Gemalto and ActivIdentity Inc.

SafesITe TOP FIPS DM GX4 with ActivIdentity Digital Identity Applet Suite v2 for PIV

FIPS140-2

Cryptographic Module Security Policy

Version 1.14

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for “SafesITe TOP FIPS DM GX4 with ActivIdentity Digital Identity Applet Suite v2 for 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 (both those derived from the security requirements of FIPS 140-2 standard and from the security requirements of the module itself) under which the cryptographic module must operate.

2. OVERVIEW

2.1 THE GEMALTO CARD

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

This cryptographic module uses a state of the art manufacturing flow in terms of security and provides applets with memory, cryptographic and I/O services. The cryptographic module 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**

The card life cycle is managed according to the **Global Platform (GP) specification**. Issued cards have been loaded with a set of applets, cryptographic keys, and a PIN, and are moreover in the “SECURED” state. The security implementation is fully compliant with the **Global Platform (GP) specification**.
The cryptographic module integrates symmetric and asymmetric cryptographic algorithms as specified in the **JavaCard specification** and offers RSA for Signature/Verification, SHA-1, hashing functions, on-board RSA Key generation (up to 2048 bits), Triple-DES CBC and ECB and AES ECB and CBC algorithms (up to 256 bits key for AES).

The card is designed in following configurations:

GCX4 (former card name is GemCombiXpresso R4 E72 PK – FIPS) ***:*** This is a dual interface card providing both contact and contactless interfaces. This card has hardware version GCX4-M2569422 or GCX4-A1004155 (hardware module depending) and firmware version GCX4-FIPS EI07 and GCX4-FIPS EI08. It is identified by three historical bytes that are present in ATS (TH8, TH9, TH10) and ATR (T6, T7, T8) having same respective values. These three bytes should be:

- 83h 11h 13h : for the configuration where RSA is supported in contactless mode (configuration 15/15)
- 83h 11h 12h : for the configuration where RSA is not supported in contactless mode (configuration 31/7)
- 83h 11h 11h : for the configuration where RSA is supported in contactless mode (configuration 31/7)

2.2 ACTIVIDENTITY DIGITAL IDENTITY APPLET SUITE V2 FOR PIV

The ActivIdentity Digital Identity Applet Suite v2 for PIV:

- Allows the configuration of ActivIdentity Digital Identity Applet Suite v2 for PIV,
- Access to the services in the v2 suite from contactless interface is restricted according to table 10.

The v2 applet suite consists of four 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 (PKI/GC) Applet** – The PKI/GC 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 buffer.
- **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 Applet package** – 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 the existing v2.6.2 applets (ASC Lib, ACA and GC/PKI above). Its purpose is to access PIV Card-Edge and objects although objects are stored in v2.6.2 applet instances. This PIV Applet cannot operate in a standalone mode; it must link with ACA and GC/PKI(s) applet to operate properly.

The exact version of each applet is provided in section 4.2. Only one version of the applet suite can be instantiated at a time.

The PIV EP Applet package is an optional module that can be loaded on the card. In the context of this validation, the PIV EP package is loaded and running.

3. SECURITY LEVEL

The ActivIdentity Digital Identity Applet Suite v2 for PIV is designed and implemented to meet the overall Level 2 requirements of FIPS140-2. This document describes the module FIPS 140-2 Level 2 security policy. The Card Security Controller (CSC) should obtain the hardmask and softmask version via the Answer-To-Reset (ATR) command and, the applet version via the GET PROPERTIES command. The CSC should set the Access Control Rule (ACR) according to table 10 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 FIPS DM GX4 with ActivIdentity Digital Identity Applet Suite v2 for PIV, 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 TOP FIPS DM GX4 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 FIPS DM GX4 Micro-Module are included in the cryptographic module boundary, as shown in the following figure:

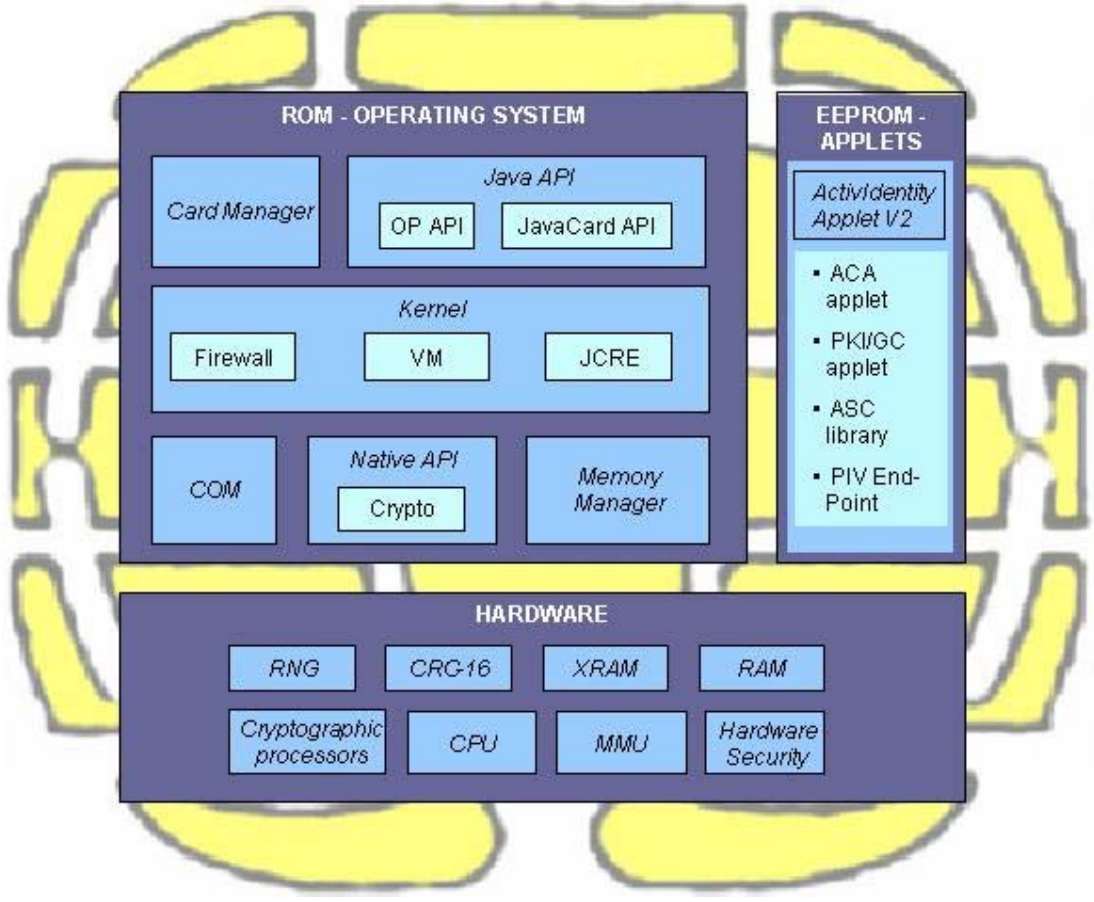


Figure 1 Cryptographic Module Boundary

SAR note: in this figure ActivIdentity must replace ActivCard and OP API should become GP API

4.2 ACTIVIDENTITY APPLET V2

The SafesITe TOP FIPS DM GX4 with ActivIdentity Digital Identity Applet Suite v2 for PIV supports identity-based authentication of the Card Holder, Application Operators, and Cryptographic Officers, using PIN 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 applets, 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 PIV is composed of the following elements: V2 suite (v2.6.2):
Combination 1:

- ACA applet package version 2.6.2.2
- PKI/GC applet package version 2.6.2.3
- ASC library package version 2.6.2.2
- PIV End-Point package version 2.6.2.6

Combination 2:

- ACA applet package version 2.6.2.2
- PKI/GC applet package version 2.6.2.3
- ASC library package version 2.6.2.2
- PIV End-Point package version 2.6.2.7

Combination 3:

- ACA applet package version 2.6.2.3
- PKI/GC applet package version 2.6.2.3
- ASC library package version 2.6.2.2
- PIV End-Point package version 2.6.2.9

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 to manage the life cycle of the card and manage its content.

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.

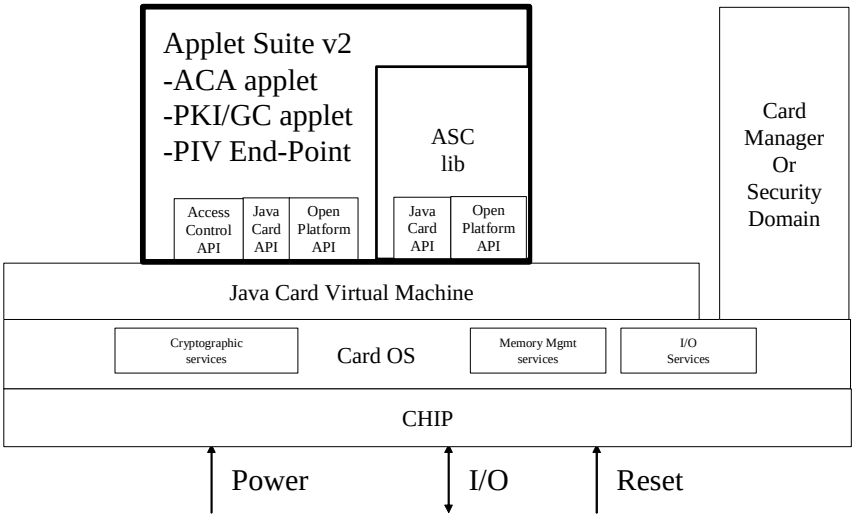


Figure 2 Functional block diagram

4.3 FIPS APPROVED SECURITY FUNCTIONS

The following table gives the list of FIPS approved security functions that are provided by the **SafesITe TOP FIPS DM GX4** 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	ECB and CBC modes	Yes

Table 2 – FIPS Approved Security Functions

5. MODULE PORTS AND INTERFACES

5.1 PHYSICAL PORT – CONTACT MODE

5.1.1 PIN assignments and contact dimensions:

GCX4 – FIPS Micro-Module follows the standards **"ISO 7816-1 Physical characteristics"** and **"ISO 7816-2 Dimensions and contact location"**.

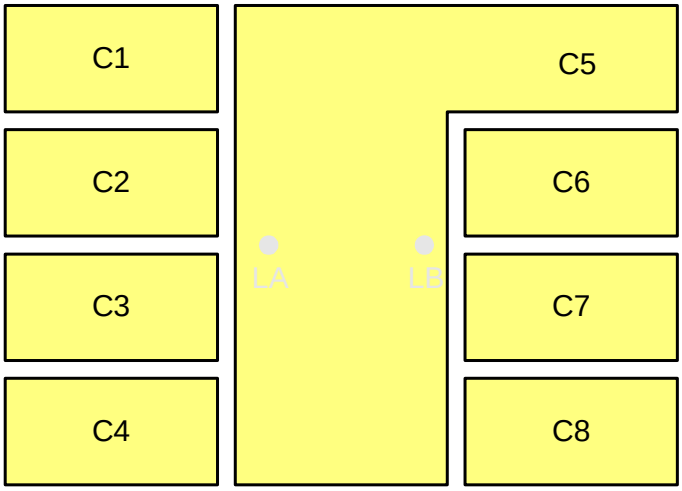


Figure 3 - Contact plate example – Contact physical interface

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 4 - Contact plate pin list – Contact mode

5.1.2 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 5 - Voltage and frequency ranges

5.2 PHYSICAL PORT – CONTACT-LESS MODE

5.2.1 Contacts assignments

In the contact-less mode the GCX4 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.**

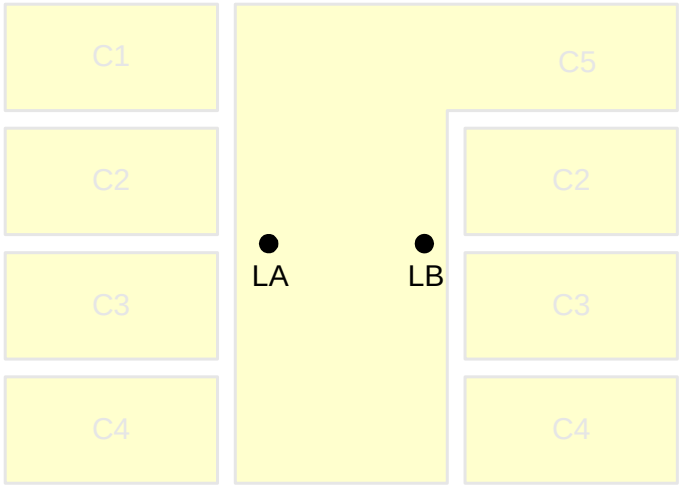


Figure 4 - Contact plate example - Contact-less antenna contacts

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

Table 6- Contact plate pin list – Contact-less mode

5.2.2 Condition of uses

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

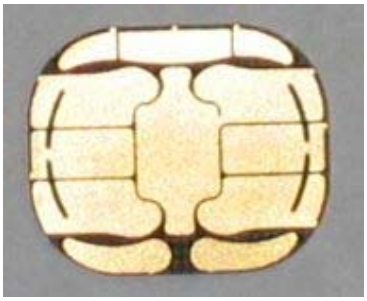
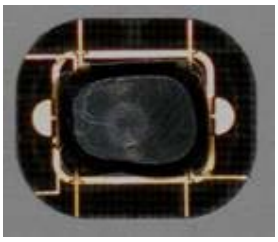
Conditions	Range
Supported bitrate	106 Kbits/s, 212 Kbits/s and 424 Kbits/s
Operating field	Between 1.5 A/m and 7.5 A/m rms
Frequency	13.56 MHz +- 7kHz

Table 7 - Voltage and frequency ranges

5.2.3 Pictures – Dual Mode

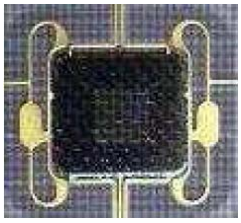
Hardware version GCX4-M2569422

GEM Combi Thermal black resin process, contact and contactless technology
Hardware version : GCX4-M2569422

	
Gem combi design **Hardware version : GCX4-M2569422**	**Thermal** black resin Technology **Hardware version : GCX4-M2569422**

Hardware version GCX4-A1004155

GEM Combi Thermal black resin process, contact and contactless technology
Hardware version : GCX4-A1004155

	
Gem combi design **Hardware version : GCX4-A1004155**	**Thermal** black resin Technology **Hardware version : GCX4-A1004155**

5.3 LOGICAL INTERFACE

GCX4 – FIPS Micro-Module provides services to both external devices and internal applets. 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, **GCX4 – FIPS Micro-Module** inhibits all data output via the data output interface when an error state is reached and during self-tests.

5.3.1 APDU commands

The data exchange protocol between the cryptographic module and an outside device follows the **ISO 7816-4 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 8 - Accepted ISO APDU types

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

5.3.2 API interface

GCX4 – FIPS Micro-Module provides trusted applets with internal services through its **JavaCard** and **GP APIs**. The cryptographic module provides an execution sandbox for the applets and performs the requested services according to its roles and services security policy.

6. ROLES & SERVICES

6.1 IDENTIFICATION

The ActivIdentity Digital Identity Applet Suite v2 for 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.

6.2 ROLES

The ActivIdentity Digital Identity Applet Suite v2 for 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.

6.2.1 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.

6.2.2 Cryptographic Officers roles:

- **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 OP 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 is also responsible for unblocking the PIN using a specific unblock PIN XAUT key with ActivIdentity external authentication protocol.

6.3 ROLE AUTHENTICATION

The SafesITe TOP FIPS DM GX4 with ActivIdentity Digital Identity Applet Suite v2 for PIV cryptographic module supports identity based role authentication using the following scheme.

6.3.1 User Role Authentication

- The Card Holder role is authenticated with a PIN
  - **PIN**: The Card Holder role must send a Verify CHV APDU to the module to access services protected with PIN access control rules. 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.
  - **Application External Authentication (XAUT) key**: The Application Operator role must prove the possession of a particular TDES key to access the PKI/GC 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).

6.3.2 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 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.

6.4 SERVICES

This section describes the services each role can perform.

6.4.1 CSC (Card Manager and Security Domain) Role Services

The following APDUs are sent to Card Manager applet:

- ***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.
- ***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:

- ***PUT KEY***: This APDU is used to enter the XAUT key used to unblock the PIN, and must be used with a secure channel established by CSC role. The APDU format is compliant with GP specifications.
- ***CHANGE REFERENCE DATA:*** This APDU is used to set the initial cardholder PIN. Note: This command is also utilized to set the initial PUK Value (8 bytes static string) and to update it. PUK is another option to unblock the PIN.
- ***RESET RETRY COUNTER:*** This APDU is used by v2 applet suite to unblock the cardholder PIN and restore the VERIFY PIN service with a new counter value if the CSC role is authenticated successfully. Note: With this command, the PIN can also be unblocked using the PUK as an option.
- ***REGISTER APPLET:*** This APDU is used by applet suite v2 to register applet instances to the ACA instance so that the access control and secure message service can be provided.
- ***REGISTER ACR:*** This APDU is used by applet suite v2 to manage the mapping between ACRID and actual APDU instruction.
- ***SET APPLICATION UID***: This APDU is sent when the UID associated with the applet instance needs to be changed.
- ***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.
- ***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.
- ***PRIVATE SIGN / DECRYPT***. This APDU uses the RSA private key in the PKI buffer to sign data.
- ***SET PROPERTIES***: Load the properties for the objects managed by the applet

6.4.2 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
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***READ BINARY:*** This APDU is used by applet suite v2 to read the data from selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***PUT DATA:*** This APDU is present for compliance with PIV specifications. This service always returns an exception with current applet v2.
- ***GENERATE ASYMMETRIC RSA KEY PAIR:*** This APDU is present for compliance with PIV specifications. This service always returns an exception with applet v2.
- ***RESET RETRY COUNTER:*** This APDU is used to unblock the PIN with PUK string.

6.4.3 Card Holder Role

- ***VERIFY***: This APDU checks the PIN presented by the cardholder against the current PIN.
- ***CHANGE REFERENCE DATA:*** This APDU is used by applet suite 2 to change the cardholder PIN if the Card Holder is correctly authenticated.
- ***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.
- ***PRIVATE SIGN / DECRYPT***. This APDU uses the RSA private key in the PKI buffer to sign data.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***READ BINARY:*** This APDU is used by applet suite v2 to read the data from selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***GET DATA***: This command is used to retrieve a single data object like PIV object content
- ***GENERAL AUTHENTICATE***: The APDU is for PKI operations (via the PIV EP wrapper)

6.4.4 No Role

- ***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)
- ***GET DATA***: this command is used to retrieve a single data object, such as the Card Identification data.
- ***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.
- ***GET PROPERTIES***: This APDU is used to obtain information about applet instance configuration.
- ***GET ACR:*** This APDU is used to retrieve the ACR definition for the services.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***READ BINARY:*** This APDU is used by applet suite v2 to read binary data stored on the card.
- ***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.
- ***GET CERTIFICATE***: This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.
- ***LOGOUT:*** To logout all authenticated roles.
- ***UPDATE PROPERTIES:*** Change the ACA applet properties regarding change pin after first use flag and Applet Mode (GSC-IS v2.1 or CAC v1)
- ***GENERAL AUTHENTICATE***: The APDU is for PKI operations (via the PIV EP wrapper)
- ***GET VERSION***: The command fetches the applet version for the PIV EP applet wrapper (it has identical format than ***GET DATA*** above)

6.5 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

Table 9: Role and possible ACR configuration for Card Manager

For applets suite v2, the access rules are listed in Table 10.

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC) / SECURE CHANNEL	Application Operator / XAUT (or PUK)	Card Holder / PIN	V2.6.2	
					ISO 7816	ISO 14443
RESET RETRY COUNTER (without PUK)		X	X		X	
(without PUK)CHANGE REFERENCE DATA (Create PIN/PUK + Update PUK)		X			X	
PUT KEY		X			X	
REGISTER APPLET		X			X	
REGISTER ACR		X			X	
SET APPLICATION UID		X			X	
AC EXTERNAL AUTHENTICATE			X		X	
PUT DATA			X		X	
GENERATE ASYMMETRIC RSA KEY PAIR			X		X	
RESET RETRY COUNTER (with PUK)			X (PUK)		X	
VERIFY				X	X	
CHANGE REFERENCE DATA (change PIN)				X	X	
SELECT	X				X	X
GET RESPONSE	X				X	X

UPDATE PROPERTIES	X				X	
GET PROPERTIES	X				X	X
GET ACR	X				X	
GET CHALLENGE	X				X	
LOGOUT	X				X	
GET VERSION	X				X	X
GENERATE KEY PAIR		X		X	X	
PRIVATE SIGN		X		X	X	X
SET PROPERTIES		X			X	
UPDATE CERTIFICATE / STATIC BUFFER		X	X	X	X	
READ CERTIFICATE / STATIC BUFFER	X	X	X	X	X	X
GET CERTIFICATE	X	X	X	X	X	
READ BINARY	X		X	X	X	X
GET DATA	X			X	X	X
GENERAL AUTHENTICATE	X			X	X	X

Table 10: Role and possible ACR configuration for Applet

7. MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the ActivIdentity Applet v2 is to provide a FIPS approved platform for applets that may in turn provide 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 ActivIdentity Applet v2.6 to provide cryptographic services. These include:

- TDES, (2 keys EDE TDES)
- SHA-1,
- RSA PKCS #1 (1024, 1536 and 2048 bit keys)

The TDES (CBC mode) algorithm is used both for authenticating the Crypto Officer (EXTERNAL AUTH command) and for 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). TDES, RSA and SHA-1 algorithms are provided as services through Java APIs to applets that may be loaded onto the cryptographic module.

7.1 CRITICAL SECURITY PARAMETERS:

- **CSC Card Manager / Security Domain key set (each key is 16-bytes):**
  - 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 out side of the cryptographic module, and loaded during initialization protected with a Global Platform secure channel using the key set that already exists in the card manager security domain (for example, Kinit)
- **Secure Channel session keys (each key is 16-bytes):**
  - S_{enc}: used to encrypt command and response APDU data encrypted mode of the secure channel to provide message confidentiality.
  - S_{mac}: used to MAC command and response APDU data in MAC mode of the secure channel to provide message integrity.
- **External Authentication Keys (XAUT)**: 16-byte TDES keys that enable the authentication of either Application Operators (PKI/GC read or PKI/GC Update) or Cryptographic Officers (Reset Retry Counter and Unblock PIN). These keys are generated out side 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, 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), 9Eh (PIV Card Authentication Key).
- **Personal Identification Numbers (PIN):** PINs and PIN 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.
- **Access Control Rule**: 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.

- **DAP TDES MAC Key:** This 16-byte Used to verify the Data Authentication Pattern (DAP) attached with the APDU during an applet load process. The DAP is calculated over the entire applet content and attached to the LOAD command when a Security Domain with mandated or optional DAP verification privilege is installed on the card.
- **Delegated Management TDES MAC receipt key:** This 16-byte key is used to calculate the TDES MAC over the token receipt provided by the card to provide evidence of a successful LOAD command. The receipt is provided as part of the response APDU when a Security Domain with Delegated Management privilege has been installed on the card.
- **PRNG Seed and seed key:** These are CSPs used in the ANSI X9.31 RNG. They are stored in EEPROM across power-cycles and in RAM during module execution.

7.2 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
PIN	RESET RETRY COUNTER	CSC	Write
	CHANGE REFERENCE DATA	Card Holder	Write
	VERIFY CHV	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
CSC Card Manager 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/DECRYPT	Card Holder	Execute
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
	LOAD	CSC	Execute
Delegated management receipt key	PUT KEY	CSC	Write
	INSTALL & DELETE	CSC	Execute
PRNG Seed and seed key	GENERATE KEY	Card Holder/ CSC	Write
	GET CHALLENGE	Card Holder/ CSC	Execute
	INIT UPDATE	CSC	Execute
Secure Channel session key S_{enc}	Message confidentiality	CSC	Execute
	INIT UPDATE	CSC	Create
Secure Channel session key S_{mac}	Message integrity	CSC	Execute
	INIT UPDATE	CSC	Create

Table 11: Access to CSPs and the Services

8. SELF TESTS

The SafesITe TOP FIPS DM GX4 performs the following self-tests to ensure that the module works properly.

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

Table 12 - Self-tests list

8.1 SELF-TEST EXECUTION

After –SafesITe TOP FIPS DM GX4 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. These tests are conducted automatically as part of the normal functions of the cryptographic module. They do not require any additional operator intervention, or applet specific functions.

Power-up self-tests are executed on reception of the first APDU command, after the module reset. 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 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, then sending any APDU command via its input data interface, provides a means by which the operator can repeat the full sequence of power-up self-tests.

9. SECURITY RULES

9.1 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 retrieves the ATR from the module to validate that the ATR bytes are the same as those listed in Section 2.1. The operator of the cryptographic module sends the GET PROPERTIES APDU to the module to validate that the applet version is 2.6.1 or 2.6.2.
- The operator of the cryptographic module sends GET ACR to the module to validate that module service Access Control Rules are configured per table 10.
- The module follows all security rules outlined in section 9 to maintain in FIPS mode.

9.2 AUTHENTICATION SECURITY RULES

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

- All CSPs are entered into the cryptographic module encrypted except the Card Holder PIN (and PUK during 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 OP 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 provides 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).
- Cryptographic services are restricted to authenticated roles.
- 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.

9.3 APPLET LIFE CYCLE SECURITY RULES

The ActivIdentity Digital Identity Applet Suite v2 for 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 command 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.

9.4 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 <= 10 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.

9.5 KEY MANAGEMENT SECURITY POLICY

9.5.1 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.

9.5.2 Cryptographic Key Entry

Keys 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 and the K_{kek} Key).

9.5.3 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

9.5.4 Cryptographic Key Zeroization

The cryptographic module zeroizes cryptographic keys by reloading either a zero-valued key set for a CSC GP secure channel key set, DAP TDES MAC Key, Delegated management receipt key or an Application Operator XAUT key with PUT KEY command, or closing the secure channel for session keys**.** The Card Holder PIN is zeroized by setting it to zero value via the CHANGE REFERENCE DATA command. The RSA private key is zeroized by reloading a zero-valued key using PUT KEY. The other CSPs such as PRNG seed and seed key can be zeroized by setting the card to the Terminated state.

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

10. MITIGATION OF ATTACKS

The GCX4 – FIPS 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 GCX4 FIPS platform.

11. SECURITY POLICY CHECK LIST TABLES

11.1 ROLES AND REQUIRED AUTHENTICATION

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

11.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	> 1:2 ^{112}
PIN	> 1:1,000,000
PUK	> 1:1,000,000

11.3 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

12. REFERENCES

- Java Card ™ 2.2.1 Virtual Machine Specification, October 2003, Sun Microsystems
- Java Card ™ 2.2.1 Application Programming Interface, revision 1.1, October 2003, Sun Microsystems
- Java Card ™applet developer's guide
- Java Card ™ 2.2.1 Runtime Environment (JCRE) Specification, October 2003, 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)
- "Identification cards - Contactless integrated circuit(s) cards –Proximity cards - Part 2: Radio frequency power and signal interface" ISO/IEC 14443-2, AMD1 (2005)
- "Identification cards - Contactless integrated circuit(s) cards –Proximity cards - Part 3: Initialization and anticollision" ISO/IEC 14443-3, AMD1 (2005)
- "Identification cards - Contactless integrated circuit(s) cards –Proximity cards - Part 4: Transmission protocol" ISO/IEC 14443-4, AMD1 (2001)
- 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
- RSA PKCS#1: RSA Cryptographic Standard (RSA Laboratories) – 2.1

13. ACRONYMS

Acronyms	Definitions
ACR	Access Control Rule
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
DAP	Data Authentication Pattern
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
GC	Generic Container
GSC-IS	Government Smart Card Interoperability Standard
JCRE	Java Card ™ Runtime Environment
PKI	Public Key Infrastructure
MAC	Message Authentication Code
GP	Global platform
PIN	Personal Identification Number
PUK	PIN Unblocking Key
RAM	Random Access Memory
ROM	Read only Memory
SD	Security Domain
SC	Secure Channel
TDES	Triple-DES (112-bit length keys)
XAUT	External Authentication