Gemplus Corp. and ActivCard Inc.

GemXpresso Pro R3 E64 PK - FIPS with ActivCard Applet v2

FIPS140-2 Level 2

Security Policy

Version 1.6

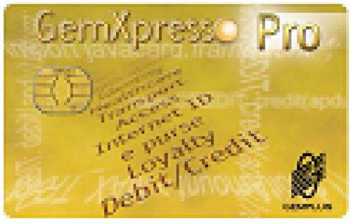

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for the "**GemXpresso Pro R3 E64 PK - FIPS with ActivCard Applet v2**" 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 MODULE OVERVIEW

The module consists of the Gemplus **GemXpresso Pro R3 E64 PK - FIPS** Java card module (which Gemplus designed to conform to FIPS 140-2 Level 3 security requirements) and the **ActivCard Applet v2**, and the synthesis of the two meets the overall level 2 security requirements of the FIPS 140-2 standard. Together, the card and applets provide authentication, encryption, and digital signature cryptographic services.

2.2 GEMPLUS SMART CARD OPEN PLATFORM

The cryptographic module is a state of the art Java Open Platform-based smart card. This highly secure platform benefits from all the Gemplus expertise in Java Card security and provides FIPS-approved cryptographic algorithms and self-tests. This cryptographic module uses a state of the art manufacturing flow in terms of security and provides resident 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[8]**.

The card life cycle is managed according to the **Open Platform (OP) specification** [4]. Issued cards have been loaded with a set of applets, cryptographic keys, and a PIN, and are moreover in the "OP_SECURE" state. The security implementation is fully compliant with the **VOP specification** [5] The cryptographic module integrates symmetric and asymmetric cryptographic algorithms as specified in the JavaCard specification [6] and offers RSA for Signature/Verification, SHA-1 hashing function, on-board RSA Key generation and 3DES CBC and ECB algorithms.

2.3 ACTIVCARD APPLET V2

ActivCard Applet v2 provides significant enhancements over the ActivCard v1 Applet in service, security, and flexibility. The ActivCard Applet v2 framework is backward compatible with earlier versions of ActivCard Applets and offers a more open, stable, and flexible platform for developers to build and deploy smart card applications. ActivCard Applet v2 also complies with GSC-IS 2.1 standard.

ActivCard Applets are a modular suite of Java applets that run on a Java card. Version 2 of this suite is distinctive from Version 1 in the following ways:

- It decouples on-card application services from security management such as authentication and secure messaging, providing a more flexible, secure, and open platform for applet developers.
- It provides a flexible architecture to allow future authentication and biometric services to be added to the module without modifying existing applications.

The two applets included in the cryptographic module are:

- **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 – OP secure messaging, PIN, and ActivCard External Authentication are included by default in the AC applet.

- **PKI/Generic Container (PKI/GC) Applet**– The PKI/GC Applet can be used to provide secure storage for both PKI credentials, and other data, 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. Up to 8 buffers can be configured for each applet instance.

3. Security Level

The cryptographic module meets the overall requirements applicable to **FIPS140-2 Level 2**. The cryptographic module enforces FIPS mode of operation at all times. The individual security requirements specified for FIPS 140-2 meet the level specifications indicated in the following table.

Security Requirements Section	Security Level
Cryptographic Module Specification	***2***
Cryptographic Module Ports and Interfaces	***2***
Roles, Services and Authentication	***2***
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	***N/A***
Overall FIPS 140-2 Security Level	***2***

Table 1 – Individual FIPS 140-2 Security Levels

4. Cryptographic Module Specification

4.1 Gemplus Crypto-Module Cryptographic Boundary

The Cryptographic Boundary is defined to be the ‘module edge’ of the GemXpresso Pro R3 E64 PK - FIPS Crypto-Module, referred to hereafter as the Micro Module, a set of “embedded” hardware and software that implements cryptographic functions and processes, including cryptographic algorithms and key generation. **GemXpresso Pro R3 E64 PK - FIPS** Micro-Module is a single chip implementation of a cryptographic module. The micro-module is designed to be embedded in a plastic card body to provide an **ISO-7816 [10]** compliant smart card. The hardware version number for the module is GP92 while the firmware version numbers are GXP3 – FIPS EI19 and GXP3 – FIPS EI19 with new ATR and fast ATR.

During the Gemplus manufacturing process, the side of the chip (ICC) with electrical contacts 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 **GemXpresso Pro R3 E64 PK – FIPS** Micro-Module are included in the cryptographic module boundary, as shown in the following figure:

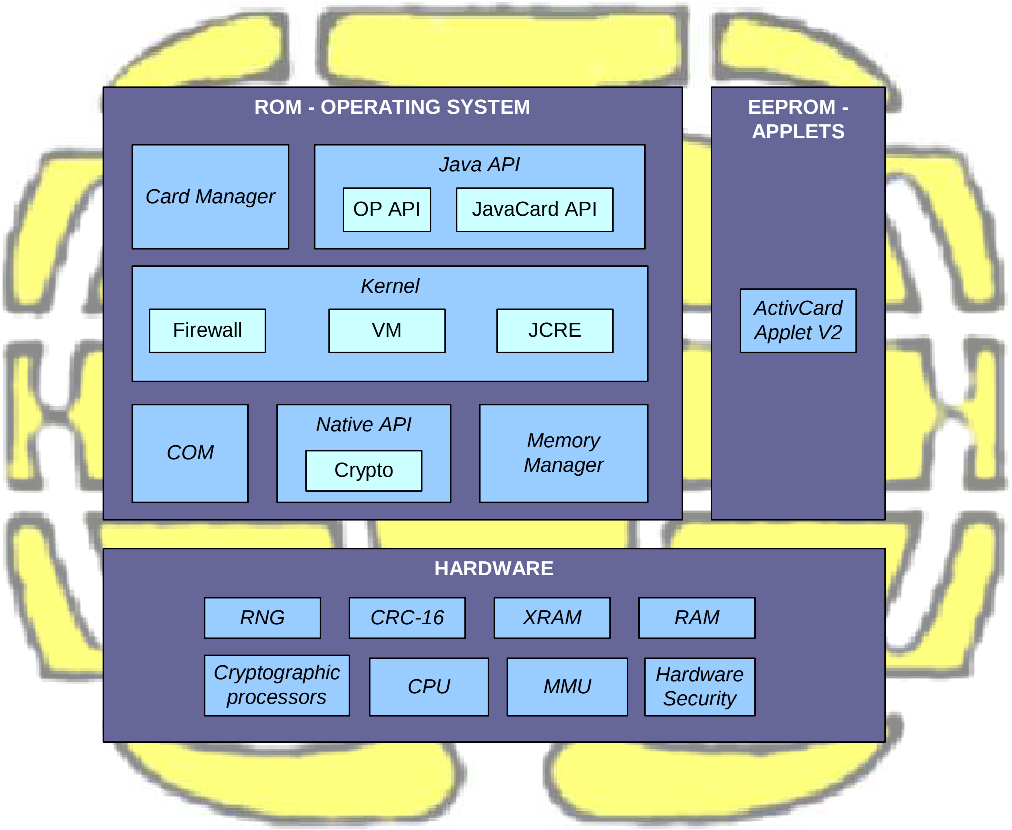

Figure 1- Cryptographic Module Boundary

The cryptographic module includes the **SLE66CX640P chip from Infineon**. It includes:

- CPU 10MHz 8051 compatible
- EEPROM 64 KB
- ROM 136 KB
- RAM 256 bytes
- XRAM 4096 bytes
- Hardware Security Mechanisms (probing detection, low frequency and supply voltage monitoring),
- Memory Access Control through MMU,
- Random Generator,
- Cryptographic Co-Processors (DES, 3DES and modular exponentiation)
- Hardware CRC 16 bits.

4.2 ActivCard Applet v2

The ActivCard Applet v2 supports role-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 a role based access control policy following the result of the authentication.

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

The ActivCard Applet v2 is composed of the following elements:

- AC applet package version v 2.3.0.1, 2.3.0.4, and 2.3.0.5
- PKI/GC applet package version 2.3.0.1, 2.3.1.1, and 2.3.1.2
- ASC library package version 2.3.0.1 and 2.3.0.3

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

The applets offer services to external applications, and rely 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 either be the Card Manager or a separate security domain. The Card Manager is itself a security domain with additional services, and applets. The Card Manager controls the global cryptographic module status.

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. The SC is generally 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 an Applet Security Controller role (ASC), which solely owns the replacement key set, can take control of the personalization of all applet instances belonging to a security domain.

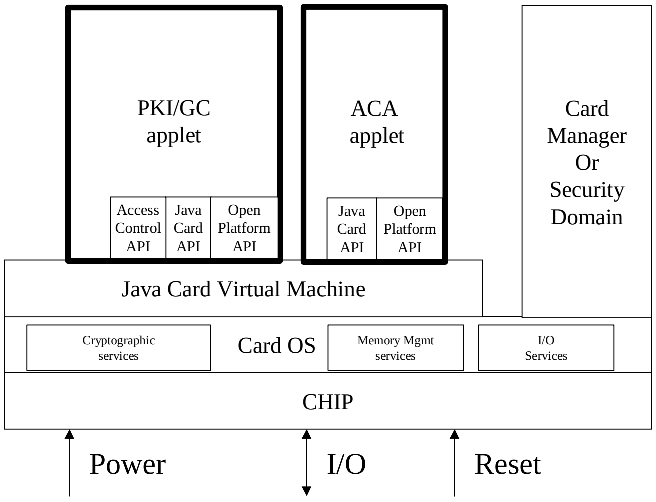

Figure 1: Functional block diagram

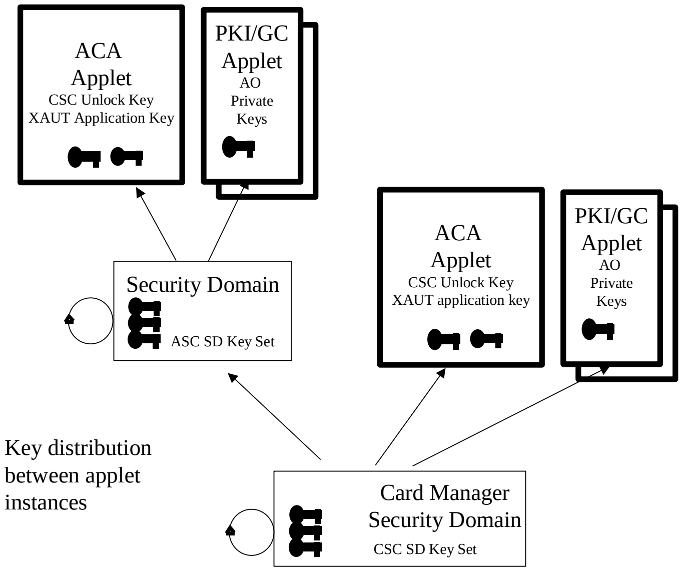

Figure 2: Key Distribution – Role separation

The Card Security Controller (CSC) role, which owns keys sets of the Card Manager, also plays an Applet Security Controller role for all applet instances depending on the Card Manager security domain.

4.3 FIPS APPROVED SECURITY FUNCTIONS

The following table gives the list of FIPS approved security functions that are provided by the **GemXpresso Pro R3 E64 PK – FIPS** Java Card API.

SECURITY FUNCTION	DETAILS	FIPS APPROVED
DES[1]	ECB mode in encryption	Yes
	ECB mode in decryption	Yes
	CBC mode in encryption	Yes
	CBC mode in decryption	Yes
3DES	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	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	Yes
3DES MAC	ECB and CBC modes	Yes

[1] DES should only be used in legacy systems

Notes:

- The CBC mode is used to establish a trusted path between **GemXpresso Pro R3 E64 PK – FIPS** and an external entity (MAC computation). Applet loading, regarding **OP specification [4]**, requires 3DES computation in CBC mode.
- The RSA Key generation is an X9.31 standard derived into a Gemplus proprietary solution (refer to section 7.1.5.1)
- The pseudo random generator (P-RNG) and the FIPS self-tests are located in EEPROM memory, are not changeable after card manufacturing and are subject to software integrity test at power-up.

Table 2 – FIPS Approved Security Functions

5. Module Ports and Interfaces

The **GemXpresso Pro R3 E64 PK – FIPS** Micro-Module restricts all information flow and physical access.
Physical and logical interfaces define all entry and exit points to and from the micro module.

5.1 Physical Ports

5.1.1 PIN assignments and contact dimensions:

GemXpresso Pro R3 E64 PK – FIPS Micro-Module follows the standards **"ISO 7816-1 Physical characteristics" [10]** and **"ISO 7816-2 Dimensions and contact location" [10]**.

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

Table 3 - Contact plate pin list

5.1.2 Conditions of use

The electrical signals and transmission protocols follow the **ISO 7816-3 [10]**. The conditions of use are the following:

Conditions	Range
Voltage	2.7 V to 5.5 V
Frequency	1MHz to 7.5MHz

Table 4 - Voltage and frequency ranges

5.2 Logical Interface

GemXpresso Pro R3 E64 PK – 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, **GemXpresso Pro R3 E64 PK – FIPS** Micro-Module inhibits all data output via the data output interface when an error state is reached and when performing self-tests.

5.2.1 APDU commands

The data exchange protocol between the cryptographic module and an outside device follows the **ISO 7816-4 [10] 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 5 - Accepted ISO APDU types

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

5.2.2 API interface

GemXpresso Pro R3 E64 PK – FIPS Micro-Module provides trusted applets with internal services through its **JavaCard [6]** and **OP [4] APIs**.
The cryptographic module provides an execution sandbox for the applets and performs the requested services according to its roles and services security policy.
The available API services are defined in the following section.

6. ROLES & SERVICES

6.1.1 Roles

The ActivCard Applet v2, defines four distinct roles that are supported by the on-module cryptographic system; Card Security Controller (CSC) role, Applet Security Controller (ASC) role, Application Operator role, and Card Holder role.

6.1.1.1 User Roles:

- **Card Holder Role** - The Card Holder role is responsible for insuring 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** – 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.

6.1.1.2 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 an OP 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.
- **Applet Security Controller (ASC) Role:** This role is responsible for managing the security configuration of the applets. The ASC role authenticates to the cryptographic module by demonstrating to the Applet security domain that he possesses the knowledge of an OP secure channel TDES key set stored within the security domain. The ASC role also has the privilege of

resetting the PIN try counter. This is performed either by authenticating himself using the OP secure channel key set, or an Unblock PIN XAUT TDES key. Note that the protection of the reset PIN retry counter service by XAUT external authentication is optional, as the reset PIN retry counter service is always accessible with the security domain OP key set.

6.1.2 Role Authentication

The ActivCard Applet v2 cryptographic module supports role authentication.

6.1.2.1 User Role Authentication

- The Card Holder role is authenticated with a PIN
  - **PIN**: this Card Holder role must send a Verify CHV APDU to any ActivCard applet or AC applet 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 order 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 must be sent before the cryptographic module is removed or a reset order is sent to the cryptographic module.

6.1.2.2 Cryptographic Officer Role Authentication

- The Cryptographic Officer role is authenticated by a TDES key or a TDES key set.
  - **Secure Channel key set:** The Cryptographic Officer (CSC or ASC) role must prove the possession of a key set composed of 3 TDES keys. Two keys (K_{MAC}, K_{ENC}) are used to derive session keys according to Global Platform specification described in [VOPS]. 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 encrypt keys transported within the APDU command.
  - **Unblock PIN External Authentication (XAUT) key**: The Cryptographic Officer (ASC) role must prove the possession of a particular TDES key to access the AC Applet RESET RETRY COUNTER service protected by External Authentication with this particular key (K_{XAUT}). The host application controlled by the Cryptographic Officer role encrypts an 8 byte card challenge with K_{XAUT}, and submits a RESET RETRY COUNTER APDU that includes the resulting cryptogram for verification to the cryptographic module.

6.1.3 Services

6.1.3.1 Crypto Officer Administrative Services

6.1.3.1.1 Card Platform Administrative Services Available to the CSC role

The following card platform services are used for the administration of the security domains, and to load applets onto the cryptographic module. This command set includes the following commands:

- ***INSTALL:*** this APDU is used to instruct 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).
- ***PUT KEY:*** this APDU is used to add or replace security domain key sets.
- ***SET STATUS:*** this APDU is used to modify the life cycle state of the cryptographic module or the life cycle state of an application.
- ***INITIALIZE UPDATE***: this APDU is used to initiate an OP Secure Channel with the Card Manager or a security domain. Cryptographic module and host session data are exchanged, and session keys are derived by the cryptographic module and host upon completion of this APDU. 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.
- ***PUT DATA***: this APDU is used to store or replace one tagged data object provided in the command data field.
- ***GET STATUS***: this APDU command is used to retrieve the Card Manager, load file (package), and application life cycle data specific to the OP specification.
- ***PIN CHANGE/UNBLOCK:*** This APDU command is used to change the value of the global PIN and to set the number of retries allowed or to unblock the current global PIN. PIN value is encrypted.

During the secured channel opening, the command access condition is specified (‘CLEAR’, ’MAC’, ’MAC+ENC’) and an access control decision is performed on the received command.

6.1.3.1.2 Applet Administrative Services available to the ASC role

The following applet administrative services are used for configuring applet specific properties and keys.

ACA Administrative Services

The following services are provided by the AC applets.

- ***INITIALIZE UPDATE.*** This APDU corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and derive 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 derive the session keys for the secure channel.
- ***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.
- ***SET APPLICATION UID***: This APDU is sent when the UID associated with the applet instance needs to be changed.
- ***REGISTER APPLET:*** This APDU registers applet instances to the ACA instance so that the access control and secure message service can be provided.
- ***REGISTER ACR:*** This APDU manages the mapping between ACRID and actual APDU instruction.
- ***RESET RETRY COUNTER:*** All PIN-protected services of all applet instances that are registered to the particular ACA instance are not accessible to the Card Holder when successive PIN verifications for that ID instance fail. These applets are then in a “PIN blocked” state.
    - o If this APDU is protected in secure channel using Cryptographic Officer OP SC key set, it is used to set a new PIN value and recover card holder access.
    - o If this APDU is protected by AC External Authenticate protocol using the Unblock External Authentication (XAUT) key, it also can be used to set a new PIN value and recover Card Holder access.
- ***PUT KEY***: This APDU is used to enter the XAUT key used to unblock the PIN, and must be used with a secure channel. The APDU format is compliant with OP specifications.

- ***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 to authenticate the Application Operator using the AC external authenticate protocol.
- ***UPDATE PROPERTIES***. This APDU sets 1) a flag that indicates that the card holder must change his PIN before any PIN protected service can be accessed; 2) return either CAC v1 status word, or GSC-IS v 2.1 status word, when the Card Holder enters the wrong PIN.

PKI/GC Applet Administrative Services

The PKI/GC Applet provides RSA-based cryptographic services. Each PKI/GC applet instance can store up to eight objects, either an RSA key pair / certificate object or T-V buffer object
.
The following services are provided by a PKI/GC applet instance:

- ***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.
- ***PUT KEY***: This APDU is used to import/unwrap the private key (Chinese Remainder Theorem) components. The APDU format follows OP specification. A unique private key exists for each RSA key pair object.
- ***SET PROPERTIES:*** This APDU is used to set the object ID of the different PKI/GC objects in the PKI/GC applet instance. Note that the access control rule is enforced at object level rather than the instance level.
- ***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.

6.1.3.2 <u>Usage services</u>

6.1.3.2.1 Card Platform and Applet Services Available to No Role (unauthenticated)

- ***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:*** the GET DATA command is used to retrieve a single data object. This command is available outside of a Secure Channel (no security condition). However, if issued within a Secure Channel, it must follow the same security level as defined in EXTERNAL AUTH.
- ***GET STATUS:*** if the Card Manager is the current application, this command is used to retrieve Card Manager information according to a given search criteria.
- ***GET RESPONSE***: this command is restricted to T = 0 ISO protocol for an incoming command which have data to send back. That data is received with the GET RESPONSE command sent immediately after the command it is related to.
- ***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.
- ***GET CERTIFICATE***. This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***Get ATR-*** This service allows a user to retrieve the module ATR by issuing a card reset.

A user can initiate module self-tests by issuing a card reset and issuing an APDU command

6.1.3.2.2 Applet Usage Services Available to Application Operator

The following services are available to the Application Operator role:

- ***GET CHALLENGE***. This APDU is used in combination with GC External Authenticate to perform an external authentication.
- ***AC EXTERNAL AUTHENTICATE***. This APDU communicates the cryptogram obtained by TDES encryption of a card challenge with the TDES key associated with the service – here read or update buffer – protected by XAUT.
- ***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.

6.1.3.2.3 Applet Usage Services Available to Card Holder

Common Usage Services

The following services (APDUs) are common to all instances of applets:

- ***VERIFY CHV***: This APDU checks the PIN presented by the Card Holder against the current PIN associated with the AC applet instance.

AC Applet Usage Services

The AC applet provides Card Holder Verification (CHV) services, access control enforcement, and secure messaging.

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

PKI/GC Applet Usage Services

The PKI/GC Applet provides RSA-based cryptographic services and secure storage. One RSA private key exists for each PKI buffer. The corresponding certificate is located in this PKI buffer.

The following APDUs / services are provided by a PKI/GC applet instance:

- ***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.
- ***PRIVATE SIGN / DECRYPT***. This APDU uses the RSA private key in the PKI buffer to sign data.

6.1.3.3 Relationship Between Roles & Services: Card Platform

Roles/Services	CSC role (Card Manager Security Domain)	No Role (Unauthenticated)
INSTALL	x	
LOAD	x	
DELETE	x	
EXTERNAL AUTHENTICATE	x	
GET DATA		x

GET STATUS	X	
GET RESPONSE		X
INITIALIZE UPDATE		X
PUT DATA	X	
PUT KEY	X	
SELECT		X
SET STATUS	X	
PIN CHANGE/UNBLOCK	X	

Table 1: Role and possible ACR configuration for Card Manager

6.1.3.4 *Relationship Between Roles & Services: Applets*

6.1.3.4.1 Access Control Rules

Each applet service is associated with a role-based Access Control Rule (ACR) that also indicates the allowed role for that service, as detailed in the previous section.
The ACR may be configurable or fixed depending on the applet service. The ACA is responsible for the configuration, management, and enforcement of the ACRs for each service provided by the applet instances.

The applet services are invoked by external APDU commands sent to the cryptographic module. The ACRs are applied on the APDU commands by the ACA. All services are specified in the respective Applet Specification documents.

6.1.3.4.2 Roles vs. Services: AC Applet

Services with configurable ACRs are in italic.

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Application Operator or ASC / XAUT	Card Holder / PIN
AC Applet				
INSTALL		X		
CHANGE REFERENCE DATA				X
GET PROPERTIES	X			
GET ACR	X			
INITIALIZE UPDATE	X			
EXTERNAL AUTHENTICATE		X		
VERIFY CHV	X			
PUT KEY		X		
GET CHALLENGE	X			
AC EXTERNAL AUTHENTICATE			X	
SET STATUS		X		
UPDATE PROPERTIES		X		
RESET RETRY COUNTER		X	X	

REGISTER APPLET		X		
REGISTER ACR		X		

Table 2. Roles & possible ACR configurations for AC applet services

6.1.3.4.3 Roles vs. Services: PKI/GC Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Card Holder / PIN	Application Operator / XAUT	Application Operator or ASC XAUT or SECURE CHANNEL
PKI/GC Applet					
INSTALL		X			
GET PROPERTIES	X				
INITIALIZE UPDATE	X				
EXTERNAL AUTHENTICATE		X			
UPDATE CERTIFICATE / STATIC BUFFER		X	X	X	X
READ CERTIFICATE / STATIC BUFFER	X	X	X	X	X
GET CHALLENGE	X				
GENERATE KEY PAIR		X	X		
PRIVATE SIGN / DECRYPT			X		
GET CERTIFICATE	X				
PUT KEY		X			
AC EXTERNAL AUTHENTICATE				X	X
VERIFY CHV	X				
SET STATUS		X			
SET PROPERTIES		X			

Table 3. Roles & possible ACR configuration for PKI/GC applet services

6.1.3.5 Module Cryptographic Functions

The purpose of the ActivCard 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 ActivCard Applet v2 to provide cryptographic services. These include:

- TDES, (2 keys EDE TDES)
- SHA-1,
- RSA PKCS #1 (512, 768, 1024 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). DES, TDES, TDES MAC, RSA and SHA-1 algorithms are provided as services through Java APIs to applets that may be loaded onto the cryptographic module.

6.1.4 Critical Security Parameters:

- **Initialization key K_{init}**: used to secure the card during its transportation from the manufacturer site to the issuance site. This is a TDES key and is replaced with the card manager OP key set as the first step of issuance.
- **Crypto Officer Card Manager / Security Domain key set (OP key set):**
  - K_{enc}: used to derive session keys for the encrypted mode of the secure channel

- K_{mac}: used to derive session keys for crypto officer authentication and MAC mode of the secure channel. This key is used to authenticate the Crypto Officer (CSC and ASC roles) to the card
- K_{kek}: used to encrypt keys to be loaded onto the cryptographic module

- **External Authentication Keys (XAUT keys)**: The Application XAUT TDES keys that enable the authentication of Application Operator role and the Unblock PIN XAUT TDES key to authenticate the ASC role for the Reset Retry Counter APDU.
- **RSA private keys**: managed (generated, unwrapped) from the PKI/GC applet using the Java card cryptographic services. These keys are used to sign data.
- **Personal Identification Number (PIN):** PIN and PIN attributes are managed from the ACA, which relies on Java Card PIN management service.
- **Authentication Method (or ACR)**: These data elements define the Authentication Method that is permanently set for the service. Several services offer a configurable Authentication Method. For such services, the authentication method should be set according to the tables in section 6.1.3.4.

6.2 ACCESS TO CSPS VS SERVICES

The following matrix identifies how different services access CSPs for each applet.

6.2.1 Card Manager applet

Card Manager applet Columns: Services(roles) Rows: Access to CSPs	**Card Holder**	**Application Operator**	**Cryptographic Officer**	I INSTALL	LOAD	DELETE	PUT KEY	SET STATUS	INITIALIZE UPDATE:	EXTERNAL AUTHENTICATE	PUT DATA	GET STATUS	PIN CHANGE/UNBLOCK
OP key set													
Enter/Delete Key			X				X						
Verify Cryptogram			X		X		X			X			
Decrypt APDU Payload			X		X		X						X

6.2.2 AC Applet

AC applet Columns: Services(roles) Rows: Access to CSPs	**Card Holder**	**Application Operator**	**Cryptographic Officer**	INSTALL/INSTANTIATE(CSC)	CHANGE REFERENCE DATA	GET PROPERTIES (NO ROLE)	GET ACR (NO ROLE)	INITIALIZE UPDATE (NO ROLE)	EXTERNAL AUTHENTICATE(ASC)	VERIFY CHV (C.H)	PUT KEY (ASC)	GET CHALLENGE (NO ROLE)	AC EXTERNAL AUTHENTICATE (ASC)	SET STATUS (CSC)	UPDATE PROPERTIES (ASC)	RESET RETRY COUNTER (ASC)	REGISTER APPLET (ASC)	REGISTER ACR (ASC)
ACR																		
Install			X	X														
Register ACR			X															X
PIN																		
Reset Retry Counter			X													X		
Change Reference Data	X				X													
Verify CHV	X									X								
XAUT Key																		
Enter/Delete Key			X								X							
Verify Cryptogram		X											X					
OP key set																		
Enter/Delete Key																		
Verify Cryptogram			X						X		X					X		
Decrypt APDU Payload			X								X					X		

6.2.3 PKI/GC Applet

PKI/GC applet services Columns: Services (roles) Rows: Access to CSPs	***Card Holder***	***Application Operator***	***Cryptographic Officer***	INSTALL/INSTATIATE (CSC)	GET PROPERTIES (any)	INITIALIZE UPDATE(any)	EXTERNAL AUTHENTICATE(ASC)	UPDATE CERT / STATIC BUFFER (A. O)	READ CERT / STATIC BUFFER (A.O)	GET CHALLENGE (No Role)	AC EXTERNAL AUTHENTICATE (A.O)	GENERATE KEY (ASCor CH)	GET CERTIFICATE (any)	PRIVATE SIGN / DECRYPT (C.H)	SET STATUS (ASC)	SET PROPERTIES (ASC)	VERIFY CHV (C.H)	PUT KEY (ASC)
PIN																		
Verify CHV	X																X	
RSA Private Key																		
Generate Key	X		X									X						
Enter CRT Components			X															X
Delete Private Key			X															X
Sign Data	X													X				
OP key set																		
Verify Cryptogram			X			X												
Decrypt Data			X			X												X

7. SECURITY RULES

7.1.1 Approved mode of Operation

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

- module service access control rules must be configured per tables 1, 2, and 3 in section 6.1.3.
- follow all security rules outlined in section 7.1.2 and 7.1.4.

7.1.2 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.

- The module shall provide the following distinct operator roles: The Card Holder role, Application Operator role, Applet Security Controller role and Card Security Controller role.
- Applets shall provide role-based authentication:
  - The Card Holder is authenticated by the knowledge of a unique PIN.
  - The Crypto Officer (CSC and ASC roles) is authenticated via OP secure channel mutual authentication protocol using the card manager/security domain key set that composed of 3 TDES double length keys. Two keys are used to authenticate and MAC the command payload. A third key is used to encrypt keys transported within the APDU command (Initialize Update & External Authenticate commands). The ASC is also authenticated via AC external authenticate protocol using the Unblock PIN XAUT TDES key.
  - The Application Operator role is authenticated via AC external authenticate protocol using the application XAUT TDES key.

- Cryptographic services are restricted to authenticated roles.
- The role authentication methods (ACRs) for each applet service are set by the Crypto Officer during applet instantiation and can only be modified by the Crypto Officer.
- When authentication of the role cannot be performed because the related key or PIN 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.
- 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.

7.1.3 Applet Life Cycle Security Rules

The ActivCard Applet v2 only permits loading of FIPS approved applets. Applets can only be loaded through an OP 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 insure that the terminal and/or Card Acceptance Device are controlled by a valid role; Card Holder, Application Operator or Cryptographic Officer / crypto-officer.
- Management of applet life cycles (load, install, delete, personalize keys), shall follow the Open Platform standard [VOP].
- 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.

7.1.4 Access Control Security Rules

- Keys must be loaded through an OP 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 other parties than the Card Holder.
  - The ACA must be configured by the Card Security Controller so that:
    - After 1 <= N <= 10 consecutive unsuccessful PIN code validation attempts, the Card Holder services must be disabled. (eg. The PIN is blocked)
    - The PIN length L verifies the following rules:
      - 6 <= L <= 255 for PIN composed with random numeric (0-9) or alpha-numeric (0-9, a - z, A – Z) characters

7.1.5 Key Management Security Policy

7.1.5.1 Cryptographic key generation

-TDES Session key generation (S_{MAC} and S_{ENC}) as per **Open Platform (OP) specification** [4] using FIPS140-2 approved ANSI X9.31 PRNG to generate random data required for Secure Channel Opening.

- RSA key pair generation using FIPS140-2 approved ANSI X9.31 PRNG.

7.1.5.2 Cryptographic key entry

Keys shall always be input in encrypted format, using the Put Key command within an OP secure channel. During this process, the keys are double encrypted (using the Session Key and the K_{kek} Key).

7.1.5.3 Cryptographic key storage

The Keys are structured to contain the following parameters:

- Key id, which is the Id of the key,
- Algo Id, which determines which algorithm to be used,
- Integrity Mechanisms.

7.1.5.4 *Cryptographic key zeroization*

The cryptographic module zeroizes cryptographic keys by reloading a zero-valued key set for Crypto Officer OP secure channel key set, or Application Operator XAUT key, or closing of secure channel for session keys**.** The cardholder PIN is zeorized by setting it to zero value. The RSA private key is zeorized by reloading a zero-valued key.

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

7.1.6 Mitigation of attacks Security Policy

This section does not apply.

8. SECURITY POLICY CHECK LIST TABLES

8.1 ROLES & REQUIRED AUTHENTICATION

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

8.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	> 1:1,000,000
PIN	> 1:1,000,000

8.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Security Controller	The Card Security Controller role services are listed in Section 6.1.3.1.1
Applet Security Controller	The Applet Security Controller role services are listed in Section 6.1.3.1.2
Application Operator	The Application Operator role services are listed in Section 6.1.3.2.2
Card Holder	The Card Holder role services are listed in Section 6.1.3.2.3

8.4 ACCESS RIGHTS WITHIN SERVICES

Service	CSP	Types of Access (i.e. Read, Write, Execute)
Crypto Officer (CSC/ASC) Service	OP secure channel TDES key set of three keys or Unblock PIN XAUT TDES key	Execute (encrypt, decrypt), write (put key)
Application Operator Service	Application XAUT TDES key	Execute (encrypt, decrypt)
Card Holder Service	PIN	Execute (Verify CHV), write (Change Reference Data)

9. EMI/EMC

The GemXpresso Pro R3 E64 PK – FIPS cryptographic module has been tested to meet the EMI/EMC requirements specified in FCC Part 15 Subpart J, Class B.

10. SELF TESTS

The **GemXpresso Pro R3 E64 PK – FIPS** 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 DES, 3DES, SHA-1, RSA)	At Power-Up
Pseudo Random Number Generator test. (Known-Answer Test for P-RNG output)	At Power-Up
Pair-wise consistency test.	Conditional
Software load test.	Conditional
Continuous random number generator test.	Conditional

Table 6 - Self-tests list

10.1 SELF-TEST EXECUTION

After **GemXpresso Pro R3 E64 PK – FIPS** is powered up and before executing any APDU commands, the module enters the self-test state and performs all of the cryptographic algorithm and software integrity self-tests as specified in FIPS 140-2 standard **[1]**. These tests are conducted automatically as part of the normal functions of the cryptographic module. They do not require any additional operator intervention, nor applet specific functions.

Power-up self-tests are executed 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.

11. References

[1] FIPS PUB 140-2 – Federal Information Processing Standard Publication – Security requirements for cryptographic modules – 2001, May the 25th.

[2] Derived Tests Requirements for FIPS PUB 140-2 - Federal Information Processing Standard Publication – Security requirements for cryptographic modules – 2001, November the 15th.

[3] NIST Web site, http://www.nist.gov

[4] Open Platform (OP) Card Specification – Release 2.0.1'

[5] Visa Open Platform (VOP) Implementation Specification– Release 2.0.1'

[6] Java Card API Specification - (SUN) – Release 2.1.1

[7] Java Card Runtime Environment (JCRE) Specification (SUN) – 2.1.1

[8] Java Card Virtual Machine (VM) Specification – SUN – Release 2.1.1

[9] RSA PKCS#1: RSA Cryptographic Standard (RSA Laboratories) – 2.1

[10] ISO 7816 parts 1-6 (ISO / IEC)

[JVM] Java Card ™ 2.1 Virtual Machine Specification v1.1 - june 1999, Sun Microsystems

[JCAPI] Java Card ™ 2.1 Application Programming Interface, Sun Microsystems

[JCDG] Java Card ™applet developer's guide

[JCRE] Java Card ™ 2.1 Runtime Environment (JCRE) Specification, Sun Microsystems

[VOPS] Global Platform - Open Platform Card Specification, v2.0.1' – April 2000

[VOPI] Visa Open Platform Card Implementation Specification - march 1999, Visa International

[X9.31] American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998.

[FIPS140-2] National Institute of Standards and Technology, FIPS 140-2 standard.

[FIPS140-2A] National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions.

[FIPS140-2B] National Institute of Standards and Technology, FIPS 140-2 Annex B: Approved Protection Profiles,

[FIPS140-2C] National Institute of Standards and Technology, FIPS 140-2 Annex C: Approved Random Number Generators

[FIPS140-2D] National Institute of Standards and Technology, FIPS 140-2 Annex D: Approved Key Establishment Techniques

[DES] National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publication 46-3, October 25, 1999.

[DES Modes] National Institute of Standards and Technology, DES Modes of Operation, Federal Information Processing Standards Publication 81, December 2, 1980.

[DSS] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000.

12. ACRONYMS

Acronyms	Definitions
ACR	Access Control Rule
AO	Application Operator
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASC	Applet Security Controller
ATR	Answer To Reset
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CH	Card Holder
CSP	Critical Security Parameter
CSC	Card Security Controller
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
GC	Generic Container
GSC-IS	Government Smart Card Interoperability Standard
JCRE	Java Card ™ Runtime Environment
PKI	Public Key Infrastructure
MAC	Message Authentication Code
OP	Open Platform
PIN	Personal Identification Number
RAM	Random Access Memory
ROM	Read only Memory
SD	Security Domain
SC	Secure Channel
TDES	Triple DES (112-bit length keys)
XAUT	External Authentication

- END OF DOCUMENT -