Oberthur CosmopolIC V4 Smart Card with ActivCard Applets

FIPS 140-1 Level 2

Security Policy

Public Version
V2.8

March 12, 2004

Oberthur Card Systems
3150 E. Ana Street
Rancho Dominguez, CA 90221
(310) 884 7900

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Document overview

This document defines the cryptographic module Security Policy for the Oberthur Card Systems CosmopolIC V4 Smart Card.

The Oberthur Card Systems CosmopolIC V4 Smart Card offers Java Card technology and Open Platform 2.0.1' services to applets such as ActivCard applets.

The Oberthur Card Systems CosmopolIC V4 Smart Card Operating System is also referred as the "Java Card platform" in the scope of this document.

The Smart Card directly provides all the low-level services such as memory management, I/O control, cryptographic algorithms and physical security.
These services can be accessed by the applets loaded onto the chip EEPROM or ROM using the Java Card API. These services include in particular Cryptographic functions such as DES and Triple DES encryption and decryption, RSA signature and verification and RSA key generation, as well as digest computation using SHA-1 algorithm.

The Card Manager applet provides the Open Platform services that are both internal (accessible by applets) and external services (accessible by external or non-chip applications).

"Applets" are applications that can be executed on the Smart Card. They provide high-level services that are accessible to the final customer through a set of software running as non-chip applications. Each applet provides a set of commands that defines its external services. The commands that trigger the applet services are called APDUs. A SELECT command must be sent to the smart card OS to activate an applet. The following commands sent to the Card OS result in the execution of the applet code providing the service.

The execution of applet code on the platform requires two preliminary steps: the download of packages including the executable code of one or several applets (this step is skipped when the applet package is in ROM), and the instantiation in EEPROM of the applet, that can be repeated several times for each applet, thus creating several instances in EEPROM. In order for the cryptographic module to be correctly operated, only FIPS approved applets (applets previously tested against FIPS) can be instantiated.

In the context of this Security Policy, the Oberthur Card Systems CosmopolIC V4 Smart Card is used with ActivCard ID, PKI and GC applets:

- The ID applet offers Card Holder Verification (CHV) services to external (off-card) entities.
- The PKI Applet offers RSA-based cryptographic services to external (off-card) entities.
- The GC Applet offers secure storage services to external (off-card) entities.

Other FIPS validated applets (tested against FIPS) may be downloaded to the smart card. Any such applets must be verified with a digital signature as part of the download process.

This document addresses two Configurations of the cryptographic module depending on whether the executable code of the applet suite is in EEPROM or in ROM. Version CAC01 refers to the code for the above ActivCard applets stored in EEPROM and version CAC02 to the same applet executable code stored in ROM. In both cases, applet instances (i.e. customer data) remain in EEPROM and can be added and deleted in accordance with the procedures identified in this Security Policy.

1.2 Acronyms and definitions

• ACR	Access Control Rule
• A.O.	Application Operator
• APDU	Application Protocol Data Unit
• API	Application Programming Interface
• C.O.	Cryptographic Officer
• C.H.	Card Holder
• EEPROM	Electrically Erasable and Programmable Read Only Memory (non-volatile but changeable)
• JCRE	Java Card Run-Time Environment
• OP	Open Platform or Global Platform
• PIN	Personal Identification Number
• P.N.	Part Number (identifying a product)
• ROM	Read Only Memory (non- volatile, non changeable)
• SRDI	Security Relevant Data Items
• XAUT	External Authentication

1.3 References

[R1] Open Platform Card Specification 2.0.1′, available from http://www.globalplatform.org, dated April, 2000.

[R2] ISO/IEC 7816-1, 1998-10-15: “Identification cards - Integrated circuit(s) cards with contacts- Part 1: Physical Characteristics”

[R3] ISO/IEC 7816-2, 1999-03-01: “Identification cards - Integrated circuit(s) cards with contacts- Part 2: Dimensions and location of the contacts”

[R4] ISO/IEC 7816-3, 1997-12-15: “Identification cards - Integrated circuit(s) cards with contacts- Part 3: Electronic signals and transmission protocols”

[R5] PKCS #1 v2.0: RSA Cryptography Standard, RSA Laboratories October 1, 1998

[redacted]

2 SECURITY LEVELS

The Oberthur Card Systems CosmopolIC V4 platform, along with the ActivCard applets meets the overall requirements applicable to Level 2 security of FIPS 140-1. The individual security requirements specified for FIPS 140-1 meet the level specifications indicated in the following table.

Security Requirements Section	Level
Cryptographic Module	2
Module Interfaces	2
Roles and Services	2
Finite State Machine	2
Physical Security	2
Software Security	3
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	3
Self-Test	2

3 Cryptographic Module Specification

The Oberthur Card Systems CosmopolIC V4 Smart Card complies with the various ISO/IEC standards and specifications for Integrated Circuit Cards with contacts (ISO/IEC 7816 standards).

The Smart Card and the applets act as a slave, only respond to commands and never start services or protocols on its own. The commands are sent to the Chip using a single I/O contact.

In the scope of this document, the Oberthur Card Systems CosmopolIC V4 Smart Card and the ActivCard applets are bound together and considered as a single chip embodiment of a cryptographic module. The software/hardware combinations included in the scope of the evaluation and tested against FIPS are the following:

This document addresses the submission for validation of the "CosmopolIC V4 Smart Card" hardware device in two software configurations: CAC01-D904, and CAC02-D906:

Software Configuration CAC01-D904 (Applets in EEPROM):

- Hardware platform number 0x52 with Firmware version 0xD904
- Additional Known Answer Tests on CosmopolIC V4 in EEPROM– Ref 058621
- ActivCard ID applet executable code – Version (hexadecimal) 01.00.00.13 in EEPROM
- ActivCard PKI applet executable code – Version (hexadecimal) 01.00.00.15 in EEPROM
- ActivCard GC applet executable code – Version (hexadecimal) 01.00.00.17 in EEPROM

In this configuration, the historical bytes returned by the card after power-on are the following:

00 31 C0 53 **CAC401** 64 52**D904**00 82 9000

Software Configuration CAC02-D906: (Applets in ROM with FIPS optimized firmware):

- Hardware platform number 0x52 with Firmware version 0xD906
- ActivCard ID applet executable code – Version (hexadecimal) 01.00.00.13 in ROM
- ActivCard PKI applet executable code – Version (hexadecimal) 01.00.00.15 in ROM
- ActivCard GC applet executable code – Version (hexadecimal) 01.00.00.17 in ROM

In this configuration, the historical bytes returned by the card after power-on are the following:

00 31 C0 53 **CAC402** 64 52**D906**00 82 9000

Firmware version 0xD906 has been optimized for FIPS compliance and includes a native implementation of the FIPS required Known Answer Tests. Such code does no longer need to be loaded in EEPROM.

By storing the applet executable code in ROM instead of EEPROM, configuration CAC402 frees up valuable EEPROM memory resources to store more applets instances and other customer data.

The cryptographic boundary for the Oberthur Card Systems CosmopolIC V4 Smart Card is the physical boundary of the smart card, which is also considered the cryptographic module. The cryptographic module, in simplest terms, is made up of an opaque plastic with the hardware chip embedded beneath a contact plate. The plastic card and contact plate perform no cryptographic functionality, but provide the tamper evidence of the cryptographic module.

3.1 Mode of Operation

The CosmopolIC V4 smart card with ActivCard Applets described in this security Policy is set in FIPS mode during manufacturing and remain in FIPS mode throughout its life. The cryptographic module is always in a FIPS approved mode of operation.

3.2 Module interfaces

The electrical and physical interface of the cryptographic module is comprised of the 8-electrical contacts from the contact plate of the card to its underlying chip. The location of the contacts complies with ISO/IEC 7816-2 standard and the physical characteristics of the chip comply with the ISO/IEC 7816-1 standard.

The logical interface of the module is provided by a set of commands that are available to external (off-card) entities. These commands are described in details in proprietary documents for each on-chip entity. An overview of these commands is provided in §4.3.
The chip entities that can process these commands are:

- The Card Manager
- The ID Applet
- The GC Applet
- The PKI Applet

3.3 Roles and services

Roles and services are described in Section 4.

3.4 Finite State Machine

The Finite State Machine diagrams are provided as separate documents.
Both the Smart Card and the applets follow a set of well-defined state transitions.

The applets provide the main cryptographic services and roles as described in §4.

3.5 Physical Security

The Physical Security of the Oberthur Card Systems CosmopolIC V4 Smart Card module is designed to meet FIPS 140-1 level 2 requirements.

The smart card is usually in possession of either a Cryptographic Officer or of the User.

In order to physically attack the module, an attacker will have to take possession of the module and gain access to the chip embedded in the card. The attacker would need to use extraordinary means such as electronic probe or electronic microscope to access the critical security parameters contained on the chip embedded inside the module. The contact plate covering the top of the chip coupled with the plastic of the smart card covering the back and sides of the chip provide the opaque, tamper-evident coating required for Physical Security Level 2. The contact plate must be pried off, the epoxy resins dissolved, or the plastic card must be penetrated to gain access to the chip for probing.

Once the smart card has been attacked through any of these physical means, the attack leaves permanent evidence which can be subsequently detected the owner.

3.6 Software Security

Most of the software of Oberthur Card Systems CosmopolIC V4 is secure from modification due to the fact that it is stored in the chip ROM.

The Oberthur Card Systems CosmopolIC V4 platform software includes an on-chip Java Card Virtual Machine.

As applets are used through the Java Card Virtual Machine, the applet runs in a “Java Sandbox”, which prevents the applet objects and services from being accessed by other applets, unless explicitly authorized.

Applets management and key management APDU commands (such as download, install, delete, put key) are protected by secure channel. They have their origin authenticated and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post issuance.

The Oberthur Card Systems CosmopolIC V4 also provides a Data Authentication Pattern for each applet that has to be loaded in EEPROM. This insures that the chip issuer has digitally signed each applet that is to be loaded on the chip, allowing prior security verification of each applet and avoiding the loading of any unauthorized applet during the manufacturing process.
This mechanism is not mandatory and is not used in the current configuration as all applets either in ROM or well identified prior to the loading process.

Additionally, all software implemented using a high-level language, except when it is essential to the performance or security of the module (cryptographic algorithms, I/O routines …).

3.7 Operating System Security

Operating system requirements only apply when untrusted software is permitted within the module, which, for FIPS 140-1 level 2, a C2 trusted operating system would be required. Since untrusted software is not currently loaded into the module the requirements in this section do not apply.

During the manufacturing process, only trusted (tested against FIPS) applets or source code is loaded (for version 0057) or activated (for version 005B) on the chip.

After completion of the manufacturing process (including pre-personalization) when the chip has reached its normal Operating Life Cycle State (Card Manager Secured State), only trusted FIPS 140-1 validated applets can be loaded or installed onto the module. Furthermore, at the time of loading, these applets must be identified as part of the cryptographic module (see section 5.2 for details).

3.8 Key Management

Details on the Key Management scheme are provided in a separate document.

The cryptographic module handles various keys:

- Card Manager and Security Domain keys
- Application keys.

The Card Manager keys are all Triple-DES keys that are securely entered in the cryptographic module during the manufacturing (pre-personalization) process.
The first Initialization Secret Key (ISK) is loaded encrypted (using Triple DES) under the Master Key that is put in place by the chip founder.
Then, the Card Manager key-loading scheme follows the Open platform specifications:

- The keys of the first loaded key-set are encrypted (using Triple DES in ECB mode) under the Initialization Secret Key.
- The other key sets are loaded encrypted under a previously loaded key also using Triple DES in ECB mode.

The application (applet) keys are either DES/Triple-DES keys securely entered using the Card Manager security features: following the Open Platform specifications, application keys are encrypted using Triple DES in ECB mode using one of the Card Manager keys. The applet internally invokes the Card Manager cryptographic services to decrypt and verify the integrity of the loaded keys.
Some applets also use RSA keys that are generated on-board using a FIPS approved random generator (compliant with FIPS 186-2 appendix 3, §3.4).

3.9 Cryptographic algorithms

The following FIPS approved algorithms are available on the Oberthur Card Systems CosmopolIC V4 with ActivCard applets:

- GC Applet:
  - TDES - ECB mode through Java Card crypto services
  - TDES – CBC mode through Open Platform secure messaging services

- PKI Applet:
  - RSA key generation (length = 1024bits) using FIPS approved random number generation
  - TDES – CBC & TDES – ECB mode through Open Platform secure messaging services

- ID Applet:
  - TDES - ECB mode through Java Card crypto services
  - TDES – CBC mode through Open Platform secure messaging services

The following general algorithms are also available from the platform:

- DES (ECB and CBC modes): to be used for legacy applications only
- Triple-DES (ECB and CBC modes)
- SHA-1
- RSA signature compliant with PKCS#1 standard

3.10 EMI/EMC

The Oberthur Card Systems CosmopolIC V4 chip meets the EMI/EMC requirements specified by United States Standard 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

Thus, it meets the FIPS 140-1 Level 3 requirements in this matter.

3.11 Self Tests

Several self-tests are performed by the Oberthur Card Systems CosmopolIC V4 Smart Card with the ActivCard applets.

These self-tests include:

- Power-Up Tests: when the chip is powered-up, the following tests are performed:
    - ROM integrity check
        - Operating System integrity check (on version 0057 and 005B)
        - ROM Applets integrity check (on version 005B)
    - Random Generator check
    - EEPROM “native” code integrity check
        - This applies to version 0057 only as 005B does not have any soft mask code loaded in EEPROM
    - Known Answer Tests for:
        - DES
        - Triple-DES
        - SHA-1
        - RSA

- Random Generation Tests: each time the Hardware Random Number Generator or the Software Pseudo-Random Number Generator is used, the module performs a continuous RNG test that verifies that it is working properly in accordance to the FIPS 186-2 (Appendix 3) standard.

- Key-Pair Consistency Tests: each time an RSA key pair is generated, the PKI applet checks that the keys are consistent by checking that a block of data can be encrypted with the public key and decrypted with the private key with no modification.

[redacted]

4 ROLES AND SERVICES

The Oberthur Card Systems CosmopolIC V4 platform with ActivCard applets insure the authentication of external (off-chip) entities and provide them with cryptographic services according to their role.

The various roles and services are defined by the applets relying on the Card Manager or on a Security Domain cryptographic services:

- OP Secure Channel
- OP key encryption (within a Secure Channel)

An OP Secure Channel can be opened with the chip by an off-chip entity by performing a mutual authentication with a specific key set. All keys used are triple DES keys. Each time a Secure Channel is opened, some session keys are computed by both the chip and the off-chip entity in order to authenticate each other.
The key computation is done according to the Open Platform specification.
The term "key computation" refers to the establishment of a secure channel. A secure channel is a commercially-available key distribution technique which implements the Open Platform specification and is compliant with FIPS 171 (Key management using ANSI X9.17).

When a Secure Channel is open, encrypted keys (DES, Triple DES or RSA) can be sent to the chip and decrypted by the Card Manager or the Security Domain using triple DES in ECB mode.

4.1 Roles

Each applet (GC, ID and PKI) is linked to the Card Manager or to a Security Domain (provided by the platform) and supports the following roles:

4.1.1 Any Role

This role is allowed to access services that do not require any authentication. This role is needed, for example, so that certain chip information can be obtained prior to services that require authentication. The corresponding authentication method is “None”.

4.1.2 User Roles

- **Card Holder** - The Card Holder is responsible for insuring the ownership of his chip (it is a Card Holder as the chip itself is usually embedded in a card) and for not communicating his PIN. The Card Holder is authenticated by verification of a password or PIN.
- **Application Operator** – The Application Operator represents an off-chip entity operating an external application requesting the services offered by the applets. The applet authenticates the Application Operator role by verifying the possession of a 3DES key.

4.1.3 Cryptographic Officer Roles

- **Cryptographic Officer** – The Cryptographic Officer is responsible for managing the security configuration of the applets, and in particular executes the necessary PIN. The Cryptographic Officer owns a Card Manager or Security Domain Key Set, and has therefore access to the services offered by the Card Manager or Security Domain. The Cryptographic Officer has also the privilege to unblock the PIN, after successive wrong PIN values have been tried.

4.2 Role Authentication

The applets implement specific methods for authenticating the different roles and provide them with cryptographic services.
The implementation consists of the binding of a Role-based Access Control Rule to each service.

User Authentication

- **PIN**: the Card Holder must send a Verify PIN command to any ActivCard applet to access any Applet service protected with PIN. The APDU corresponding to the applet service must be sent before the chip is removed from the reader or a reset order is send to the chip.
- **PIN Always**: the Card Holder must send a Verify PIN command to any ActivCard applet to access any applet service protected with PIN Always. The APDU corresponding to the applet service must be sent immediately after the PIN has been verified.
- **External Authentication (XAUT)**: The Application Operator must prove the possession of a particular 3DES key to access the GC Applet read or update service protected with External Authentication with this particular key.

Cryptographic Officer Authentication

- **Secure Channel**: The Cryptographic Officer must prove the possession of a Key Set composed of 3 3DES keys. Two keys are used to derive session keys that insure the confidentiality of the command payload, mutually authenticate the parties and protect the APDU command integrity. A third key is used to encrypt keys transported within the APDU command. The applets rely on the OP secure channel service to perform the corresponding decryptions and verifications. To access an applet service protected by secure channel, the application controlled by the Cryptographic Officer must first mutually authenticate with the applet[1], thus creating the session keys.

[1] The mutual authentication follows the OP specification: an initialize update APDU is first sent followed by an external authenticate APDU. The applet relies on the internal secure channel API to perform the mutual authentication and further decryptions and verifications

- **External Authentication (XAUT)**: The Cryptographic Officer must prove the possession of a particular 3DES key to access the ID Applet PIN unblock service protected with External Authentication with this particular key.

4.3 Services

Each applet service is associated with a Role-based Access Control Rule that also indicates the allowed role for that service, as detailed in the previous section.

The Access Control Rule may be configurable or fixed depending on the Applet service.
The applet services are invoked by external APDU commands sent to the chip. The ACRs are applied on the APDU commands.

In the following, the applet services are explained in detail. In addition, a table that describes what roles can access what services (or what services are available to what roles) is presented.

The first column of the table lists the services (corresponding to APDU name), and the first row corresponds to the roles, followed by the authentication method required for that role in the second row. Certain combinations of roles are explicitly defined.

4.3.1 ID Applet Services

The ID applet provides Card Holder Verification (CHV) services. Here are the different APDUs / Services that are provided by an ID applet instance:

- **Select**: This APDU causes the selection of the applet or of the Card Manager.
- **Install**: This APDU causes the installation of the applet. It is not sent to the Applet, but to the Card Manager.
- **Change PIN/Unblock**. All PIN-protected services of all applet instances that are attached to a particular ID instance are not accessible to the Card Holder when these applets are in “PIN blocked” state. The Change PIN APDU is used to set a new PIN value and/or recover Card Holder.
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Initialize update**. This APDU corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and generate the session keys.
- **External Authenticate**. This APDU corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and generate the session keys for the secure channel.
- **Verify CHV**. This APDU checks the PIN presented by the Card Holder against the current PIN associated with the ID applet instance.
- **Put Key**. This APDU is used to set the XAUT key used to unblock the PIN, and must be used with a secure channel. The APDU format is compliant with OP specification.
- **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.

- **AC External Authenticate**. This APDU is used in combination with a Get Challenge. This APDU is used to unblock the PIN.
- **Change PIN after First Use**. This APDU indicates that the Card Holder must change his PIN before any PIN protected service can be accessed.
- **Set Status**: This APDU is sent when the applet instance life cycle needs to be changed.
- **Set Application UID**: This APDU is sent when the UID associated with the applet instance needs to be changed.

Role	Any Role	Crypto-graphic Officer	Crypto-graphic Officer	Card Holder
Authentication Method	None	SECURE CHANNEL	XAUT	PIN
ID Applet services				
INSTALL		☒		
CHANGE PIN/UNBLOCK		☒	☒	☒
GET PROPERTIES	☒			
INITIALIZE UPDATE	☒			
EXTERNAL AUTHENTICATE		☒		
VERIFY CHV				☒
PUT KEY		☒		
GET CHALLENGE	☒			
AC EXTERNAL AUTHENTICATE			☒	
CHANGE PIN AFTER FIRST USE	☒			
SET STATUS		☒		
SET APPLICATION UID		☒		

Roles & possible ACR configuration for ID applet services

Only roles and services relevant to the FIPS are represented in this chart.

4.3.2 PKI Applet Services

The PKI Applet provides RSA-based cryptographic services. There is one RSA private key for each PKI applet instance. The corresponding certificate is located in the attached GC instance.
Here are the different APDUs / Services that are provided by a PKI applet instance:

- **Select**: This APDU causes the selection of the applet**Install**: This APDU causes the installation of the applet. It is not sent to the Applet, but to the Card Manager.
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Initialize update**. This APDU follows the OP secure channel specification. It is necessary to mutually authenticate with the Cryptographic Officer and generate the session keys.
- **External Authenticate**. This APDU follows the OP secure channel specification. It is necessary to mutually authenticate with the Cryptographic Officer and generate the session keys.
- **Generate Key Pair**. This APDU is used to generate a Key Pair in the Chip. The Private Key is associated to a PKI applet instance.
- **Get Certificate**. This APDU is used to obtain the certificate corresponding to the PKI applet instance private key. **Sign**. This APDU uses the RSA private key in the applet instance to sign data.
- **PIN Verify**. This APDU checks the PIN presented by the Card Holder against the current PIN associated with the ID applet instance.
- **Put Key**. This APDU is used to import/unwrap the private key (Chinese Remainder Theorem) components. The APDU format follows OP specification. **Set Status**: This APDU is sent when the applet instance OP life cycle needs to be changed.
- **Set Application UID**: This APDU is sent when the UID associated with the applet instance needs to be changed.

Role	Any Role	Crypto-graphic Officer	Card Holder	**Card Holder**	
Authentication Method	None	SECURE CHANNEL	PIN	PIN ALWAYS	NEVER (*)
PKI Applet Services					
INSTALL		X			
GET PROPERTIES	X				
INITIALIZE UPDATE	X				
EXTERNAL AUTHENTICATE		X			
GENERATE KEY PAIR		X	X	X	X
GET CERTIFICATE	X		X	X	X
SIGN			X	X	X
PIN VERIFY			X	X	
PUT KEY		X			
SET STATUS		X			
SET APPLICATION UID		X			

Roles & possible ACR configuration for PKI applet services

Only roles and services relevant to the FIPS are represented in this chart.

(*) The module has the capability of having more than one instance of each applet. Some applets, i.e. the PKI applet, have the option of setting some services to "never execute". In other words some options can be disabled. For example, two instances of the PKI applet could exist on the same module. One instance has full functionality and the other could have GENERATE KEY, GET CERTIFICATE, and/or SIGN disabled (never executed).

4.3.3 GC Applet Services

The GC Applet provides secure storage services.
Here are the different APDUs / Services that are provided by a PKI applet instance:

- **Select**: This APDU causes the selection of the applet. The select() method of the applet instance is called.
- **Install**: This APDU causes the installation of the applet. It is not sent to the Applet, but to the Card Manager.
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Initialize update**. This APDU follows the OP secure channel specification. It is necessary to mutually authenticate with the Cryptographic Officer and generate the session keys.
- **External Authenticate**. This APDU follows the OP secure channel specification. It is necessary to mutually authenticate with the Cryptographic Officer and generate the session keys.
- **Update Buffer**. This APDU is used to write or modify data elements in storage area.
- **Read Buffer**. This APDU is used to read data elements from storage area.
- **Get Challenge**. This APDU is used in combination with GC external Authenticate to perform an external authentication.
- **Put Key**. This APDU imports/unwraps the 3DES XAUT keys. The APDU format follows OP specification.
- **AC External Authenticate**. This APDU enables read or update access to GC secure storage–protected by XAUT.
- **PIN Verify**. This APDU checks the PIN presented by the Card Holder against the current PIN associated with the ID applet instance.
- **Set Status**: This APDU is sent when the OP applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, or PERSONALIZED.
- **Set Application UID**: This APDU is sent when the UID associated with the applet instance needs to be changed.

Role	Any Role	Crypto-graphic Officer	Card Holder	Card Holder	Application Operator	A.O. or C.H.	A.O. and C.H
Authentication Method	None	SECURE CHANNEL	PIN	PIN ALWAYS	XAUT	XAUT or PIN	XAUT then PIN
GC Applet services							
INSTALL		☒					
GET PROPERTIES	☒						
INITIALIZE UPDATE	☒						
EXTERNAL AUTHENTICATE		☒					
UPDATE BUFFER	☒	☒	☒	☒	☒	☒	☒
READ BUFFER	☒	☒	☒	☒	☒	☒	☒
GET CHALLENGE	☒						
PUT KEY		☒					
GC EXTERNAL AUTHENTICATE					☒		
PIN VERIFY			☒	☒			
SET STATUS		☒					
SET APPLICATION UID		☒					

Roles & possible ACR configuration for GC applet services

Only roles and services relevant to the FIPS are represented in this chart.

5 SECURITY RULES

5.1 Applet environment

- The Card Holder must take the necessary measures to insure that the terminal and/or the Card Acceptance Device are controlled by a valid role: Card Holder, application operator or Cryptographic Officer / crypto-officer.

5.2 Content Management

- The management of the life cycle of the applets – instantiate, delete, personalize keys, shall follow the Open Platform standard.
- Applets management and key management APDU commands (such as, instantiate, delete, put key) are protected by secure channel.
- The download of certified applets packages[2] and the instantiation of applet instances may either occur at pre-issuance, issuance or post-issuance, by any entity owning one Open Platform key set of the Card Manager.
- There may be as many instances of each applet as there are available chip resources.

5.3 Role Authentication

- The applets shall provide the following distinct operator roles: The user role – Application Operator or Card Holder, and Cryptographic officer role.
- The applets shall provide role-based authentication.
- Cryptographic services are restricted to authenticated roles.
- The Role authentication methods (ACRs) for each applet service are set by the Cryptographic officer during Applet instantiation following the settings described in §4.3 and cannot be modified during the lifetime of the ID applet instance.
- When authentication of the role cannot be performed because the related key or password or key attributes are missing, the corresponding service must be disabled.
- The results of authentication must be set in transient memory and therefore cleared when the module is powered down.
- The Applet instance configuration may require the combined authentication of different roles to access a particular service. For instance the Application Operator and then the Card Holder must both authenticate themselves to access the UpdateBuffer service.
- The Card Holder can access services requiring Application Operator authentication after the Application Operator has been authenticated successfully.

[2] Only applet code defined as part of the cryptographic module can be loaded and installed.

- The Application Operator can access services requiring Card Holder authentication by PIN after the Card Holder has been authenticated successfully. This rule is not applicable for services requiring Card Holder authentication with PIN ALWAYS.

5.4 Key management

- RSA private keys and 3DES keys must be transported encrypted to the chip. This is done the Card Manager cryptographic services, meaning that each key is encrypted under one of the Card Manager keys using Triple DES in ECB mode.

5.5 PIN management

- The password or PIN that is used by the applet to authenticate the Card Holder must not be divulged to other parties than the Card Holder.
- The ID applet must be configured by the cryptographic officer so that:
  - After M consecutive unsuccessful PIN code validation attempts, the Card Holder services must be disabled. (e.g. The PIN is blocked)
  - After N consecutive unsuccessful PIN unblocking attempts using a secure channel with incorrect key or parameters, the Card Holder services are permanently disabled (e.g. The PIN is locked)
  - The PIN length must always be comprised between P and Q alphanumeric characters
  - M, N, P and Q are set by the Cryptographic officer at Applet instantiation time and cannot be modified during the lifetime of the ID applet instance.
- If separation of roles between the Card Holder and Cryptographic officer is required for a particular service, such as the RSA Signature service the PIN always ACR must be selected.

6 DEFINITION OF SECURITY RELEVANT DATA ITEMS

6.1 List of SRDIs

The following Security Relevant Data Items (SRDIs) are managed from the applets:

- **Authentication Method (or ACR)**: These data elements define the Authentication Method that is permanently set for the service. Only some services offer a configurable Authentication Method (see chapter 3.3).
- **Open Platform Applet life cycle states**: The OP application status information (PERSONALIZED, BLOCKED, SELECTABLE). These states are managed by the Card Manager, but the state transitions are managed from the applets.
- **External Authentication Keys**: These are 3DES keys that enable the authentication of Application Operators (GC read / GC Write) or Cryptographic Officers (PIN Unblock).
- **RSA private keys**: are managed (generated, unwrapped) from the PKI applet using the Java Card cryptographic services. These keys are used to sign data.
- **RSA public keys**: Public keys are generated on chip from the RSA key pair generation, and exported off chip.
- **X.509 Certificates**: The certificates corresponding to the private keys present in the chip are managed by the applets.
- **Personal Identification Numbers or passwords (**PIN): PINs and PIN attributes are managed from the ID applet, which relies on the Java Card PIN management service.

The following Security Relevant Data Items are used (but not managed) from the applets:

- **Open Platform Key Sets:** are managed by the Card Manager or security domain. These keys enable the authentication of the Cryptographic Officer, and the encryption of data or keys incoming from these entities. Although the applets do not manage these SRDIs, the OP key sets are used by the applets to enable the secure channel service at the applet level.

The different applet services rely on the Java Card API to generate, create, modify, control, protect, transport, use or delete the SRDIs.

The following Security Relevant Data Items are managed directly by the Card Manager and are not accessible to the applets:

- **Security Audit Log:** is managed by the Card Manager. This log allows the Card Manager to keep trace of security events such as loss of integrity of Sensitive Data Elements (PIN and keys), Security Exceptions, EEPROM error, Authentication failures of Card Manager and of Security Domains.

6.2 Access to Security Audit Log

The audit log can be read freely by an off-chip entity. It does not contain any sensitive information, only public data and information.

During the manufacturing of the chip (chip initialization), only the Cryptographic Officer is allowed to modify the content of the audit log (in order to reset its content for example).

Once the card is issued (manufacturing state has ended), the audit log cannot be modified by any entity.

6.3 Applet Access to SRDIs vs. Services

The following matrices show for each applet how services access SRDIs. The rows list SRDI (shown in bold) and the operations on the SRDI. The column describes which applet service (APDU command) is performing the operation on the SRDI. The role that is associated with the operation is shown in the second and third column. To see what role, and using which service (APDU command) to perform the operation on a specific SRDI:

- Locate the operation under the SRDI (for example import key under External Authentication Keys)
- See which role or roles can perform it (only Cryptographic Officer can perform the import key)
- See which service (APDU command) delivers this service (in this case PUT KEY).

6.3.1 ID Applet

ID applet Columns: Services (roles) Rows: Access to SRDIs	**Card Holder**	**Cryptographic Officer**	INSTALL-instantiate (C.O)	CHANGE PIN/UNBLOCK (C.O)	GET PROPERTIES (any)	INITIALIZE UPDATE (any)	EXTERNAL AUTHENTICATE (C.O)	VERIFY CHV (C.H)	PUT KEY (C.O)	GET CHALLENGE (any)	AC EXTERNAL AUTHENTICATE (C.O)	CHANGE PIN AFTER FIRST USE (any)	SET STATUS
Access Control Rules													
Install ACR		X	X										
PIN or Password													
Install PIN		X	X										
Change/Unblock PIN	X	X		X									
Verify PIN	X							X					
External Authentication Keys													
Delete key		X							X				
Import key		X							X				
Verify cryptogram		X		X							X		
Card Manager Key set													
Verify Cryptogram		X		X			X		X				
Decrypt APDU payload		X		X					X				
Applet Instance Status													
Change status													X

6.3.2 PKI Applet

PKI applet services Columns: Services (roles) Rows: Access to SRDIs	***Card Holder***	***Cryptographic Officer***	INSTALL instantiate (C.O)	GET PROPERTIES (any)	INITIALIZE UPDATE (any)	EXTERNAL AUTHENTICATE (C.O)	GENERATE KEY PAIR (C.O or CH)	GET CERTIFICATE (any)	SIGN (C.H)	PIN VERIFY (C.H)	PUT KEY (C.O)	SET STATUS
Access Control Rules												
Install ACR		☒	☒									
PIN or Password												
Verify PIN	☒									☒		
RSA Key Pair												
Generate Key Pair	☒	☒					☒					
Import CRT components		☒									☒	
Delete private key		☒									☒	
Sign data	☒								☒			
Card Manager Key set												
Verify Cryptogram		☒									☒	
Decrypt Data		☒				☒					☒	
Applet Instance Status												
Change status												☒

6.3.3 GC Applet

GC applet services Columns: Services (roles) Rows: Access to SRDIs	**Card Holder**	**Cryptographic Officer**	**Application Operator**	INSTALL (Instantiate)	GET PROPERTIES (any)	INITIALIZE UPDATE (any)	EXTERNAL AUTHENTICATE (C.O)	UPDATE BUFFER (C.0 or A.O or C.H)	READ BUFFER (C.0 or A.O or C.H)	GET CHALLENGE (any)	PUT KEY (C.O)	GC EXTERNAL AUTHENT (A.0)	PIN VERIFY (C.H)	SET STATUS
Access Control Rules														
Install ACR		☒		☒										
PIN or Password														
Verify PIN	☒												☒	
External Authentication Keys														
Delete key		☒									☒			
Import key		☒									☒			
Verify cryptogram			☒									☒		
Card Manager Key set														
Verify Cryptogram		☒						☒	☒		☒			
Decrypt Data		☒					☒	☒	☒		☒			
Applet Instance Status														
Change status														☒