TOP DL V2- FIPS 140-2 L3

Security Policy

TITLE	TOP DL V2- FIPS 140-2 L3 - Security Policy
REF.	SP01R20033G - _11
DATE:	March 2009, the 30 th
AUTHOR	FDefrance, SL, R&D, Gemalto
	Frederic Garnier, IAM R&D, Gemalto
APPROVED	Arnaud Lotigier, Program Manager, Gemalto

REVISION HISTORY

Release *(Xyy)*	Date *(dd/ mm/ yy)*	Author	Modifications
01	17/03/09	F.Defrance	Initial issue.
02	30/03/09	F.Defrance	Take into account Frederic Garnier remarks
03	05/06/09	F.Garnier/ F.Defrance	Product name is now TOP DL V2, Update GP references, Add table “Table 5 – Additional Security Functions”, ...
04	17/07/09	F.Garnier/ F.Defrance	Add CMAC reference
05	29/09/09	F.Defrance	Update configuration list
06	14/01/10	F.Garnier/ F.Defrance	Review William’s comments; minor updates;
07	26/01/10	F.Garnier/ F.Defrance	After Ed/William comments: add DAP verification and Security Domain (ISD/SD) precisions.
08	29/01/10	F.Garnier/ F.Defrance	Only esthetic updates (Accept a change, update color of text)
09	05/03/10	F.Garnier/ F.Defrance	Add Softmask number due to CRC 16
10	15/10/10	F.Defrance	Following remarks : updates table 16 and 17
11	19/10/10	F.Defrance	Update softmask version in appendix

DISTRIBUTION LIST

N°	Name	Role	Society
1	F.Defrance	FIPS Coordinator	Gemalto
2	E. Morris	FIPS Evaluator	SAIC Laboratories
3	A.Lotigier	Program Manager	Gemalto
4	F. Garnier	Project Leader	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;

[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)

1 Scope

This Security Policy specifies the security rules under which the Gemalto Smart Card, herein identified as the **"TOP DL V2"** platform, 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).

2 Introduction

2.1 Gemalto Smart Card Overview

Gemalto aims to provide **FIPS140-2 Level 3** cryptographic smart cards. The cards are based on a Gemalto Open OS Platform and on which FIPS 140-2 L3 validated platform-independent applets may be loaded and instantiated at post issuance. As a basis the card provides authentication, encryption and digital signature cryptographic services. It is under the charge of the applets to be loaded and instantiated within the card to use in conformance with specifications the different services offered by the platform. Moreover, FIPS 140-2 L3 validation is required for the applets to be loaded and instantiated within the card in order to reach the FIPS 140-2 L3 compliance for the **whole and composite product (i.e. platform plus post issued applets).**Together, the card and applets provide authentication, encryption, and digital signature cryptographic services. This **whole product**, made up of the **Gemalto platform and the applet suite is aimed to reach FIPS 140-2 L3 compliance**. However, the present document is only dedicated and focused to the Gemalto TOP DL V2 platform part without any installed applet or package other than the Issuer Security Domain (ISD) and Supplementary Security Domain (SSD or SD) if any.

This security policy specifies the security rules under which the Java Card **TOP DL V2 (cryptographic module)** platform operates.

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, and provides FIPS approved cryptographic algorithms and self-tests.

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 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**
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 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 3**. The individual security requirements meet the level specifications as follows.

Security Requirements Section	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 1 – FIPS 140-2 Security Levels

3 Cryptographic Module Specification

3.1 Gemalto Crypto-Module Cryptographic Boundary

The Cryptographic Boundary is defined to be the 'module edge' of the **TOP DL V2** referred to hereafter as the Micro Module, a set of "embedded" hardware and software that implements cryptographic functions and processes, including cryptographic algorithms and key generation. **TOP DL V2 – Micro-Module** 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 [9]** compliant smart card.

The Cryptographic Module provides dual interfaces (i.e. contact and contact-less) where the same security level is achieved.
Depending on the market and the end-customer requirements, PK support (i.e. PK enabled or PK disabled) and Secure Channel Protocol can be configured during the manufacturing in order to answer as precisely possible to the market and the end-customer requirements:

- **CONFIGURATION 1**: The product is initialized in dual interface mode; it means that both contact and contact-less mode are operated, with FIPS PK self-tests and PK services enabled. The secure channel protocol is based on AES keys : GP-SCP03-00 (option i=00 as per **GP specification [12])**..
- **CONFIGURATION 2**: The product is initialized in dual interface mode; it means that both contact and contact-less mode are operated, with FIPS PK self-tests and PK services enabled. The secure channel protocol is based on AES keys : GP-SCP03-10 (option i=10 as per **GP specification [12]**)
- **CONFIGURATION 3**: The product is initialized in dual interface mode; it means that both contact and contact-less mode are operated, with FIPS PK self-tests and PK services enabled. The secure channel protocol is based on Triple-DES : GP-SCP01

The following table gives an overview of those 3 different configurations regarding SCP (Secure Channel Protocol) support.

	SCP (Secure Channel Protocol)
CONFIGURATION 1	SCP03-00
CONFIGURATION 2	SCP03-10
CONFIGURATION 3	SCP01

Table 2 –SCP 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.**

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

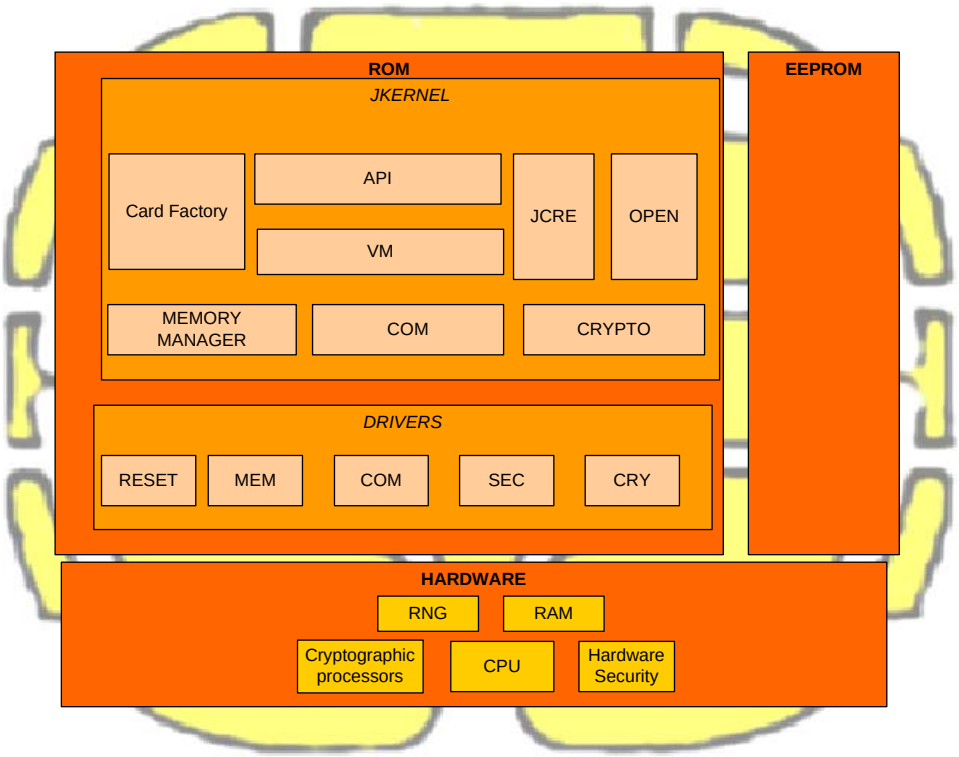

Figure 1- Cryptographic Module Boundary

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

3.2 ROM

The chip's ROM includes the **TOP DL V2** Operating System (OS) meaning that the OS is protected against disclosure and modification. Some applets are present in the ROM code. **However, the applets are to be independently validated for FIPS 140-2 compliance and this is not the scope of this security policy that is only focused on the Java Card Platform**. 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. This OS includes the following design entities:

Design item	Functionality
JKERNEL layer	
The Jkernel sub-system provides a Java Card-oriented environment for the Applications sub-system, including: - (**JCRE**) **the Java Card [6]** runtime environment including OS dispatcher, registry, loader, logical channel management, RMI. - (**API**) the public JC API: **JavaCard [5]** and other optional APIs (e.g. proprietary…). - (**VM**) the virtual machine, **Java Card standard [7]**, including byte code interpreter, firewall, exception management, VM extension for byte code optimizer. - (**OPEN**) the Global Platform environment [4] [12] including card content management, key management, card and applet life cycle management, security policy. - (**Card Factory**) the Card Factory, including OS bootstrap, OS initialization, self-tests, industrialization command. - (**MEMORY MANAGER**) the Memory Manager including services such as memory access, allocation, delete, GC. - (**COM**) the Communication handler including services, such as ATR, PSS, T=0, T=1, T=CL. - (**CRYPTO**) the Cryptography engines including services such as Triple-DES (ECB, CBC), hash functions (SHA), RSA (including paddings such as PKCS), ECC, on-board key generation (RSA, ECC), AES (ECB, CBC), CMAC.	
DRIVERS layer	
The drivers layer provides the following services: - (**RESET**) OS startup and chip initialization, IT/exception vectors, MMU/banking configuration… - (**MEM**) memory module including NVM access, atomicity and transaction management… - (**COM**) communication module including IO exchanges, timing control… - (**SEC**) security module including counter-measures and fault attack management, CRC, RNG… - (**CRY**) Cryptography module including basic algorithms such as Triple-DES, AES, SHA, RSA, ECC	

Table 3 – ROM – content description

3.3 EEPROM – Applets

The chip's EEPROM can store applets. However, in order to remain FIPS 140-2 L3 validated for the resulting TOP DL V2 with subsequently instantiated applets, those applets would have to be FIPS 140-2 L3 validated independently and are not tested as part of this validation. As such, t**hese applets are outside the scope of this Security Policy that only focuses on the Java Card platform.**

3.4 Hardware Chip

The cryptographic module includes the 66CLX1280PEM **chip from Infineon**.
It includes:

- EEPROM 128 KB
- ROM 240KB
- XRAM 6KB
- Active shield
- Hardware and enhanced security sensors
- Memory Security for XRAM, EEPROM and ROM.
- Memory Management and Protection Unit through MMU,
- Random Generator,
- Cryptographic coprocessor
- Hardware high speed 16bits CRC.
- Both contact and contact-less interfaces.

3.5 FIPS Approved Security Functions

The following table gives the list of FIPS approved security functions that are provided by the **TOP DL V2** Java Card API.

SECURITY FUNCTION	DETAILS	FIPS APPROVED
Triple-DES	ECB mode in encryption	Yes
	ECB mode in decryption	Yes
	CBC mode in encryption	Yes
	CBC mode in decryption	Yes
SHA-1, SHA-256, SHA-384, SHA-512	Hashing operation	Yes
ECFP	Key pair generation following X9.62	Yes
ECDSA (P-192, P-224, P-256, P-384, P-521)	Signature following X9.62 with SHA-1 hashing	Yes
	Verification following X9.62 with SHA-1 hashing	Yes
RSA	Key generation	No
	Signature following PKCS#1with SHA-1 hashing	Yes
	Verification following PKCS#1with SHA-1 hashing	Yes
P-RNG	Pseudo Random Number Generation following X9.17	Yes
AES	ECB mode in encryption	Yes
	ECB mode in decryption	Yes
	CBC mode in encryption	Yes
	CBC mode in decryption	Yes
CMAC	Mode for authentication	Yes

Table 4 – 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	Yes
	Verification following X9.62 with SHA-256 / SHA-384 / SHA-512 hashing	Yes

Table 5 – Additional Security Functions

4 Cryptographic Module Ports and Interfaces

The **TOP DL V2 – Micro-Module** restricts all information flow and physical access.
Physical and logical interfaces define all entry and exit points to and from the micro module.

4.1 Physical Port – Contact mode

4.1.1 PIN assignments and contact dimensions:

TOP DL V2 – Micro-Module follows the standards **"ISO 7816-1 Physical characteristics" [9]** and **"ISO 7816-2 Dimensions and contact location" [9]**.

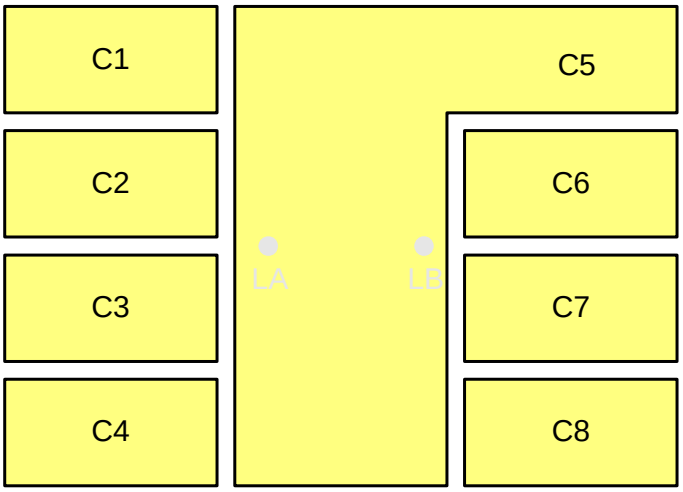

Figure 2 - Contact plate example – Contact physical interface

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 6 - 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 7 - Voltage and frequency ranges

4.2 Physical Port – Contact-less mode

4.2.1 Contacts assignments

In the contact-less mode the TOP DL V2 cryptographic module 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**

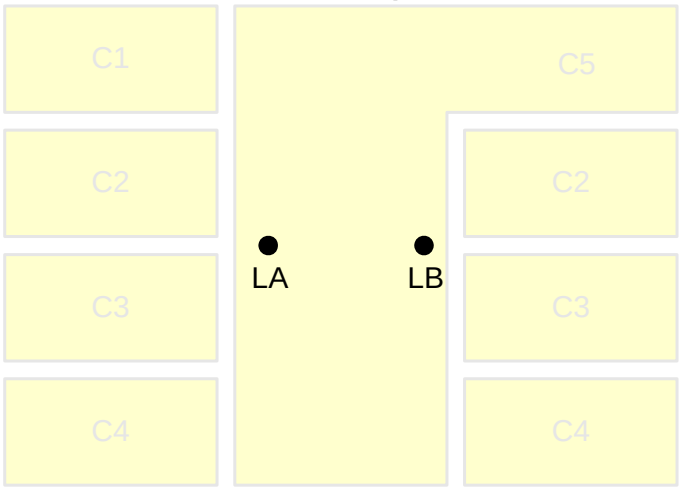

Figure 3 - Contact plate example - Contact-less antenna contacts

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

Table 8- Contact plate pin list – Contact-less mode

4.2.2 Condition of uses

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

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

Table 9 - Voltage and frequency ranges

4.2.3 Picture – Dual Mode

Thermal black resin process, contact and contactless technology

WORLD module dual interface	
	
design	**Thermal** black resin Technology

4.3 Logical Interface

TOP DL V2 – Micro-Module provides services to both external devices and internal applets with services. External devices have access to services by sending APDU commands while internal applets have access to services through internal API entry points.

For security reasons, **TOP DL V2 – Micro-Module** inhibits all data output via the data output interface when an error state is reached and during self-tests.

4.3.1 APDU commands

The data exchange protocol between the cryptographic module and an outside device follows the **ISO 7816-4 [9] standard**. The cryptographic module acts as a slave device, receiving and executing APDU commands from outside devices. The cryptographic module receives APDU commands, performs the related internal processes according to its security policy, and then answers with APDU responses.

An APDU command consists of a mandatory command header of four bytes conditionally followed by a command body (Input Data). The response APDU consists of a conditional response body followed by a mandatory response trailer of two bytes. ISO APDU Types 1, 2, 3 and 4 are supported.

ISO Command Type	Description
Type 1 – ISO command	No input data, no response data
Type 2 – ISO “Out” command	No input data, response data
Type 3 – ISO “In” command	Input data, no response data
Type 4 – ISO “In” and “Out” command	Input data, response data

Table 10 - Accepted ISO APDU types

The cryptographic module enforces the establishment and use of a secure path for exchanging sensitive data with an external device.

4.3.2 API interface

TOP DL V2 – Micro-Module provides trusted applets with internal services through its JavaCard [5] and GP[4] APIs. The cryptographic module provides an execution sandbox for the applets and performs the requested services according to its roles and services security policy. Internal applets are not part of this validation; however, the JavaCard API and services are defined in the following section for informational purposes.

5 Roles, Services and Authentication

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.

The Cryptographic module introduces particular user classification. The external boundaries of the cryptographic module allow applets to use it. Thus, the communication between the cryptographic module and outside is not restricted to APDU communication. Actually, applets can interact with the cryptographic module by using Java interfaces (methods or object references). Some of these interfaces are identity-based services and require authentication. Some are not.

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:

Cryptographic Officer Role	**Description**
Cryptographic Officer	Cryptographic Officer is considered as the smart card administrator of the Issuer Security Domain (ISD) and the Supplementary Securiy Domains (SSD). The Cryptographic Officer has possession of the Secure Channel keyset stored within the Security Domain (ISD and SSD if any).
User Role	**Description**
User	User is considered as an entity which has possession of the secure channel keyset and can request services provided by either the Issuer Security Domain or a dedicated Security Domain on the card. User authenticates in the same way as a Cryptographic Officer.
Maintenance Role	**Description**
None	

Table 11 - Role profile definitions

Each role is assumed implicitly as the module does not provide for explicit role selection. The services provided by the module to each role is specified in the table below

Roles/Services	Crypto Officer role Authenticated	User role Authenticated	No role Unauthenticated
INSTALL	x	x	
LOAD	x	x	
DELETE	x	x	
EXTERNAL AUTHENTICATE	x	x	x
GET DATA	x	x	x
GET STATUS	x	x	
INITIALIZE UPDATE	x	x	x
PUT DATA	x	x	
PUT KEY	x	x	
SELECT	x	x	x
SET STATUS	x	x	
STORE DATA	x	x	
SET ATR	x	x	
GET MEMORY SPACE	x	x	
MANAGE CHANNEL	x	x	x

Table 12- Issuer Security Domain services Vs Roles

An operator can initiate module self-tests by issuing a card reset and issuing an APDU command. A user can also retrieve the module ATR on card power-up

5.1.3 Mechanism interfaces

The following table describes the mechanisms for identity authentication:

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 13 - Mechanism interfaces

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 PIN is corrupted.
ia_co_rule.1	The Cryptographic Officer cannot get authenticated if the authorized number of attempts is reached.
ia_co_rule.2	The Cryptographic Officer must be re-authenticated if the card is reset.
ia_co_rule.3	The Cryptographic Officer must be re-authenticated if the cryptographic module detects APDU communication corruption.

Table 14 - Security rules

5.1.5 Mechanism strengths

The strength of the mechanism used for GP authentication depends on the Secure Channel Protocol: SCP01 or SCP03.

For Configuration 1 and 2 (SCP03), the strength of GP mutual authentication relies on AES key length:

- $\left(\frac{1}{2^{256}}\right)$ for AES 32-byte-long keys (default);
- $\left(\frac{1}{2^{128}}\right)$ for AES 16-byte-long keys;

For Configuration 3 (SCP01), the strength of GP mutual authentication: $\left(\frac{1}{2^{112}}\right)$

5.2 Access Control Policy

5.2.1 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.

- The **PIN** can only be managed by the applet that owns this PIN.
- The **administrative commands** are restricted: these APDU commands can be used only in a secure channel (**session**). A secure channel is open when the card user has been authenticated through the GP mechanism as being the owner of the **Cryptographic Officer** secrets. The secure channel is closed if the card is reset or if the system closes it.
- The Java objects created by the applets are protected by the **Firewall** mechanism of the JCRE. The rules that are applied to **Java object accesses** are specified in the **JCRE specification [5]**. The firewall is a means of protecting applet information.
- The Cryptographic Officer can manage **loaded applets life cycle state** (Issuer Security Domain applet included). It ensures that the proposed transitions are coherent with the **GP specification**. An applet can manage its own life cycle state under the same conditions. An additional condition is imposed to applets that attempt to change the Issuer Security Domain life cycle state: they must have the privilege for **Card life cycle management**.

5.2.2 Services

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

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 or a key.
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 Issuer Security Domain, 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 byte code 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 used and managed by the Issuer Security Domain (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 (Issuer Security Domain, Security Domain or applet instance)..
SET STATUS – *APDU*	This APDU command is used to change the state of a Security Domain (ISD / SD) 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 (ISD / SD) processing the command.

Table 15 - Cryptographic officer accorded interfaces and services

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.
GET DATA – *APDU*	This APDU command is used to retrieve a single data object.
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.
SELECT – *APDU*	This APDU command is used for selecting an application (Issuer Security Domain, Security Domain or applet instance).

Table 16 – Unauthenticated role accorded interfaces and services

	Cryptographic officer role Authenticated	User role Authenticated	User role Unauthenticated
DELETE	X	X	
EXTERNAL AUTHENTICATE	X	X	X
GET DATA	X	X	X
GET STATUS	X	X	
INITIALIZE UPDATE	X	X	X
INSTALL	X	X	
LOAD	X	X	
MANAGE CHANNEL	X	X	X
PUT DATA	X	X	
PUT KEY	X	X	
SELECT	X	X	X
SET STATUS	X	X	
STORE DATA	X	X	
DAP VERIFICATION		X	

Table 17 – Authenticated and unauthenticated role accorded interfaces and services

Regarding the applet allowed interfaces; those interfaces are this API defined in [5] and [4]

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 18 - 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 19 - Gemalto additional security rules

5.4 Security Relevant Data Item

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

- **GP key set of a Security Domain (ISD/SD)**
- **Secure channel session key**
- **DRNG seed and DRNG key**
- **RSA public key for DAP verification**

The following table proposes 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	U
EXTERNAL AUTHENTICATE	GP key set of a Security Domain (ISD/SD) Secure channel session leys	U U
GET STATUS	Secure channel session keys	U
INITIALIZE UPDATE	Secure channel session keys	U
INSTALL	Secure channel session keys	U
LOAD	Secure channel session keys	U
PUT DATA	Secure channel session keys	U
PUT KEY [TRIPLE-DES, AES]	GP key set of a Security Domain (ISD/SD) Secure channel session leys	W 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

Table 20 - Security Relevant Data Items

6 Finite State Model

The **TOP DL V2** 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.

7 Physical Security

The **TOP DL V2** 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.

7.2 Hardware Security Mechanisms

Though not tested as part of the module's FIPS 140-2 validation conformance testing, the embedded 66CLX1280PEM **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.

8 Operational Environment

This section does not apply to **TOP DL V2**. 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.

9 Cryptographic Key Management

9.1 Issuer Security Domain Keys

The cryptographic module implements **GP[4] & GP[12]** 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 Issuer Security Domain applet and the Cryptographic Officer.

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 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.

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.

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 Key Generation

The cryptographic module on-board key generation is able to generate ECDSA key, RSA key and RSA Chinese Remainder Keys. This functionality is available to on-board applets only, which are not part of this validation.

9.4 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.

9.4.1 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.

9.5 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	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 21 - Key types and components mapping table

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

9.6 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. All CSPs, including the GP key set, Secure channel session key, DRNG seed and DRNG key, and RSA public key can be zeroized by setting the card state to TERMINATED.

10 EMI/EMC

The **TOP DL 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 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)	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
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 22 - Self-tests list

11.1 Self-Test Execution

After **TOP DL V2** is powered up and before executing any APDU commands, the module enters the self-test state and performs all cryptographic algorithm and software integrity self-tests as specified in FIPS 140-2 standard **[1]**.

The cryptographic module start-up process has been designed in such a way that it cannot be bypassed. This enforces the execution of self-tests before allowing any use and administration of the module, thus guaranteeing a secure execution of the module cryptographic services.

If these self-tests are passed successfully, incoming APDUs are processed.

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

11.2 Self-Test Failure

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

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

If an error occurs during another self-test, the card enters a state where no more command 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 (DRNG continuous test and pair wise consistency test), internal error counter is incremented, the card returns an error status before becoming mute.

An error while loading an applet closes the secure channel with the Issuer Security Domain. It shall be re-opened, to retry applet loading: the Cryptographic Officer has to be re-authenticated.

Other errors require resetting the card.

12 Mitigation of other attacks

The TOP DL V2 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 mitigation of attacks policy provided by the TOP DL V2 platform.

13 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 23 - 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.

14 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 V03`** and the Part (Hardware version): **`A1023378`** of the validated module**.**

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 V2***
T7 = OSV	**11h**	Gemalto OS Version – ***TOP DL 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 -