Gemalto and ActivIdentity Inc.

SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite V2 for Extended PIV

FIPS140-2 Cryptographic Module Security Policy

Version 1.2

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for "SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite V2 for Extended PIV" cryptographic module, submitted for validation, in accordance with FIPS140-2 Level 2 requirements. Included are a description of the security requirements for the module, and a qualitative description of how each security requirement is achieved. In particular, this security policy specifies the security rules under which the cryptographic module must operate.

2. OVERVIEW

2.1 GEMALTO TOP DL GX4 - FIPS

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

The platform ensures on-card applets safe coexistence thanks to its secure Virtual Machine (VM) and firewall. The Java VM is fully compliant with the **Java Card standard 2.2.1**.

The card life cycle is managed according to the **Global Platform (GP) specification 2.1.1**. Issued cards have been loaded with a set of applets, cryptographic keys, and a PIN, and are moreover in the "SECURED" state. The security implementation is fully compliant with the **Global Platform (GP) specification**.
The cryptographic module integrates symmetric and asymmetric cryptographic algorithms as specified in the **JavaCard specification** and offers RSA for Signature/Verification, SHA-1 hashing, on-board RSA Key generation, Triple-DES CBC and ECB and AES ECB and CBC algorithms.

The card is designed in the following configuration:
TOP DL GX4: This is a dual interface card providing both contact and contactless interfaces. This card has two hardware versions A1005291 - CHIP.P5CD144.MPH051B and A1011108 - CHIP.P5CD144.MPH051B, and firmware version GX4-FIPS EI08.

2.2 ACTIVIDENTITY DIGITAL IDENTITY APPLET SUITE V2 FOR EXTENDED PIV

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV supports execution of services via contact and contacless interfaces. Only a few services are contactless enabled, while all applet commands can execute with a contact reader.

The v2 applet suite consists of six applets:

- **Access Control Applet (ACA)** – This applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. Three off-card entity authentication methods – GP secure messaging, PIN, and ActivIdentity External Authentication are included by default in the ACA applet.
- **PKI/Generic Container/ SKI (PKI/GC/SKI) Applet** – The PKI/GC/SKI Applet can be used to provide secure storage for PKI credentials, and other data that are required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based cryptographic operations using the RSA private key stored in the

PKI buffers. The applet also exposes services for OTP (One Time Password) through a synchronous or asynchronous authentication

- **ASC Library package** – This is the library package that implements functions required by other applets. The library functions are not directly accessible via the cryptographic module command interface.
- **PIV EP Wrapper Applet** – This Applet implements the Personal Identity Verification services from NIST SP800-73-1. It exposes the End Point (EP) APDU commands from this specification. The Applet is a wrapper on top of v2.6.2b applets (ASC Lib, ACA and GC/PKI/SKI above). Its purpose is to access PIV Card-Edge and objects although objects are stored in v2.6.2b applet instances. This PIV Applet cannot operate in a standalone mode; it must link with ACA and GC/PKI/SKI(s) applet to operate properly. This applet can only be instantiated in a strictly compliant mode to SP800-73-1 and data model
- **PIV EP Extended (Ext) Applet** – This Applet implements SP800-73-1 (both at card-edge and data model levels) and is extended to support additional features on top of native PIV such as support of additional PKI RSA keys (example for administrator login. PKI Key Encryption Key, SSO (single sign-on) storage, support of SKI authentication mechanisms, etc. This applet can be instantiated in PIV EP mode (native PIV features) or in PIV Ext mode (extensions are accessible through the 800-73-1 card edge.).
- **Secure Messaging Anonymous (SMA) plug-in Applet** – this is an authentication and secure messaging plug-in to the ACA applet. It provides PKI based card authentication and secure messaging (using Triple-DES) to secure the communication between an off-card entity and any card applications

3. SECURITY LEVEL

The SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite V2 for Extended PIV is designed and implemented to meet the overall Level 2 requirements of FIPS140-2.

The Card Security Controller (CSC) should obtain the hardmask and softmask version via the Answer-To-Reset (ATR). The CSC should set the Access Control Rule (ACR) according to table 8 to put the module into the Approved mode of operation.

The individual security requirements specified for FIPS 140-2 meet the level specifications indicated in the following table.

Security Requirements Section	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	2
Mitigation of other attacks	2

Table 1 – Individual FIPS 140-2 Security Levels

4. CRYPTOGRAPHIC MODULE SPECIFICATION

4.1 GEMALTO CRYPTO-MODULE CRYPTOGRAPHIC BOUNDARY

The Cryptographic Boundary is defined to be the 'module edge' of the SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite V2 for Extended PIV Crypto-Module, 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. SafesITe TPC DM - FIPS Micro-Module is a single chip implementation of a cryptographic module. The micro-module is designed to be embedded in a plastic card body.

During the Gemalto manufacturing process, the chip (ICC) is wire-bonded on the inner side of a contact plate, then globe-topped with resin. The resulting Micro-Module meets the physical security requirements of FIPS140-2 Level 3.

All components of the SafesITe TOP DL GX4 – FIPS Micro-Module are included in the cryptographic module boundary, as shown in the following figure:

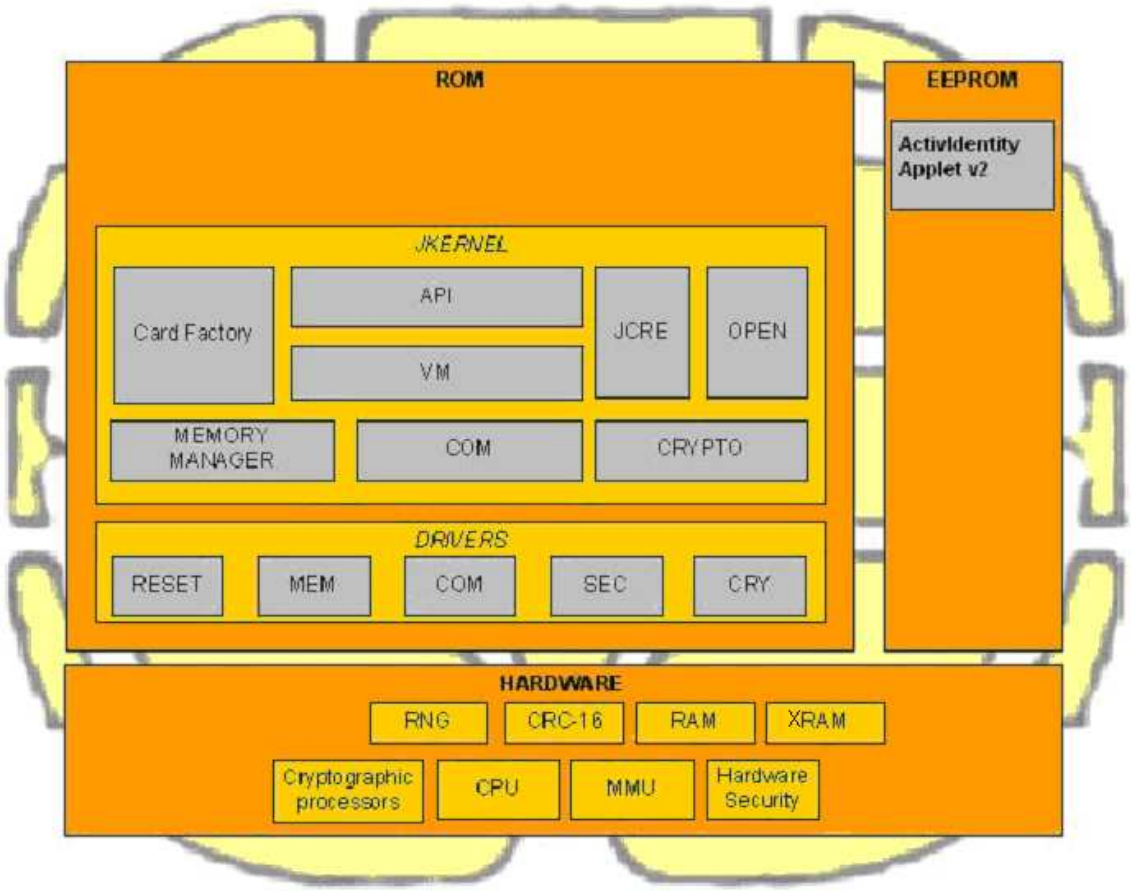


Figure 1 Cryptographic Module Boundary

.

4.2 ACTIVIDENTITY APPLET V2 FOR EXTENDED PIV

The ActivIdentity Digital Identity Applet Suite V2.6.2B for Extended PIV supports identity-based authentication of the Card Holder, Application Operators, and Cryptographic Officer, using PIN/ PUK or TDES keys. All services provided by the cryptographic module are protected by an identity based access control policy following the result of the authentication.

This validation effort is aimed at the systems software, virtual machines, Card Manager application, and ActivIdentity applets. If additional applets are loaded into this cryptographic module, then these additional applets require a separate validation, and they must be FIPS 140-2 validated. The cryptographic module checks all validated applets, and will not load any applets that do not have the correct MAC.

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV is composed of the following elements:
- **Applet V2.6.2b**:

- ASC library package version 2.6.2B.3
- ACA applet package version 2.6.2B.4
- PKI/GC/SKI applet package version 2.6.2B.4
- PIV End Point Wrapper module 2.6.2B.4
- PIV End Point Extended module 2.6.2B.3
- SMA applet package version 2.6.2B.3

The applet and library package byte code is loaded in the cryptographic module memory. Note that the ASC library package consists of static utility classes only accessed by the applet, and the library cannot be accessed directly by off-card entity.

The applets offer services to external applications, relying on key management, secure memory management and cryptographic services, provided by the cryptographic module. The services are activated with “APDU commands” sent to the cryptographic module.

Applets depend on a unique security domain (SD) for the security configuration. This SD can be either the Card Manager or a separate security domain. The Card Manager is itself a security domain with additional services.

Every security domain holds one or more security domain key sets composed of TDES keys.
The ownership of a key set allows for establishing a Secure Channel (SC) between the host and either the security domain or the security domain applets. Generally, the SC is used for administrative operations such as entering the application keys in the applet instances belonging to the security domain, or entering new key sets in the security domain itself. Note that a security domain key set can be used to enter a replacement key set in the same security domain – the replacement involves the deletion of the original key set. This is how a Card Security Controller role (CSC), which solely owns the replacement key set, can take control of the personalization of all applet instances belonging to a security domain.

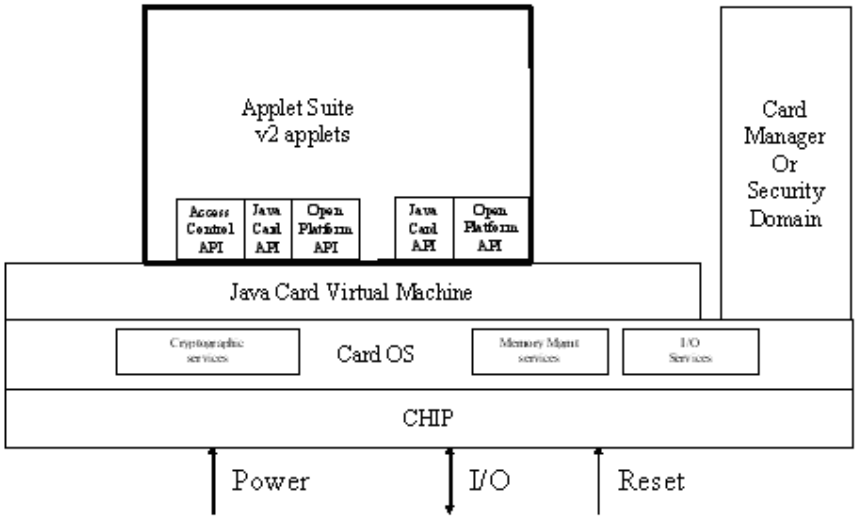


Figure 2: Functional block diagram

4.3 FIPS APPROVED SECURITY FUNCTIONS

The following table gives the list of FIPS approved security functions that are provided by the **SafesITe TOP DL GX4 – FIPS** Java Card API.

SECURITY FUNCTION	DETAILS	FIPS APPROVED
AES	ECB mode in encryption	Yes
	ECB mode in decryption	Yes
	CBC mode in encryption	Yes
	CBC mode in decryption	Yes
Triple-DES	ECB mode in encryption	Yes
	ECB mode in decryption	Yes
	CBC mode in encryption	Yes
	CBC mode in decryption	Yes
SHA-1	Hashing operation	Yes
RSA	Key generation as per ANSI X9.31	Yes
	Signature following PKCS#1 with SHA-1 hashing	Yes
	Verification following PKCS#1 with SHA-1 hashing	Yes
P-RNG	Pseudo Random Number Generation based on ANSI X9.31 Appendix A.2.4 using 2Key TDES	Yes
Triple-DES MAC	CBC mode	Yes

Table 2 – FIPS Approved Security Functions

4.4 MODULE PORTS AND INTERFACES

The integrated circuit used on the **card** can support the following interfaces:

- ISO/IEC 7816: Identification Cards – Integrated Circuit Cards with Contacts
- ISO/IEC 14443: Identification Cards – Contactless Integrated Circuit Cards – Proximity cards

The ActivIdentity Digital Identity Applet Suite V2.6.2B for Extended PIV is validated both on the ISO/IEC 7816 and ISO/IEC 14443 interfaces.

4.4.1 ISO/IEC 7816 Physical Interface (contact mode)

4.4.1.1 Interface Physical Specifications

GX4 – FIPS follows the standards **"ISO 7816-1 Physical characteristics"** and **"ISO 7816-2 Dimensions and contact location"**.

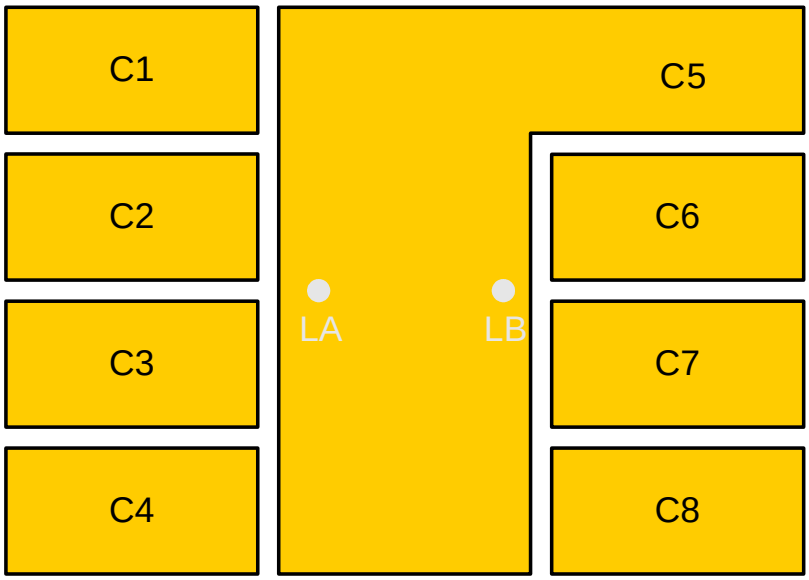


Figure 3 - Contact plate example – Contact physical interface

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 3 - Contact plate pin list – Contact mode

4.4.1.2 Conditions of use

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

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

Table 4 - Voltage and frequency ranges

4.4.2 ISO/IEC 14443 RF Interface (contactless mode)

4.4.2.1 Interface Physical Specifications

In the contact-less mode the GX4 - FIPS cryptographic module follows the standard **"ISO 14443 RF Interface"** 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.**

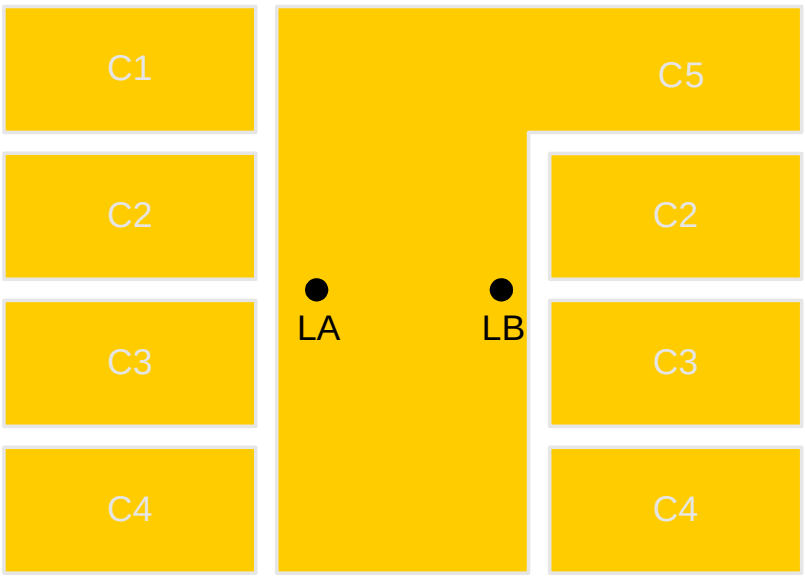


Figure 4 - Contact plate example - Contact-less antenna contacts

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

Table 5 - Contact plate pin list – Contact-less mode

4.4.2.2 Condition of use

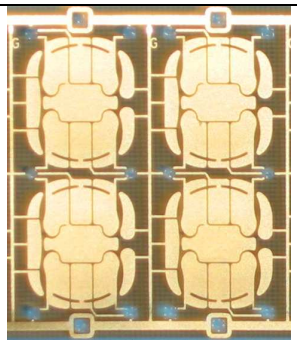
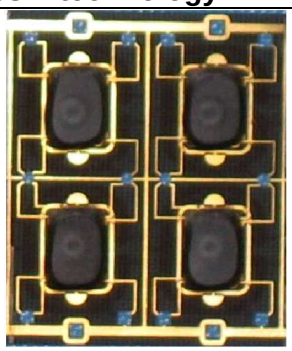
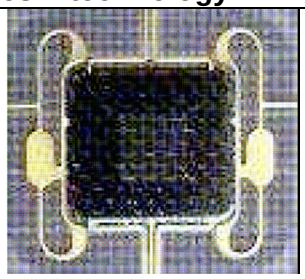
The radio frequencies and transmission protocols follow the **"ISO 14443 RF Interface".** The conditions of use are the following:

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

Table 6 - Voltage and frequency ranges

4.4.3 Picture – Dual Mode

Thermal black resin process, contact and contactless technology

BI DUAL black resin technology	
	
Bi Dual design	**Thermal** black resin Technology
A1011108 black resin technology	
	
A1011108 design	**Thermal** black resin Technology

5. ROLES & SERVICES

5.1 IDENTIFICATION

The SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite v2 for Extended PIV 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.

5.2 ROLES

The SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite v2 for Extended PIV defines three distinct roles that are supported by the on-module cryptographic system; the Card Security Controller (CSC) role, the Application Operator role, and the Card Holder role.

5.2.1 User Roles:

- **Card Holder Role (CH)** - The Card Holder role is responsible for ensuring the ownership of his cryptographic module, and for not communicating his PIN to other parties. An applet authenticates the Card Holder by verifying his PIN.
- **Application Operator Role (AO)** – The Application Operator role represents an external application requesting the services offered by the applets. An applet authenticates the

Application Operator role by verifying possession of the Application External Authenticate (XAUT) TDES key. The AO is also able to provide the PUK credential to unblock the PIN (SP800-73-1).

5.2.2 Cryptographic Officer role:

- **Card Security Controller (CSC) Role:** This role is responsible for managing the security configuration of the card manager and security domains. The CSC role authenticates to the cryptographic module by demonstrating to the Card Manager application that he possesses the knowledge of a GP secure channel TDES key set stored within the Card Manager. By successfully executing the GP secure channel mutual authentication protocol, the CSC role establishes a secure channel to the Card Manager and execute services allowed to the CSC role in a secure manner. The CSC role can also be responsible for unblocking the PIN using a specific unblock PIN XAUT key with ActivIdentity external authentication protocol.

5.3 ROLE AUTHENTICATION

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV cryptographic module supports identity based role authentication using the following scheme.

5.3.1 User Role Authentication

- The Card Holder role is authenticated with a PIN
  - **PIN**: The Card Holder role must send a VERIFY APDU to the module to access services protected with PIN access control rules (PIN once for session or PIN-Always). The APDU corresponding to the applet service protected by the PIN, can access the service before the cryptographic module is removed or a reset command is sent to the cryptographic module.
- The Application Operator role is authenticated by the possession of a TDES key or a 8 bytes-string for PIN Unblocking Key (PUK).
  - **Application External Authentication (XAUT) key**: The Application Operator role must prove the possession of a particular TDES key to access the PKI/GC/SKI buffer read, or update service protected with the External Authentication protocol using this particular key. An 8-byte challenge is first obtained from the applet. The application controlled by the operator encrypts the challenge with a 112-bit TDES key, and submits the resulting cryptogram to the module for verification. The APDU corresponding to the particular applet service protected by the XAUT key, can access the service before the cryptographic module is removed or a reset command is sent to the cryptographic module.
  - **Unblock with PUK:** The AO can also complete the PIN unblock operation with the PUK (which is loaded under the CSC role).

5.3.2 Cryptographic Officer Role Authentication

- The Cryptographic Officer role is authenticated by a TDES key set in the case of secure channel key set, or a TDES key in the case of XAUT key.
  - **Secure Channel key set:** The Cryptographic Officer (CSC) role must prove the possession of a key set composed of three TDES keys. Two keys (K_{MAC}, K_{ENC}) are used to generate session keys according to Global Platform specification. The session keys ensure the confidentiality of the command payload, allow the mutual authentication of the parties and protect the APDU command integrity. A third key (K_{KEK}) is used to wrap keys transported within the APDU command.
  - **Unblock PIN with XAUT key:** The Cryptographic Officer (CSC) role performs the ActivIdentity external authentication protocol using the XAUT TDES key. The PIN is unblocked if the CSC role is successfully authenticated.

5.4 SERVICES

This section describes the services each role can perform.

5.4.1 CSC (Card Manager and Security Domain) Role Services

The following APDUs are sent to Card manager/Security Domain:

- ***INSTALL:*** this APDU is used to instruct either a security domain, or the Card Manager as to which installation/instantiation step it shall perform during an applet installation process.
- ***LOAD:*** this APDU is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- ***DELETE:*** this APDU is used by the CSC role to delete a Load File (package) or an applet (applet instance).
- ***GET STATUS:*** this APDU is used to get the life cycle state of the cryptographic module or the life cycle state of an application
- ***SELECT:*** this APDU is used for selecting an application.
- ***SET STATUS***: this APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, and PERSONALIZED.
- ***INITIALIZE UPDATE***: this APDU is used to initiate an GP Secure Channel with the Card Manager or a security domain. Cryptographic module and host session data are exchanged, and the cryptographic module and host upon completion of this APDU generates session keys. However, the Secure Channel is considered open upon completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- ***EXTERNAL AUTHENTICATE***: this APDU is used by the cryptographic module to authenticate the host, to establish the Secure Channel, and to determine the level of security required for all subsequent commands within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.
- ***STORE DATA***: this APDU is used to store or replace one tagged data object provided in the command data field.
- ***GET DATA***: this APDU is used to retrieve a single data object.
- ***PUT KEY:*** This APDU is used to add or replace TDES keys such as security domain key sets, DAP TDES MAC Key, TDES MAC receipt key and also RSA public keys such as the Token Verification Key or the DAP Verification Key**.** These public keys are used for Delegated Management and DAP verification as specified by Global Platform.
- ***PUT DATA:*** This APDU command is used to set the value of the various data elements utilized and managed by the Card Manager (deprecated OP command)
- ***MANAGE CHANNEL***: This command allows the terminal to open or close a logical channel in the card. Up to 4 logical channels may be open at a time, if the multiple-channel option is enabled.

The following APDUs are sent to ActivIdentity applets:

- ***CHANGE REFERENCE DATA:*** This APDU intends to create the PIN and PUK in the card. It is also used to update the PUK value.
- ***INITIALIZE UPDATE***: Similar to command set to Card manager/Security Domain
- ***EXTERNAL AUTHENTICATE***: Similar to command set to Card manager/Security Domain
- ***GENERATE ASYMMETRIC RSA KEY PAIR:*** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications
- ***GENERATE KEY PAIR:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.
- ***GET DATA***: This command is used to retrieve a single data object

- ***PRIVATE SIGN/DECRYPT:*** This APDU uses the RSA private key in the PKI buffer to sign data.
- ***PUT DATA:*** This APDU intends to set the applet properties, load keys as well as personalize the container managed under the PIV Ext applet. This APDU is present for compliance with PIV specifications.
- ***PUT KEY***: This APDU is used to either enter the XAUT keys (like used to unblock the PIN), the RSA private key component or the SKI key for One Time Password generation. The APDU must be used with a secure channel established by CSC role. The APDU format is compliant with GP specifications.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***REGISTER ACR:*** This APDU manages the mapping between ACRID and actual APDU instruction as well as record the ACR definition for the applet services.
- ***REGISTER APPLET:*** This APDU is to register applet instances to the ACA instance so that the access control and secure message service can be provided.
- ***RESET RETRY COUNTER:*** This APDU is used to unblock the cardholder PIN and restore the VERIFY service with a new counter value if the CSC role is authenticated successfully. The command operates as long as the unblock counter has not expired.
- ***SET APPLICATION UID***: This APDU is sent when the UID associated with the applet instance needs to be changed
- ***SET PROPERTIES:*** This APDU creates and sets the object properties for GC/PKI/SKI applet.
- ***SET STATUS***: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, and PERSONALIZED
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***UPDATE PROPERTIES:*** This command updates the ACA properties

5.4.2 Application Operator Role

- ***AC EXTERNAL AUTHENTICATE***: This APDU is used in combination with a Get Challenge to authenticate the Application Operator using the AC external authenticate protocol.
- ***GENERATE ASYMMETRIC RSA KEY PAIR:*** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications. This APDU is present for compliance with PIV specifications.
- ***GENERATE KEY PAIR:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.
- ***GET DATA***: This command is used to retrieve a single data object like PIV object content
- ***PUT DATA:*** This APDU is present for compliance with PIV specifications and it is used to personalize containers managed under the PIV Ext applet
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***RESET CARD:*** This command resets the card content (buffer content, PKI credentials, SKI keys as well the PIN/PUK)
- ***RESET RETRY COUNTER:*** This APDU is used to unblock the PIN with PUK string.

5.4.3 Card Holder Role

- ***CHANGE REFERENCE DATA:*** This APDU is used to change the cardholder PIN if the Card Holder is correctly authenticated.

- ***GENERATE ASYMMETRIC RSA KEY PAIR:*** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications. This APDU is present for compliance with PIV specifications.
- ***GENERAL AUTHENTICATE***: The APDU is for PKI operations (via the PIV EP wrapper and PIV EP Ext)
- ***GENERATE KEY PAIR:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.
- ***GET DATA***: This command is used to retrieve a single data object like PIV object content
- ***INTERNAL AUTHENTICATE (GENERAL AUTHENTICATE command)***: The APDU is for SKI operations and to generate a cryptogram from the card for verification by the calling application.
- ***PRIVATE SIGN/DECRYPT:*** This APDU uses the RSA private key in the PKI buffer to sign data.
- ***PUT DATA:*** This APDU intends to personalize the card objects. This APDU is present for compliance with PIV specifications.
- ***PUT KEY***: This APDU is used to either enter the XAUT keys, the RSA private key component or the SKI key for One Time Password generation. In a Cardholder role, the APDU must be used with a SMA channel to encrypt the key component.

- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***UPDATE PROPERTIES:*** This command updates the ACA properties
- ***VERIFY***: This APDU checks the PIN presented by the cardholder against the current PIN.

5.4.4 No Role

- ***GET CHALLENGE:*** This APDU is used in combination with AC external authenticate to perform an external authentication of the Application Operator in order to unblock the PIN. It is also involved when opening a SMA session.
- ***GENERAL AUTHENTICATE***: The APDU is for PKI operations (via the PIV EP wrapper and PIV EP Ext) as well as when opening a SMA session
- ***GET ACR:*** This APDU is used to retrieve the ACR definition for the services.
- ***GET DATA***: This command is used to retrieve a single data object, such as the Card Identification data.
- ***GET PROPERTIES***: This APDU is used to obtain information about applet instance configuration.
- ***GET RESPONSE***: This command is restricted to T=0 ISO protocol for an incoming command which has data to send back. That data is received with the GET RESPONSE command sent immediately after the command to which it is related.
- ***LOGOUT:*** To logout all authenticated roles.
- ***UPDATE PROPERTIES:*** This APDU modifies the applet properties The APDU is accessible from ACA applet.
- ***READ BINARY:*** This APDU reads binary data stored on the card. This command is deprecated in v2.6.2a.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***SELECT***: This command is used for selecting an application (Card Manager, security domain or Applet). The Card Manager may be selected either for the loading of a Load File or for installing a previously loaded application (or security domain)

- ***PRIVATE SIGN/DECRYPT:*** This APDU uses the RSA private key in the PKI buffer to sign data (involved with PIV Card Authentication Key)
- ***MANAGE SMA***: The APDU is used to explicitly close the SMA secure session

5.5 RELATIONSHIP BETWEEN ROLES AND SERVICES

For the Card Manager services, the access rules are listed in the following table.

Roles/Services	CSC Role (Card Manager)	CSC Role (Security Domain)	No Role (Unauthenticated)
INSTALL	X		
LOAD	X		
DELETE	X		
GET DATA			X
GET STATUS	X		
SET STATUS	X	X	
INITIALIZE UPDATE	X		
EXTERNAL AUTHENTICATE	X		
STORE DATA	X		
PUT KEY	X	X	
SELECT			X
PUT DATA	X		
MANAGE CHANNEL	X	X	X

Table 7: Role and possible ACR configuration for Card Manager

For applets suite v2, the access rules are listed in Table 8.

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC) / SECURE CHANNEL	Application Operator / XAUT (or PUK)	Card Holder / PIN	Applet V2.6.2b	
					ISO 7816	ISO 14443
AC EXTERNAL AUTHENTICATE			X		X	
CHANGE REFERENCE DATA (change PIN)				X	X	
CHANGE REFERENCE DATA (Create PIN/PUK + Update PUK)		X			X	
EXTERNAL AUTHENTICATE	X				X	
GENERATE KEY PAIR		X	X	X	X	
GENERATE ASYMMETRIC RSA KEY PAIR		X	X	X	X	
GENERAL AUTHENTICATE	X			X	X	X
GET ACR	X				X	
GET CHALLENGE	X				X	X
GET DATA	X	X	X	X	X	X
GET PROPERTIES	X				X	X
GET RESPONSE	X				X	X
INITIALIZE UPDATE	X				X	
INTERNAL AUTHENTICATE				X	X	X
LOGOUT	X				X	
MANAGE SMA	X				X	X
PRIVATE SIGN/DECRYPT	X	X		X	X	X
PUT KEY		X		X (SMA-ENC minimum)	X	
PUT DATA		X	X	X	X	
READ BINARY	X				X	X
READ CERTIFICATE / STATIC BUFFER	X	X	X	X	X	X
REGISTER APPLET		X			X	
REGISTER ACR		X			X	

RESET CARD			X		X	
RESET RETRY COUNTER (with PUK)			X (PUK)		X	
RESET RETRY COUNTER (without PUK)		X	X		X	
SET APPLICATION UID		X			X	
SELECT	X				X	X
SET PROPERTIES		X			X	
SET STATUS		X			X	
UPDATE CERTIFICATE / STATIC BUFFER	X	X	X	X	X	
UPDATE PROPERTIES	X	X		X	X	
VERIFY				X	X	X

Table 8: Role and possible ACR configuration for Applet

6. MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite v2 for Extended PIV is to provide a FIPS approved platform that in turn provides cryptographic services to end-user applications. The keys represent the roles involved in controlling the cryptographic module. A variety of FIPS 140-2 validated algorithms are used in the SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite v2 for Extended PIV on **card platform** to provide cryptographic services.

6.1 CRYPTOGRAPHIC ALGORITHMS, MODE AND KEY LENGTH

These include:

- TDES (2TDEA and 3TDEA: TDES CBC/ECB)
- TDES MAC
- SHA-1
- RSA PKCS1 (1024, 2048 bit keys for all keys)
- RNG

The TDES (CBC mode) algorithm is used for both authenticating the CSC (EXTERNAL AUTH command) and encrypting data flow from the external application to the cryptographic module environment. The reverse direction is not encrypted (i.e. the status words returned in response to an APDU are not encrypted).

6.2 RANDOM NUMBER GENERATOR

The cryptographic module offers the services of a FIPS 140-2 Approved DRNG (Deterministic Random Number Generator). The random number generation algorithm is compliant with the ANSI X9.31 PRNG .

The initial counter and seed for the approved RNG are input into the module at manufacture time. These values are generated by a RACAL HSM (which is FIPS validated).

6.3 CRITICAL SECURITY PARAMETERS

- **Initialization key set K_{init}**: used to secure the card during its transportation from the manufacturer site to the issuance site. This key set is generated outside of the cryptographic module and then loaded into the card manager security domain during the card manufacturing and initialization process. This key set is zeroized via the PUT KEY command.
- **DAP TDES MAC Key:** This key is used to verify the MAC pattern for DAP and Mandated DAP
- **Key for receipts generation during Delegated Management (Receipt Signature Key):** It is called Receipt Signature Key and it is Triple-DES, this key generates the receipt to confirm the execution of the Delegated Management-based operation. This key is not managed by ActivIdentity Applets.
- **Secure Channel Key Set:**
    - K_{enc}: used to generate session keys for the encrypted mode of the secure channel
    - K_{mac}: used to generate session keys for CSC authentication and MAC mode of the secure channel. This key is used to authenticate the CSC to the card
    - K_{kek}: used to wrap keys to be loaded onto the cryptographic module

  This key set is generated outside of the cryptographic module in an HSM, and the loaded protected with a Global Platform secure channel using the key set that already exists in the card manager security domain (for example, Kinit). This key set is zeroized via the Put Key command.
- **External Authentication Keys (XAUT)**: TDES keys that enable the authentication of either Application Operators or Cryptographic Officer (RESET RETRY COUNTER command for Unblocking the PIN). These keys are generated outside of the cryptographic module in an HSM, and then are loaded protected with a Global Platform secure channel using the CSC Card Manager / Security Domain key set.
- **RSA private keys**: managed (generated or unwrapped) from the PKI/GC applet using the Java Card cryptographic services. These keys are used to generate signatures. They are either generated on the card or outside of the cryptographic module in an HSM, and then loaded protected with a Global Platform secure channel using the CSC Card Manager / Security Domain key set.
- **PIV private key objects**: Four RSA keys are managed in the Applet Suite. Those keys are defined in the PIV specification (SP800-73-1) and are attached with key Identifiers: 9Ah (PIV Authentication Key), 9Ch (PIV Digital Signature Key), 9Dh (PIV Key Management Key), and 9Eh (PIV Card Authentication Key).
- **Card Holder Personal Identification Number (CH PIN)**: It is used to authenticate the Card Holder and it is loaded or modified via the Change Reference Data command. The PIN object is minimum 6 bytes in the card and it contains authentication string that belongs to the Card Holder. CH PIN and associated attributes are managed from the ACA Applet, which relies on Java Card PIN management service. The initial PIN is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set, and can be changed later by the user after a successful user authentication event.
- **PIN Unblocking Key (PUK):** The PUK is managed inside the ACA Applet too. It is used to authenticate the AO and the command Change Reference Data initializes the PUK. Its role is to unblock the PIN. The PUK is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set. The PUK pattern is 8 bytes long in the card and it contains a static byte sequence unique in each card issued.
- **SKI Key for OTP:** TDES key is involved during generation of the One Time Password and then authentication from the card to the calling application.
- **Access Control Rule (ACR)**: These data elements define the Authentication Method that is permanently set for the service. Several services offer a configurable Authentication Method. For such services, the authentication method should be set according to table 2. The Access Control

Rule are set by the Card Security Controller via a Global Platform secure channel using the CSC Card Manager / Security Domain key set.

6.4 PUBLIC KEYS

- **RSA public keys in the ActivIdentity Applet** : Public keys are stored under the form of public key certificate and recorded in GC buffers that belongs from the GC/PKI/SKI applet. There is a certificate slot booked for each RSA private key defined in the card.
- **RSA public keys from the Card Manager/Security Domain (DAP Verification Key)**: This key is a 1024-bits key stored in the Card Manager/Security Domain. This key is not used by the ActivIdentity applet and is under responsibility of the Card Manager/Security Domain application attached to the ActivIdentity applet
- **RSA public key for Delegated Management:** This key is stored in the Card Manager and is 1024 bits long. This key is also called Token Verification Key and is not managed by ActivIdentity applets.

6.5 ACCESS TO CSPS VS SERVICES

The following matrix identifies how different services access CSPs defined above.

CSP	Service	Role	Type of Access
ACR	INSTALL/INSTANTIATE	CSC	Write
	REGISTER ACR	CSC	Execute
CH PIN	RESET RETRY COUNTER	CSC/AO	Write
	CHANGE REFERENCE DATA	Card Holder	Write
	VERIFY	Card Holder	Execute
PUK	RESET RETRY COUNTER	AO	Execute
	CHANGE REFERENCE DATA	CSC	Write
XAUT Key	PUT KEY	CSC	Write
	GET CHALLENGE & AC EXT AUTH	AO	Execute
SKI Key for OTP	PUT KEY	CSC	Write
	INTERNAL AUTHENTICATE	Card Holder	Execute
Secure Channel Key Set	PUT KEY	CSC	Write
	INIT UPDATE & EXT AUTH	CSC	Execute
RSA private key	PUT KEY	CSC	Write
	GENERATE KEY	Card Holder/ CSC	Create
	PRIVATE SIGN	Card Holder	Execute
	GENERAL AUTHENTICATE	Card Holder	Execute
Initialization Key Set	PUT KEY	CSC	Write
Receipt Signature Key	PUT KEY	CSC	Write
PIV Private Key Objects	GENERATE ASYMMETRIC RSA KEY PAIR	AO	Create
	GENERAL AUTHENTICATE	Card Holder / No Role	Execute
DAP TDES MAC Key	PUT KEY	CSC	Write
PRNG Seed and Seed key	GENERATE KEY	Card Holder/ CSC	Write
	GET CHALLENGE	Card Holder/ CSC	Execute

	INIT UPDATE	CSC	Execute
TDES MAC Key	LOAD	CSC	Execute

Table 9: Access to CSPs and the Services

7. SELF TESTS

7.1 POWER-UP SELF TESTS

The **GX4 – FIPS** platform performs the following self-tests to ensure that the module works properly. All the self tests are done by the platform.

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

Table 10 - Self-tests list

7.2 SELF-TEST EXECUTION

After **GX4 – FIPS** is powered up and before executing any APDU commands, the module enters the self-test state and performs all of the cryptographic algorithm and software integrity self-tests as specified in FIPS 140-2 standard. In addition to those tests, it also performs chip sensors verification and security status verification:

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

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

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

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

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

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

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

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

8. SECURITY RULES

8.1 APPROVED MODE OF OPERATION

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

- The operator of the cryptographic module sends ATR, GET PROPERTIES, GET VERSION (for PIV EP applet) to the module to validate that the hardware and software version are the same as those below:
  ATR T=0 :(Cold = Warm) = 3Bh 7Dh **TA1h** 00h 00h 80h 31h 80h 65h B0h 83h 11h **FlowIDh** D6h 83h 00h 90h 00h with TA1= 94h, 95h or 96h and FlowID = 17h & 13h.
  ATS (Type A) = 14h 77h 33h 93h 02h 80h 91h E1h 31h 80h 65h B0h 83h 11h **FlowIDh** D6h 83h 00h 90h 00h and FlowID = 17h & 13h.
- The operator of the cryptographic module sends GET ACR to the module to validate that module service Access Control Rules are configured per table 8.
- The module follows all security rules outlined in section 9 to maintain in FIPS mode.

8.2 AUTHENTICATION SECURITY RULES

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of binding a identity-based ACR to each service.

- All CSPs are entered into the cryptographic module encrypted (for Administrative operations: CSP creation). Card holder PIN (and PUK during unblock with PUK) can be either conveyed in the clear or encrypted during usage operations (PIN verification or unblock with PUK).
- A PIN ID represents the identity of the Card Holder.
- The key ID of the XAUT key represents the identity of the Application Operator.
- The key ID of the GP secure channel key represents the identity of the CSC.
- The module provides the following distinct operator roles: Card Holder role, Application Operator role, and Card Security Controller role.
- The applets provide identity-based authentication:
    - The Card Holder is identified by a PIN ID and authenticated by the knowledge of a PIN
    - The CSC is identified by a key ID and authenticated via a GP secure channel mutual authentication protocol using the card manager/security domain key set that is composed of three TDES double length keys. Two keys are used to authenticate and MAC the command payload. A third key is used to wrap keys transported within the APDU command (Initialize Update and External Authenticate commands).
    - The Application Operator role is identified by a key ID and authenticated via AC external authenticate protocol using the application XAUT TDES key. The PUK is also seen as a key with Key ID (=81h, this value is not used by applet PIV EP).
- The role authentication methods (ACRs) for each service are set by the CSC during applet instantiation and can only be modified by the CSC.
- When authentication of the role cannot be performed because the related key or PIN attributes are missing, the corresponding service must not be available.
- The results of authentication must be set in transient memory and therefore cleared when the module is powered down.
- Applet instance configuration may require the combined authentication of different roles to access a particular service. For instance the Application Operator, or the Cryptographic Officer, must both authenticate to access the Update Certificate / Static Buffer service.

8.3 APPLET LIFE CYCLE SECURITY RULES

The SafesITe TOP DL GX4 – FIPS with ActivIdentity Digital Identity Applet Suite v2 for Extended PIV only permits loading of FIPS Approved applets. Applets can only be loaded through a GP secure channel (i.e. they pass from the external application to the cryptographic module in an encrypted and MACed form).

- The Card Holder must take the necessary measures to ensure that the terminal and/or Card Acceptance Device are controlled by a valid role; Card Holder, Application Operator or CSC.
- Management of applet life cycles (load, install, delete, personalize keys), follows the Global platform standard.
- Applet and key APDU commands management (i.e. download, install, delete, put key) are protected by secure channel MAC (TDES-CBC). Their origin is authenticated, and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post-issuance.
- The download of validated applet packages, and the installation of applet instances, may occur either at pre-issuance, issuance or post-issuance.
- There may be as many instances of each applet as there are cryptographic module resources available.

8.4 ACCESS CONTROL SECURITY RULES

- Keys must be loaded through a GP secure channel. Consequently, keys are always loaded in the encrypted form.
- The password or PIN that is used by the applet to authenticate the Card Holder must not be divulged to parties other than the Card Holder.
- The ACA applet must be configured by the cryptographic officer so that:
    - After 1 <= N <= 127 consecutive unsuccessful PIN code validation attempts, the Card Holder services must be disabled. (e.g., the PIN is blocked)
    - The PIN length L verifies the following rules:
        - 6 <= L <= 255 for PIN composed with random numeric (0-9) and 4<= L <= 255 for PIN composed with alpha-numeric (0-9, a - z, A – Z) characters
- The ACA applet stores the unblock counter for the Cardholder PIN. The counter is set with a value between 1 <= M <= 127. The ACA Applet records the PUK pattern which is 8 bytes long.

8.5 KEY MANAGEMENT SECURITY POLICY

8.5.1 Cryptographic Key Generation

- TDES Session key generation using FIPS140-2 Approved ANSI X9.31 DRNG for Secure Channel Opening.
- RSA key pair generation using FIPS140-2 Approved ANSI X9.31 DRNG.

8.5.2 Cryptographic Key Entry

Keys (including PUK) shall always be input in wrapped format, using the Put Key command within an GP secure channel. During this process, the keys are double wrapped (using the Session Key K_{enc} and the K_{kek} Key described in section 6.3.

8.5.3 Cryptographic Key Storage

The Keys are structured to contain the following parameters:

- Key set version
- Key index, which is the ID of the key,
- Algo ID, which determines which algorithm to be used,
- Integrity Mechanisms

The cryptographic keys storage integrity mechanism is described in a separate confidential document called Self Test Description.

8.5.4 Cryptographic Key Zerorization

The cryptographic module zerorizes cryptographic keys by reloading either a zero-valued key set for a CSC GP secure channel key set, or an Application Operator XAUT key with PUT KEY command, or closing of secure channel for session keys**.** The Card Holder PIN is zerorized by setting it to zero value via the CHANGE REFERENCE DATA command (same for the PUK pattern). The RSA private key is zerorized by reloading a zero-valued key using PUT KEY. Setting the card status to OP_TERMINATED can also zeroize all the keys on the module.

Key Management Details can be found in a specific proprietary document.

8.6 MITIGATION OF ATTACKS

The GX4 – FIPS has been designed to mitigate the following attacks:
- Timing Attacks,
- Differential Power Analysis,
- Simple Power Analysis,
- Electomagnetic Analysis,
- Fault Attack.
- Card Tearing

A separate and proprietary document describes the mitigation of attacks policy provided by the GX4 - FIPS platform.

8.7 HARDWARE SECURITY MECHANISMS

Additionally, the embedded **P5CD144 chip from Philips** provides the cryptographic module with hardware security mechanisms such as temper evidence, probing detection, low frequency and supply voltage monitoring. The chip reacts to a low/high clock frequency, and low/high power supply voltage by resetting the cryptographic module. Any unprotected sensitive data are lost.

8.7.1 Tamper Evidence

The module provides visual evidence in the event of physical tampering. Attempting to extract the chip from the micro-module has a high probability of causing serious damage to the chip. Furthermore, attempts to attack the chip or micro-module will result in signs of tampering such as scratches and deformation. The operator of the card needs to check the card periodically for evidence of physical tempering through visual inspection for scratches and deformation.

8.7.2 High/Low Frequency Sensor

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

8.7.3 High/Low Voltage Sensor

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

8.7.4 High/Low Temperature Sensor

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

8.7.5 Shields

Shields cover different chip areas

8.7.6 Fault injection detection

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

8.7.7 Light sensor

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

8.7.8 Glitch sensor

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

8.7.9 Protection of BUS system

Physical and logical addresses have no correlation.

8.7.10 Filters

Filter is present on the CLK (clock signal) line.

8.7.11 Memory Ciphering

Some dedicated and Philips proprietary ciphering algorithms are implemented in order to protect data in the different memory areas such as EEPROM, ROM and RAM. Data protected by this ciphering is considered as plaintext for the purposes of FIPS 140-2.

9. SECURITY POLICY CHECK LIST TABLES

9.1 ROLES AND REQUIRED AUTHENTICATION

Role	Type of authentication	Authentication data
Card Security Controller	GP secure channel mutual authentication protocol	GP secure channel TDES key set of three
Application Operator	AC External Authenticate protocol	Application XAUT TDES key
Card Holder	Verify service	PIN

9.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	$> 1:2^{112}$
TDES authentication	As specified in GP 2.1.1 a ratification counter can be used in order to limit the number of bad attempts and reduce the risk of attacks (velocity checking). This counter is decremented by 1 at each unsuccessful authentication. With an attempt counter of 3, probability that a random attempt in 1 minute succeeds is much less than 1/100,000.
PIN	2^{64}; A counter can be used in order to limit the number of bad attempts and reduce the risk of attacks (velocity checking). This counter is decremented by 1 at each unsuccessful authentication. With an attempt counter of 15, probability that a random attempt in 1 minute succeeds is much less than 1/100,000.
PUK	2^{64}; A counter can be used in order to limit the number of bad attempts and reduce the risk of attacks (velocity

	checking). This counter is decremented by 1 at each unsuccessful authentication. With an attempt counter of 15, probability that a random attempt in 1 minute succeeds is much less than 1/100,000.

9.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Security Controller	The Card Security Controller role services are listed in Section 5.2
Application Operator	The Application Operator role services are listed in Section 5.2
Card Holder	The Card Holder role services are listed in Section 5.2

9.4 ACCESS RIGHTS WITHIN SERVICES

Service	CSP	Types of Access (i.e. Read, Write, Execute)
CSC (CSC) Service	GP secure channel TDES key set of three (K_{enc}, K_{Mac}, K_{Kek}), or Unblock PIN XAUT TDES key as well as , Create/Update PIN/PUK	Execute (encrypt, decrypt, update PUK), write (put key, create PIN/PUK)
Application Operator Service	Application XAUT TDES key or Unblock PIN with PUK	Execute (encrypt, decrypt, unblock with PUK)
Card Holder Service	PIN	Execute (Verify), write (Change Reference Data)

9.5 MITIGATION OF OTHER ATTACKS

Other Attacks	Mitigation Mechnism	Specific Limitations
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A
Timing Analysis	Counter Measures against TA	N/A
Fault Induction	Counter Measures against FI	N/A
Flash Gun	Counter Measures against FG	N/A

10. EMI/EMC

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B. Testing was performed at an independent lab for verification and the module was found to meet Level 3 requirements for EMI/EMC.

11. REFERENCES

- Java Card ™ 2.2 Virtual Machine Specification, June 2002, Sun Microsystems
- Java Card ™ 2.2 Application Programming Interface, revision 1.1, September 2002, Sun Microsystems
- Java Card ™applet developer's guide
- Java Card ™ 2.2 Runtime Environment (JCRE) Specification, June 2002, Sun Microsystems
- Global platform Card Specification, v2.1.1, March 2003, Global Platform
- Global platform Card Specification, v2.1.1, Amendment A, February 2004, Global Platform
- "Integrated circuit(s) cards with contacts – Part 2 Dimension and Location of the contacts." ISO/IEC 7816-2 (1999)
- "Integrated circuit(s) cards with contacts – Part 3 Electronic signal and transmission protocols." ISO/IEC 7816-3, AMD1 (2002)
- "Integrated circuit(s) cards with contacts – Part 4 Inter industry commands for interchange." ISO/IEC 7816-4, AMD1 (1997)
- American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998.
- "Security Requirements for Cryptographic Modules", FIPS PUB140-2, May 2001, National Institute of Standards and Technology
- "FIPS 140-2 Annex A: Approved Security Functions", May 2001,National Institute of Standards and Technology
- "FIPS 140-2 Annex C: Approved Random Number Generators", May 2001, National Institute of Standards and Technology
- "FIPS 140-2 Annex D: Approved Key Establishment Techniques", May 2001, National Institute of Standards and Technology
- "FIPS PUB 46-3: Data Encryption Standard", October 25, 1999, National Institute of Standards and Technology
- "FIPS PUB 81: DES Modes of Operation", December 2, 1980, National Institute of Standards and Technology
- "Special Publication SP800-73-1", April 20, 2006 with May 2 errata, National Institute of Standards and Technology
- "Cryptographic Algorithms and Key Sizes for PIV, SP800-78", April 2005, National Institute of Standards and Technology

12. ACRONYMS

Acronyms	Definitions
AC	ActivCard (former company name for ActivIdentity)
ACA	Access Control Applet
ACR	Access Control Rule
ACR ID	1 byte identifier for the ACR (PIN ACR is assigned with an ACR ID different from a XAUT ACR)
AO	Application Operator
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASC	ActivIdentity Smart Card
ATR	Answer To Reset
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CH	Card Holder
CSP	Critical Security Parameter
CSC	Card Security Controller
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
GC	Generic Container
GP	Global Platform
GSC-IS	Government Smart Card Interoperability Standard
JCRE	Java Card ™ Runtime Environment
PKI	Public Key Infrastructure
MAC	Message Authentication Code
GP	Global platform
OTP	One Time Password
PIN	Personal Identification Number
PIV	Personal Identity Verification
PUK	PIN Unblocking Key
RAM	Random Access Memory
ROM	Read only Memory
SD	Security Domain
SC	Secure Channel
SKI	Secret Key Infrastructure
SMA	Secure Messaging Anonymous
TDES	Triple DES (112-bit length keys)
UID	Unique Identifier for the Profile loaded on the card (The profile is the electrical card layout)
XAUT	External Authentication