Athena IDProtect Duo PIV

FIPS 140-2 Cryptographic Module

Security Policy

Version: 0.5

Date: 22 July 2008

Athena Smartcard Inc., 20380 Town Center Lane, Suite 240, Cupertino, CA 95014

CONTENTS

List of Figures

List of tables

1 CRYPTOGRAPHIC MODULE OVERVIEW

1.1 INTRODUCTION

This document defines the Security Policy for the Athena IDProtect Duo PIV Cryptographic Module (CM). This module is validated to overall FIPS 140-2 level 2 with Cryptographic Module Specification; Roles, Services and Authentication; Cryptographic Key Management; EMI/EMC and Design Assurance level 3; and Physical Security level 4.

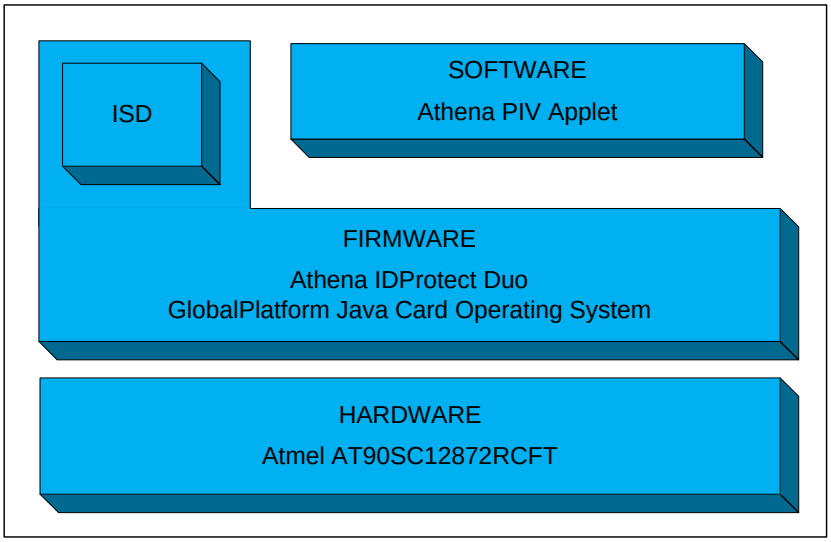
This document contains a description of the CM, its interfaces and services, the intended operators and the security policies enforced in the approved mode of operation.

The primary purpose of this device is to enable the creation of a single-chip dual interface PIV smart card as described in [FIPS201] that is fully compliant with the end-point service specified in [SP800-73-1].

The CM is a single Integrated Circuit Chip and is specifically designed to resist non-evident tampering by both physical and electronic means. The CM is physically connected to the following external interfaces:

- a smart card contact plate as defined in [7816-1] and [7816-2] and communicates in T=0 and T=1 as specified in [7816-3]
- an antenna as defined in [14443-1] and [14443-2] and communicates in T=CL as specified in [14443-3] and [14443-4]

The CM contains one Java Card applet implementing the PIV functionality (the Software) running on a GlobalPlatform Java Card operating system (the Firmware).



***Software*:**
Athena PIV Applet Version 1.0
***Firmware*:**
Athena IDProtect Duo Version 0107.7099.0105
***Hardware*:**
Atmel AT90SC12872RCFT Revision M

1.2 PHYSICAL CRYPTOGRAPHIC MODULE

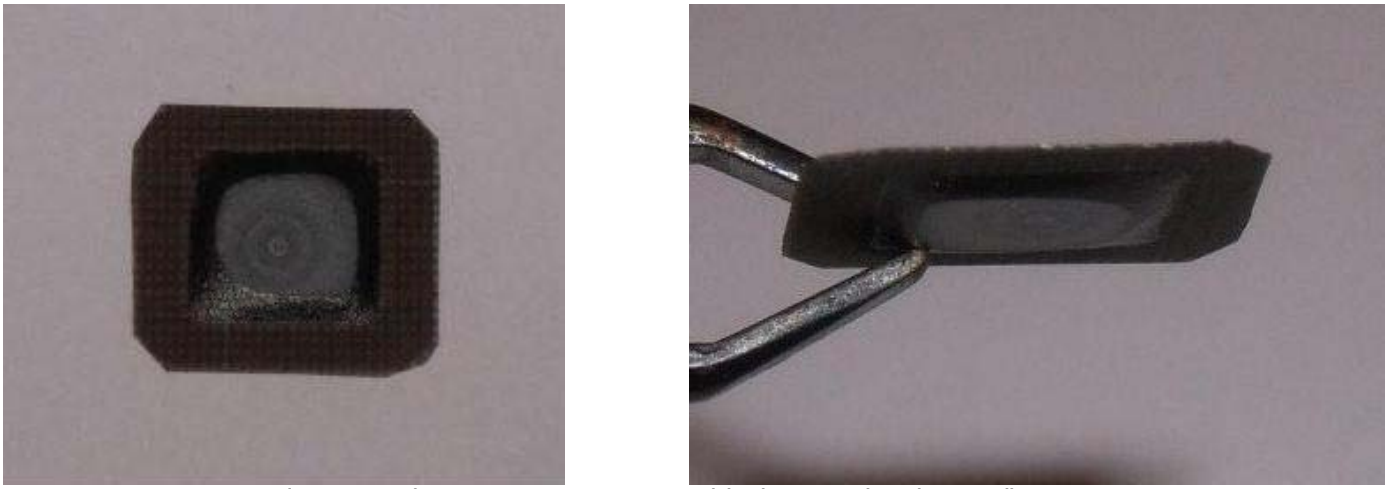


Figure 1- Athena IDProtect Duo PIV chip (mounted and potted)

1.3 CRYPTOGRAPHIC MODULE BOUNDARY

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

The CM will typically be embedded into a plastic smart card body and connected to an ISO 7816 compliant contact plate and an ISO 14443 compliant antenna. The CM boundary separates the chip from the card, contact plate and antenna.

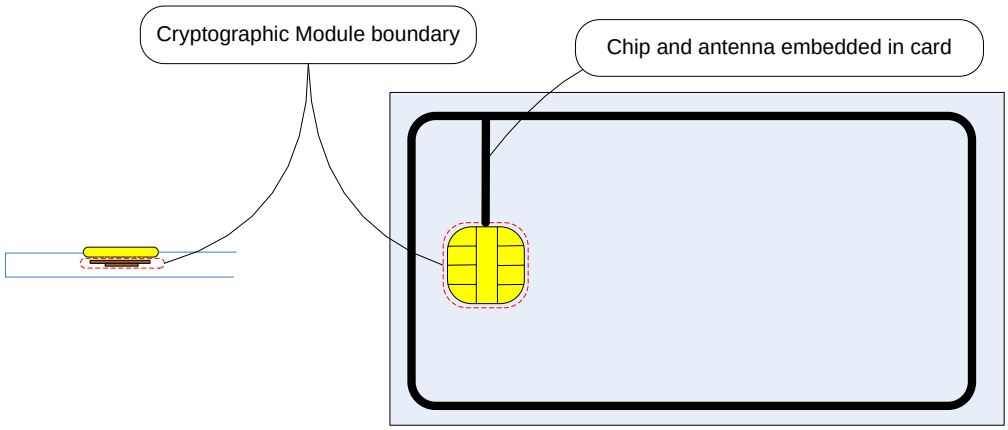


Figure 2- Athena IDProtect Duo PIV CM and connectors

1.4 HARDWARE

The Atmel secureAVR family is a low-power, high-performance, 8-/16-bit microcontroller with ROM program memory, EEPROM code or data memory, based on an enhanced RISC architecture.

By executing powerful instructions in a single clock cycle, the Atmel secureAVR family 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 Atmel secureAVR family allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data as well as a number of functional and security features.

The Atmel secureAVR family features high-performance EEPROM (fast erase/write time, high endurance). 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 Atmel secureAVR family is the new AdvX, an N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. All cryptographic routines are executed on the secureAVR 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 ID applications.

The CM chip is an Atmel AT90SC12872RCFT Revision M.

1.5 FIRMWARE

The embedded operating system is GlobalPlatform and Java Card compliant, is loaded on an Atmel secureAVR family smart card chip and 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 2.2.2, March 2006
- Application Programming Interface, Java Card Platform, Version 2.2.2, March 2006
- Virtual Machine Specification, Java Card Platform, Version 2.2.2, March 2006

Communication

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

The GlobalPlatform external interface and internal API allows for application loading and deletion and for secure communication between an application and a terminal. In particular, it allows for the loading of a special application called a Supplementary Security Domain that allows an Application Provider to separate their key space from the Card Administrator.

The Java Card API provides a large set of cryptographic services. Some of these services rely on 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-, 192- and 256-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

1.6 SOFTWARE

The PIV Applet is written in Java (as limited by the Java Card standards).

2 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	3
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 2 – Security Level of Security Requirements

3 CRYPTOGRAPHIC MODULE SPECIFICATION

This module includes the Issuer Security Domain which allows the Card Issuer to manage the operating system and card content, and the PIV Applet that provides the end-point services specified in [800-73-1].

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).

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

3.1 PHYSICAL INTERFACES

This module includes two distinct and non-concurrent physical interfaces.

3.1.1 Contact mode

This module provides a contact interface that is fully compliant with ISO/IEC 7816.

Interface	Description
RST	External Reset signal
I/O	Input/Output
CLK	External Clock signal 1 – 10.1MHz
VCC	Supply Voltage Power 1.62 – 5V
GRD	Ground

Table 3 – Contact Physical Interfaces

This module supports two transmission half-duplex oriented protocols: T=0 and T=1.

Up to 256 bytes of data can be exchanged through one APDU command.

3.1.2 Contactless mode

This module provides a contactless interface that is fully compliant with ISO/IEC 14443.

It uses two electrical connections 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.

3.2 LOGICAL INTERFACES

The cryptographic module functions as a slave processor to process 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	RF1/2 Pin
Data Out	I/O Pin	RF1/2 Pin
Status Out	I/O Pin	RF1/2 Pin
Control In	I/O, CLK and RST Pins	RF1/2 Pin

Table 4 – Logical Interfaces

4 MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the Athena IDProtect Duo PIV CM is to be integrated into a FIPS 201 end-point compliant PIV smart card as a dual interface chip.

4.1 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 #368.
- A hardware random number generator (HRNG) that is used to seed the DRNG.

4.2 CRYPTOGRAPHIC ALGORITHMS

The module includes the following cryptographic algorithms:

- SHA-1 and SHA-256
  CAVP SHS Certificate #680
- TDES
  CAVP TDES Certificate #598
  - Encrypt/decrypt (for confidentiality purposes)
  - MAC (vendor affirmed, for integrity and authentication purposes)
  - CBC and ECB modes
  - 112- and 168-bit key lengths
- AES
  CAVP AES Certificate #646
  - Encrypt/decrypt
  - CBC and ECB modes
  - 128-, 192- and 256-bit key lengths
- RSA
  CAVP RSA Certificate #296
  - PKCS#1 sign/verify
  - 1024- and 2048-bit key lengths

The module supports the following non-FIPS Approved algorithms:

- RSA encrypt/decrypt (key wrapping; key establishment methodology provides between 80- and 112-bits of encryption strength)

4.3 CRITICAL SECURITY PARAMETERS

This module includes the following CSPs.

No interface is provided to retrieve any CSP.

See Section 7.5 KEY AND PIN MANAGEMENT SECURITY RULES for the Type, Length and Strength of each CSP.

Key Secure Storage Key

This CSP (KSSK) is a TDES Key used to encrypt all other secret and private keys of this module when stored in EEPROM (that is, all TDES, AES and RSA keys).

It is generated at first reset of the card using the DRNG.

Keys secured with the KSSK are encrypted when created and decrypted each time they are used.

PIN Secure Storage Key

This CSP (PSSK) is a TDES Key used to encrypt all PINs of this module when stored in EEPROM (that is, Java Card OwnerPIN objects).

It is generated at first reset of the card using the DRNG.

PIN values are encrypted when created and never decrypted. Candidate PINs are encrypted with PSSK to perform the comparison.

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 using Secure Channel Protocol 01 option 05:

- CA-Kenc: Used to derive CA Session Key that will encrypt command data within a Secure Channel Session with C-DECRYPTION Security Level.
- CA-Kmac: Used to derive CA Session Key that will guarantee integrity of any data within a Secure Channel Session with C-MAC Security Level.
- CA-Kkek: Key Encryption Key used to encrypt the CA ISD Key Sets that are loaded in the CM with the 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 using Secure Channel Protocol 01 option 05. These two keys are used to secure exchanges from the Card Administrator to the ISD:

- CA-Senc: Encryption Session Key used to encrypt data exchanged within a Secure Channel Session with C-DECRYPTION Security Level.
- CA-Smac: MAC Session Key used to guarantee integrity of any data exchanged within a Secure Channel Session with C-MAC Security Level and to authenticate the Card Administrator.

PIV User PIN

This CSP is the PIV User PIN available on the PIV Applet API. It is created by the PIV Applet (as a Java OwnerPIN object) and is used to authenticate the PIV User.

PIV User PIN Unblock PIN (PUK)

This CSP is the PIN that is used to unblock the PIV User PIN. It is created by the PIV Applet (as a Java OwnerPIN object).

PIV Card Application Administration Key

This CSP is a TDES or AES key that is used to establish and control access to the data objects and keys within the PIV Applet.

PIV Authentication Key

This CSP is the RSA Private Key that corresponds to the X.509 Certificate for PIV Authentication as defined in the PIV specifications (see [SP800-73-1]). Only the PIV User can use this key and only the PIV Application Administrator can generate or replace this key.

PIV Card Application Digital Signature Key

This CSP is the RSA Private Key that corresponds to the X.509 Certificate for Digital Signature as defined in the PIV specifications (see [SP800-73-1]). Only the PIV User can use this key and only the PIV Application Administrator can generate or replace this key.

PIV Card Application Key Management Key

This CSP is the RSA Private Key that corresponds to the X.509 Certificate for Key Management as defined in the PIV specifications (see [SP800-73-1]). Only the PIV User can use this key and only the PIV Application Administrator can generate or replace this key.

PIV Card Authentication Key

This CSP is a TDES, AES or RSA Private Key used for card authentication. If it is a RSA Private Key it corresponds to the X.509 Certificate for PIV Card Authentication as defined in the PIV specifications (see [SP800-73-1]). Any User can use this key and only the PIV Application Administrator can generate or replace this key.

Public PIV Authentication Key

This CSP is the RSA Public key that is generated by the card and used to create the X.509 Certificate for PIV Authentication as defined in the PIV specifications (see [SP800-73-1]). This key is returned by the card when the matching RSA Private Key is generated. Only the PIV Application Administrator can generate this key. This key is not stored on the card when it is generated. No card services can use this key.

Public PIV Card Application Digital Signature Key

This CSP is the RSA Public key that is generated by the card and used to create the X.509 Certificate for PIV Card Application Digital Signature as defined in the PIV specifications (see [SP800-73-1]). This key is returned by the card when the matching RSA Private Key is generated. Only the PIV Application Administrator can generate this key. This key is not stored on the card when it is generated. No card services can use this key.

Public PIV Card Application Key Management Key

This CSP is the RSA Public key that is generated by the card and used to create the X.509 Certificate for PIV Card Application Key Management as defined in the PIV specifications (see [SP800-73-1]). This key is returned by the card when the matching RSA Private Key is generated. Only the PIV Application Administrator can generate this key. This key is not stored on the card when it is generated. No card services can use this key.

Public PIV Card Authentication Key

If the PIV Card Authentication Key is a RSA Private Key, this CSP is the RSA Public key that is generated by the card and used to create the X.509 Certificate for PIV card authentication as defined in the PIV specifications (see [SP800-73-1]). This key is returned by the card when the matching RSA Private Key is generated. Only the PIV Application Administrator can generate this key. This key is not stored on the card when it is generated. No card services can use this key.

5 ROLES AND SERVICES

5.1 ROLES

Cryptographic Officer Roles	
Card Administrator	This role is responsible for managing the security configuration of the module and for managing the security configuration of a loaded 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), which is the embedded Security Domain (SD) associated with the PIV Applet. Once authenticated, the Card Administrator is able to execute the services provided by the ISD in a Secure Channel Session (see [GP] for more details).
User Roles	
PIV Application Administrator	This role has knowledge of the PIV Card Application Administration Key and is allowed to perform PIV Applet personalization tasks. The PIV Application Administrator authenticates to the module through the PIV Applet by properly completing a challenge/response authentication using the PIV Card Application Administration Key. The PIV Application Administrator is allowed to perform the GENERAL AUTHENTICATE, PUT DATA and GENERATE ASYMMETRIC KEY PAIR commands in the PIV Applet.
PIV User	This role has knowledge of the PIV User PIN and can perform cryptographic operations using the keys stored in the PIV Applet. The PIV User authenticates to the module through the PIV Applet by presenting the PIV User PIN. The PIV User is allowed to perform the GET DATA, VERIFY, GENERAL AUTHENTICATE and CHANGE REFERENCE DATA commands in the PIV Applet.
PIV PIN Administrator	This role has knowledge of the PIV User PIN Unblock PIN (PUK) and can unblock the PIV User PIN and establish a new PIV User PIN. The PIV PIN Administrator authenticates to the module through the PIV Applet by presenting the PUK in the CHANGE REFERENCE DATA or RESET RETRY COUNTER APDU commands. The PIV PIN Administrator is allowed to perform the CHANGE REFERENCE DATA and RESET RETRY COUNTER APDU commands in the PIV Applet.

No Roles	
Public Operator	No-role operator who does not know any secrets related to the ISD or PIV Applet. This non-authenticated operator can only access non-security relevant services provided by the ISD and PIV Applet that do not require any prior authentication.
Maintenance Roles	
None	This CM does not support any maintenance role.

Table 5 - Roles description

5.2 IDENTIFICATION

This Cryptographic Module performs identity based authentication using cryptographic keys and PINs. A unique identifier is associated with each cryptographic key and PIN to uniquely identify the operator performing the authentication.

The ISD cryptographic keys are identified by a two-byte value, Key Version Number (KVN) and Key ID (KID), as defined in the GlobalPlatform standard (see [GP]).

The PIV cryptographic keys and PINs are identified by a one-byte value as defined in the PIV standard (see [SP800-73-1]).

Identity Authentication	
CA ISD Key Set	KVN, KID
PIV User PIN	80
PIV User PIN Unblock PIN (PUK)	81
PIV Authentication Key	9A
PIV Card Application Administration Key	9B
PIV Card Application Digital Signature Key	9C
PIV Card Application Key Management Key	9D
PIV Card Authentication Key	9E

Table 6 – Identity Authentication

5.3 ROLE AUTHENTICATION

Role Authentication services are not similar in contact and contactless modes: all roles can authenticate in contact mode, whereas some roles are not allowed to authenticate in contactless mode.

Role Authentication	Contact	Contactless
Card Administrator	Yes	Yes
PIV Application Administrator	Yes	No
PIV User	Yes	No
PIV PIN Administrator	Yes	No

Table 7 – Role Authentication Applicable Modes

5.3.1 Card Administrator Authentication

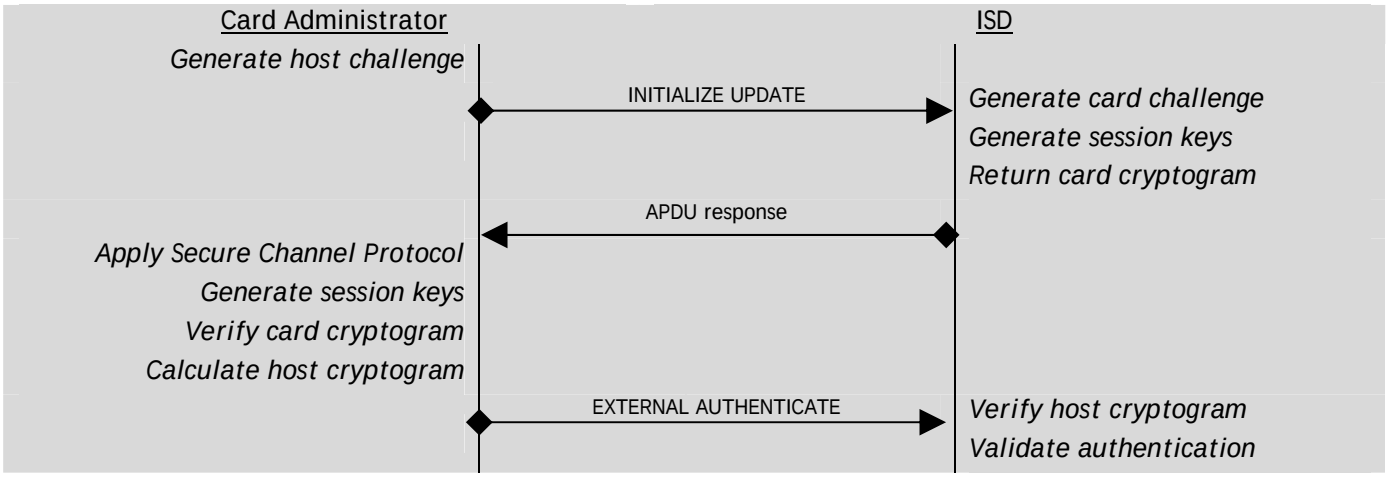
This Cryptographic Module supports identity based authentication of the Card Administrator in both contact and contactless modes. For this mechanism, the two following properties stand:

- 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

This mechanism includes a counter of failed authentication and a blocking mechanism. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication. The authentication mechanism is blocked when the associated counter reaches zero. The counter threshold is in the range one to 255 with default value 80. This mechanism is called velocity checking (see [GP]).

If the authentication mechanism of the ISD is blocked the CM is irreversibly 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 GET DATA (ISD) APDU command is available).

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



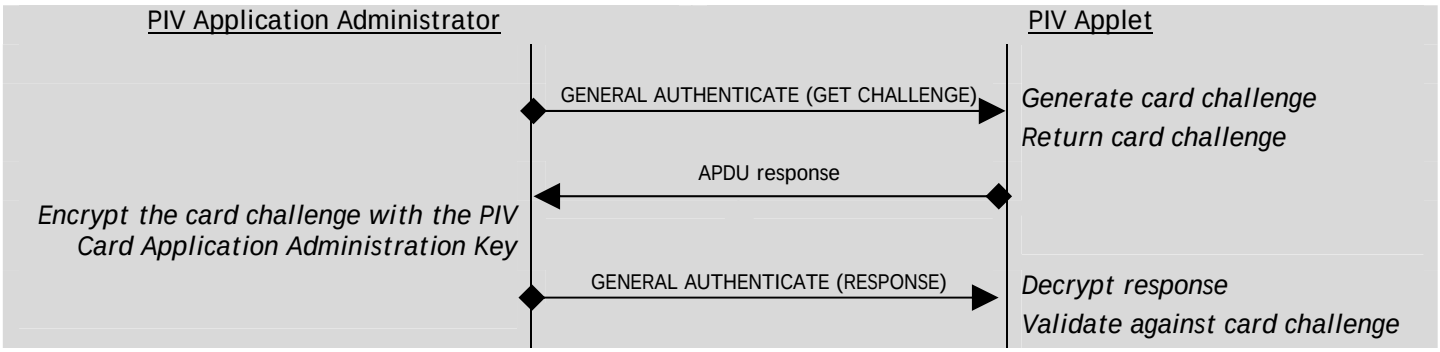
5.3.2 PIV Application Administrator Authentication

This Cryptographic Module supports identity based authentication of the PIV Application Administrator only in contact mode. For this mechanism, the two following properties stand:

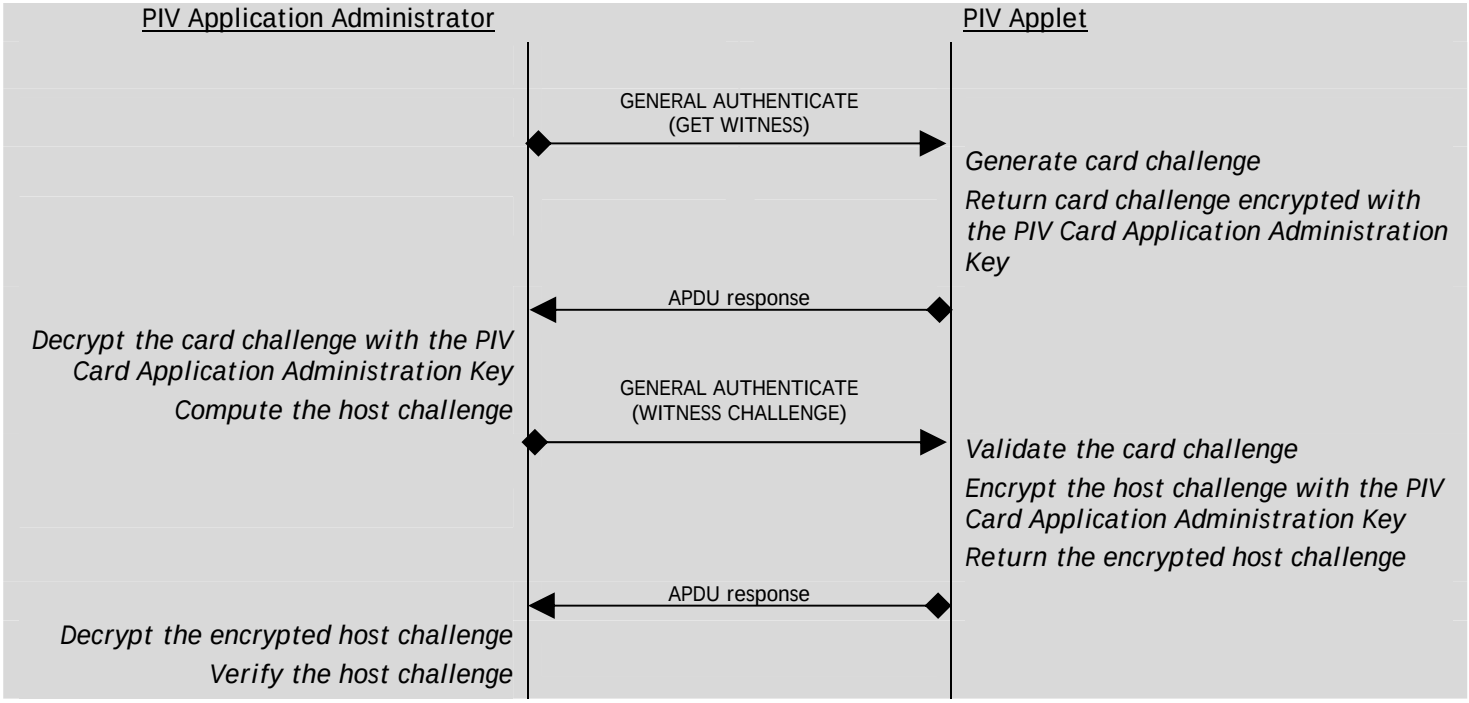
- the probability is less than one in 1,000,000 that a random attempt at authentication will succeed
- during any one minute period, the probability is less than 1 in 100,000 that a random authentication attempt will succeed

The PIV Application Administrator authenticates by performing a GENERAL AUTHENTICATE command sequence with either the EXTERNAL or MUTUAL AUTHENTICATE protocol.

The following diagram illustrates the EXTERNAL AUTHENTICATE APDU command sequence.



The following diagram illustrates the MUTUAL AUTHENTICATE APDU command sequence.



5.3.3 PIV User Authentication

This Cryptographic Module supports identity based authentication of the PIV User in contact mode only. For this mechanism, the two following properties stand:

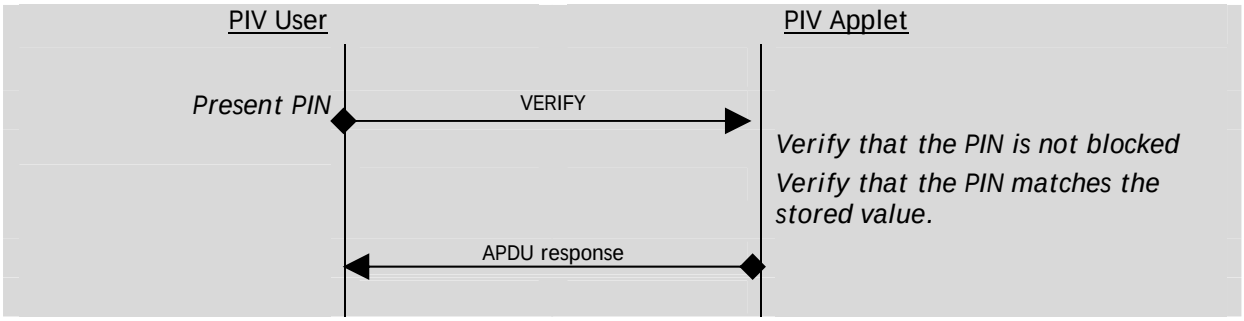
- the probability is less than one in 1,000,000 that a random attempt at authentication will succeed
- during any one minute period, the probability is less than 1 in 100,000 that a random authentication attempt will succeed

This mechanism includes a counter of failed authentication and a blocking mechanism. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication. The authentication mechanism is blocked when the associated counter reaches zero. The counter threshold is in the range one to 15 with default value 5. This mechanism is called velocity checking (see [GP]).

The PIV User PIN consists of a minimum of three and a maximum of eight bytes. Each byte may take a value from '00' to 'FE' ('FF' is not a valid value).

If the authentication mechanism is blocked the PIV PIN Administrator must unblock the PIV User PIN before any authentication of the PIV User is allowed to proceed.

The PIV User is authenticated to the PIV Applet through the use of the VERIFY APDU command. The following diagram illustrates the VERIFY command.



5.3.4 PIV PIN Administrator Authentication

This Cryptographic Module supports identity based authentication of the PIV PIN Administrator in contact mode only. For this mechanism, the two following properties stand:

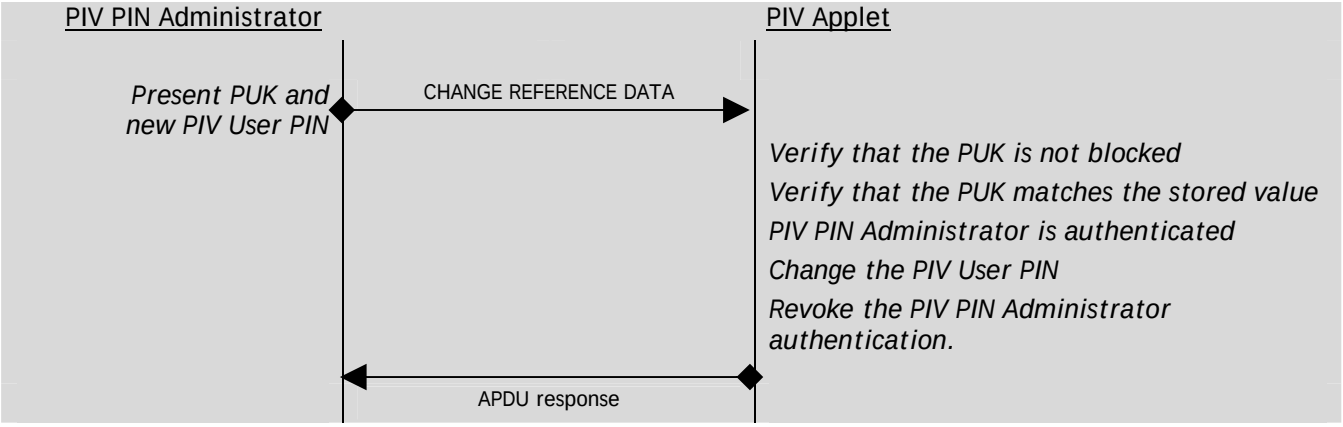
- the probability is less than one in 1,000,000 that a random attempt at authentication will succeed
- during any one minute period, the probability is less than 1 in 100,000 that a random authentication attempt will succeed

This mechanism includes a counter of failed authentication and a blocking mechanism. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication. The authentication mechanism is blocked when the associated counter reaches zero. The counter threshold is in the range one to 15 with default value 5. This mechanism is called velocity checking (see [GP]).

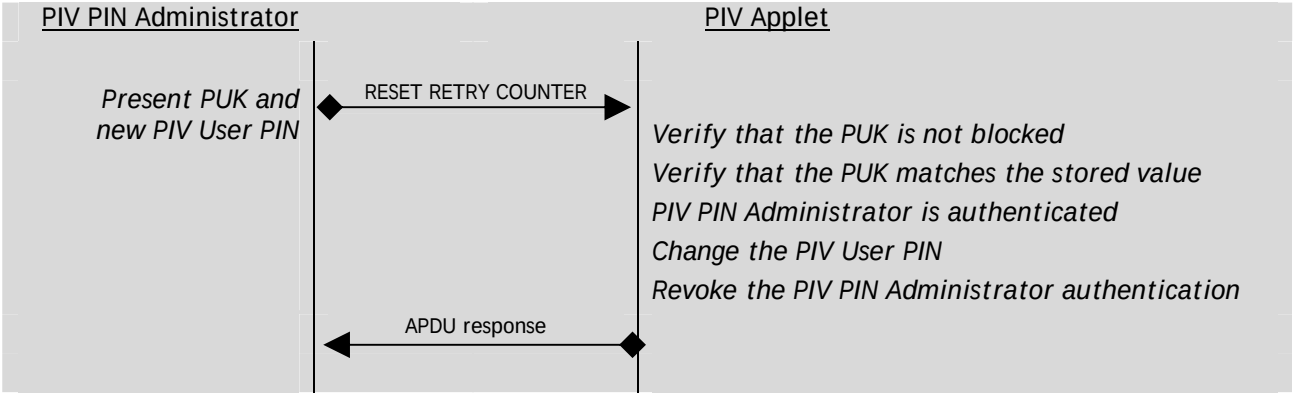
The PIV User PIN Unblock PIN (PUK) consists of a minimum of three and a maximum of eight bytes. Each byte may take a value from '00' to 'FE' ('FF' is not a valid value).

If the authentication mechanism of the PIV PIN Administrator is blocked the PIV PIN Administrator is no longer able to authenticate.

The PIV PIN Administrator is authenticated only during the successful execution of the PIV CHANGE REFERENCE DATA or PIV RESET RETRY COUNTER APDU commands. The following diagram illustrates the CHANGE REFERENCE DATA APDU command.



This diagram illustrates the RESET RETRY COUNTER APDU command.



5.4 SERVICES

Some services are not available in contactless mode. Each table describing the services includes two columns where the availability of each service is discussed in contact (C) and contactless (CL) modes.

5.4.1 Card Administrator Services

This role can only be active when the ISD is currently selected.

		C	CL
Authentication			
INITIALIZE UPDATE	CA can initiate a GlobalPlatform Secure Channel Session using the CA ISD Key Set indicated by the key set version and index.	X	X
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.	X	X
Card Content Management			
INSTALL	CA can initiate or perform the various steps required for CM content management, including installation of the PIV Applet.	X	X
LOAD	CA can transfer a Load File to the CM.	X	X
DELETE (card content)	CA can delete a uniquely identifiable object such as an Executable Load File (package) or an Application (applet) or an Executable Load File and its related Applications.	X	X
PUT KEY	Regarding ISD keys, 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	X	X
DELETE (key)	CA can delete an ISD key uniquely identified by the KID and KVN.	X	X
SET STATUS	CA can modify the Card Life Cycle State or an associated Application, including PIV Applet, Life Cycle State.	X	X
GET STATUS	CA can retrieve Life Cycle status information of the ISD, and all Executable Load Files, Executable Modules, Applications (including PIV Applet) or Security Domains.	X	X
STORE DATA	CA can transfer data to the ISD.	X	X
Public Commands			
SELECT	Operator can select an Application. This command also logs out the current role.	X	X
GET DATA (ISD)	Operator can retrieve public data from the ISD. No CSPs can be read using this service.	X	X
GET DATA (PIV Public)	Operator can retrieve public data from the PIV Applet: Card Capabilities Container, CHUID, Security Object and X.509 Certificates. No CSPs can be read using this service.	X	X

GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE) PIV Card Authentication Key	Operator can authenticate the card to the terminal by performing the INTERNAL AUTHENTICATE APDU command sequence with the PIV Card Authentication Key.	X	X

5.4.2 PIV Application Administrator Services

This role can only be active when the PIV Applet is currently selected.

		C	CL
Authentication			
GENERAL AUTHENTICATE (EXTERNAL AUTHENTICATE)	PIV Application Administrator can authenticate by performing the EXTERNAL AUTHENTICATE APDU command sequence with the PIV Card Application Administrator Key.	X	-
GENERAL AUTHENTICATE (MUTUAL AUTHENTICATE)	PIV Application Administrator can authenticate by performing the MUTUAL AUTHENTICATE APDU command sequence with the PIV Card Application Administrator Key.	X	-
PIV Application Administration			
GENERATE ASYMMETRIC KEY PAIR	PIV Application Administrator can generate and store in the PIV Applet the PIV Authentication Key, PIV Card Application Digital Signature Key, PIV Card Application Key Management Key and PIV Card Authentication Key (if it is an RSA Private Key).	X	-
PUT DATA	PIV Application Administrator can replace the contents of PIV data objects.	X	-
Cryptographic Operations			
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)	PIV Application Administrator can authenticate the card to the terminal by performing the INTERNAL AUTHENTICATE APDU command sequence with the PIV Card Application Administrator Key.	X	-
Public Commands			
SELECT	Operator can select an Application. This command also logs out the current role.	X	X
GET DATA (ISD)	Operator can retrieve public data from the ISD. No CSPs can be read using this service.	X	X
GET DATA (PIV Public)	Operator can retrieve public data from the PIV Applet: Card Capabilities Container, CHUID, Security Object and X.509 Certificates. No CSPs can be read using this service.	X	X
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE) PIV Card Authentication Key	Operator can authenticate the card to the terminal by performing the INTERNAL AUTHENTICATE APDU command sequence with the PIV Card Authentication Key.	X	X

5.4.3 PIV User Services

This role can only be active when the PIV Applet is currently selected.

		C	CL
Authentication			
VERIFY	PIV User can authenticate by presenting the PIV User PIN in the VERIFY APDU command.	X	-
Card Content Management			
CHANGE REFERENCE DATA	PIV User can change the PIV User PIN.	X	-
GET DATA (PIV User)	PIV User can retrieve any of the PIV data objects.	X	-
Cryptographic Operations			
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)	PIV User can authenticate the card to the terminal by performing the INTERNAL AUTHENTICATE APDU command sequence with the PIV Authentication Key, PIV Card Application Digital Signature Key and PIV Card Application Key Management Key.	X	-
Public Commands			
SELECT	Operator can select an Application. This command also logs out the current role.	X	X
GET DATA (ISD)	Operator can retrieve public data from the ISD. No CSPs can be read using this service.	X	X
GET DATA (PIV Public)	Operator can retrieve public data from the PIV Applet: Card Capabilities Container, CHUID, Security Object and X.509 Certificates. No CSPs can be read using this service.	X	X
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE) PIV Card Authentication Key	Operator can authenticate the card to the terminal by performing the INTERNAL AUTHENTICATE APDU command sequence with the PIV Card Authentication Key.	X	X

5.4.4 PIV PIN Administrator Services

This role can only be active when the PIV Applet is currently selected.

		C	CL
Authentication and PIV PIN Administration			
CHANGE REFERENCE DATA	The PIV PIN Administrator can change the PIV User PIN Unblock PIN (PUK).	X	-
RESET RETRY COUNTER	The PIV PIN Administrator can change the PIV User PIN.	X	-
Public Commands			
SELECT	Operator can select an Application. This command also logs out the current role.	X	X
GET DATA (ISD)	Operator can retrieve public data from the ISD. No CSPs can be read using this service.	X	X
GET DATA (PIV Public)	Operator can retrieve public data from the PIV Applet: Card Capabilities Container, CHUID, Security Object and X.509 Certificates. No CSPs can be read using this service.	X	X
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE) PIV Card Authentication Key	Operator can authenticate the card to the terminal by performing the INTERNAL AUTHENTICATE APDU command sequence with the PIV Card Authentication Key.	X	X

5.4.5 Public Operator Services

		C	CL
Public Commands			
SELECT	Operator can select an Application to which subsequent commands are routed. The response contains various data depending on the application that is selected.	X	X
GET DATA (ISD)	Operator can retrieve public data from the ISD. No CSPs can be read using this service.	X	X
GET DATA (PIV Public)	Operator can retrieve public data from the PIV Applet: Card Capabilities Container, CHUID, Security Object and X.509 Certificates. No CSPs can be read using this service.	X	X
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE) PIV Card Authentication Key	Operator can authenticate the card to the terminal by performing the INTERNAL AUTHENTICATE APDU command sequence with the PIV Card Authentication Key.	X	X

5.4.6 Relationship between services and roles

5.4.6.1 Contact

	Card Administrator	PIV Application Administrator	PIV User	PIV PIN Administrator	Public Operator
SELECT	X	X	X	X	X
DELETE (card content)	X				
DELETE (key)	X				
EXTERNAL AUTHENTICATE	X				
GET DATA (ISD)	X	X	X	X	X
GET STATUS	X				
INITIALIZE UPDATE	X				
INSTALL	X				
LOAD	X				
PUT KEY	X				
SET STATUS	X				
STORE DATA	X				
CHANGE REFERENCE DATA			X	X	
GENERATE ASYMMETRIC KEY PAIR		X			
GENERAL AUTHENTICATE (EXTERNAL AUTHENTICATE)		X[1]			
GENERAL AUTHENTICATE (MUTUAL AUTHENTICATE)		X[1]			
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)		X[1]	X[2]		
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE) PIV Card Authentication Key	X	X	X	X	X
GET DATA (PIV User)			X		
GET DATA (PIV Public)	X	X	X	X	X
PUT DATA		X			
RESET RETRY COUNTER				X	
VERIFY			X		

Table 8 - Services and associated roles (Contact)

[1] PIV Card Application Administrator Key

[2] PIV Authentication Key
PIV Card Application Digital Signature Key
PIV Card Application Key Management Key

5.4.6.2 Contactless

	Card Administrator	PIV Application Administrator	PIV User	PIV PIN Administrator	Public Operator
SELECT	X	X	X	X	X
DELETE (card content)	X				
DELETE (key)	X				
EXTERNAL AUTHENTICATE	X				
GET DATA (ISD)	X	X	X	X	X
GET STATUS	X				
INITIALIZE UPDATE	X				
INSTALL	X				
LOAD	X				
PUT KEY	X				
SET STATUS	X				
STORE DATA	X				
CHANGE REFERENCE DATA					
GENERATE ASYMMETRIC KEY PAIR					
GENERAL AUTHENTICATE (EXTERNAL AUTHENTICATE)					
GENERAL AUTHENTICATE (MUTUAL AUTHENTICATE)					
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)					
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE) PIV Card Authentication Key	X	X	X	X	X
GET DATA (PIV User)					
GET DATA (PIV Public)	X	X	X	X	X
PUT DATA					
RESET RETRY COUNTER					
VERIFY					

Table 9 - Services and associated roles (Contactless)

5.4.7 Relationship between services and CSPs

Relationship can be:

- Write
- Generate
- Execute (computation involving the CSP)
- Delete
- Zeroize

Key Secure Storage Key

Service	Type of access
First Card reset	Generate
INITIALIZE UPDATE	Execute
EXTERNAL AUTHENTICATE	Execute
LOAD	Execute
PUT KEY	Execute
SET STATUS (TERMINATED)	Zeroize

PIN Secure Storage Key

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

CA ISD Key Set

Service	Type of access	Key
INITIALIZE UPDATE	Execute	CA-Kenc, CA-Kmac
EXTERNAL AUTHENTICATE	Execute	CA-Kenc, CA-Kmac
PUT KEY	Execute/Write	CA-Kenc, CA-Kmac, CA-Kkek
DELETE (key)	Delete	CA-Kenc, CA-Kmac, CA-Kkek

CA Session Key Set

Service	Type of access	Key
INITIALIZE UPDATE	Generate	CA-Senc, CA-Smac
Card reset	Delete	CA-Senc, CA-Smac

In a Secure Channel Session with Security Level C-MAC:

Service	Type of access	Key
DELETE	Execute	CA-Smac
EXTERNAL AUTHENTICATE	Execute	CA-Smac
GET DATA (ISD)	Execute	CA-Smac
GET STATUS	Execute	CA-Smac
INSTALL	Execute	CA-Smac
LOAD	Execute	CA-Smac
PUT KEY	Execute	CA-Smac
SET STATUS	Execute	CA-Smac
STORE DATA	Execute	CA-Smac

In a Secure Channel Session with Security Level C-DECRYPTION and C-MAC:

Service	Type of access	Key
DELETE (card content)	Execute	CA-Senc, CA-Smac
DELETE (key)	Execute	CA-Senc, CA-Smac
EXTERNAL AUTHENTICATE	Execute	CA-Senc, CA-Smac
GET DATA (ISD)	Execute	CA-Senc, CA-Smac
GET STATUS	Execute	CA-Senc, CA-Smac
INSTALL	Execute	CA-Senc, CA-Smac
LOAD	Execute	CA-Senc, CA-Smac
PUT KEY	Execute	CA-Senc, CA-Smac
SET STATUS	Execute	CA-Senc, CA-Smac
STORE DATA	Execute	CA-Senc, CA-Smac

PIV User PIN

Service	Type of access
PIV Applet instantiate	Generate
VERIFY	Execute
CHANGE REFERENCE DATA (PIV User PIN)	Execute/Write
RESET RETRY COUNTER	Write
SET STATUS (TERMINATED)	Zeroize

PIV User PIN Unblock PIN (PUK)

Service	Type of access
PIV Applet instantiate	Generate
CHANGE REFERENCE DATA (PUK)	Execute/Write
RESET RETRY COUNTER	Execute
SET STATUS (TERMINATED)	Zeroize

PIV Card Application Administration Key

Service	Type of access
PIV Applet instantiate	Generate
GENERAL AUTHENTICATE (EXTERNAL AUTHENTICATE)	Execute
GENERAL AUTHENTICATE (MUTUAL AUTHENTICATE)	Execute
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)	Execute
SET STATUS (TERMINATED)	Zeroize

PIV Authentication Key

Service	Type of access
GENERATE ASYMMETRIC KEY PAIR	Generate
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)	Execute
SET STATUS (TERMINATED)	Zeroize

PIV Card Application Digital Signature Key

Service	Type of access
GENERATE ASYMMETRIC KEY PAIR	Generate
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)	Execute
SET STATUS (TERMINATED)	Zeroize

PIV Card Application Key Management Key

Service	Type of access
GENERATE ASYMMETRIC KEY PAIR	Generate
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)	Execute
SET STATUS (TERMINATED)	Zeroize

PIV Card Authentication Key

Service	Type of access
GENERATE ASYMMETRIC KEY PAIR	Generate
GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)	Execute
SET STATUS (TERMINATED)	Zeroize

Public PIV Authentication Key

Service	Type of access
GENERATE ASYMMETRIC KEY PAIR	Generate

Public PIV Card Application Digital Signature Key

Service	Type of access
GENERATE ASYMMETRIC KEY PAIR	Generate

Public PIV Card Application Key Management Key

Service	Type of access
GENERATE ASYMMETRIC KEY PAIR	Generate

Public PIV Card Authentication Key

Service	Type of access
GENERATE ASYMMETRIC KEY PAIR	Generate

5.5 SETTING MODULE IN APPROVED MODE OF OPERATION

The module is always in the approved mode of operation.

5.6 VERIFYING MODULE IS IN APPROVED MODE OF OPERATION

It is possible to verify that a module is in the approved mode of operation.

The Card Administrator must:

1. SELECT the ISD and send a GET DATA (ISD) 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 operating system.

Data Element	Length	Value	Version
IC type	2	'0107'	Atmel AT90SC12872RCFT Revision M
Operating system release date	2	'7099'	Firmware Version Part 1
Operating system release level	2	'0105'	Firmware Version Part 2

2. SELECT the PIV Applet and send a GET DATA (PIV) command with the tag '0103' and verify that the returned data contains fields as follows (other fields are not relevant here). This verifies the version of the PIV Applet.

Data Element	Length	Position	Value
Applet Version	2	0 - 1	'0100'

6 SELF-TESTS

6.1 POWER-ON SELF-TESTS

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

Cryptographic algorithm testing:

Known Answer Tests (KATs) are conducted for each cryptographic algorithm 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 (performs no further data or status input or output and must be reset).

Firmware integrity testing:

A standard CRC16 checksum is used to verify that no 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 firmware integrity verification. If a test fails the card is irreversibly 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 GET DATA (ISD) APDU command is available).

6.2 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 Load Test:

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

7 SECURITY RULES

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

7.1 PHYSICAL SECURITY

The Cryptographic Module (CM) is a single-chip implementation which Cryptographic boundaries encompass the chip. The physical component of the 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 metal cover), 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+

7.2 AUTHENTICATION SECURITY RULES

This CM implements authentication 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.

Each of these secrets has a unique object reference that is used by the external operator to identify them:

- The CA ISD Key Set represents the role of the Card Administrator
- The PIV Card Application Administration Key represents the role of the PIV Application Administrator
- The PIV User PIN represents the role of the PIV User
- The PIV User PIN Unblock PIN (PUK) represents the role of the PIV PIN Administrator

Note that only the Card Administrator can authenticate in contactless mode.

7.3 APPLICATION LIFECYCLE SECURITY RULES

Additional applications can be loaded in the module after card issuance as specified in GlobalPlatform. However, these additional applications must be FIPS 140-2 validated before being loaded.

- Application 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. Application loading is protected by a TDES MAC on every block of data.
- The application loading service is available before and after card issuance.
- The CA is responsible for application personalization and lifecycle management following GlobalPlatform.
- The CA is responsible for creating as many instances of loaded applets as required, according to card resources.

7.4 ACCESS CONTROL SECURITY RULES

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

- CA ISD Key Set must be loaded through a GlobalPlatform Secure Channel Session ensuring their integrity and confidentiality (112-bit TDES encryption for confidentiality and a 112-bit TDES MAC for integrity).
- The PIV User PIN, PIV User PIN Unblock PIN (PUK) and PIV Card Application Administration Key are loaded during manufacturing.
- The PIV Authentication Key, PIV Card Application Digital Signature Key and PIV Card Application Key Management Key are generated on card.
- If the PIV Card Authentication Key is an AES or TDES Key it is loaded during manufacturing, otherwise it is an RSA Private Key and is generated on card.

7.5 KEY AND PIN MANAGEMENT SECURITY RULES

7.5.1 Key and PIN Material

This card supports the following CSPs:

Key name (CSP)	Type	Length	Strength
Key Secure Storage Key	TDES	112-bits	80-bits
PIN Secure Storage Key	TDES	112-bits	80-bits
CA ISD Key Set	TDES	112-bits	80-bits
CA Session Key Set	TDES	112-bits	80-bits
PIV User PIN	PIN	24- to 64-bits in 4-bit increments	255^3 (~$1.7x10^7$)
PIV User PIN Unblock PIN (PUK)	PIN	24- to 64-bits in 4-bit increments	255^3 (~$1.7x10^7$)

Key name (CSP)	Type	Length	Strength
PIV Card Application Administration Key	TDES AES	112-bits 168-bits 128-bits 192-bits 256-bits	80-bits 112-bits 128-bits 192-bits 256-bits
PIV Authentication Key (both public and private keys)	RSA	1024-bits 2048-bits	80-bits 112-bits
PIV Card Application Digital Signature Key (both public and private keys)	RSA	1024-bits 2048-bits	80-bits 112-bits
PIV Card Application Key Management Key (both public and private keys)	RSA	1024-bits 2048-bits	80-bits 112-bits
PIV Card Authentication Key (if RSA, both public and private keys)	TDES AES RSA	112-bits 168-bits 128-bits 192-bits 256-bits 1024-bits 2048-bits	80-bits 112-bits 128-bits 192-bits 256-bits 80-bits 112-bits

This card can also support a range of symmetric and asymmetric keys:

Key name (CSP)	Type	Length	Strength
TDES keys	TDES	112-bits 168-bits	80-bits 112-bits
AES keys	AES	128-bits 192-bits 256-bits	128-bits 192-bits 256-bits
RSA keys	RSA	1024-bits 2048-bits	80-bits 112-bits

7.5.2 Key Generation

Key Secure Storage Key

PIN Secure Storage Key

These keys are generated at first reset of the card using the DRNG.

PIV Authentication Key (both public and private keys)

PIV Card Application Digital Signature Key (both public and private keys)

PIV Card Application Key Management Key (both public and private keys)

PIV Card Authentication Key (if RSA, both public and private keys)

These keys are generated by the PIV Application Administrator using the GENERATE ASYMMETRIC KEY PAIR service.

7.5.3 Key Derivation

CA Session Key Set

[GP] ISD Session keys are derived using Secure Channel Protocol 01 option 05 by the operating system 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).

7.5.4 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 key
- Replacing existing key set with new key set
- Adding a single new key
- Adding a new key set

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

7.5.5 Key and PIN Storage

Key Secure Storage Key (KSSK)

PIN Secure Storage Key (PSSK)

These keys are stored plaintext in EEPROM.

CA ISD Key Set

PIV Card Application Administration Key

PIV Authentication Key

PIV Card Application Digital Signature Key

PIV Card Application Key Management Key

PIV Card Authentication Key

These keys are stored encrypted with the TDES key KSSK in EEPROM. The CM also applies an integrity checksum to these keys.

CA Session Key Set

These keys are stored plaintext in RAM.

PIV User PIN, PIV User PIN Unblock PIN (PUK)

These PINs are stored encrypted with the TDES key PSSK in EEPROM. The CM also applies an integrity checksum to these PINs.

7.5.6 Key and PIN Output

No secret keys (TDES and AES), private keys (RSA) or PINs can be output from the module.

Public keys (RSA) are output from the module on completion of the GENERATE ASYMMETRIC KEY PAIR service.

7.5.7 Key and PIN Zeroization

The CM offers services to zeroize all the keys and PINs stored in EEPROM:

- The KSSK and PSSK are zeroized when Card lifecycle state is set to TERMINATED. The Card Administrator can achieve this explicitly using the SET STATUS APDU command, or a severe security event may occur (failure of an integrity check on patches, EEPROM code, PINs or keys). By zeroizing the KSSK and the PSSK, all other keys and PINs stored in the module are made irreversibly unusable.

The CM offers services to zeroize all keys stored in RAM:

- When a Secure Channel Session is closed for any reason other than power-off, the CM overwrites the session keys with random data from the DRNG. When a Secure Channel Session is closed due to a power-off, the session keys are lost as they are stored in RAM. The RAM is actively cleared to zero on the next power-on.

7.6 ELECTROMAGNETIC INTERFERENCE/COMPATIBILITY (EMI/EMC)

The Cryptographic Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

8 MITIGATION OF OTHER ATTACKS

Typical smart card attacks are Simple Power Analysis, Differential Power Analysis, Timing Analysis and Fault Induction that may lead to revealing sensitive information such as PINs 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 firmware 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 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.

9 SECURITY POLICY CHECK LIST

9.1 ROLES AND REQUIRED AUTHENTICATION

Role	Type of Authentication	Authentication Data
Card Administrator	TDES authentication	CA ISD Key Set
PIV Application Administrator	AES or TDES authentication	PIV Card Application Administration Key
PIV User	PIN	PIV User PIN
PIV PIN Administrator	PIN	PIV User PIN Unblock PIN (PUK)

Table 10- Roles and Required Identification and Authentication

9.2 STRENGTH OF AUTHENTICATION MECHANISM

Authentication Mechanism	Strength of Mechanism
TDES 112-bit authentication with CA ISD Key Set	2^{80}
TDES 112- and 168-bit authentication with PIV Card Application Administration Key	2^{80} and 2^{112}
AES 128-, 192- and 256-bit authentication with PIV Card Application Administration Key	2^{128}, 2^{192} and 2^{256}
PIN authentication with PIV User PIN and PIV User PIN Unblock PIN (PUK)	255^3 (~$1.7x10^7$)

Table 11- Strengths of Authentication Mechanisms

All these authentication objects except for the PIV Card Application Administration Key implement a limited retry counter.

9.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Administrator	Section 0 lists authorized services for this role
PIV Application Administrator	Section 0 lists authorized services for this role
PIV User	Section 5.4.3 lists authorized services for this role
PIV PIN Administrator	Section 5.4.4 lists authorized services for this role

Table 12- Services Authorized for Roles

9.4 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 13 - Mitigation of Other Attacks

10 REFERENCES

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS201]	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006 Change Notice 1, June 23, 2006
[SP800-73-1]	Interfaces for Personal Identity Verification, March 2006 Errata, May 2006
[JCRE]	Java Card™ 2.2.1 Runtime Environment Revision 1.0, 18 May 2000
[JCAPI]	Java Card™ 2.2.1 Application Programming Interface Revision 1.0, 18 May 2000
[JCVM]	Java Card™ 2.2.1 Virtual Machine Revision 1.0, 18 May 2000
[GP]	GlobalPlatform Card Specification, Version 2.1.1, March 2003
[7816-1]	ISO/IEC 7816-1, First edition 1998-10-15, Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics
[7816-2]	ISO/IEC 7816-3, First edition 1999-03-01, Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts
[7816-3]	ISO/IEC 7816-3, Third edition 2006-11-01, Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols
[7816-4]	ISO/IEC 7816-4, Second edition 2005-01-15, Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange

Table 14 - References

11 ACRONYMS AND DEFINITIONS

Acronym	Definition
AdvX	Advance Crypto
APDU	Application Protocol Data Unit
API	Application Programming Interface
AVR	Automatic Voltage Regulation
CA	Card Administrator
CM	Cryptographic Module
CSP	Critical Security Parameter
DRNG	Deterministic Random Number Generator
GP	GlobalPlatform
HRNG	Hardware Random Number Generator
ISD	Issuer Security Domain
KSSK	Key Secure Storage Key
KID	Key Identifier, see [GP]
KVN	Key Version Number, see [GP]
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standard
PSSK	PIN Secure Storage Key
PUK	PIV User PIN Unblock PIN
RNG	Random Number Generator

Table 15 – Acronyms and Definitions

[END OF THE DOCUMENT]