Gemplus Corp.

GemXpresso Pro R3 E64 PK - FIPS

FIPS 140-2 Level 3

Security Policy

Version 1.5

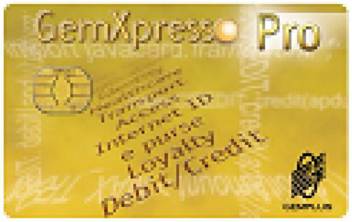

Table OF CONTENTS

Table of figures:

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 (OP) – Release 2.0.1'

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

1 Scope

This Security Policy specifies the security rules under which the Gemplus Smart Card, herein identified as the **"Gemχpresso Pro R3 E64 PK - FIPS"** platform, must operate. . 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. Some of these rules are derived from the security requirements of **FIPS140-2' standard [1]**, others are derived from the Gemplus' experience in embedded security software.

These rules define the interrelationship between the:

- Module users and administrators,
- Module services and
- Security Relevant Data Items (SRDIs).

2 Introduction

2.1 Gemplus Smart Card Overview

Gemplus aims to provide **FIPS140-2 Level 3** cryptographic smart cards. The cards are based on a Gemplus Open OS Platform on which FIPS 140-2 LEVEL 3 validated platform-independent applets may be loaded and instantiated at post issuance. As a basis the card provides cryptographic services such as secure channel, authentication, encryption/decryption and digital signature. It is under the charge of the applets to be loaded and instantiated within the card to use in conformance with specifications the different services offered by the platform. Moreover, FIPS 140-2 LEVEL 3 validation is required for the applets to be loaded and instantiated within the card in order to reach the FIPS 140-2 LEVEL 3 compliance for the **whole and composite product (i.e. platform plus post issued applets).** The present document is only dedicated and focused to the Gemplus GemXpresso Pro R3 E64 PK platform.

This security policy specifies the security rules under which our Java Card **Gemχpresso Pro R3 E64 PK - FIPS** platform operates.

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, from the latest developments in cryptographic resistance against known attacks, and provides FIPS approved cryptographic algorithms and self-tests. Additional software countermeasures have also been added by Gemplus.

This cryptographic module also uses a state of the art manufacturing flow in terms of security and provides applets with memory, cryptographic and I/O services.
The cryptographic module ensures on-card applets safe coexistence thanks to its secure Virtual Machine (VM) and firewall. The Java VM is fully compliant with the **Java Card standards[8]**.

The card life cycle is managed according to the **Open Platform (OP) specification [4]**. Issued cards have been loaded with cryptographic keys, 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 Security Level

The cryptographic module meets the overall requirements applicable to **FIPS140-2 Level 3**. The individual security requirements meet the level specifications as follows.

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 1 - FIPS 140-2 Security Levels

3 Cryptographic Module Specification

3.1 Gemplus Crypto-Module Cryptographic Boundary

The Cryptographic Boundary is defined to be the 'module edge' of the **Gemχpresso Pro R3 E64 PK - FIPS**, 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. **Gemχpresso 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.

During the Gemplus manufacturing process, the chip (ICC) is wire-bonded on the inner side of a contact plate, then globe-topped with resin. The resulting Micro-Module meets the physical security requirements of FIPS140-2 Level 3.
EEPROM-APPLETS area is free since FIPS 140-2 LEVEL 3 validated applets are intended to loaded and issued at post issuance.

All components of the **Gemχpresso Pro R3 E64 PK – FIPS Micro-Module** are included in the cryptographic module boundary, as shown in the following figure:

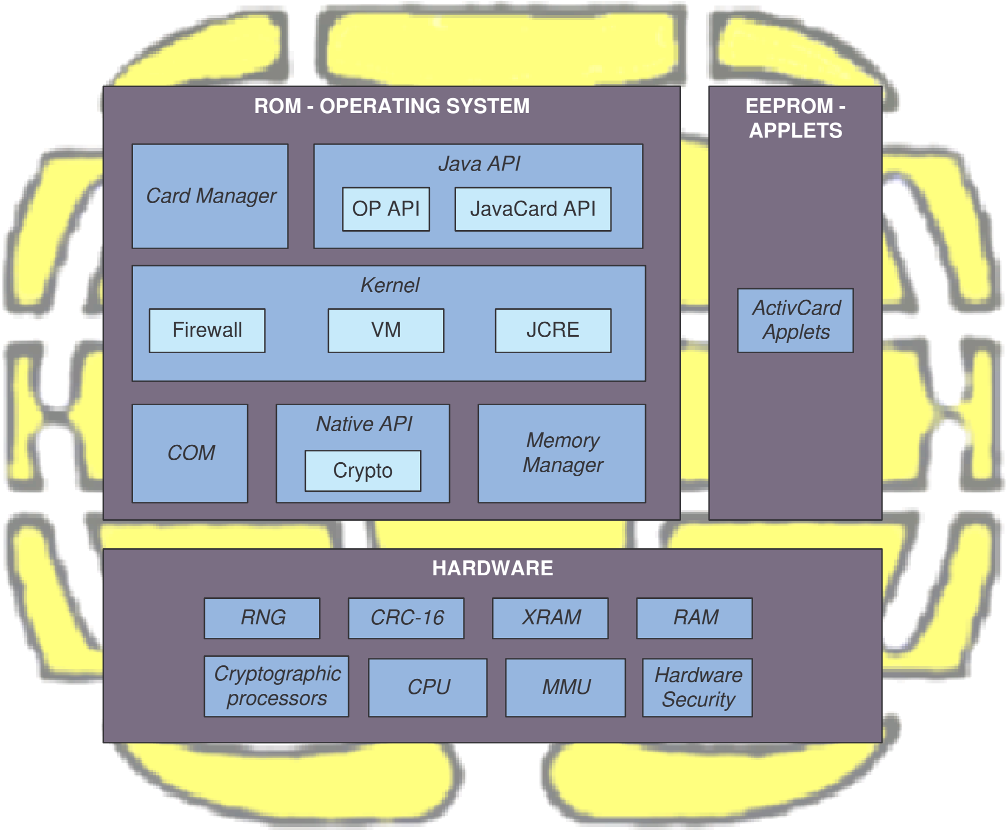

Figure 1- Cryptographic Module Boundary

The following sections provide a description of the different entities presented in this scheme

3.2 ROM – Operating System

The chip's ROM includes the **Gemχpresso Pro R3 E64 PK – FIPS** Operating System (OS) meaning that it is protected against disclosure and modification. 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. This OS includes the following design entities:

Design item	Functionality
Card manager	
The card manager applet is in charge of secure applet loading, Global PIN and card life cycle management according to the **OP specification [4] and VOP specification [5]**: ○ At post issuance, applets are downloaded according to the **OP specification [4]**. The use of a secure channel with the Card Manager is required. During applet loading, the applet code integrity is verified and its origin (**Card Manager Security Officer**) is authenticated. The applet code is rejected in case of authentication and/or verification failure. This prohibits unauthorized downloading. ○ The Card Manager controls the card life cycle state. Cards are issued in the "OP_SECURED" state and contain a set of cryptographic keys, and a PIN. The card life cycle implementation is fully compliant with the **VOP specification [5]**. ○ The Card Manager controls the sensitive operations defined in the **'Roles, Services and Authentication'** section, requiring the opening of a secure communication channel based on the knowledge of a secret. The related secure messaging protocol follows the **VOP specification [5]**.	
Java API	
OP API	The OP API provides entry points according to the **OP specification [4].**
Java Card API	The Java Card API provides services according to the **Java Card specification [6]**.
Kernel	
Firewall	The Firewall is a security mechanism that permits several applets to coexist safely in the Cryptographic Module memory. The Firewall protects the applets from illegal access to their objects and methods, in accordance with the **JCRE specification [7].** The firewall also protects the Card Manager Java objects from illegal access (Global PIN, Key set).
VM	The Java Virtual Machine is the mechanism responsible for Java applets execution according to the Java Card VM specification. The virtual machine interprets the applet byte code. Its implementation is fully compliant with the **Java Card [8]** standard.
JCRE	The Java Card Runtime Environment manages the environment variables and associated tasks that intervene during byte code execution. Its implementation is fully compliant with the **JCRE specification [7].**
COM	
The COM is in charge of managing the **ISO 7816 [10] communication protocols**.	
Native API	
The native API provides internal services built on top of the chip hardware services.	
Crypto	The Crypto entity groups together all the native API
Memory Manager	
The Memory Manager Unit (MMU) is in charge of the secure system memory addressing.	

Table 2 - ROM - Operating System content description

3.3 EEPROM – Applets

The chip's EEPROM can store post issued applets. **These applets are outside the scope of this Security Policy. However, in order for the whole and composite product made up of the GemXpresso Pro E64 PK and the post issued applets to reach the FIPS 140-2 Level 3, those applets shall be validated and tested on the GemXpresso Pro E64 PK platform, against FIPS 140-2 Level 3 requirements. Then post-issuance loading and instantiating processes can be performed in a**

secure mode by an authorized entity. If a non-validated applet is loaded on the card, the FIPS 140-2 certification of the card no longer holds.

3.4 Hardware Chip

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.

3.5 FIPS Approved Security Functions

The following table gives the list of FIPS approved security functions that are provided by the **Gemχpresso Pro R3 E64 PK – FIPS** JavaCard 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 (2key)	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#1with SHA-1 hashing	Yes
	Verification following PKCS#1with SHA-1 hashing	Yes
P-RNG	Pseudo Random Number Generation	Yes
DES MAC	ECB and CBC modes	Yes
3DES MAC	ECB and CBC modes	Yes

Notes:

- The CBC mode is used to establish a trusted path between **Gemχpresso Pro R3 E64 PK – FIPS** and an external entity (MAC computation). Loading post issuance applets, regarding **OP specification [4]**, requires 3DES in CBC mode.
- The RSA key generation is an X9.31 standard derived Gemplus proprietary solution (refer to section **8.3**).
- 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 3 – FIPS Approved Security Functions

The module is always in an Approved mode of operation as it only supports FIPS Approved algorithms. The FIPS mode indicator is considered the ATR returned by the card.

[1] DES should only be used in legacy systems

4 Cryptographic Module Ports and Interfaces

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

4.1 Physical Port

4.1.1 PIN assignments and contact dimensions:

Gemχpresso 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 4- Contact plate pin list

4.1.2 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 5 - Voltage and frequency ranges

4.2 Logical Interface

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

4.2.1 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, 3and 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/OUT” command	Input data, response data

Table 6 - Accepted ISO APDU types

The cryptographic module enforces the establishment and use of a secure path for exchanging sensitive data with an external device, according to its roles and services security policy.

4.2.2 API interface

Gemχpresso 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.

5 Roles, Services and Authentication

This section specifies the roles, security rules, services, and Security Relevant Data Items (SRDI) of the cryptographic module. The Identification and Authentication Policy, and Access Control Policy define the interrelationship between roles, identities, through the services and security rules.

The services that are provided by the cryptographic module are listed in the subsection labeled "SERVICES" in the Access Control Policy description.

5.1 Identification and Authentication Policy

5.1.1 Introduction

This section is dedicated to our identity-based authentication policy, and the related security rules of the mechanism interfaces and SRDI.

5.1.2 Identity based authentication policy

The module supports a single identity: the Card Manager Security Officer. The Card Manager Security Officer identifies himself by selecting the Card Manager applet and issuing the Init Update APDU with the keyset version used to authenticate to the card by establishing a Secure Channel.

The module supports two roles: The Crypto-Officer and User roles that are the followings:

- Crypto-Officer role:
  - **Cryptographic Officer** has to be considered as the smart card administrator and knows a secret (i.e. 3DES key) in order to communicate, via a secure channel, with the card manager.
- User role:
  - **User** has to be considered as an entity that has possession of the Security Domain keyset and can request the services provided by the Security Domain on the card.

The Card Manager Security Officer has authority to assume both roles. Each role is assumed implicitly as the module does not provide for explicit role selection. The services provided by the module to each role is specified in the table below. The Card Manager Security Officer can authenticate to both roles using the same TDES keyset.

Roles/Services	Crypto Officer role Authenticated	User role Authenticated	User role Unauthenticated
INSTALL	x	x	
LOAD	x	x	
DELETE	x	x	
EXTERNAL AUTHENTICATE	x	x	x
GET DATA	x	x	x
GET STATUS	x	x	
INITIALIZE UPDATE	x	x	x
PUT DATA	x	x	
PUT KEY	x	x	

SELECT	x	x	x
SET STATUS	x	x	
PIN CHANGE/UNBLOCK	x	x	

Table 7- Card Manager services Vs Roles

A user can initiate module self-tests by issuing a card reset and issuing an APDU command. A user can retrieve the module ATR on card power-up

Please note that the module provides functionality to change/unblock Global PIN. However, the Gemplus card does not use the Global PIN to provide authentication to its users. Any applets loaded on the card may use this PIN for authenticating Card Holders.

5.1.3 Mechanism interfaces

The following table describes the mechanisms for identity authentication:

Interface	Description
OPSystem.verifyPin *Java method*	This is an internal OP API method is used by an applet to present a PIN to the module that will be compared with the global PIN.
INITIALIZE UPDATE *APDU*	This APDU command initiates the setting up of a secure channel. The card generates the session keys and exchanges data with the host.
EXTERNAL AUTHENTICATE *APDU*	This APDU command is used by the card to authenticate the host and to determine the level of security required for all subsequent commands. A previous and successful execution of the INITIALIZE UPDATE command is necessary prior to processing this command.

Table 8 - Mechanism interfaces

5.1.4 Security rules

The following table presents the security rules applied to these mechanisms:

Rule Identifier	Description
IA_PIN_RULE.1	It is not possible to get authenticated through the global PIN authentication mechanism if the authorized number of attempts is reached.
IA_PIN_RULE.2	It is not possible to get authenticated through the global PIN authentication mechanism if the global PIN is corrupted.
IA_CO_RULE.1	The **Card Manager Security Officer** cannot get authenticated if the authorized number of attempts is reached.
IA_CO_RULE.2	The **Card Manager Security Officer** must be re-authenticated if the card is reset.
IA_CO_RULE.3	The **Card Manager Security Officer** must be re-authenticated if the cryptographic module detects APDU communication corruption.

Table 9 - Security rules

5.1.5 Mechanism strengths

The strength of the mechanisms exceeds the FIPS 140-2 expectation and is the following:

Identification Mechanism	Strength of Mechanism
OP mutual authentication	$\left(\frac{1}{\left(2^{4}\right)^{8}}\right)$
The cryptogram (authentication data) sent is 8 bytes long	
Global PIN check	$\left(\frac{retrycounter}{10^{4}11^{8}}\right)$
Retry counter is the maximum retry counter and is initially set to 10	

Table 10 - Mechanism strengths

5.2 Access Control Policy

5.2.1 Introduction

This chapter is dedicated to access control security rules. Some services provided by the cryptographic module are subject to privileges. Privileges can be obtained by construction (for example at applet initialization) or by being identified as a privileged user.

- The **Global PIN** can only be managed by privileged applets. The privilege is associated to the applet at applet installation.
- The **administrative commands** are restricted: these APDU commands can be used only in a secure channel (**session**). A secure channel is open when the card user has been authenticated through the OP mechanism as being the owner of the **Card Manager Security Officer** keyset. The secure channel is closed if the card is reset or if the system closes it.
- The Java objects created by the applets are protected by the **Firewall** mechanism of the JCRE. The rules that are applied to **Java object accesses** are specified in the **JCRE specification [7]**. The firewall is a means of protecting applet information.
- **The loaded applets life cycle state** (Card Manager applet included) can be managed by the **Card Manager Security Officer**. Proposed transitions must be coherent with the **OP specification**. An applet can manage its own life cycle state under the same conditions. An additional condition is imposed to applets that attempt to change the Card Manager life cycle state: they must have the privilege for **Card life cycle management**.

5.2.2 Services

The rules are applied to all the following service interfaces. (The service interfaces have been grouped according to the role to which they provide a service.)

Interface	Service Description
DELETE – *APDU*	One or more DELETE commands are used to delete an instance of an applet and optionally the package containing one or more applets.
EXTERNAL AUTHENTICATE – *APDU*	This APDU command is used by the card to authenticate the host and to determine the level of security required for all subsequent commands. A previous and successful execution of the INITIALIZE UPDATE command is necessary prior to processing this command.
GET STATUS – *APDU*	This APDU command is used to retrieve the Card Manager, load file (package), and application life cycle data specific to the OP specification.
INITIALIZE UPDATE – *APDU*	

This APDU command initiates the setting up of a secure channel. The card generates the session keys and exchanges data with the host.
INSTALL – *APDU* This APDU command informs the card of the various steps required to load, install and make an applet selectable within the card.
LOAD – *APDU* One or more LOAD commands are used to load the bytecode of the load file (package) defined in the previously issued INSTALL command to the card.
PIN CHANGE/UNBLOCK – *APDU* 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.
PUT DATA – *APDU* This APDU command is used to set the value of the various data elements utilized and managed by the Card Manager.
PUT KEY – *APDU* This APDU is used to: 1. Replace a single or multiple keys within an existing key set version; 2. Replace an existing key set version with a new key version; 3. Add a new key set version containing a single or multiple keys Key value is encrypted.
SET STATUS – *APDU* This APDU command is used to change the state of the Card Manager or to change the life cycle state of an application.

Table 11 - Card Manager Security Officer accorded interfaces and services

5.2.3 Security rules

The following table presents the security rules applied to these mechanisms:

Rule Identifier	Description
AC_PIN_RULE.1	The **Card Manager Security Officer** is responsible for Global PIN update.
AC_PIN_RULE.2	The **Card Manager Security Officer** is responsible for Global PIN unblock and resets.
AC_CO_RULE.1	Administrative commands can only be used by the **Card Manager Security Officer.**
AC_JAVA_RULE.1	**JCRE firewall** checks are enforced by the cryptographic module to ensure Java object protection.
AC_LIFE_RULE.1	The **Card Manager Security Officer** is responsible for locking and terminating the Card Manager life cycle state.
AC_LIFE_RULE.2	An **applet** is responsible for managing its own life cycle state, in accordance with the OP specification.
AC_LIFE_RULE.3	The **Card Manager Security Officer** is responsible for managing the life cycle state of any applet (including system applets), in accordance with the OP specification.

Table 12 - Security rules

5.3 Additional Gemplus Security Rules

The following rules apply in addition to the FIPS140-2 requirements. The cryptographic module:

Rule Identifier	Description
AD_RULE.1	Does not input/output plain-text private/secret keys or other critical security parameters.
AD_RULE.2	Does not support a multiple concurrent operators.
AD_RULE.3	Does not support a bypass mode.
AD_RULE.4	Does not provide a maintenance role/interface.
AD_RULE.5	Requires re-authentication when changing roles.
AD_RULE.6	Does not allow the loading of Software/Firmware - only FIPS 140-2 LEVEL 3 validated applets have to be loaded and instantiated at post issuance.

Table 13 - Gemplus additional security rules

5.4 Security Relevant Data Item

The Security Relevant Data Items (SRDIs) of the cryptographic module are the following:

- **OP key set of the Card Manager (a set of three TDES keys)**
- **Secure Channel session keys (TDES 128-bit keys)**
- **Global PIN**

The following table proposes an association between the services or authentication mechanisms (the interface name is provided) and the SRDI they access. The access types are labeled as follows:

-
- W: write access
- U: the value is not explicitly read, but used within the scope of a comparison or computation process

Interface	SRDI	Access type
INITIALIZE UPDATE	OP key set of the Card Manager	U
EXTERNAL AUTHENTICATE	OP key set of the Card Manager Secure Channel session keys	U U
PIN CHANGE/UNBLOCK	Global PIN Secure Channel session keys	W U
PUT KEY	OP key set of the Card Manager Secure Channel session keys	W U
INSTALL	Secure Channel session keys	U
LOAD	Secure Channel session keys	U
DELETE	Secure Channel session keys	U
SET STATUS	Secure Channel session keys	U
GET STATUS	Secure Channel session keys	U
PUT DATA	Secure Channel session keys	U

Table 14 - Security Relevant Data Items

6 Physical Security

The **Gemχpresso Pro R3 E64 PK – FIPS** single chip module is designed to meet the **FIPS140-2 level 3 Physical Security requirements**.

6.1 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 opaque black epoxy coating polymerized with temperature.
Any mechanical attack attempting to extract the chip from the micro-module results in damaging the chip so that it cannot work anymore. Furthermore, attempts to attack the chip or micro-module will results in signs of tampering such as scratches and deformation.
The module is designed for embedding in a plastic card body for Smart Card manufacturing.

6.2 Hardware Security Mechanisms

The embedded **SLE66CX640P chip from Infineon** provides the cryptographic module with hardware security mechanisms 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 resetting the cryptographic module. Any unprotected sensitive data are lost. These mechanisms are not tested as part of FIPS 140-2 testing.

7 Operational Environment

This section does not apply to **Gemχpresso Pro R3 E64 PK – FIPS**. No code modifying the behavior of the cryptographic module operating system can be added after its manufacturing process.

Only authorized FIPS 140-2 LEVEL 3 validated applets shall be downloaded at post-issuance. Their execution is controlled by the cryptographic module operating system following its security policy rules.

8 Cryptographic Key Management

8.1 Card Manager Key Set

The cryptographic module implements **OP [4]** and **VOP [5]** 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 Card Manager applet and the **Card Manager Security 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**. (NO_SECURITY mode is not available). 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 CBC 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:

Index 1. The **encryption/authentication key** is used to generate an encryption session key for both mutual authentication and APDU command data encryption.
Index 2. The **MAC key** is used to generate a MAC session key for APDU commands (command header and command data) MAC generation.
Index 3. The **Key Encryption Key** is used to encrypt key data.

The session keys are stored in RAM and zeroized upon card reset and termination of the Secure Channel.

8.2 Application Key Sets

FIPS 140-2 LEVEL 3 validated applets may use keys of different types through the cryptographic services of the JavaCard API. These include DES keys, RSA public and private keys, and RSA Chinese Remainder public and private keys.

Application security domains and applet key management are out of the scope of this security policy.

8.3 Key Generation

The cryptographic module on-board key generation is able to generate RSA key and RSA Chinese Remainder Keys. Strong prime numbers are generated following a Gemplus proprietary algorithm derived from the X9.31 standard.

8.4 Key Entry

The Card Manager applet enforces entering cryptographic 3DES keys securely within a secure channel. The Card Manager Security Officer must authenticate before entering keys into the module.

The Card Manager Security Officer sends the PUT KEY APDU command to:

- Replace multiple keys within an existing key set version.
- Replace an existing key set version with a new key set version.
- Add a new key set version containing multiple key(s).

The Card Manager key set is already present within the cryptographic module is the default key set. If this key set version is replaced, the replacement becomes the default.

8.4.1 Key Input

While the key set structure can be presented to the card in encrypted form or in plaintext, **the keys values are always encrypted with the Key Encrypting Key** (key index 3 of the key set version used to set up the current Secure Channel).

The key set structure includes a check value for each key. Verifying these check values ensures the validity of the keys.

8.4.2 Key Output

The module does not provide key output.

8.5 Key Storage

Keys are protected against unauthorized disclosure, unauthorized modification, and unauthorized substitution.

Secret and private keys are Java objects. As a consequence, they are protected by the firewall from illegal access. **An applet that owns a key is responsible for not sharing it.**

8.6 Key Zeroization

The cryptographic module provides applets with the capability to set all plaintext cryptographic keys and other unprotected critical security parameters within the module to zero. This also can be done by setting the Card Manager state to OP_Terminated.

9 EMI/EMC

The **Gemχpresso 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 **Gemχpresso Pro R3 E64 PK – FIPS** performs the following self-tests to ensure that the module works properly.

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
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 15 - Self-tests list

10.1 Self-Test Execution

After **Gemχpresso 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.

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.

All data output via the output interface are inhibited while any power-up and conditional self-tests are performed.

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 operating tests.

10.2 Self-Test Failure

No cryptographic operations can be processed and no data can be output via the data output interface, while in the error state.

If an error occurs during the SW load self-test, an error code is returned via the status interface and the loading secure channel is closed.

If an error occurs during the other self-tests, the card becomes mute. For security reasons, no explicit information is returned, no data is available, and no command is processed. Only a card reset is possible.

An error while loading an applet closes the secure channel with the Card Manager. It must be re-opened, to retry applet loading and the **Card Manager Security Officer** has to be re-authenticated.

11 Acronyms

Acronyms	Definitions
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
JCRE	Java Card ™ Runtime Environment
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