performed using AES encryption or decryption.
- All MAC generations are computed on 16 bytes.

Key sets are identified by Key Version Numbers ('01' to '7F'). The keys within a key set version are used to derive secure channel session keys for the following functionalities:
- Secure Channel Encryption (S-Enc) is used for secure channel authentication and encryption.
- Secure Channel Message Authentication Code Key (S-Mac) is used for secure channel MAC verification.
- Data Encryption Key (DEK) is used for sensitive data encryption.

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.

9.2 Application provider Security Domain Keys

As the Issuer Security Domain is the on-card representative of the Card Issuer, an Application Provider Security Domain, or simply a Security Domain, is the on-card representative of an Application Provider.

Applets may rely on a Security Domain different from the Issuer Security Domain and use keys of various types through the cryptographic services of the module: Triple-DES keys, AES keys, RSA public and private

keys, RSA Chinese Remainder public and private keys, and ECDSA public and private keys (supported by the platform).

In addition, a Public RSA key (1024 bits) may be loaded into the module, to verify the Data Authentication Pattern (DAP) when loading an applet. This feature is only available in a Security Domain with DAP verification privilege. For more detail, see **GP[4]** specification.

Applet key management is out of the scope of this security policy.

9.3 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

9.3.1 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 or ECC) 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 or AES 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 or ECC) 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 or ECC) 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 or ECC) 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.

9.3.2 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".

9.4 Key Generation

The platform on-board key generation is able to generate ECDSA key, RSA key and RSA Chinese Remainder Keys.

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.

9.5 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.

9.6 Security Domain Key Entry

Keys are entered in the cryptographic module using the PUT KEY APDU command and under the responsibility of the applets. Non-system applets are out of the scope of this Security Policy.

The Issuer Security Domain or a Security Domain enforces entering cryptographic symmetric keys securely within a secure channel.

The Cryptographic Officer (of the Card Issuer) sends the PUT KEY APDU command to:

- Replace multiple keys within an existing key set version.
- Replace an existing key set version with a new key set version.
- Add a new key set version containing multiple key(s).

The Security Domain key set already present within the cryptographic module is the default key set. If this key set version is replaced, the replacement becomes the default.

The User (of the Application Provider) sends the PUT KEY APDU command to:
- Add a RSA public key for DAP verification.

9.6.1 Input Data

While the key set structure can be presented to the card in encrypted form or in plaintext, **the key values are always encrypted with the Data Encryption Key**.
The key set structure includes a check value for each key in order to ensure their integrity.

9.7 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.

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

The cryptographic module stores key components according to the key type.

KEY TYPE	KEY COMPONENT
Triple-DES keys	Key value component
AES keys	Key value component
RSA keys	Public exponent **e** component Modulus **N** component Private exponent **d** component
ECDSA (supported by the platform)	Private scalar d
RSA Keys CRT	Chinese Remainder **P** component Chinese Remainder **Q** component Chinese Remainder **PQ** component Chinese Remainder **DP1** component Chinese Remainder **DQ1** component

Table 23 - Key types and components mapping table

The PIN is a critical security parameter that is a java object and is stored encrypted.

9.8 Key Zeroization

The cryptographic module provides applets with the capability to set all plaintext cryptographic keys and other unprotected critical security parameters within the module to zero or random values (see **Table 14 – PIV Applet Interfaces and Services**)

All CSPs, including the GP key set, Secure channel session key, DRNG seed and DRNG key, and RSA public key can be zeroized with a PUT KEY command and then by setting the card state to TERMINATED with a SET STATUS command (see Table 13 – System Applet Interfaces and ServicesError! Reference source not found..

10 EMI/EMC

The TOP DL/IL v2 cryptographic module has been tested to meet the EMI/EMC requirements specified in FCC Part 15 Subpart J, Class B.

11 Self Tests

The **TOP DL/IL V2** performs the following self-tests to ensure that the module works properly.

SELF-TESTS	EXECUTION
Cryptographic algorithm test (Known-answer tests for Triple-DES, AES, SHA-1, SHA-256, SHA-384, SHA-512, RSA, ECDSA, ECDH)	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 (RSA On Board key Generation and EC Key Generation)	Conditional
Software load test.	Conditional
Continuous random number generator test.	Conditional

Table 24 - 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 **Software load 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 command can be performed. The behavior of the card depends on error:

- **Severity level 1 error:**
    - Integrity test, internal error counter is increased, the card returns an error status before becoming mute.
- **Severity level 2 error:**
    - Cryptographic algorithm tests, internal error counter is incremented, the card returns an error status before becoming mute.
    - Conditional self-tests (DRNG 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 Design Assurance

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

12.1 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 that allow 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.

12.2 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', and 'Card Initialization Specification' documents) define and describe the steps necessary to deliver and operate the **CM** securely.

12.3 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.

13 PIV Applet Guidance

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

The following rules must be observed for conformance to FIPS 201-1 and FIPS 140-2:
1. The PIN shall be 8 bytes.
2. The PIN shall be composed of numeric characters.

14 OATH Applet Guidance

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

The following rules must be observed for conformance to FIPS 140-2:
1. The PIN shall be 8 bytes.
2. The PIN shall be composed of numeric characters.

15 Mitigation of other attacks

The TOP DL/IL V2 has been designed to mitigate the following attacks:

Side channel attacks :
- Timing Attacks : The attacker analyzes the time consumption used to execute cryptographic algorithms.
- Simple Power Analysis : The attacker interprets power traces, or graphs of electrical activity over time.
- Differential Power Analysis : The attacker studies the power consumption of a cryptographic hardware device. And compute intermediate values by statistically analyzing data collected from multiple cryptographic operations.
- Electromagnetic Analysis : The attacker measures the electromagnetic emissions. This attack aims to recover secret.

In these cases the main major task of the countermeasures is to remove the dependencies that exist between processed data and the current and/or time, electromagnetic consumption/processing/emission. To mitigate these side channel attacks the platforms implements countermeasures in order to make blurring instrumentation & signal analysis and a wide variety of numerical/logical tricks that decorrelate the side channel from the secret data.
Software countermeasures are random order execution, random delay, parallel processing to add noise, usage of encrypted logical data to remove correlation between current consumption and logical data and hardware countermeasures is desynchronization as dummy cycles, unstable clocking, noise (current scrambling, smoothing) and sensors activation, memory ciphering.

Fault Attacks :
The fault attacks are semi-invasive attacks. The goal of this kind of attacks is to perturb the 'normal' execution of the chip in order to find out or corrupt sensitive or critical parameters. Faults may be used to create exploitable vulnerabilities.
Card Tearing is a fault attack. Card tearing (or power failure) may cause inconsistency data.

To mitigate fault attacks countermeasures implemented are the activation of the hardware sensors before sensitive processes, the detection of repetitive fault attacks using detection counter and putting the cryptographic module in terminated state once the number of detection has reached its maximum quota, the backup for operations on sensitive data, the redundancy to check consistency of secure processes, the check of data integrity, the usage of non reversible life cycle states, the memory ciphering and bus protection.

A separate and proprietary document describes the mitigation of attacks policy provided by the TOP DL/IL V2 platform.

16 Appendix A – GP Specification

This chapter provides relationships between the cryptographic module APDU commands and the GP specifications.

APDU COMMAND	DOCUMENTATION: GLOBAL PLATFORM SPECIFICATION GP211 [4] OR GP22 [12].	
DELETE	CHAPTER 9	SECTION 2
EXTERNAL AUTHENTICATE	APPENDIX D	SECTION 4 (SCP 01)
EXTERNAL AUTHENTICATE	CHAPTER 7	SECTION 1 (SCP 03 – GP22)
GET DATA	CHAPTER 9	SECTION 3
GET STATUS	CHAPTER 9	SECTION 4
INITIALIZE UPDATE	APPENDIX D	SECTION 4 (SCP 01)
INITIALIZE UPDATE	CHAPTER 7	SECTION 1 (SCP 03 – GP22)
INSTALL	CHAPTER 9	SECTION 5
LOAD	CHAPTER 9	SECTION 6
MANAGE CHANNEL	CHAPTER 9	SECTION 7
PUT DATA	CHAPTER 4	SECTION 12 (OP 2.0.1' SPECIFICATION)
PUT KEY	CHAPTER 9	SECTION 8
PUT KEY	CHAPTER 7	SECTION 2 (AES KEYS – GP22)
SELECT	CHAPTER 9	SECTION 9
SET STATUS	CHAPTER 9	SECTION 10
STORE DATA	CHAPTER 9	SECTION 11

Table 25 - Relationships between APDU commands and GP Specifications

The **constraints of use** for each APDU commands are described in subsection 1 "Definition and scope".

The correct values of the **APDU parameters** (P1, P2, LC, and LE) are described in subsection 2 "Command message".

The **conditions of use** of the APDU commands correspond to the authorized sequences of APDU commands.

17 Appendix B – Identification and FIPS mode :

1. CPLC data element can be read with a Get Data command (tag 9F7Fh):
   In the FIPS mode, the first 6 bytes of the CPLC data (tag 9F 7Fh) must be :
   > IC Fabricator – 40 90h
   > IC Type – 61 28h
   > Operating System Identifier: 12 91h
   > Operating System release level: 01 00h

   These values identify clearly:
   The Firmware version: **Build#11 - M1005011 + Softmask V04**
   With **PIV Applet v2.00** + **OATH Applet v2.10**,
   And,
   The Part (Hardware version): **A1025258 for TOP DL v2 and A1023393 for TOP IL v2.**

2. The flow Identification byte must be **1x** value to indicate **FIPS configuration**.
   x depends on the SCP configuration of the card (x = 11h for SCP01, x = 13h for SCP03-00 and x = 17h for SCP03-10)
   This byte can be retrieved issuing a Get Data using tag 01 01h.
   The tag 01 01h can be broken down as follow:
   > Card serial number: 8 bytes
   > Reserved bytes: 3 bytes
   > **Flow identification: 1 byte**
   > Reserved bytes: 4 bytes

3. A card in **FIPS configuration** must have following historical bytes T5-T9 in the ATR :

T5 = FMN	**B0h**	Gemalto Family Name – *JavaCard financial/e-business*
T6 = PRN	**83h**	Gemalto Product Name – *TOP DL/IL V2*
T7 = OSV	**11h**	Gemalto OS Version – *TOP DL/IL V2*
T8 = PRV	**1xh**	Gemalto Program Version or Custom – *Flow ID byte*
T9 = CID	**E5h**	Gemalto Chip Identifier – *Infineon SLE66CLX1280PE*

"SECURED" must be the required state for card delivery outside Gemalto.
The CO must check the state to ensure it is OP_SECURED to be in FIPS mode. If card state is not OP_SECURED both CO and User must open secure channel in at least MAC mode.

- END OF DOCUMENT -