FIPS 140-1 CRYPTOGRAPHIC MODULE SECURITY POLICY

GEMPLUS GEMXPRESSO PRO E64 PK – FIPS ICC WITH ACTIVCARD APPLET SUITE

November 9, 2004

ActivCard®

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

This document describes the security policy for the "Gemplus GemXpresso Pro E64 PK - FIPS ICC with ActivCard Applet Suite", the correct operation of the device, and the security rules governing the device. Some of these rules are derived from the security requirements of FIPS PUB 140-1, while others are derived from Gemplus and Activcard's collective experience in embedded security software.

1.2 OVERVIEW

The cryptographic module is the combination of the "Gemplus GemXpresso Pro E64 PK – FIPS" ICC and the "ActivCard Applet Suite" (a combination of card and applets). Gemplus aims to provide FIPS140-1 Level 2 cryptographic Smart Cards. The cards are based on a Gemplus implementation of an Open Platform compliant OS and on platform-independent cryptographic applets developed by ActivCard. When the ActivCard Applets are installed on the Gemplus Smart Card platform, the card and applets provide authentication and digital signature cryptographic services to end users.

The card is a state of the art Java Open Platform-based Smart Card. This highly secure platform benefits from all the Gemplus expertise in Java Card security and provides FIPS approved cryptographic algorithms and self-tests. The card provides a fully compliant Java Virtual Machine (VM) [3] [4], an Open Platform operating environment [1] that complies with the VOP specification [2], the cryptographic module integrates symmetric and asymmetric cryptographic algorithms as specified in the Java Card specification [3] and offers RSA for Signature/Verification, SHA-1 hashing function, On-board RSA Key generation and 3DES CBC and ECB algorithms.

The ActivCard Applet Suite transforms the card platform into the validated device with which end users interact. The three validated ActivCard "applets" composing the suite include the ID, PKI, and GC applet; which offer Card Holder Verification (CHV) services, RSA-based cryptographic services, and secure storage services (respectively) to off-card/end-user entities. Execution of ActivCard applets on the card platform requires two preliminary steps: the downloading of packages including the code of one or several applets, and the instantiation of the applets, a process that can be repeated several times for each applet, thus creating multiple instances.

1.3 REFERENCES

Ref. #	Specifications	Release
[1]	Open Platform Card Specification (OP)	2.0.1'
[2]	Visa Open Platform Implementation Specification (VOP)	2.0.1'
[3]	Java Card API Specification (Sun)	2.1.1
[4]	Java Card Runtime Environment (JCRE) Specification (Sun)	2.1.1
[5]	ISO 7816 parts 1-6 (ISO/IEC)	-

1.4 ACRONYMS

Acronym	Description
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
JCRE	Java Card Run-Time Environment
OP	Open Platform or Global Platform
MAC	Message Authentication Code
PIN	Personal Identification Number
SRDI	Security Relevant Data Items
XAUT	External Authentication

1.5 SECURITY LEVEL

The cryptographic module meets the overall requirements applicable to FIPS140-1 Level 2. The individual security requirements meet the level specifications as follows:

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

2 CRYPTOGRAPHIC MODULE SPECIFICATION

The "Gemplus GemXpresso Pro E64 PK – FIPS ICC with ActivCard Applet Suite" is a FIPS validated device that meets FIPS 140-1 Level 2 requirements. As stated before, the cryptographic module is the combination of "ActivCard Applet Suite" installed on the "Gemplus GemXpresso Pro E64 PK – FIPS" ICC. Physically, the module is a single-chip implementation that includes the chip (ICC), the contact plate (to which the ICC is wire-bonded), and the resin that covers the ICC. The ICC of the module includes a Smart Card–dedicated micro controller featuring 64 KB EEPROM, RAM, XRAM, Hardware Security Mechanisms, Memory Access Control through MMU, Hardware Random Generator, Cryptographic Co-Processors (DES, 3DES and modular exponentiation), and Hardware CRC 16 bits.

The chip's ROM contains the "GemXpresso Pro E64 PK – FIPS" Operating System (OS). It includes the following:

- The Gemplus Card Manager applet is in charge of secure applet loading, Global PIN and card life cycle management according to the OP specification.
- The OP API provides the entry points following the OP specification [1].
- The Java Card API provides the services according to the Java Card specification [3].
- The COM is in charge of managing the ISO 7816 communication protocols.
- The native API provides internal services built on top of the chip hardware services.
- The Memory Manager Unit (MMU) is in charge of the secure system memory addressing.

The random number generator and the FIPS self-tests are located in EEPROM memory. However they are non changeable after card manufacturing and are subject to software integrity test at power-up.

The chip's EEPROM memory stores the ActivCard applets. These applets along with the Gemplus Card Manager applet are included within the FIPS cryptographic boundary along with the physical components of the module (hardware version GP92 firmware version GXP3 – FIPS). Specifically, the ID applet (v1.0.0.19, v1.13.0.19, or v1.0.0.24), the PKI applet (v1.0.0.18, v1.13.0.18, or v1.0.0.30), and the GC applet (v1.0.0.23, v1.13.0.23, or v1.0.0.28) are defined to be part of the module. The word "Applet" in this Security Policy refers to either on or all of these three Applets.

3 MODULE INTERFACES

Physically, the interfaces to the cryptographic module are those defined by the ISO 7816 standards (parts 1 and 2 of [5]), while the logical interfaces are defined by the various APDU commands provided by the applets and Card Manager [1].

The physical interfaces of the module follow the standards "ISO 7816-1 Physical characteristics" and "ISO 7816-2 Dimensions and contact location."

Contact No.	Assignments	Contact No.	Assignments
C1	VCC (Supply voltage)	C5	GND (Ground)
C2	RST (Reset signal)	C6	Not Used
C3	CLK (Clock signal)	C7	I/O (Data Input/Output)
C4	Reserved for Future Use	C8	Reserved for Future Use

The logical interfaces provided by the module are composed of the APDU commands that can be sent to the module and the responses that the card sends back.

The data exchange protocol between the cryptographic module and an outside device follows the ISO 7816-4 [5]. 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

4 PHYSICAL SECURITY

The "Gemplus GemXpresso Pro E64 PK – FIPS ICC with ActivCard Applet Suite" single chip module is designed to meet the FIPS140-1 Level 3 Physical Security requirements.

4.2 MANUFACTURING PROCESS

The manufacturing process consists of wire-bonding the ICC over printed circuit plate providing ISO contacts and sealing the chip and wires in Epoxy coating.

Any mechanical attack attempting to extract the chip from the micro-module results in damaging the chip and prevents it from working. Furthermore, attempts to attack the chip or micro-module will result in signs of tampering such as scratches and deformation.

The module is designed for embedding in a plastic card body for Smart Card manufacturing.

4.3 HARDWARE SECURITY MECHANISMS

The embedded chip provides the cryptographic module with hardware security mechanisms commonly featured in Smart Card dedicated chips such as probing detection, low frequency and supply voltage monitoring. The chip reacts to a low/high clock frequency, and low/high power supply voltage by filtering the signal or resetting the cryptographic module.

5 SOFTWARE SECURITY

The cryptographic module Operating System is stored within the chip's ROM, and is therefore protected against unauthorized disclosure and modification. It includes a firewall, a Java Virtual Machine (VM) and a Java Card Runtime Environment [4].

The cryptographic module is implemented using a high level language. A limited number of software modules that require fast processing have been written in a low-level language.

5.2 VIRTUAL MACHINE AND FIREWALL

The cryptographic module allows several applets to coexist safely in its memory thanks to its secure Virtual Machine and firewall.

The firewall protects an applet's objects from illegal access by another applet, conforming to the JCRE specification. This means that the firewall also protects the Card Manager Java objects from illegal access (Global PIN, Key set). The virtual machine interprets the applet byte code. Its implementation is fully compliant with the Java Card [3] standard.

Moreover the cryptographic module performs the requested services according to its roles and services security policy.

5.3 CARD LIFE CYCLE

The card life cycle is managed according to the Open Platform Card Specification [1]. Issued cards are pre-loaded with a set of applets, cryptographic keys, and PIN, and are in the OP "SECURED" state. This life cycle state is irreversible and its security implementation is fully compliant with the VOP specification [2].

5.4 SECURE COMMUNICATION

The Gemplus Card Manager applet controls the sensitive operations defined in the 'Roles and Services' section, requiring the opening of a secure communication channel based on the knowledge of a secret. The related secure messaging protocol follows the VOP [2] specification.

5.5 APPLET LOADING

At post–issuance, applets are downloaded according to the OP specification [1]: the use of a secure channel with the Gemplus Card Manager is required. During applet loading, the applet code integrity is verified and its origin (Cryptographic Officer) is authenticated. The applet code is rejected in case of authentication and/or verification failure. This prohibits unauthorized downloading.

During loading an integrity checksum is dynamically computed by the platform and stored in EEPROM. It is used at next power-up to perform integrity check of the newly loaded Applet.

6 KEY MANAGEMENT

The module governs/manages key at two levels: the Card Manager key set and applet or application specific keys.

6.1 CARD MANAGER KEY SET

The cryptographic module implements OP [1] and VOP [2] specifications. The card issuer security domain includes key sets for card administration purposes. These key sets are used to establish a secure communication between the Gemplus Card Manager applet and the Cryptographic Officer.

When the Card Manager is the selected applet, all commands besides those required to set up the secure channel must be performed within a secure channel. The one exception to this rule relates to the Get Data APDU command that can be issued to the Card Manager without first setting up a secure channel.

The card life cycle state determines which modes are available for the secure channel. In the OP_SECURED card life cycle state, all command data must be secured by at least a MAC. As specified in the OP specification, there exist earlier states in which a MAC might not be necessary to send Card Manager commands. However the cryptographic module as defined is already switched to OP_SECURED mode when issued. The key set associated with the secure channel is such that:

- All DES keys are double length keys (16 bytes),
- All DES operations are performed using triple DES encryption or decryption.
- All MAC generations result in an 8-byte field. These 8 bytes constitute the MAC.

Key sets are identified by Key Set Versions ('01' to '7F'). The keys within a key set version have the following different functionality:

1. The Secure Channel Encryption/Authentication key (index 1, S-ENC) is used to generate an encryption session key that is then used both for mutual authentication and to encrypt APDU command data.
2. The Secure Channel Message Authentication Code key (index 2, S-MAC) is used to generate a MAC session key that is then used to generate a MAC for APDU commands (command header and command data).
3. The Data Encryption Key (index 3, DEK) is used as is to encrypt key data.

6.2 APPLICATION/APPLET KEY SETS

Applets may use keys with key types in conjunction with the cryptographic services of the module. DES keys, RSA public and private keys, and RSA Chinese Remainder Theorem public and private keys are available for applets. Specifically, the applets of the module make use of 3DES keys and RSA public and private keys.

7 CRYPTOGRAPHIC ALGORITHMS AND SELF-TESTS

"GemXpresso Pro E64 PK – FIPS ICC with ActivCard Applet Suite" provides the following FIPS approved security algorithms:

- DES & 3DES (ECB & CBC modes)
- SHA-1
- PKCS#1 RSA Signature/Verification (vendor affirmed)[1]
- X9.17 Random Number Generation

The "GemXpresso Pro E64 PK – FIPS" platform performs the following self-tests to ensure that the module works correctly.

Self-Tests	**Execution**
Cryptographic algorithm test (Known-answer tests for DES, 3DES, SHA-1, RSA)	At Power-Up
Software/firmware integrity test.	At Power-Up
Pair-wise consistency test.	Conditional
Software load test.	Conditional
Continuous random number generator test.	Conditional

[1] "GemXpresso Pro E64 PK – FIPS" Java Card API also provides applets with X9.31 RSA Signature/Verification (vendor affirmed) in addition to PKCS#1 functionality; however, this functionality in not available with the "ActivCard Applet Suite," which implements only PKCS#1 RSA Signature/Verification.

8 ROLES AND SERVICES

The applets insure the authentication of off-card entities and provide them with cryptographic services according to their role.

8.1 ROLES

Each applet supports the following roles:

8.1.1 ANY ROLE

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

8.1.2 USER ROLES

- **Cardholder** - The Cardholder is responsible for ensuring the ownership of his or her card and for not communicating his or her PIN. The Cardholder is authenticated by verification of a password or PIN
- **Application Operator** – The Application Operator represents an off-card 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.

8.1.3 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, and key management operations for the applet. The Cryptographic Officer owns a Card Manager or Security Domain Key Set (a set of three triple DES keys), and has therefore access to the services offered by the Card Manager or Security Domain. The Cryptographic Officer also has the privilege to unblock the PIN, after successive wrong PIN values have been tried. This is done by externally authenticating himself by proving the possession of a 3DES key, in order to access the PIN unblock service of an ID applet instance.

8.2 ROLE AUTHENTICATION

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

8.2.1 USER AUTHENTICATION

- **PIN**: the Cardholder 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 card is removed or a reset order is send to the card.

- **PIN Always**: the Cardholder 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 an applet specific 3DES key to access that applet service.

8.2.2 CRYPTOGRAPHIC OFFICER AUTHENTICATION

- **Secure Channel**: The Cryptographic Officer must prove the possession of a Key Set composed of three 3DES keys.
- **External Authentication (XAUT)**: The Cryptographic Officer must prove the possession of a particular 3DES key to access the ID Applet PIN unblock service.

8.3 SERVICES

8.3.1 PLATFORM SERVICES

The Platform provides the following services as specified in OP specification [1] and [2]:

Delete, External Authentication, Get Status, Initial Update, Install, Load, PIN Change, Unblock, Put Data, Put Key, Set Status.

All these services are only available to the Cryptographic Officer owning the Card Manager keys.

8.3.2 APPLET 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. Each applet instance may be configured independently. Once set, the ACR cannot be deleted or modified during the life of the applet instance.

The applet services are invoked by external APDU commands sent to the card. The ACRs are applied on the APDU commands.

All services are specified in the respective Applet Specification documents.
In the following paragraphs, the applet services are explained in detail. In addition, a table that describes which roles can access which services (or which services are available for which roles) is presented. The first column of the table lists the services (corresponding to APDU name), and the second column corresponds to the roles, followed by the authentication method required for that role. Certain combinations of roles are explicitly defined and access control rules can be set to enforce them.

Similar services are provided by the three applets. Here are the different APDUs / Services that are provided by an instance of one of the three applets:

- **Select**: This APDU selects the applet.
- **Install**: This APDU installs the applet. It is not sent to the Applet, but to the card manager.
- **Get Properties**. This APDU obtains 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 complete the mutual authentication with the Cryptographic Officer and the generation of the session keys for the secure channel.
- **Set Status**: This APDU is sent when the applet OP 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.

8.3.3 ID APPLET SERVICES

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

- **Change PIN/Unblock**. The Change PIN APDU is used to set a new PIN value and recover Cardholder access.
- **Verify CHV**. This APDU checks the PIN presented by the Cardholder 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.
- **Get Challenge**. This APDU is used in combination with AC (ActivCard) 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 and set a new PIN.
- **Change PIN after First Use**. This APDU indicates that the Cardholder must change his PIN before any PIN protected service can be accessed.

Role / Authentication Method vs. Services	Any Role / None	Cryptographic Officer SECURE CHANNEL	Cryptographic Officer XAUT	Cardholder PIN
ID Applet				
INSTALL		X		
CHANGE PIN/UNBLOCK		X	X	X
GET PROPERTIES	X			
INITIALIZE UPDATE	X			
EXTERNAL AUTHENTICATE		X		
VERIFY CHV				X
PUT KEY		X		
GET CHALLENGE	X			
AC EXTERNAL AUTHENTICATE			X	
CHANGE PIN AFTER FIRST USE	X			
SET STATUS		X		
SET APPLICATION UID		X		

Roles & possible ACR configuration for ID applet services
Only FIPS-modes are represented in this chart.

8.3.4 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 specific APDUs / Services that are provided by a PKI applet instance:

- **Generate Key Pair**. This APDU is used to generate a key pair within the Smart Card.
- **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 Cardholder 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.

Role / Authentication Method vs. Services	Any Role / None	Crypto-graphic Officer SECURE CHANNEL	Cardholder PIN	Cardholder PIN ALWAYS	NEVER
PKI Applet					
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 FIPS-modes are represented in this chart.

8.3.5 GC APPLET SERVICES

The GC Applet provides secure storage services. Each GC applet instance corresponds to one storage area consisting of two buffers: one buffer contains the TAGs and Lengths of stored data elements, and the other buffer contains the values of each data element.
Here are the different specific APDUs / Services that are provided by a PKI applet instance:

- **Update Buffer**. This APDU is used to write or modify data elements in the storage area.
- **Read Buffer**. This APDU is used to read data elements from the 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 the OP specification.
- **AC External Authenticate**. This APDU enables the external authentication of the host to the applet service – here the Read or Update Buffer – protected by XAUT.
- **PIN Verify**. This APDU checks the PIN presented by the Cardholder against the current PIN associated with the ID applet instance.

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

Roles & possible ACR configuration for GC applet services
Only FIPS-modes are represented in this chart.

9 SECURITY RULES

9.1 APPLET ENVIRONMENT

- The applets must be installed on the Gemplus GemXpresso PRO E64 PK – FIPS ICC.
- The Cardholder must take the necessary measures to ensure that the terminal and/or the Card Acceptance Device are controlled by a valid role: Cardholder, application operator or Cryptographic Officer.

9.2 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 a secure channel.
- The downloading of certified applets packages[2] and the instantiation of applet instances may occur at pre-issuance, issuance or post-issuance, and be performed by an authenticated Cryptographic Officer, i.e. an entity owning Open Platform key sets of the Card Manager or security domain.
- There may be as many instances of each applet as there are available Smart Card resources.

9.3 ROLE AUTHENTICATION

- The applets shall provide the following distinct operator roles: The user role – Application Operator or Cardholder – and the 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 and cannot be modified during the lifetime of the applet instance.
- The ACRs must be set in accordance with section 10.3 (Access to SRDIs vs. Services).
- 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.

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

- 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 Cardholder must both authenticate themselves to access the Update Buffer service.
- The Cardholder can access services requiring Application Operator authentication after the Application Operator has been authenticated successfully.
- The Application Operator can access services requiring Cardholder authentication by PIN after the Cardholder has been authenticated successfully. This rule is not applicable for services requiring Cardholder authentication with PIN ALWAYS.

9.4 KEY MANAGEMENT

- RSA private keys and 3DES keys must be transported encrypted to the card.

9.5 PIN MANAGEMENT

- The password or PIN that is used by the applet to authenticate the Cardholder must not be divulged to parties other than the Cardholder.
- 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 (that is, 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 (eg. The PIN is locked).
  - The PIN length must always be from P to 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.
  - Although M, N, P, Q are not specified, care must be taken in choosing these values. For example, M and N should be larger than 3. P should be larger than 4.
- If the separation of roles between the Cardholder and Cryptographic Officer is required for a particular service, such as the RSA Signature service the PIN Always ACR must be selected.

10 DEFINITION OF SECURITY RELEVANT DATA ITEMS

10.1 PLATFORM SRDIS

The SRDIs of the cryptographic module related to the Platform are:

- OP key set of the Card Manager
- Global PIN
- Applet header

The following table presents the association between the services or authentication mechanisms and the SRDI they access. The access types are labeled as follows:

- R: Read access
- W: Write access
- U: Used - the SRDI is used internally only. The SRDI data itself is neither read from nor written to the crypto-module.

SRDI	Interface allowing interaction	Access type
OP key set of the Card Manager	**EXTERNAL AUTHENTICATE**	U
OP key set of the Card Manager	**PUT KEY**	W
Global PIN	**PIN CHANGE/UNBLOCK**	W
Applet header	**INSTALL**	W

10.2 LIST OF APPLETS 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 section 8.3).
- **Open Platform Applet life cycle states**: The applet 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 card from the RSA key pair generation, and exported off card.
- **X.509 Certificates**: The certificates corresponding to the private keys present in the card 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 incoming data or keys 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.

10.3 ACCESS TO APPLETS SRDIS VS. APPLETS SERVICES

The tables indicate, for each applet, which access operations on Security Relevant Data Items occur during the execution of the different applet services (APDUs). In parentheses are indicated what roles must be authenticated for these operations. Please see the Acronyms section page 5.

10.3.1 ID APPLET

PIN applet Columns: Services (roles) Rows: Access to SRDIs	**ROLES**		Services (roles)										
	Cardholder	**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**											**X**

10.3.2 PKI APPLET

PKI applet services Columns: Services (roles) Rows: Access to SRDIs	**ROLES**		Services (roles)										
	Cardholder	**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)	Set Status	PIN VERIFY(C.H)	PUT KEY(C.O)	
Access Control Rules													
Install ACR		**X**	**X**										
PIN or Password													
Verify PIN	**X**										**X**		
RSA Key Pair													
Generate Key Pair	**X**	**X**					**X**						
Import CRT components		**X**										**X**	
Delete private key		**X**										**X**	
Sign data	**X**								**X**				
Card Manager Key set													
Verify Cryptogram		**X**										**X**	
Decrypt Data		**X**				**X**						**X**	
Applet Instance Status													
Change Status		**X**								**X**			

10.3.3 GC APPLET

GC applet services Columns: Services (roles) Rows: Access to SRDIs	**ROLES**			Services (roles)										
	Card Holder	**Cryptographic Officer**	**Application Operator**	INSTALL (Instantiate)	GET PROPERTIES (any)	INITIALIZE UPDATE (any)	EXTERNAL AUTHENTICATE (C.O)	Set Status	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)
Access Control Rules														
Install ACR		**X**		**X**										
PIN or Password														
Verify PIN	**X**													**X**
External Authentication Keys														
Delete key		**X**										**X**		
Import key		**X**										**X**		
Verify cryptogram			**X**										**X**	
Card Manager Key set														
Verify Cryptogram		**X**							**X**	**X**		**X**		
Decrypt Data		**X**					**X**		**X**	**X**		**X**		
Applet Instance Status														
Change Status		**X**						**X**						