SETECS

Secure Transactions and Electronic Commerce Systems

Tel: (301) 587-3000 **Fax:** (301) 587-7877 **E-mail:** info@setecs.com **Web:** www.setecs.com

SETECS OneCARD™ PIV–II Java Card Applet

on Gemalto GemCombi'Xpresso R4 E72K PK card

(Applet Version 1.2)

FIPS 140-2 Security Policy

August 16, 2006

Document Revision v1.0

TABLE OF CONTENTS

1 References

[1] FIPS PUB 140-2 – Federal Information Processing Standard Publication – Security requirements for cryptographic modules – 2001, May the 25th, with change notice (12-03-2002).

[2] Derived Tests Requirements for FIPS PUB 140-2 - Federal Information Processing Standard Publication – Security requirements for cryptographic modules – 2004, March the 24th.

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

[4] Global Platform – Release 2.1.1

[5] Visa Global Platform – Release 2.1.1

[6] Java Card API Specification – (SUN) – Release 2.2.1

[7] Java Card Runtime Environment (JCRE) Specification (SUN) – 2.2.1

[8] Java Card Virtual Machine (VM) Specification – SUN – Release 2.2.1

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

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

[11] ISO X9.31

[12] ISO 14443 RF Interface (ISO / IEC)

[13] NIST Special Publication 800-73-1,
Interfaces for Personal Identity Verification - Information Security – March 2006

[14] FIPS PUB 201 - Federal Information Processing Standards Publication
Personal Identity Verification of Federal Employees and Contractors - February 25, 2005

2 Scope

This Security Policy specifies the security rules under which the SETECS Inc. OneCARD^{TM} PIV-II Java Card Applet (Version 1.2) on Gemalto GemCombi'Xpresso R4 E72K PK card, herein identified as the **"SETECS OneCARD^{TM} PIV-II – FIPS"** product, operates. Some of these rules are derived from the security requirements of **FIPS140-2' standard [1]**, others are derived from the features and properties of the Gemalto' smart card and most are based on SETECS's expertise and experience in developing smart cards security applets.

These rules define the interrelationships between the:

- Module users and administrators, enforced as PIV roles
- Module services, provided as FIPS 201 and other APDUs
- Security Relevant Data Items (SRDIs), represented by FIPS 201 compliant data objects.

The commercial name of the product is:

SETECS Inc. OneCARD™ PIV-II Java Card Applet on Gemalto GemCombi'Xpresso R4 E72K PK card

Where:

- Gemalto GemCombi'Xpresso R4 E72K PK card is a Java platform with Card Manager applet. This Java Card platform may also be referred as "GCX4" in this document.
- SETECS Inc. OneCARD^{TM} PIV-II Java Card Applet is an applet loaded on the Java Card platform. This applet may also be referred as "PIV applet" or "PIV-II Applet" in this document.

3 Introduction

3.1 Gemalto Smart Card Overview

Gemalto GemCombi'Xpresso R4 E72K PK card is **FIPS140-2 Level 2** Approved cryptographic smart card. Together, the card and PIV–II applet provide authentication, encryption, and digital signature cryptographic services. This **module** made up of the Gemalto GCX4 platform and the SETECS PIV–II applet is aimed to reach FIPS 140-2 Level 2 compliance. The present document is dedicated and focused on both the Gemalto GCX4 platform and the SETECS PIV-II applet.

This security policy specifies the security rules under which our Java Card **GCX4 platform and the SETECS PIV-II applet** operate.

3.2 Gemalto Smart Card Open Platform

The **GCX4** cryptographic module is a state of the art Java Open Platform-based smart card. This highly secure platform benefits from all the Gemalto expertise in Java Card security, from the latest developments in cryptographic resistance against known attacks, and provides FIPS approved cryptographic algorithms and self-tests. Additional software countermeasures have also been added by Gemalto.

The PIV–II applet doesn't implement any cryptographic services. But when needed the applet uses cryptographic services provided by the card platform. The platform 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 **Global Platform (GP) specification**. Issued cards have been loaded with two applets, cryptographic keys, and a PIN, and are moreover in the "SECURED" state. The security implementation is fully compliant with the **Global Platform (GP) specification**. The cryptographic module integrates symmetric and asymmetric cryptographic algorithms as specified in the **JavaCard specification [6]** and offers RSA for Signature/Verification, SHA-1 hashing, on-board RSA Key generation, Triple-DES CBC and ECB and AES ECB and CBC algorithms.

3.3 Security Level

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

Security Requirements Section	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	2

Table 1 – FIPS 140-2 Security Levels

4 Cryptographic Module Specification

4.1 Gemalto Crypto-Module Cryptographic Boundary

The Cryptographic Boundary is defined to be the ‘ICC micro-module edge’ of the **GCX4 ICC** a set of “embedded” hardware and firmware that implements cryptographic functions and processes, including cryptographic algorithms, key generation and applications services. **The module** is a single chip implementation. The micro-module is designed to be embedded in a plastic card body to provide an **ISO-7816 [10]** compliant smart card.

The Cryptographic Module provides dual interfaces (i.e. contact and contact-less) where the same security level is achieved. The card is designed in following configurations:

GCX4: This is a dual-interface ICC providing both contact and contactless interfaces. It has hardware version GCX4-M2569420 and firmware version GCX4-FIPS EI07 (MPH051). It is identified by three historical bytes that are present in ATS (TH8, TH9, TH10) and ATR (T6, T7, T8) having same respective values. These three bytes should be:

- 83h 11h 11h : for the configuration where RSA is supported in contactless mode

During the Gemalto manufacturing process, the chip (ICC) is wire-bonded on the inner side of a contact plate, then globe-topped with resin. **The resulting Micro-Module meets the physical security requirements of FIPS140-2 Level 3.**

All components of the **module** that are included in the cryptographic boundary are as shown in the following figure:

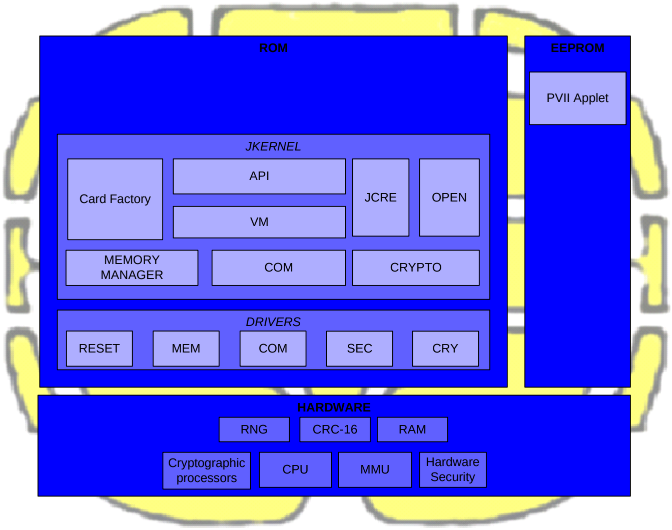


Figure 1- Cryptographic Module Boundary

4.2 FIPS Approved Security Functions

The following table gives the list of FIPS approved security functions that are provided by the Java Card API of the card platform.

SECURITY FUNCTION	DETAILS	FIPS APPROVED
Triple-DES	ECB mode in encryption	Yes

	ECB mode in decryption	Yes
	CBC mode in encryption	Yes
	CBC mode in decryption	Yes
SHA-1	Hashing operation	Yes
RSA	Key generation following X9.31	Yes
	Signature following PKCS#1with SHA-1 hashing	Yes
	Verification following PKCS#1with SHA-1 hashing	Yes
P-RNG	Pseudo Random Number Generation	Yes
AES	ECB mode in encryption	Yes
	ECB mode in decryption	Yes
	CBC mode in encryption	Yes
	CBC mode in decryption	Yes
Triple-DES MAC	ECB and CBC modes	Yes

Table 2 – FIPS Approved Security Functions

FIPS approved security functions used specifically by the **SETECS PIV-II Applet** are:

- **Triple-DES**
- **SHA-1**
- **RSA**
- **P-RNG**

5 Cryptographic Module Ports and Interfaces

The **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 Port – Contact Mode

5.1.1 PIN assignments and contact dimensions

The smart card ICC conforms to the standards **"ISO 7816-1 Physical characteristics" [10]** and **"ISO 7816-2 Dimensions and contact location" [10]**.

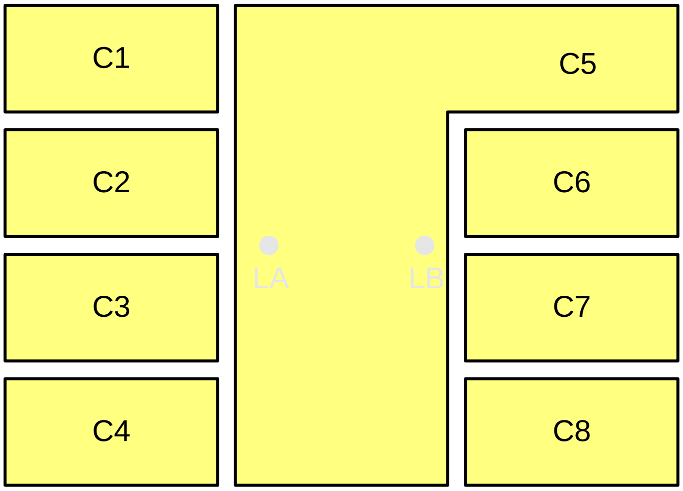


Figure 2 - Contact plate example – Contact physical interface

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

Table 3 - Contact plate pin list – Contact mode

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	3 V and 5.5 V
Frequency	1MHz to 10MHz

Table 4 - Voltage and frequency ranges

5.2 Physical Port – Contact-less mode

5.2.1 Contacts Assignments

In the contact-less mode the SETECS GCX4-PIVII FIPS cryptographic module follows the standard **"ISO 14443 RF Interface" [12]** and only uses two connections that are physically different and distinct from the connections used in the contact mode. Those electrical connections, LA and LB, are placed on the module backside and are used to connect an external **antenna loop that is not within the cryptographic boundaries of the module.**

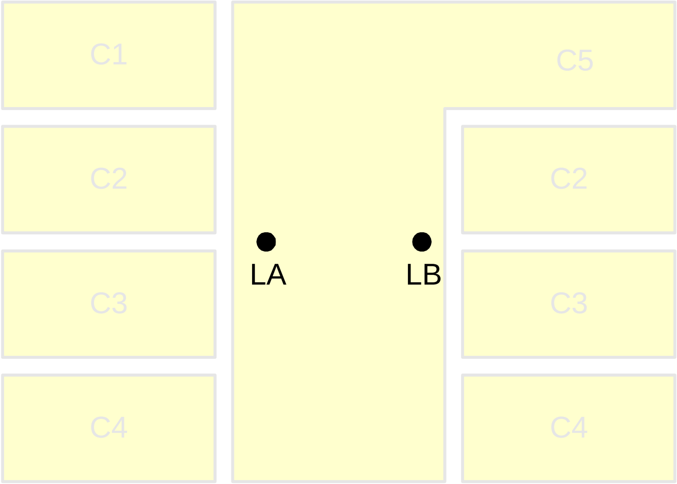


Figure 3 - Contact plate example - Contact-less antenna contacts

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

Table 5- Contact plate pin list – Contact-less mode

5.2.1 Condition of uses

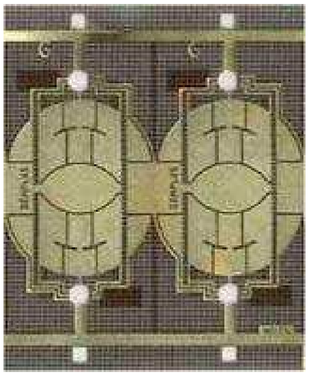
The radio frequencies and transmission protocols follow the **"ISO 14443 RF Interface" [12].** The conditions of use are the following:

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

Table 6 - Voltage and frequency ranges

Pictures – Dual Mode

GEM Combi Thermal black resin process, contact and contactless technology

	
Gem combi design[1]	**Thermal** black resin Technology

5.3 Logical Interface

The module provides services to both external devices and internal applets such as the SETECS PIV II applet.

External devices have access to services by sending APDU commands while internal applets such as PIV–II applet have access to services through internal JavaCard API entry points.

The cryptographic module provides an execution **sandbox for the PIV–II applet** and performs the requested services according to its roles and services security policy.

For security reasons, **the module** inhibits all data output via the data output interface when an error state is reached and during self-tests.

[1] The contact plate of the module may not be marked “Gemalto”. This cosmetic feature is not security relevant.

6 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 the Access Control Policy define the interrelationships 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.

6.1 Identification and Authentication Policy

6.1.1 Introduction

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

6.1.2 Identity based authentication policy

The module performs identity-based authentication using PIN and cryptographic keys. A unique index value is associated with the PIN or the cryptographic key to uniquely identify the off-card entity performing the authentication.

The following table describes the roles associated to the Cryptographic Module:

Cryptographic Officer Role	**Description**
Cryptographic Officer (CO) **(PIV Card Issuer)**	This role is responsible for managing the security configuration of the Card Manager. The CO role authenticates to the cryptographic module by demonstrating to the Card Manager or PIV II application knowledge of a GP secure channel TRIPLE-DES key set stored within the Card Manager. By successfully executing the GP secure channel mutual authentication protocol, the CO role establishes a secure channel to the Card Manager and executes services allowed to the CO role in a secure manner.
PIV Card Application Administrator **(PIV Card Activator)**	The PIV Card Application Administrator role represents an external application requesting the services offered by the PIV II applet. An applet authenticates the Card Application Administrator role by verifying possession of the External Authentication TRIPLE-DES key
User Role	**Description**
Card Holder role	The Card Holder role is responsible for ensuring the ownership of his cryptographic module, and for not communicating his PIN to other parties. The PIV II applet authenticates the Card Holder by verifying the PIN value.
PIV Card Activator	The PIV Card Activator role is responsible for unblocking and/or changing the Card Holder PIN. The PIV II authenticates the Card Holder II by verifying the PIN value.
Maintenance Role	**Description**
None	

Table 7 – PIV Roles profile definitions

6.1.3 Mechanism interfaces

The following tables describes the mechanisms for authentication of the roles:

Interface	Description
INITIALIZE UPDATE *APDU*	This APDU command initiates the setting up of a secure channel. The card uses shared Master Key to generate unique card management key. This key is used for CMS–to–card authentication. When completed, 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. The card is always issued in OP_SECURED state so a security level of MAC or MAC+Encryption is required to establish Secure Messaging.

Table 8 - Mechanism interfaces in personalization and applicative phase

Interface	Description
GENERAL AUTHENTICATE *APDU*	The APDU command is used to perform a cryptographic operation such as an authentication protocol using the data provided in the data field of the command and returns the result of the cryptographic operation in the response data field. The GENERAL AUTHENTICATE command shall be used to authenticate the card or a card application to the client-application (INTERNAL AUTHENTICATE), to authenticate an entity to the card (EXTERNAL AUTHENTICATE), and to perform a mutual authentication between the card and an entity external to the card (MUTUAL AUTHENTICATE). The GENERAL AUTHENTICATE command shall be used to realize the signing functionality on the PIV client-application programming interface.
VERIFY *APDU*	This APDU command initiates the comparison in the card of the reference data with data field of the command. The referenced PIN must be successfully verified.
RESET RETRY COUNTER *APDU*	This APDU command authenticates Card Holder II by comparing the supplied PIN with the value stored on the Card. Once PIN is verified, the command is executed.

Table 9 - Mechanism interfaces in applicative phase

6.1.4 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 PIN authentication mechanism if the authorized number of attempts is reached.
IA_PIN_RULE.2	It is not possible to get authenticated through the PIN authentication mechanism if the referenced PIN is not found
IA_PIN_RULE.3	It is not possible to get authenticated through the PIN authentication mechanism if the submitted PIN is incorrect
IA_PIN_RULE.4	The PIN must be re-authenticated if the card is reset
IA_PIN_RULE.5	The PIN must be re-authenticated if a new application is selected on the same channel
IA_PIN_RULE.6	The PIN remains active if another application is selected on another channel
IA_PIN_RULE.7	The minimum PIN length must be 7.digits
IA_PIN_RULE.8	The number of retries for incorrect authentication must be 10.
ia_co_rule.2	The Cryptographic Officer must be re-authenticated if the card is reset.
ia_co_rule.3	The Cryptographic Officer must be re-authenticated if the cryptographic module detects a secure messaging corruption.

Table 10 - Security Rules

6.1.5 Strengths of Authentication Mechanisms:

Authentication Mechanism	Strength of Mechanism
GP mutual authentication	$\left(\frac{1}{2^{112}}\right)$
	The cryptogram sent is 8 bytes long and Triple-DES 2keys is used (i.e. 2 x 56 relevant bits key length).
PIN verification	$\left(\frac{1}{10^{7}}\right)$
	Pin verification is the responsibility of the PIVII applet (only decimal digits are allowed) that defines and maintains its own security policy regarding PIN but uses the PIN management services provided by the platform.
Card Application Administrator authentication	$\left(\frac{1}{2^{168}}\right)$
	CAA authentication is the responsibility of the PIVII applet using External Authenticate option of the GENERAL AUTHENTICATE command that involves verifying decryption of an 8-byte challenge using the External Authenticate key.

Table 11 - Mechanism strengths

6.2 Access Control Policy

6.2.1 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.

List of the security related process or mechanisms specified for the PIVII applet during the applicative life cycle:

- **Secure messaging** : It is possible to open a secure channel during the personalization phase of the PIV-II applet (between the personalization device and the card, when the applet is in the SELECTABLE state) by using the security domain of the java platform. Secure Messaging is also required for executing commands protected by Secure Messaging access rule.

- **Access Conditions :** Each object stored in the card embeds its own access conditions. These conditions defines the minimum security required to access to the object. As the access to the object is done through a command, a security condition is defined for each command accessing the object.

  An **Access Rule** is encoded with an **Access Mode byte**, followed by one or more **Security Condition bytes**

  The PIV Data objects Access management rules:

  - **Free (always)**: No access condition.
  - **Never**: No execution possible.
  - **PIN**: The referenced PIN must be successfully verified. This flag is set until an incorrect PIN verification or an application selection or a reset.
  - **PIN Always**: The referenced PIN must be successfully verified by the previous command.
  - **Authentication**: The external authentication (using GENERAL AUTHENTICATE command) must have been successfully performed with the referenced key. The authentication flag is set until a new successful authentication, an application selection or a reset.

6.3 Services

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

When the Card Manager applet is selected the following commands are available :

Interface	Service Description
DELETE – *APDU*	
	This APDU is used to delete a uniquely identifiable object such as an Executable Load File, an application, optionally an Executable Load File and its related Applications or a key.
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 DATA – *APDU*	

	This APDU command is used to retrieve a single data object.
GET STATUS – *APDU*	This APDU command is used to retrieve the Card Manager, load file (package), and application life cycle data specific to the GP 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.
MANAGE CHANNEL - *APDU*	This command is used to open and close supplementary logical channels.
PUT DATA – *APDU*	This APDU command is used to set the value of the various data elements utilized and managed by the Card Manager (deprecated OP command)
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.
SELECT – *APDU*	This APDU command is used for selecting an application.
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.
STORE DATA – *APDU*	This APDU command is used to transfer data to an application or the security domain (Card Manager) processing the command.

Table 12 – System applet Interfaces and services

When the PIV Applet is selected the following PIV APDU (Card Commands) are available:

* APDU not available in contactless mode

Interface	Service Description
VERIFY* – *APDU*	The APDU is used to initiate the comparison in the card of the reference data indicated with authentication data in the data field of the command.
GET DATA – *APDU*	This APDU command retrieves the data content of the single data object whose tag is given in the data field. The entire object is returned.
GENERAL AUTHENTICATE – *APDU*	The APDU command performs a cryptographic operation such as INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE The GENERAL AUTHENTICATE command shall be used to realize the signing functionality on the PIV client-application programming interface.
GENERATE ASYMETRIC KEY PAIR* – *APDU*	The APDU command initiates the generation and storing in the card of the reference data of an

asymmetric key pair, i.e., a public key and a private key. The public key of the generated key pair is returned as the response to the command.
CHANGE REFERENCE DATA[*] – *APDU* The APDU command initiates the comparison of the verification data with the current value of the reference data and if this comparison is successful replaces the reference data with new reference data.
RESET RETRY COUNTER[*] – *APDU* The APDU command resets the retry counter of the key reference to its initial value and changes the reference data associated with the key reference. The command enables recovery of the PIN card application in the case that the cardholder forgot a PIV Card Application PIN.
PUT DATA[*] – *APDU* During the personalization the APDU command is used to create and/or update Data Objects, PIN, Triple-DES secret keys, RSA private keys & property template.
SELECT – *APDU*
The ADPU command is used to select an application

Table 13 – PIV-II Applet APDUs

	Cryptographic officer role	Card Application Administrator role	Card Holder role	Card Holder II role	Unauthenticated role
DELETE	X				
EXTERNAL AUTHENTICATE	X				
GET DATA (Card Manager)	X	X	X	X	X
GET STATUS	X				
INITIALIZE UPDATE	X				
INSTALL	X				
LOAD	X				
MANAGE CHANNEL	X	X	X	X	X
PUT DATA (Card manager)	X				
PUT KEY	X				
SELECT	X	X	X	X	X
SET STATUS	X				
STORE DATA	X				
GET DATA (PIV Applet)	X	X	X	X	X
PUT DATA (PIV applet)		X			
CHANGE REFERENCE DATA			X		
GENERAL AUTHENTICATE		X	X		
GENERATE ASYMETRIC KEY PAIR		X			
RESET RETRY COUNTER				X	
VERIFY			X		

Table 14 – Authenticated and unauthenticated role accorded interfaces and services

6.3.1 Security Rules

The following table presents the security rules applied:

Rule Identifier	Description
ac_co_rule.1	Administrative commands can only be used by the **Cryptographic Officer.**
ac_java_rule.1	**JCRE firewall** checks are enforced by the cryptographic module to ensure Java object protection.
ac_life_rule.1	The **Cryptographic 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 GP specification.
ac_life_rule.3	The **Cryptographic Officer** is responsible for managing the life cycle state of any applet (including system applets), in accordance with the GP specification.

Table 15 - Security rules

6.4 Additional Gemalto Card Security Rules

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

Rule Identifier	Description
AD_RULE.1	Does not support a multiple concurrent operators.
AD_RULE.2	Does not support a bypass mode.
AD_RULE.3	Does not provide a maintenance role/interface.
AD_RULE.4	Requires re-authentication when changing roles.
AD_RULE.5	Does not allow the loading of Software/Firmware - only applets.

Table 16 - Gemalto additional security rules

6.5 Security Relevant Data Items

The Security Relevant Data Items (SRDIs), i.e. PIV data objects in the PIV–II applet are the following:

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

1. GP key set of the Card Manager
2. Secure channel session keys
3. Card Holder PIN
4. Card Holder II PIN
5. The PIV authentication key
6. The PIV card application authentication key
7. The PIV card application digital signature key
8. The PIV card application key management key
9. External Authentication Key
10. PRNG Seed and seed key

Keys 5-8 are collectively referred to as the PIV II keys.

The following table defines 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
DELETE	Secure channel session keys	U
EXTERNAL AUTHENTICATE	GP key set of the Card Manager Secure channel session leys	U U
GET STATUS	Secure channel session keys	U
INITIALIZE UPDATE	GP key set of the Card Manager Secure channel session keys PRNG seed and seed key	U W U
INSTALL	Secure channel session keys	U
LOAD	Secure channel session keys	U
PUT DATA	Secure channel session keys	U
PUT KEY	GP key set of the Card Manager Secure channel session leys	W U
SET STATUS	Secure channel session keys	U
STORE DATA	Secure channel session keys	U
GENERAL AUTHENTICATE	PIVII keys External Authentication Key PRNG seed and seed key	U
VERIFY	Card Holder PIN	U
RESET RETRY COUNTER	Unblocking PIN (Card Holder II PIN) Card Holder PIN	U W
CHANGE REFERENCE DATA	Card Holder PIN	W U
GENERATE ASYMMETRIC KEY PAIR	PIV II keys PRNG seed and seed key	W U

Table 17 - Security Relevant Data Items

7 Finite State Model

The **module** is designed using a finite state machine model that explicitly specifies every operational and error state.

An additional document ("Finite State Model") identifies and describes all the states of the module including all corresponding state transitions for both platform and PIVII applet.

8 Physical Security

The single chip module is designed to meet the **FIPS140-2 level 3 Physical Security requirements**.

8.1 Manufacturing Process

The manufacturing process consist of wire bonding the ICC over printed circuit plate providing ISO contacts and sealing the chip and wires in a 'glue globe':

- 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 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.

Note: the chip is designed in such a way that no data can be collected by visual inspection.

8.2 Hardware Security Mechanisms

The embedded **P5CD072/P5CC072 chip from Philips** 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.

8.2.1 High/Low Frequency Sensor

The external clock frequency is monitored. If it is higher than the maximum value or lower than the minimum value, a security reset is generated.

8.2.2 High/Low Voltage Sensor

The supply voltage is monitored. If it is higher than the maximum value or lower than the minimum value, a security reset is generated.

8.2.3 High/Low Temperature Sensor

The temperature is monitored. If it is higher than the maximum value or lower than the minimum value, a security reset is generated.

8.2.4 Shields

Shields cover different chip areas

8.2.5 Fault injection detection

Fault injection mechanisms are implemented such as redundancy checking (parity, duplication) on internal data and transmissions. When an error is detected a reset is generated.
Light sensors are implemented to detect light attacks commonly used when trying to inject faults.

8.2.6 Light sensor

Light sensors are spread in different parts of the chip. When light attack is detected a reset is generated.

8.2.7 Glitch sensor

Glitch sensor is present and monitors Vcc and Vss. When the sensor is triggered a reset is generated.

8.2.8 Filters

Filter is present on the RST (reset signal) and CLK (clock signal) lines.

8.2.9 BUS Scrambling

Physical and logical addresses have no correlation thanks to the use of 'address scrambling' at the BUS level.

8.2.10 Memory Ciphering

Some dedicated and Philips proprietary ciphering algorithms are implemented in order to protect data in the different memory areas such as EEPROM, ROM and RAM. For FIPS 140-2 purposes, this data is considered to be in plaintext.

9 Operational Environment

This section does not apply to **the module**. No code modifying the behavior of the cryptographic module operating system can be added after its manufacturing process.

Only authorized applets can be loaded at post-issuance under control of the Cryptographic Officer. Their execution is controlled by the cryptographic module operating system following its security policy rules.

10 Cryptographic Key Management

10.1 Card Manager Keys

The cryptographic module implements **GP[4]** 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 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 SECURED card life cycle state, all command data must be **secured by at least a MAC**. As specified in the GP specification, there exist earlier states (before card issuance) in which a MAC might not be necessary to send Card Manager commands. The key set associated with the secure channel is such that:

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

Key sets are identified by Key Version Numbers (‘01’ to ‘7F’). The keys within a key set version have the following different functionality:

- Secure Channel Encryption (K-Enc) is used for generation of keys used for secure channel encryption.
- Secure Channel Message Authentication Code Key (K-Mac) is used for generation of keys used for secure channel MAC verification.
- Data Encryption Key (DEK) is used for sensitive data encryption.

Secure Channel session keys (each key is 16-bytes):
The Secure Channel session keys are generated as per the GP specifications using random challenge values and Card Manager Key Set.

- S_{enc}: used to encrypt command and response APDU data encrypted mode of the secure channel to provide message confidentiality.
- S_{mac}: used to MAC command and response APDU data in MAC mode of the secure channel to provide message integrity.

DAP Public key: The 1024-bit RSA DAP public key used for verifying loading of applets is also managed by the Card Manager applet. DAP is only used when a Security Domain with mandated DAP privileges has been loaded on the card.

PRNG Seed and seed key: These are CSPs used in the ANSI X9.31 RNG. They are stored in EEPROM across power-cycles and in RAM during module execution.

10.1.1 Card Manager Key Entry

The Card Manager applet provides the PUT KEY APDU to replace the Card Manager keyset. This service is only available to the Crypto Officer. The Card Manager enforces entering cryptographic Triple-DES keys securely within a secure channel. The Card Manager key set already present within the cryptographic module is the default key set. If this key set version is replaced, the replacement becomes the default.

10.2 PIV II Application Keys

The PIV II applet uses keys of the following key types through the cryptographic services of the module:

Triple-DES Keys, RSA public and private keys

The following is a list of PIV-II Applet's Keys and associated access conditions as installed in the product. Is also given for information list of data objects managed by the applet and their respective access conditions.

10.3 PIV II Applet Key Management

The PIV II applet manages five types of keys through the platform cryptographic services:

- The ***PIV authentication key***: This key (1024-bit asymmetric RSA) is generated on the card. This key is used to support card authentication for an interoperable environment, and it is a **mandatory non exportable key.**

  This key is generated on the PIV Card. The PIV Card does not permit exportation of the PIV authentication key. Cryptographic operations using the PIV authentication key may only be performed after Card Holder authentication using the contact interface of the PIV Card. Private key operations may be performed using a PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).

  The ***PIV card management key (External Authenticate key)****:* This key is a symmetric Triple DES key, unique for each card. It must be used for all CMS functions, such as personalization and post-issuance activities, as required by FIPS 201. The PIV Card does not permit exportation of the card management key. FIPS 201 requires this key to be unique for each card, so keys shared between the card and the CMS are not acceptable.

- The ***PIV card application digital signature key****:* This key (1024-bit asymmetric RSA) may support document signing. The PIV digital signature key is generated on the PIV Card. The PIV Card does not permit exportation of the digital signature key. Cryptographic operations using the digital signature key can only be performed using the contact interface of the PIV Card. Private key operations may not be performed without explicit PIN verification before each operation.

- The ***PIV card application key management key****:* This key (1024-bit asymmetric RSA) supports key encryption and data encryption protocols. This Key may only be used as an encryption key for key transport purposes. This key is generated on the PIV Card. Cryptographic operations using the key management key is only accessible can only be performed after Card Holder authentication using the contact interface of the PIV Card. The PIV Card does not permit exportation of the card authentication key. This key is sometimes called an encryption key or an encipherment key. Private key operations may be performed using a PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation). This key should be used to transport symmetric keys only upto 80-bits.

- The ***PIV card authentication key****:* This key (1024-bit asymmetric RSA) may be used for physical access control. The PIV card authentication key shall be generated on the PIV Card. The PIV Card does not permit exportation of the card authentication key. Cryptographic operations using the key management key is only accessible can only be performed after Card Holder authentication using the contact interface of the PIV Card. The PIV Card does not permit exportation of the card authentication key. Private key operations may be performed using a PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).

10.4 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 in compliance with X9.31 standard.

For the **PIV II applet asymmetric keys**, the card stores a corresponding X.509 certificate. to support validation of the corresponding private key. This certificate can be imported on the card using the Put Data command.

Keys are generated in the cryptographic module using the GENERATE ASSYMETRIC KEY PAIR command.

10.5 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.
Triple-DES keys are stored in the physical security of the Philips chip and are under the protection of the firewall that prevents key from being accessed by non-authorized applets. Moreover, RSA keys are checksumed, Triple-DES keys are checksumed and masked. All keys are stored in plaintext in the module. All keys are automatically zeroized when the Card State has been set to Terminated.

The Java inheritance mechanism ensures that a created Java object such as a key belongs to its owner, that is an applet and its execution context.

The cryptographic module stores key components according to the key type.

KEY TYPE	KEY COMPONENT
Triple-DES keys	Key value component
RSA Keys pair	Private portion in CRT (Chinese remainder theorem): Chinese Remainder **P** component Chinese Remainder **Q** component Chinese Remainder **PQ** component Chinese Remainder **DP1** component Chinese Remainder **DQ1** component Public portion Public exponent e component Modulus N component

Table 18 - Key types and components mapping table

The PIN is a critical security parameter that implements the JavaCard OwnerPin class.

11 EMI/EMC

The cryptographic module has been tested to meet the EMI/EMC requirements specified in FCC Part 15 Subpart J, Class B.

12 Self Tests

The **card** platform performs the following self-tests to ensure that the module works properly. All the self tests are done by the platform.

SELF-TESTS	EXECUTION
Cryptographic algorithm test (Known-answer tests for Triple-DES, AES, 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
Security error test	At Power-UP
Sensors test	At Power-Up
Pair-wise consistency test.	Conditional
Software load test.	Conditional
Continuous random number generator test.	Conditional

Table 19 - Self-tests list

12.1 Self-Test Execution

After **the ICC** 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]**. In addition to those tests, it also performs chip sensors verification and security status verification:

- **Sensors test:** at startup, the card detects if a hardware security error has been held during the previous session. If so, the card enters a mute state.
- **Security errors test:** at startup, if a pre-defined number of security errors is reached, the card is terminated as per Global Platform specifications. The Get Data command is the only command that remains available.

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 upon reset after the first APDU command is issued. 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’s 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 provides a means by which the operator can repeat the full sequence of power-up operating tests.

12.2 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 secure channel is closed (loading is aborted).

If an error occurs during another self-test, the card enters a state where no more command can be performed. The behavior of the card depends on error:

- **Severity level 1 error:**
    - integrity test, internal error counter is incremented, the card returns an error status before becoming mute.
- **Severity level 2 error:**
    - cryptographic algorithms tests, internal error counter is incremented, the card returns an error status before becoming mute.
    - conditional self-tests (PRNG continuous test and pair wise consistency test), internal error counter is incremented, the card returns an error status before becoming mute.

When the internal error counter reaches a certain value the card becomes mute.
An error while loading an applet closes the secure channel with the Card Manager. It shall be re-opened, to retry applet loading: the Cryptographic Officer has to be re-authenticated.

13 Design Assurance

13.1 Configuration Management

The **module** is designed and developed using a configuration management system that is clearly ruled and operated.

An additional document (SETECS OneCARD™ PIV-II Java Card Applet (Version 1.1) Configuration Management) defines the methods, mechanisms and tools that allow to identify and place under control all the data and information concerning specification, design, implementation, generation, test and validation of the card software all along the development and validation cycle.

13.2 Delivery and Operation

The **SETECS Gemalto GCX4 platform** is designed and developed using a configuration management system that is clearly ruled and operated.

Some additional documents ('SETECS PIV Card Finite State Model') define and describe the step necessary to deliver and operate securely the **SETECS PIV Card**.

13.3 Guidance Documents

Guidance document to be provided with **GCX4 platform** is intended to be the 'Reference Manual'. Such a document is designed to in order to allow a secure operation of **the Card Manager applet** by its users as defined in the '**Roles, Services and Authentication'** chapter

14 Mitigation of Other Attacks

The GCX4 has been designed to mitigate the following attacks:

- Timing Attacks,
- Differential Power Analysis,
- Simple Power Analysis,
- Electomagnetic Analysis,
- Fault Attack.
- Card Tearing

A separate and proprietary document describes the mitigation of attacks policy provided by the GCX4 platform.

- END OF DOCUMENT -