CARDLOGIX CREDENTSYS-J

FIPS 140-2 CRYPTOGRAPHIC MODULE SECURITY POLICY

Version: 2.0
Date: 31 January 2008

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

This document defines the Security Policy for the CardLogix Credentsys-J Cryptographic Module (CM). This module is submitted for validation to the FIPS 140-2 level 2 requirements.

This document contains a description of the module, its interfaces and services, the intended operators and the security policies enforced in the approved mode of operation.

Acronym	Definition
AA	Application Administrator
AdvX	Advance Crypto
API	Application Programming Interface
AVR	Automatic Voltage Regulation
CA	Card Administrator
CH	Card Holder
CL	Contactless
CM	Cryptographic Module
CSP	Critical Security Parameter
DF	Directory File
EF	Elementary File
FID	File ID
GP	GlobalPlatform
ISD	Issuer Security Domain
KSSK	Key Secure Storage Key
MF	Master File
OS	Operating System
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standard
PSSK	PIN Secure Storage Key
PUK	PIN unblocking PIN
RNG	Random Number Generator
VPN	Virtual Private Network

2. PRODUCT OVERVIEW

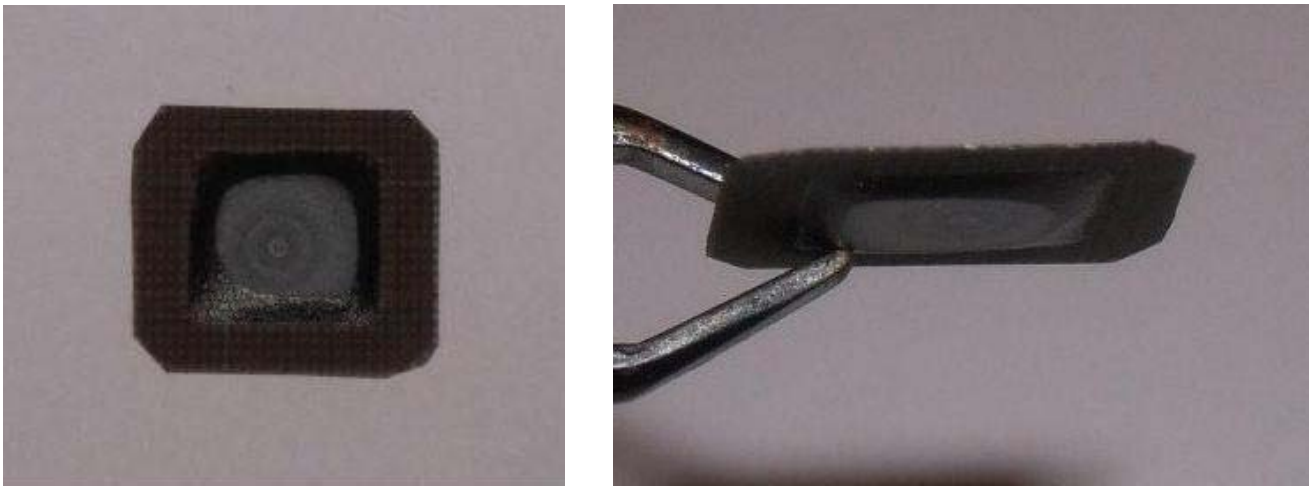


Figure 1 – PIV dual interface Smart Card chip

2.1. APPLICATION

The embedded application is a PIV compliant Java Card applet with extra services. These additional services enrich PIV functionalities with a range of cryptographic functions.

The PIV Card Application fully implements the end-point card services as described in NIST SP800-73-1. See http://csrc.nist.gov/piv-program/fips201-support-docs.html.

In addition to the standard PIV features, the module provides an extended range of services which enable single sign-on solutions through industry standard APIs such as PKCS #11 and Microsoft CryptoAPI. For example, this module allows the operator to perform secure web authentication, logical access to computer systems and to leverage token-secured VPN solutions.

The module is HW P/N AT90SC12872RCFT Rev. J, Credentsys-J PIV applet Version 2.3.0.8, OS755 Version 07.0107.04.

OPERATING SYSTEM

The embedded OS is a Java Card compliant operating system that provides all the services of GlobalPlatform. Ported on a dual interface chip, this embedded OS supports communication protocols T=0, T=1 and T=CL.

GlobalPlatform

- GlobalPlatform, Card Specification, Version 2.1.1, March 2003
- GlobalPlatform, Card Specification 2.1.1, Amendment A, March 2004

Java Card

- Runtime Environment Specification, Java Card Platform, Version 2.2.1 October, 2003
- Application Programming Interface, Java Card Platform, Version 2.2.1 October 21, 2003
- Virtual Machine Specification, Java Card Platform, Version 2.2.1 October, 2003

Communication

- Protocol T=0 with PPS for speed enhancement
- Protocol T=1 with PPS for speed enhancement
- Protocol T=CL of Type B

The Java Card API provides a large set of cryptographic related services to the PIV Card Application. Some of these services rely on the hardware.

Support for Random Numbers	DRNG	ANSI X9.31 two key TDES deterministic RNG seeded with the hardware RNG
Support for Message Digest	SHA-1	FIPS 180-2 Secure Hash Standard compliant hashing algorithms
	SHA-256	
Support for Signature	RSA PKCS #1	1024- to 2048-bit in 32-bit increments
Support for Cipher	TDES	112- and 168-bit ECB and CBC
	TDES MAC	Vendor affirmed
	AES	128-bit ECB and CBC
	RSA	1024- to 2048-bit in 32-bit increments
Support for On-Card Key Generation	RSA PKCS #1	1024- to 2048-bit in 32-bit increments

Table 1 – Supported Cryptographic Services

2.2. INTEGRATED CIRCUIT

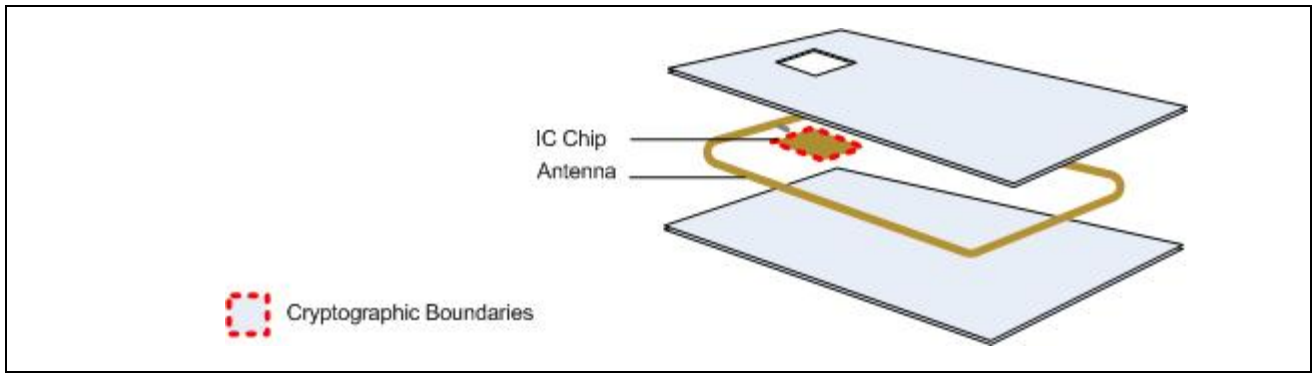


Figure 2 – Dual Interface IC module and connectors

The AT90SC12872RCFT is a low-power, high-performance, 8-/16-bit microcontroller with ROM program memory, EEPROM code or data memory, based on the secure AVR enhanced RISC architecture and with a dual interface (contact and contactless).

The cryptographic boundary is the edge of the chip itself, and not the entire smart card.

By executing powerful instructions in a single clock cycle, the AT90SC12872RCFT achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 general-purpose working registers directly connected to the Arithmetic Logical Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

The AT90SC12872RCFT uses the secure AVR architecture that allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data as well as a number of new functional and security features. The AT90SC12872RCFT features 72K bytes of high-performance EEPROM (fast erase/write time, high endurance).This allows system developers to offer their customers a true 64K bytes EEPROM, while still being able to use the remaining 8K bytes for their own purposes (customization and patches, for example). The ability to map the EEPROM in the code space allows parts of the program memory to be reprogrammed in-system.

The cryptographic accelerator featured in the AT90SC12872RCFT is the new AdvX, a N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. All cryptographic routines are executed on the secure AVR core which uses the AdvX accelerator during encryption/ decryption. AdvX is based on a 32-bit technology, thus enabling fast computation and low power operation. AdvX supports standard finite field arithmetic functions (including RSA) and arithmetic functions.

Additional security features include power, frequency and temperature protection logic, logical scrambling on program data and addresses, power analysis countermeasures, and memory accesses controlled by a supervisor mode.

This product is specifically designed for Smart Cards and targets Access Control and ID applications.

3. SECURITY LEVEL

This section details the security level met by this Cryptographic Module for each Security Requirement.

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	4
Operational Environment	NA
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 2 – Security Level of Security Requirements

4. CRYPTOGRAPHIC MODULE SPECIFICATION

This module includes two applications that offer a range of services enforcing an access control policy based on various authentication mechanisms. One of these applications is the OS755 Issuer Security Domain, allowing the Issuer to manage the operating system and card content. The second is the PIV Card Application, offering PIV management and PIV usage services.

The Issuer Security Domain is the on-card representative of the Card Issuer. The ISD has application characteristics such as application AID, application privileges, and Life Cycle State (the Issuer Security Domain inherits the Life Cycle State of the card).

The PIV Card Application is loaded into the cryptographic module library and offers services to the external application. The services are activated by the middleware sending APDU commands to the card reader connected to the module.

If additional applets are loaded into this module, then these applets require a separate FIPS 140-2 validation.

4.1. PHYSICAL INTERFACES FOR CONTACT MODE

The physical interfaces of the Cryptographic Module depend on the physical characteristics of the module itself. This module provides the following physical interfaces for contact mode (ISO/IEC 7816 parts 2 and 3):

Interface	Description
RST	External Reset signal
I/O	Input/Output
CLK	External Clock signal
VCC	Supply Voltage Power
GRD	Ground

Table 3 – Physical Interfaces for contact mode

This module supports two transmission half-duplex oriented ISO protocols: T=0 and T=1.
Up to 256 bytes of data can be exchanged through one APDU command.

4.2. PHYSICAL INTERFACES FOR CONTACTLESS MODE

This module provides contactless interfaces that are fully compliant with the ISO/IEC 14443 RF.
It uses two electrical connections (separated from any electrical connection used in the contact mode) that link the antenna and the cryptographic boundaries of the module.

Power and data are transmitted to the module from the antenna using a modulation signal at 13.56 MHz. The contactless reader produces an energizing RF field that transfers power to the module by coupling. Data communication is achieved through a modulation of the energizing RF field, using Amplitude Shift Keying (ASK) type of modulation.

The module operates independently of the external clock applied on the interfaces. The main processor and all three cryptographic co-processors are driven independently of the external clock by an interrupted internal oscillator.

During contactless communication, an on-chip capacitor provides all power to the internal oscillator, and a low frequency sensor monitors the external frequency. When an out-of-range frequency is detected, module is reset.

4.3. LOGICAL INTERFACES

The cryptographic module behaves as any other cards, providing responses to commands. The platform functions as a slave processor to implement and respond to the reader commands. The I/O ports of the platform provide the following logical interfaces:

Interface	ISO 7816	ISO 14443
Data In	I/O Pin	I/O Pins
Data Out	I/O Pin	I/O Pins
Status Out	I/O Pin	I/O Pins
Control In	I/O, CLK and RST Pins	I/O Pins

Table 4 – Logical Interfaces for all modes

5. MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the CardLogix Credentsys-J cryptographic module is to provide cryptographic services to the external PIV application.

5.1. RANDOM NUMBER GENERATORS

The module includes the following random number generators:

- An ANSI X9.31 112-bit key TDES deterministic random number generator (DRNG).
  CAVP RNG Certificate #339
- A hardware random number generator (HRNG) that is used for seeding the DRNG.

5.2. CRYPTOGRAPHIC ALGORITHMS

The module includes the following cryptographic algorithms:

- SHA-1and SHA-256
  CAVP SHS Certificate #644
- TDES
  CAVP TDES Certificate #566
  - Encrypt / decrypt (for confidentiality for authentication purposes)
  - MAC (vendor affirmed; for authentication purposes)
  - CBC and ECB modes
  - 112- and 168-bit key lengths
- AES
  CAVP AES Certificate #595
  - Encrypt/decrypt (for authentication purpose)
  - CBC and ECB modes
  - 128-bit key length
- RSA
  CAVP RSA Certificate #272
  - PKCS#1 sign/verify
  - 1024- and 2048-bit key lengths

The module includes the following non-FIPS Approved algorithms:

- RSA
  - PKCS#1 encrypt/decrypt (key wrapping; key establishment methodology provides between 80-bits and 112-bits of encryption strength)
- A hardware random number generator (HRNG) that is used for seeding the FIPS Approved DRNG.

5.3. CRITICAL SECURITY PARAMETERS

This module includes the following CSPs, sorted by owners:

- CA for Card Administrator
- AA for Application Administrator
- CH for Card Holder

PIV Card Authentication Key (9E)
This CSP is an optional key that can be of different types: RSA 1024 or 2048-bits, AES 128-bits or TDES 112 or 168-bits.
It is used to authenticate the card from an external middleware using the contact or contactless interface.
All keys can be generated outside the card and then loaded wrapped with the AA PIV Session Key; RSA

keys can be generated by the module itself. Cryptographic operations may be performed on this Key without explicit operator action (e.g., the PIN need not be supplied).
It is possible to securely export this key from the module in case and only in case of an RSA Key, using the WRAP PRIVATE KEY interface. Export is protected (encrypted) by a TDES session key (AA PIV Session Key).

5.3.1. TDES KEYS

No interface is provided to retrieve any of these CSPs (TDES Keys).

Key Secure Storage Key
This CSP (KSSK) is a 16-byte TDES Key used to wrap any of the all of the other secret and private keys of this module when stored in EEPROM (e.g. any other TDES and RSA keys listed as a CSP that is not a session key).
It is generated at first reset of the card using the DRNG.
Key values are securely unwrapped each time they are used and wrapped when set.

PIN Secure Storage Key
This CSP (PSSK) is a 16-byte TDES Key used to wrap all PINs of this module, when stored in EEPROM (e.g. AA Master PIN, CH PIV PIN and CH PIV PUK).
It is generated at first reset of the card using the DRNG.
PIN values are securely unwrapped each time they are used and wrapped when set.

CA ISD Key Set
This CSP is a set of three TDES keys used to manage GlobalPlatform Secure Channel Sessions between the ISD and the Card Administrator:

- CA-Kenc: Used to derive CA session Key that will wrap data (except keys) within a Secure Channel Session with ENCRYPTION mode set.
- CA-Kmac: Used to derive CA session Key that will guarantee integrity of any data within a Secure Channel Session with MAC mode set.
- CA-Kkek: Key Encryption Key used to wrap the additional CA ISD Key Sets that are loaded in the CM with PUT KEY APDU command within a Secure Channel Session.

CA Session Key Set
This CSP is a set of two TDES keys derived during the GlobalPlatform Secure Channel Session establishment from a selected CA ISD Key Set. These two keys are used to secure exchanges from the Card Administrator to the ISD:

- CA-Senc: Encryption Session Key used to wrap data (except keys) exchanged within a Secure Channel Session with ENCRYPTION mode set.
- CA-Smac: MAC Session Key used to guarantee integrity of any data exchanged within a Secure Channel Session with MAC mode set.

AA PIV Card Application Administration Key (9B)
This CSP is a TDES key (ECB 168-bits) that is used to authenticate the Application Administrator in order to allow the access to application management sensitive services. This key is shared between the module and the external device that is used for administration purposes. This key is generated off-card and loaded in the card wrapped with an RSA key used for secure key transport: the AA RSA Key Transport Key.

AA PIV Session Key

This CSP is a TDES key (CBC 112-bits or 168-bits) loaded in the module wrapped with the PIV Card Application Key Management Key (9D) to decrypt further loaded RSA Key components and to encrypt further exported RSA private keys.

5.3.2. PINS

No interface is provided to retrieve any of these CSPs (PINs).

AA Master PIN
This CSP is the only PIN owned by the Application Administrator and allows access to application management services. It is initialized when the PIV Card Application is initialized (INITIALISE APPLET APDU command) and can be updated by the Application Administrator (CHANGE REFERENCE DATA APDU command).
The PIN minimum and maximum lengths and the default retry count are set by the Application Administrator during personalization to 4, 15 and 15 respectively. Values from '01' to 'FF' are accepted and '00' is used for padding.

CH PIV PIN
This CSP is the PIN that is associated to the Card Holder to authenticate with the module. It is set by the Application Administrator and securely stored in the module. It can be unlocked after successful presentation of the PIV PUK.
The PIN minimum and maximum lengths and the default retry count are set by the Application Administrator during personalization to 4, 8 and 15 respectively. Its format is expected to be the ASCII representation of the digits 0 to 9 (that is '31' to '39'); however values from '00' to 'FE' are accepted ('FF' is used for padding).

CH PIV PUK
This CSP is also associated to the Card Holder and presented to him by the Application Administrator when the Card Holder wishes to unlock his PIN. It is also set by the Application Administrator and securely stored in the module.
The PIN minimum and maximum lengths and the default retry count are set by the Application Administrator during personalization to 4, 8 and 15 respectively. Its format is expected to be the ASCII representation of the digits 0 to 9 (that is '31' to '39'); however values from '00' to 'FE' are accepted ('FF' is used for padding).

5.3.3. RSA PRIVATE KEYS

It is possible to securely export these RSA Private Keys from the module using the WRAP PRIVATE KEY interface. Export is protected (encrypted) by a TDES session key (AA PIV Session Key).

PIV Authentication Key (9A)
This key is managed (generated, stored or imported) on-card using the Java Card services provided by the Operating System, and off-card by the application middleware.
It is usually generated by the module during personalization and provided to the Card Holder to perform security operations such as data signature.
It can also be generated off-card and loaded wrapped with the AA PIV Session Key.

PIV Card Application Digital Signature Key (9C)
This key is managed (generated, stored or imported) on-card using the Java Card services provided by the Operating System, and off-card by the application middleware.
This key is used to generate signatures.
When loaded, this key is wrapped using the AA PIV Session Key.

PIV Card Application Key Management Key (9D)
This key is managed (generated, stored or imported) on-card using the Java Card services provided by the Operating System, and off-card by the application middleware.

This key is used to exchange the AA PIV Session Key between the application middleware and the module.
This can be generated on-card or loaded wrapped with the AA PIV Session Key.

AA RSA Key Transport Key
This key is used to load the TDES Keys of the PIV Card Application (9B and possibly 9E) into the module.
The application middleware uses the module to create the key and to generate its value. It then gets the associated public component to use as a transport key for loading secret keys in the module. This Key is voluntarily deleted from the module by the application middleware when Key transport is complete.

CH RSA Key Pair
The Card Holder can manage additional RSA Key Pairs (1024 or 2048-bits) that can be used by any application middleware compliant with SafeSign.
These Key Pair are distinguished from the PIV Key Pairs (9A, 9D, 9C and possibly 9E) being owned by two different roles:

- CH RSA Key Pairs are owned by the Card Holder: accessed after validation of the CH PIV PIN or CH PIV PUK,
- other PIV Key Pairs are owned by the Application Administrator: accessed after validation of the AA Master PIN or AA PIV Card Application Administration Key

5.3.4. RSA PUBLIC KEYS

Public RSA component of the following CSPs:

- PIV Authentication Key (9A)
- PIV Card Application Digital Signature Key (9C)
- PIV Card Application Key Management Key (9D)
- PIV Card Authentication Key (9E)
- AA RSA Key Transport Key
- CH RSA Key Pair

These public components are not necessarily present in the module, except when the external application generates a Key Pair on-card.

These public components are possibly stored within the module, but not used by the module.

6. ROLES AND SERVICES

6.1. ROLES

This module references the following roles:

Cryptographic Officer Roles	
Card Administrator	This role is responsible for managing the security configuration of the module and for loading and installing the PIV Card Application. The Card Administrator authenticates to the module through the GlobalPlatform mutual authentication protocol. This protocol is based on the sharing of a TDES key set between him and the embedded Issuer Security Domain (ISD). Once authenticated, the Card Administrator is able to execute the services provided by the ISD Card Manager application in a Secure Channel Session (see [GP] for more details).
User Roles	
Application Administrator	This role represents an external application responsible for PIV Credential Initialization and Administration. The module authenticates the Application Administrator role by verifying the possession of the AA PIV Card Application Administration Key or the AA Master PIN.
Card Holder	This role is the owner of the CM. He is responsible for ensuring this ownership and for not communicating any of the secrets he shares with the PIV application with other parties. The Card Holder authenticates with the module verifying his CH PIV PIN. He can also unblock his CH PIV PIN by presenting the CH PIV PUK.
No Role	
Public Operator	No-role operator who does not know any secrets related to the ISD or the PIV Card Application. This non-authenticated operator can only access non-security relevant services provided by Card API and the ISD that do not require any prior authentication.
Maintenance Role	
None	This CM does not support any maintenance role.

Table 5 – Roles description

Concurrent operators are not supported by this cryptographic module: only one external physical interface and one logical channel are available to the external operators.

6.2. IDENTIFICATION

This Cryptographic Module performs identity-based authentication using PINs and cryptographic keys. A unique java card object reference and a unique ID are associated with each PIN and cryptographic key to uniquely identify the off-card entity performing the authentication.

ISD objects description	
CA ISD Key Set	KVN, KID (see [GP])
Global PIN	0x11
PIV objects description	
AA Master PIN	0x01
CH PIV PIN	0x80
CH PIV PUK	0x81
PIV Authentication Key	0x9A
AA PIV Card Application Administration Key	0x9B
PIV Card Application Digital Signature Key	0x9C
PIV Card Application Key Management Key	0x9D
PIV Card Authentication Key	0x9E

6.3. ROLES AUTHENTICATION

This Cryptographic Module supports identity based authentication of the Card Administrator, Application Administrator and Card Holder using the following mechanisms:

- Card Administrator authentication
- Application Administrator authentication
- Card Holder authentication

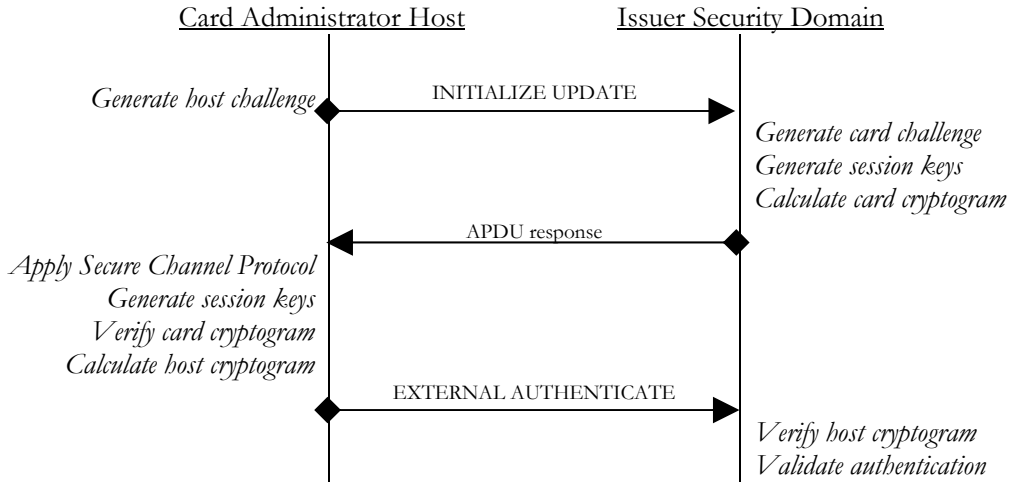
For these three mechanisms, the two following properties stand:

- the probability is less than one in 1,000,000 that a random attempt at authentication will succeed
- during any one minute period, the probability is less than 1 in 100,000 that a random authentication attempt will succeed

Actually, these three mechanisms include a counter of failed authentication and a blocking mechanism. The counter is decremented prior any attempt to authenticate and is only reset to its maximum (and limited) value upon successful and complete authentication. The authentication mechanism is blocked when associated counter reaches zero: the authentication is not processed.

6.3.1. CARD ADMINISTRATOR AUTHENTICATION

The Card Administrator authenticates himself by opening a GlobalPlatform Secure Channel Session with the ISD. This Secure Channel Session establishment involves two APDU commands as follows:



Authentication of the Card Administrator can be performed using the contact or the contactless interface of the module.

6.3.2. APPLICATION ADMINISTRATOR AUTHENTICATION

The Application Administrator is authenticated by:

- demonstrating the possession of the AA PIV Card Application Administration Key using the **GENERAL AUTHENTICATE** or **GET CHALLENGE/ ISO EXTERNAL AUTHENTICATE** APDU commands, or
- submitting the AA Master PIN to the PIV embedded application using the **VERIFY PIN** APDU command

For these two authentication mechanisms, the PIV Card Application shall be selected.
Each of these authentication remains until one of the following occurs:

- another applet is selected
- a new authentication attempt fails

- the module is reset (card tearing/power-off and cold reset, or warm reset)

Authentication of the Application Administrator can only be performed using the contact interface of the module.

6.3.3. CARD HOLDER AUTHENTICATION

The Card Holder is authenticated by submitting the CH PIV PIN to the PIV embedded application using the **VERIFY PIN** or **CHANGE REFERENCE DATA** APDU commands.

Being authenticated, the Card Holder can access services protected by the PIN access control rules. The authentication remains valid until one of the Card Holder PINs is unauthenticated after:

- another applet is selected
- a new authentication attempt fails
- the module is reset (card tearing/power-off and cold reset, or warm reset)

Authentication of the Card Holder can only be performed using the contact interface of the module.

Additionally the Card Holder is able to use the **RESET RETRY COUNTER** APDU command by submitting the CH PIV PUK only for CH PIV PIN unblocking.

6.4. SERVICES

6.4.1. CARD ADMINISTRATOR SERVICES

This role can only be active when the ISD is currently selected. All services are available on the contact and contactless interfaces.

Authenticate	
GP INITIALIZE UPDATE	CA can initiate a GlobalPlatform Secure Channel Session, setting key set version and index.
GP EXTERNAL AUTHENTICATE	CA can open a GlobalPlatform Secure Channel Session with the ISD in order to communicate with it in a secure and confidential way.
Card Content Management	
INSTALL	CA can initiate or perform the various steps required for Module Content management.
LOAD	CA can transfer a Load File to the CM.
DELETE (applet)	CA can delete a uniquely identifiable object such as an Executable Load File (library), an Application (applet), optionally an Executable Load File and its related Applications.
PUT KEY	Regarding CA ISD Key Sets, CA can either: - Replace an existing ISD key with a new key - Replace multiple existing ISD keys with new keys - Add a single new ISD key - Add multiple new ISD keys - Zeroize ISD Keys
DELETE (key)	CA can delete a uniquely identifiable ISD object such as a key. This service is also used for ISD keys zeroization.
SET STATUS	CA can modify the module Life Cycle State or the Application Life Cycle State.
GET STATUS	CA can retrieve Life Cycle status information of the ISD, Executable Load File, Executable Module, Application or Security Domain. No CSPs can be read using this service.
STORE DATA	CA can transfer data to the ISD.

6.4.2. APPLICATION ADMINISTRATOR SERVICES

This role can only be active when the PIV Card Application is currently selected. All services are available on the contact interface. Services are available on the contactless interface unless restrictions are specified.

Authenticate		**Contactless restrictions**
VERIFY PIN	To set the security status of the AA Master PIN by presenting the expected value	
GENERAL AUTHENTICATE - PIV Card Application Administrator Key	To authenticate with the PIV Card Application proving the knowledge of the AA PIV Card Application Administration Key.	
GET CHALLENGE ISO EXTERNAL AUTHENTICATE	Sequence of ISO APDU commands used to verify the AA PIV Card Application Administration Key.	
DE-AUTHENTICATE	To put the module in an unauthenticated state.	

Initializing Applet		
INITIALISE APPLET	To initialize: - AA Master PIN, - Maximum number of files under the virtual MF, - Maximum number of RSA Key Pairs,	
Clearing applet data structure		
DELETE AUTHENTICATION OBJECT	To delete a designated authentication object: CH PIV PIN, CH PIV PUK or AA PIV Card Application Administration Key.	
DELETE KEY PAIR - PIV Key Pair - CH RSA Key Pair	To delete a designated Key Pair (PIV Key Pair or CH RSA Key Pair)	
DELETE FILE - MF - under MF - under Admin DF	Deletes a file (container or containers directory) by FID relative to the currently active directory (default DF is MF). Note that if a DF or the MF is deleted, all their sub-files are deleted recursively.	
Creating PIV applet data structure		
CREATE PIN CONTAINER - CH PIV PIN - CH PIV PUK	To create a new PIN object (CH PIV PIN or CH PIV PUK) during the personalization stage of the applet.	
CREATE CHALLENGE/RESPONSE KEY CONTAINER	To create the AA PIV Card Application Administration Key and its parameters (retry counter, privilege for Key Manipulation, …)	
CREATE KEY PAIR CONTAINER - PIV Key Pair	To create a new PIV RSA Key Pair object with specific parameters (length, modes of operation, PIV key reference, conditions for generating, importing and using the key-pair). The value fields are not set.	
CREATE FILE - PIV container	To create a PIV container.	
Personalize PIV applet data		
GENERATE ASYMMETRIC KEY PAIR - PIV Key Pair	To generate the value of a created PIV Key Pair. The public exponent and public modulus of the generated key pair are output using TLV format (plaintext, no signature).	Not available
PUT DATA	To set or change the content of a PIV container	
UPDATE CHALLENGE/RESPONSE KEY	To set the value of the AA PIV Card Application Administration Key. The input value is wrapped with the AA RSA Key Transport Key.	
UNWRAP SECRET KEY - PIV Key Pair	To securely load the AA PIV Session Key into the module, encrypted with the PIV Card Application Key Management Key	Not available
UNWRAP PRIVATE/PUBLIC KEY - PIV Key Pair	To securely import the private and public component of a PIV Key Pair: - PIV Authentication Key - PIV Card Application Digital Signature Key - PIV Card Application Key Management Key - PIV Card Authentication Key	Not available

CHANGE REFERENCE DATA - CH PIV PIN - CH PIV PUK - AA Master PIN	To initialize the reference data and retry counter of the CH PIV PIN, CH PIV PUK or AA Master PIN.	Not available for: - CH PIV PIN - CH PIV PUK
Administrate PIV applet data		
WRAP PRIVATE KEY - PIV Key Pair	To securely export the private component of a PIV Key Pair: - PIV Authentication Key - PIV Card Application Digital Signature Key - PIV Card Application Key Management Key - PIV Card Authentication Key	Not available
EXPIRE PIN	To mandate a change of the reference data (CH PIV PIN or CH PIV PUK) before the PIN can be used for authentication (transport PIN management).	Not available
Manage PIV applet containers (PKCS#15 data)		
CREATE FILE - under MF - under PIV container DF	To create a new file (EF or DF) in the currently active directory (default DF is MF) with specific parameters (file ID, type, size, and applicable access control conditions)	
RESIZE FILE - PIV container EF	To resize the currently selected EF.	
UPDATE BINARY - PIV container EF	Writes data in a file or an implicitly selected file (EF).	
READ BINARY - PIV container EF	Reads data from a file or an implicitly selected file	
ERASE BINARY - PIV container EF	Partially erases the content of a file or an implicitly selected file (EF).	

Note 1: *When creating new objects (Key Pairs or files), the Application Administrator is responsible for setting their access conditions to secrets owned by the intended recipient of these objects:*

- *access conditions of his objects involve the AA Master PIN and the Card Application Administration Key*
- *access conditions of Card Holder objects involve the CH PIV PIN and the CH PIV PUK*

Note 2: *The PKCS #15 file structure is initialized by the Application Administrator; all DFs and EFs created during this initialization phase are owned by the Application Administrator. The contents of some of the EFs may be modified by the Card Holder (the access condition will be set accordingly if necessary). The card holder cannot delete any of the files created in this phase, this is the sole privilege of the Application Administrator.*

6.4.3. CARD HOLDER SERVICES

This role can only be active when the PIV Card Application is currently selected. All services are available on the contact interface. No services are available on the contactless interface as the CH PIV PIN and CH PIV PUK cannot be presented.

Authentication Commands	
VERIFY PIN	To set the security status of the CH PIV PIN or CH PIV PUK by presenting the expected value
DE-AUTHENTICATE	To de-authenticate the CH PIV PIN and CH PIV PUK in order to avoid that PINs remain authenticated after the restricted APDU commands are completed

PIN related Commands	
CHANGE REFERENCE DATA - CH PIV PIN - CH PIV PUK	Verifies the specified PIN (CH PIV PIN or CH PIV PUK) and change it to the specified value if verification succeeds.
RESET RETRY COUNTER	To reset the reference data and the retry counter of the CH PIV PIN by presenting the CH PIV PUK
PIV Container related Commands	
PIV GET DATA - protected PIV Container	Sequence of APDU commands used to read the content of a PIV container that is protected by the CH PIV PIN.
GET RESPONSE	
Cryptographic Commands	
GENERAL AUTHENTICATE - PIV Key Pair	To sign or decipher data with a PIV RSA Key Pair
MANAGE SECURITY ENVIRONMENT	Sequence of APDU commands used to perform three different operations: **PUT HASH** This command can be used to write a hash value to the card to be used in a subsequent call to the COMPUTE DIGITAL SIGNATURE operation. The access control condition for use key for the key selected in the previous call to MANAGE SECURITY ENVIRONMENT must be satisfied. **COMPUTE DIGITAL SIGNATURE** This command can be used to compute a digital signature over a hash, or – in case of a raw RSA operation – over raw data. The algorithm and key to use have been selected using a call to the MANAGE SECURITY ENVIRONMENT APDU command. **DECIPHER** This command can be used to decipher encrypted data. The algorithm and key to use have been selected using a call to the MANAGE SECURITY ENVIRONMENT APDU command
PERFORM SECURITY OPERATION	
Key Management Additional Commands	
GENERATE ASYMMETRIC KEY PAIR - CH RSA Key Pair	To generate the value of a created CH RSA Key Pair
CREATE KEY PAIR CONTAINER - CH RSA Key Pair	To create a new Card Holder RSA Key Pair with specific parameters: length, mode of operation, AC conditions for generation, import and use
UNWRAP SECRET KEY - CH RSA Key Pair	To securely load the AA PIV Session Key into the module, encrypted with an existing CH RSA Key Pair
UNWRAP PRIVATE/PUBLIC KEY - CH RSA Key Pair	To securely import the private and public components of a CH RSA Key Pair encrypted with a previously loaded AA PIV Session Key
WRAP PRIVATE KEY - CH RSA Key Pair	To securely export the private components of a CH RSA Key Pair
DELETE KEY PAIR - CH RSA Key Pair	To delete a designated CH RSA Key Pair
PKCS#15 File Management Additional Commands	
CREATE FILE - under Card Holder DF	To create a new file (EF or DF) in the currently active directory (default DF is MF) with specific parameters (file ID, type, size, and applicable AC conditions)

RESIZE FILE - Card Holder EF	To resize the currently selected EF.
UPDATE BINARY - Card Holder EF	Writes data in a file or an implicitly selected file (EF).
READ BINARY - Card Holder EF	Reads data from a file or an implicitly selected file
ERASE BINARY - Card Holder EF	Partially erases the content of a file or an implicitly selected file (EF).
DELETE FILE - under Card Holder DF	Deletes a file (or all sub-files recursively in case of a DF) by FID relative to the currently active directory (default DF is MF and is not acceptable)

Note: *When creating his own objects (Key Pairs or files), the Card Holder is responsible for setting their access conditions to his own authentication data (CH PIV PIN or CH PIV PUK).*

Note2: *The card holder may create, modify and delete EFs under certain DFs (notably PublicSpace and PrivateSpace) that are part of the PKCS #15 structure.*

6.4.4. NO ROLE SERVICES

All services are available on the contact and contactless interfaces.

Public Commands	
SELECT	Operator can select an Application.
Public ISD Commands	
GP GET DATA	Operator can retrieve public data from the ISD. No CSPs can be read using this service.
Public Applet Commands	
PIV GET DATA - public PIV Container	Operator can get the content of a PIV container that is public
ISO GET DATA	Operator can get the public information from the data (serial number, memory status, applet version, communication protocol, card capabilities)
READ/QUERY PUBLIC KEY	Retrieve the public components of any RSA Key Pair (plaintext, no signature) or find the matching Key Pair of an input public modulus.
GET CHALLENGE	To get up to 256 bytes of FIPS 140-2 compliant random number.
GET RETRY COUNTER	To get the status information from a designated authentication object (AA Master PIN, CH PIV PIN, CH PIV PUK or AA PIV Card Application Administration Key): max tries (initial number of tries), current retry counter and state.
SELECT FILE	To select the PIV application or a file (MF, DF or EF).
CREATE FILE - under public DF	To create a new file (EF or DF) in the currently active directory (default DF is MF) with specific parameters (file ID, type, size)
RESIZE FILE - public EF	To resize the currently selected EF.
UPDATE BINARY - public EF	To write data in a file or an implicitly selected file (EF).

READ BINARY - public EF	To read certificates which are public in PKCS#15.
ERASE BINARY - public EF	Partially erases the content of a file or an implicitly selected file (EF).
DELETE FILE - under public DF	Deletes a file by FID relative to the currently active directory (default DF is MF and is not acceptable). Note that if a DF is deleted, all sub-files are deleted recursively.

6.4.5. RELATIONSHIP BETWEEN SERVICES AND ROLES

	Card Administrator	Application Administrator	Card Holder	No Role
CHANGE REFERENCE DATA				
- CH PIV PIN		X	X	
- CH PIV PUK		X	X	
CREATE CHALLENGE/RESPONSE KEY CONTAINER		X		
CREATE FILE				
- PIV container		X		
- under MF		X		
- under public DF				X
- under PIV container DF		X		
- under Card Holder DF			X	
CREATE KEY PAIR CONTAINER				
- PIV Key Pair		X		
- CH RSA Key Pair		X	X	
CREATE PIN CONTAINER				
- CH PIV PIN		X		
- CH PIV PUK		X		
DE-AUTHENTICATE		X	X	
DELETE	X			
DELETE AUTHENTICATION OBJECT		X		
DELETE FILE				
- MF		X		
- under MF		X		
- under public DF				X
- under PIV container DF		X		
- under Card Holder DF			X	
DELETE KEY PAIR				
- PIV Key Pair		X		
- CH RSA Key Pair		X	X	
ERASE BINARY				
- public EF				X
- PIV container EF		X		
- Card Holder EF			X	
EXPIRE PIN		X		
GENERAL AUTHENTICATE				
- PIV Card Application Administrator Key		X		
- PIV Key Pair			X	
GENERATE ASYMMETRIC KEY PAIR				
- CH RSA Key Pair			X	
- PIV Key Pair		X		
GET CHALLENGE				X
PIV GET DATA				
- protected PIV Container			X	
- public PIV Container				X

	Card Administrator	Application Administrator	Card Holder	No Role
ISO GET DATA				X
GP GET DATA				X
GET RETRY COUNTER				X
GET STATUS	X			
GP EXTERNAL AUTHENTICATE	X			
GP INITIALIZE UPDATE	X			
INITIALISE APPLET		X		
INSTALL	X			
ISO EXTERNAL AUTHENTICATE		X		
LOAD	X			
MANAGE SECURITY ENVIRONMENT		X	X	
PERFORM SECURITY OPERATION		X	X	
PUT DATA		X		
PUT KEY	X			
READ BINARY				
- public EF				X
- PIV container EF		X		
- Card Holder EF			X	
READ/QUERY PUBLIC KEY				X
RESET RETRY COUNTER			X	
RESIZE FILE				
- public EF				X
- PIV container EF		X		
- Card Holder EF			X	
SELECT				X
SELECT FILE				X
SET STATUS	X			
STORE DATA	X			
UNWRAP PRIVATE/PUBLIC KEY				
- CH RSA Key Pair			X	
- PIV Key Pair		X		
UNWRAP SECRET KEY				
- CH RSA Key Pair			X	
- PIV Key Pair		X		
UPDATE BINARY				
- public EF				X
- PIV container EF		X		
- Card Holder EF			X	
UPDATE CHALLENGE/RESPONSE KEY		X		
VERIFY PIN				
- AA Master PIN		X		
- CH PIV PIN - CH PIV PUK			X	
WRAP PRIVATE KEY				
- CH RSA Key Pair			X	
- PIV Key Pair		X		

Table 6 – Services and associated roles

6.4.6. RELATIONSHIP BETWEEN SERVICES AND CSPS

Relationship can be:

- Create (creation of the CSP object)
- Read
- Write
- Generate
- Execute (computation involving the CSP)
- Zeroize

- Delete

Key Secure Storage Key

Service	Type of access
First Card reset	Generate
GP INITIALIZE UPDATE	Execute
GP EXTERNAL AUTHENTICATE	Execute
LOAD	Execute
PUT KEY	Execute
UPDATE CHALLENGE/RESPONSE KEY	Execute
GENERAL AUTHENTICATE	Execute
ISO EXTERNAL AUTHENTICATE	Execute
SET STATUS (TERMINATED)	Zeroize

PIN Secure Storage Key

Service	Type of access
First Card reset	Generate
CHANGE REFERENCE DATA	Execute
VERIFY PIN	Execute
RESET RETRY COUNTER	Execute
SET STATUS (TERMINATED)	Zeroize

CA ISD Key Set

Service	Type of access	Key
GP INITIALIZE UPDATE	Execute	CA-Kenc, CA-Kmac
GP EXTERNAL AUTHENTICATE	Execute	CA-Kenc, CA-Kmac
PUT KEY	Execute	CA-Kkek
DELETE	Zeroize	CA-Kenc, CA-Kmac, CA-Kkek

CA session Key Set

Service	Type of access
GP INITIALIZE UPDATE	Generate
GP EXTERNAL AUTHENTICATE	Generate
GET STATUS	Execute
LOAD	Execute
PUT KEY	Execute
SET STATUS	Execute
STORE DATA	Execute
Card reset	Zeroize

AA PIV Card Application Administration Key (9B), and
PIV Card Authentication Key (9E) when it is an AES or a TDES Key

Some of the following services only involve the attributes of this CSP (retry counter, security status), and not the CSP secret itself.

Service	Type of access
CREATE CHALLENGE/RESPONSE KEY CONTAINER	Create
UPDATE CHALLENGE/RESPONSE KEY	Write

GENERAL AUTHENTICATE	Execute
ISO EXTERNAL AUTHENTICATE	Execute
DELETE AUTHENTICATION OBJECT	Zeroize
GET RETRY COUNTER	Read (attribute)
DE-AUTHENTICATE	Write (attribute)

AA PIV Session Key

Note that the AA PIV Session Key is written encrypted in a file (1), then decrypted (2) before being used (3) and deleted (4) by the external application middleware. A card reset also implies that this key is erased.

Service	Type of access
(1) UPDATE BINARY	Write
(2) UNWRAP SECRET KEY	Write
(3) UNWRAP PRIVATE/PUBLIC KEY	Execute
(4) SELECT (other applet)	Zeroize

AA Master PIN

Some of the following services only involve the attributes of this CSP (retry counter, validity status), and not the CSP secret itself.

Service	Type of access
INITIALIZE APPLET	Write
CHANGE REFERENCE DATA	Write
VERIFY PIN	Execute
GET RETRY COUNTER	Read (attribute)
EXPIRE PIN	Write (attribute)
DELETE (PIV applet)	Zeroize

CH PIV PIN

Some of the following services only involve the attributes of this CSP (retry counter, validity status, security status), and not the CSP secret itself.

Service	Type of access
CREATE PIN CONTAINER	Create
CHANGE REFERENCE DATA	Write
RESET RETRY COUNTER	Write
VERIFY PIN	Execute
DELETE AUTHENTICATION OBJECT	Zeroize
GET RETRY COUNTER	Read (attribute)
EXPIRE PIN	Write (attribute)
DE-AUTHENTICATE	Write (attribute)

CH PIV PUK

Some of the following services only involve the attributes of this CSP (retry counter, validity status, security status), and not the CSP secret itself.

Service	Type of access
CREATE PIN CONTAINER	Create
CHANGE REFERENCE DATA	Write
VERIFY PIN	Execute
RESET RETRY COUNTER	Execute
DELETE AUTHENTICATION OBJECT	Zeroize

GET RETRY COUNTER	Read (attribute)
EXPIRE PIN	Write (attribute)
DE-AUTHENTICATE	Write (attribute)

PIV Authentication Key (9A),
PIV Card Application Digital Signature Key (9C),
PIV Card Application Key Management Key (9D),
PIV Card Authentication Key (9E) when it is an RSA Key Pair,
AA RSA Key Transport Key, and
CH RSA Key Pair

Service	**Type of access**
CREATE KEY PAIR CONTAINER	Create
GENERATE ASYMMETRIC KEY PAIR	Write
PERFORM SECURITY OPERATION	Execute
GENERAL AUTHENTICATE	Execute
UNWRAP PRIVATE/PUBLIC KEY	Write (private)
READ/QUERY PUBLIC KEY	Read (public)
WRAP PRIVATE KEY	Read (private)
DELETE KEY PAIR	Zeroize

6.5. APPROVED MODE OF OPERATION

The module is always in the approved mode of operation.

6.6. VERIFYING APPROVED MODE OF OPERATION

It is possible to verify that a module that was known to be in the approved mode of operation is still in the approved mode of operation.

The Card Administrator must:

1. SELECT the ISD and send a GET DATA APDU command with the CPLC Data tag '9F7F' and verify that the returned data contains fields as follows (other fields are not relevant here). This verifies the version of the OS.

Data Element	Length	Value	Version
IC type	2	'0107'	Atmel AT90SC12872RCFT Revision J
Operating system release date	2	'6250'	
Operating system release level	2	'x7x4'	7: Firmware Version Part 1 4: Firmware Version Part 2 x: N/A

2. Open a Secure Channel Session with the ISD. This authenticates the CA ISD Key Set in the module.

The Applet Administrator must:

3. SELECT the PIV Card Application send a GET DATA APDU command with tag '0103' and verify that the returned data is '02030008'. This verifies the version of the PIV Card Application.

4. Authenticate to the PIV Card Application with either the AA PIV Card Application Administration Key or the AA Master PIN.

7. SELF-TESTS

7.1. POWER-UP SELF-TESTS

Each time this cryptographic module is powered up by a contact or contactless reader it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged.

Cryptographic algorithms testing:
Known Answer Tests (KATs) are conducted for each cryptographic function in one mode of operation. Known input data and answers are stored in EEPROM. The following KATs are performed in random order:

- ANSI X9.31 DRNG,
- SHA-1,
- SHA-256,
- TDES (encrypt and decrypt with 112-bit key in CBC mode),
- AES (encrypt and decrypt with 128-bit key in CBC mode),
- RSA PKCS#1 (sign and verify with 1024-bit private and public key),

KATs are performed prior to the dispatch of the first APDU command for processing. If one of the KATs fails the card goes mute.

Software integrity testing:
A standard CRC16 checksum is used to verify that no FIPS applications present in EEPROM have been modified. It also checks the integrity of all additions and corrections that have been added to the module (patch code and patch table). ROM code is excluded from software integrity verification. If a test fails the card is terminated (the KSSK and PSSK are zeroized and the CM enters the GlobalPlatform TERMINATED state in which only the ISD may be selected with the SELECT APDU command and only the GP GET DATA APDU command is available).

7.2. CONDITIONAL SELF-TESTS

Key Pair-Wise Consistency Test:
This test is performed during RSA Key Pair generation once the CM has generated the RSA Key Pair values (both signature generation/verification and encryption/decryption are tested). If the test fails the card goes mute.

Continuous RNG Tests:
The hardware RNG and DRNG are tested for repetition of serially output 64-bit values. If the test fails the card goes mute.

Software/Firmware Load Test:
Applet loading follows the GlobalPlatform 2.1.1 specifications (GlobalPlatform Secure Channel Session with TDES MAC), see [GP]. Note that a failed application load rolls back to the state prior to the load starting.

Note: *Power-up self–tests on demand: resetting the module is an approved self-test on demand function.*

8. SECURITY RULES

This section details the rules that form the policy of the Cryptographic Module.

8.1. PHYSICAL SECURITY

The Cryptographic Module (CM) is a single-chip implementation which Cryptographic boundaries encompass the chip. The physical component of CM is protected by a hard opaque tamper-evident metal active shield.

The CM employs physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module (including substitution of the entire module) when installed. All hardware and firmware within the cryptographic boundary are protected.

Physical security features meet FIPS-140-2 level 4 requirements with:

- Production-grade component including passivation techniques and state-of-the-art physical security features:
  - Dedicated Hardware for Protection Against SPA/DPA/DEMA Attacks
  - Advanced Protection Against Physical Attack, Including Active Shield
  - Environmental Protection Systems
  - Voltage Monitor
  - Frequency Monitor
  - Temperature Monitor
  - Light Protection
  - Secure Memory Management/Access Protection (Supervisor Mode)

- Opaque coating on chip that deter direct observation within the visible spectrum,

- Hard tamper-evident coating that provides evidence of tampering (visible signs on the resin cover and/or contact face plates), with high probability of causing serious damage to the chip while attempting to probe it or remove it from the module.

This IC is designed to meet Common Criteria EAL4+

8.2. AUTHENTICATION SECURITY RULES

This CM implements different authentication dedicated mechanisms for each role. Each authentication mechanism includes the verification of the knowledge of a secret shared between the CM and the external operator, and, for each restricted service, verification that the authentication security status is granted.
The external operator will use different mechanisms, depending on the secret for which he wants to claim the possession. Each of these secrets has a unique object reference on card that is used by the external operator to identify them:

- The CA ISD Key Set represents the identity of the Card Administrator
- The AA PIV Card Application Administration Key or the AA Master PIN represents the identity of the Application Administrator
- The CH PIV PIN or the CH PIV PUK represents the Card Holder.

8.3. APPLET LIFECYCLE SECURITY RULES

The PIV Applet is loaded into EEPROM on the production line. Additional applets can be loaded in the module after card issuance as specified in GlobalPlatform. However, these additional applets must be FIPS 140-2 validated before being loaded.

- Applet loading is one of the services provided by the Operating System that is restricted to the Card Administrator: a Secure Channel Session must be open between the external operator (more precisely the middleware the CA is using to manage card content) and the ISD. Applet loading is done protected by a TDES MAC on every block of data
- Applet loading service is available before and after card issuance
- The CA is responsible for applet personalization and lifecycle management following GlobalPlatform
- The CA is responsible for creating as many instances of loaded applets as required, according to card resources.

8.4. ACCESS CONTROL SECURITY RULES

This module manages sensitive data and services whose access is controlled by the following rules:

- Card Administrator Key Set must be loaded through a GlobalPlatform Secure Channel Session ensuring their integrity and confidentiality (double TDES encryption).
- The CH PIV PIN and CH PIV PUK that are used by the Card Holder to authenticate with the module shall not be disclosed to other parties.
- The AA Master PIN or AA PIV Card Application Administration Key (9B) ensure access control on other PIV RSA Key Pairs and shall not be disclosed.
- The applet shall be personalized to ensure access control policies:
    - AA Master PIN, CH PIV PIN and CH PIV PUK shall be locked after a restricted amount of failures
    - Application Provider is responsible for revoking the CH PIV PIN

8.5. KEY MANAGEMENT SECURITY RULES

8.5.1. KEY MATERIAL

This card supports a range of symmetric and asymmetric keys:

Key name (CSP)	Type	Length
Key Secure Storage Key	TDES	112-bits
PIN Secure Storage Key		
CA ISD Key Set		
AA PIV Card Application Administration Key (9B)		112- or 168-bits
CA Session Key Set	TDES session key	112-bits
AA PIV Session Key		112- or 168-bits
PIV Authentication Key (9A)	RSA	1024-bits
PIV Card Application Digital Signature Key (9C)		
PIV Card Application Key Management Key (9D)		
PIV Card Authentication Key (9E)	RSA	1024- or 2048-bits
	AES	128-bits
	TDES	112- or 168-bits
AA RSA Key Transport Key	RSA	1024-bits
CH RSA Key Pair	RSA	1024- or 2048-bits

8.5.2. KEY GENERATION

Four groups of Keys can be generated using the CM:

Key Secure Storage Key
The KSSK is generated at first reset of the card using the DRNG.

PIN Secure Storage Key
The PSSK is generated at first reset of the card using the DRNG.

CA Session Key Set
[GP] ISD Session keys are generated by OS upon opening a Secure Channel Session (successful mutual-authentication):

- CA-Smac Session Key: generated from CA-Kmac, used for protecting data integrity in GlobalPlatform Secure Channel Session secure mode (MAC).
- CA-Senc Session Key: generated from CA-Kenc, used for protection data confidentiality in GlobalPlatform Secure Channel Session mode (Encryption).

RSA Key Pairs

- PIV Authentication Key (9A)
- PIV Card Application Digital Signature Key (9C)
- PIV Card Application Key Management Key (9D)
- PIV Card Authentication Key (9E) when it is an RSA Key Pair
- AA RSA Key Transport Key
- CH RSA Key Pair

The OS755 provides PIV applet with an on-board 1024-bit key generation that uses an approved key generation method.

8.5.3. KEY ENTRY

CA ISD Key Set
These Keys are entered in the module using the PUT KEY APDU command for:

- Replacing an existing key with a new ISD key
- Replacing existing key set with new ISD key set
- Adding a single new ISD key
- Adding a new ISD key set

The CM enforces confidentiality while entering Issuer Security Domain secret keys using key encryption following [GP] (FIPS approved algorithms and operation mode). The CM provides no ISD secret key output. All Secret values of these keys are entered wrapped with the TDES CA-Kkek identified during the GlobalPlatform Secure Channel Session initialization, when one of the ISD Key set is selected.

AA PIV Session Key
This key is entered in a file of the module by the external operator using the ISO APDU command UPDATE BINARY. It is entered wrapped with the public RSA key of the PIV Card Application Key Management Key.

Asymmetric PIV Keys
The following RSA keys are entered in the module wrapped with the AA PIV Session Key using the UNWRAP PRIVATE/PUBLIC KEY APDU command:

- PIV Authentication Key (9A)
- PIV Card Application Digital Signature Key (9C)

- PIV Card Application Key Management Key (9D)
- PIV Card Authentication Key (9E) when it is an RSA Key Pair
- AA RSA Key Transport Key
- CH RSA Key Pair

Symmetric PIV Keys
The following TDES keys are entered using the UPDATE CHALLENGE/RESPONSE APDU command, wrapped with the AA RSA Key Transport Key:

- AA PIV Card Application Administration Key (9B)
- PIV Card Authentication Key (9E) when it is a TDES or an AES key

8.5.4. KEY STORAGE

Key storage is detailed for all persistent keys managed by the CM:

Key Secure Storage Key (KSSK)
PIN Secure Storage Key (PSSK)
These two keys are stored in EEPROM plaintext

CA ISD Key Set
PIV Authentication Key (9A)
PIV Card Application Digital Signature Key (9C)
PIV Card Application Key Management Key (9D)
PIV Card Authentication Key (9E)
AA PIV Card Application Administration Key (9B)
AA RSA Key Transport Key
CH RSA Key Pair
All these keys are stored in EEPROM encrypted with the TDES key KSSK. The CM also applies an integrity checksum to these Keys.

8.5.5. KEY OUTPUT

The only keys that can be output from the module are the following PIV RSA Keys:

PIV Authentication Key (9A)
PIV Card Application Digital Signature Key (9C)
PIV Card Application Key Management Key (9D)
PIV Card Authentication Key (9E)
These Keys can be output using the following APDU commands:

- READ/QUERY PUBLIC KEY Read (public key)
- WRAP PRIVATE KEY Read (private key)

When the private key is output, it is encrypted with the AA PIV Session Key that has just been loaded in the card. This output ability is authorized or not when each Key Pair is created (CREATE KEY PAIR CONTAINER APDU command).
Public keys are output plaintext.

8.5.6. KEY ZEROIZATION

The CM offers services to zeroize all the persistent keys.

Key Secure Storage Key and PIN Secure Storage Key are zeroized when Card lifecycle state is set to TERMINATED using the SET STATUS APDU command provided by [GP] layer of the Card OS or setting the card in insecure and irrecoverable state (i.e. integrity check on patches, EEPROM code, PINs

or Keys fails). By zeroizing the KSSK and the PSSK, all other Keys and PINs stored in the module are made irreversibly unusable.

Other zeroization commands are provided for each keys (update and delete commands). See section 6.4.6 for a complete list of these commands).

8.6. ELECTROMAGNETIC INTERFERENCE/COMPATIBILITY (EMI/EMC)

The Cryptographic Module conforms to the EMI/EMC requirements specified by 57 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

9. MITIGATION OF OTHER ATTACKS

Typical smart card attacks are Single Power Analysis, Differential Power Analysis, Timing Analysis, Fault Induction that may lead to revealing sensitive information such as PIN and Keys by monitoring the module power consumption and timing of operations or bypass sensitive operations.

This Cryptographic Module is protected against SPA, DPA, Timing Analysis and Fault Induction by combining State of the Art Software and Hardware counter-measures.

The Cryptographic Module is protected from attacks on the operation of the IC hardware. The protection features include detection of out-of-range supply voltages, frequencies or temperatures, detection of illegal address or instruction, and physical security. For more information see specification AT90SC Vulnerability Analysis Lite, General Business Use, AT90SC_EVA_Lite_V1.0 (17 Jul 06).

All cryptographic computations and sensitive operations such as PIN comparison provided by the Cryptographic Module are designed to be resistant to timing and power analysis. Sensitive information of the embedded Operating System is securely stored and integrity protected. Sensitive operations are performed in constant time, regardless of the execution context (parameters, keys, etc…), owing to a combination of hardware and firmware features.

The Cryptographic Module does not operate in abnormal conditions such as extreme temperature, power and external clock, increasing its protection against fault induction.

10. SECURITY POLICY CHECK LIST

10.1. ROLES AND REQUIRED AUTHENTICATION

Role	Type of Authentication	Authentication Data
Card Administrator	TDES authentication	CA ISD Key Set
Application Administrator	PIN verification	AA Master PIN
	TDES authentication	AA PIV Card Application Administration Key
Card Holder	PIN verification	CH PIV PIN or CH PIV PUK

Table 7 – Roles and Required Identification and Authentication

10.2. STRENGTH OF AUTHENTICATION MECHANISM

Authentication Mechanism	Strength of Mechanism
TDES authentication with : - AA PIV Card Application Administration Key - CA ISD Key Set	2^{80}
AA Master PIN	2^{32}
CH PIV PIN	2^{32}
CH PIV PUK	2^{32}

Table 8 – Strengths of Authentication Mechanisms

All these authentication objects implement a limited retry counter.

10.3. SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Administrator	Section 6.4.1 lists authorized services for this role
Application Administrator	Section 6.4.2 lists authorized services for this role
Card Holder	Section 6.4.3 lists authorized services for this role

Table 9 – Services Authorized for Roles

10.4. ACCESS RIGHTS WITHIN SERVICES

Service	Cryptographic Keys and CSPs	Type(s) of Access
Card Administrator	GlobalPlatform Secure Channel Session with ISD and ISD TDES key set	Execute (encrypt, decrypt, MAC) Write (PUT KEY)
Application Administrator	AA Master PIN and AA PIV Card Application Administration Key	Execute (encrypt, decrypt, verify) Write (UPDATE C/R KEY)
Card Holder	CH PIV PIN and CH PIV PUK	Execute (verify) Write (CHANGE REF. DATA)

Table 10 – Access Rights within Services

10.5. MITIGATION OF ATTACKS

Other Attacks	Mitigation Mechanism	Specific Limitations
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A
Timing Attacks	Counter Measures against TA	N/A
Fault Induction	Counter Measures against FI	N/A

Table 11 – Mitigation of Other Attacks

[END OF THE DOCUMENT]