TecSec PIV Eagle Card - Contactless
FIPS 140-2 Cryptographic Module
Security Policy

Version: 1.0

Date: March 11, 2009

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

TecSec Inc., 1048 Dead Run Drive, McLean VA, 22101

CONTENTS

List of Figures

List of Tables

1 CRYPTOGRAPHIC MODULE OVERVIEW

1.1 INTRODUCTION

This document defines the Security Policy for the TecSec PIV Eagle Card - Contactless cryptographic module (CM). This module is validated to overall FIPS 140-2 Level 3 with all areas meeting Level 3 except Physical Security which has been verified to meet Level 4.

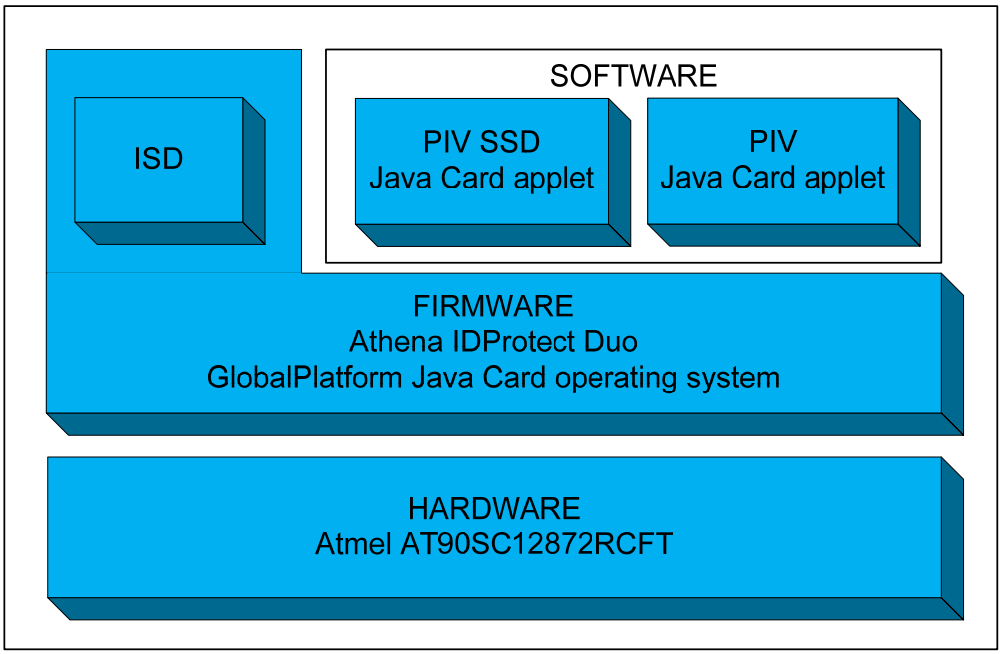
This document contains a description of the CM, its interfaces and services, the intended operators and the security policies enforced in the approved mode of operation.

The primary purpose of this device is to enable the creation of a dual-chip 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 an antenna as defined in [14443-1] and [14443-2] and communicates in T=CL as specified in [14443-3] and [14443-4].

The NPIVP Certificate associated with this module is PIV Card Application Cert. #11.

The CM is a hardware module which contains two Java Card applets implementing the PIV functionality (the software) running on a GlobalPlatform Java Card operating system (the firmware).



***Software*:**

P/N TecSec Contactless PIV Applet Version 1.0 JCL

***Firmware*:**

P/N Athena IDProtect Duo Version 0107.7099.0105

***Hardware*:**

P/N Atmel AT90SC12872RCFT Revision M

1.2 PHYSICAL CRYPTOGRAPHIC MODULE

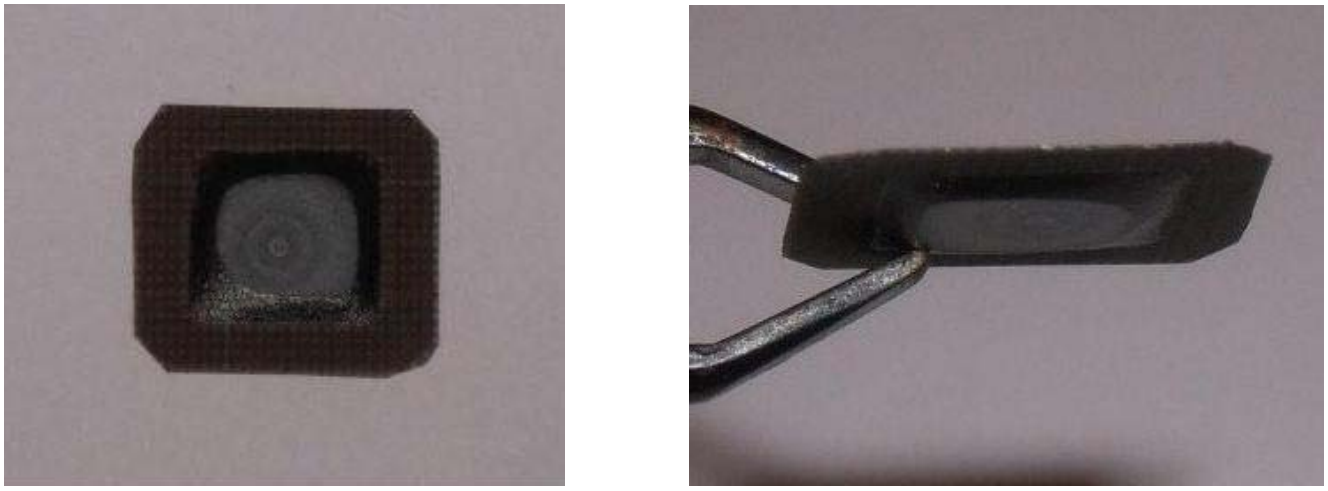


Figure 1 - TecSec PIV Eagle Card – Contactless (chip mounted and potted)

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 14443 compliant antenna. The CM boundary separates the chip from the card and antenna.

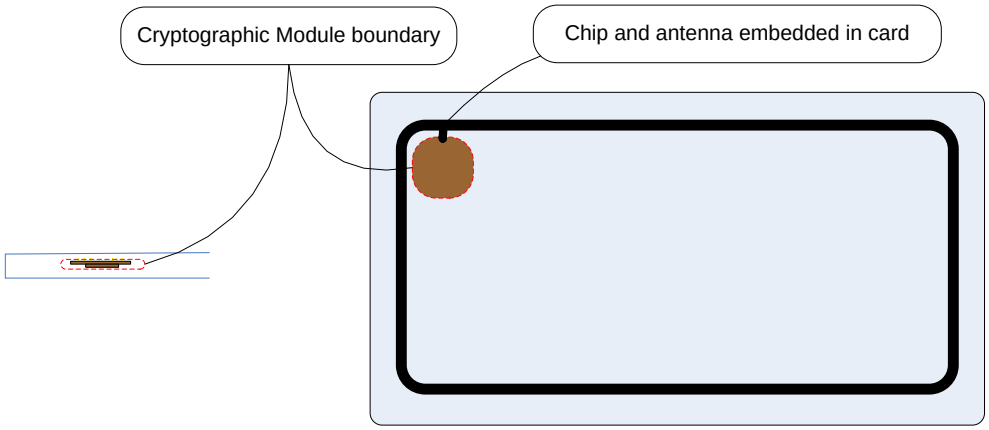


Figure 2- TecSec PIV Eagle Card - Contactless CM and connectors

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 protocol 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=CL over Type B

The GlobalPlatform external interface and internal API allows for application loading and unloading and for secure communication between applications. 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 (non-callable) in 32-bit increments

Table 1 – Supported Cryptographic Services

1.6 SOFTWARE

The PIV and PIV SSD applets are 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	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	NA
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

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 application 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).

The PIV application comprises two Java Card technology applets: the PIV applet itself and the PIV SSD applet that allows personalization of the PIV applet.

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. It is not intended that the contact interface will be connected.

3.1.1 Contact

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
GND	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

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	**Contact**	**Contactless**
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 TecSec PIV Eagle Card - Contactless CM is to be integrated into a FIPS 201 end-point compliant dual-chip PIV smart card as the contactless chip.

4.1 RANDOM NUMBER GENERATORS

The module includes the following Approved random number generators:

- An ANSI X9.31 112-bit key TDES deterministic random number generator (DRNG). CAVP RNG Certificate #368.

4.2 CRYPTOGRAPHIC ALGORITHMS

The module includes the following Approved 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
  - PKCS#1 Key Pair generation
  - 1024- and 2048-bit key lengths

The module supports the following FIPS non-Approved security functions:

- RSA PKCS#1 encrypt/decrypt (key wrapping; key establishment methodology provides 80-bits or 112-bits of encryption strength), this functionality is only used for interoperability purposes. This service is only used to authenticate the module to external systems.
- A hardware random number generator (HRNG) that is used for seeding the FIPS Approved DRNG.

4.3 CRITICAL SECURITY PARAMETERS

This module includes the following CSPs.

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 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.

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 SSD Key Set

This CSP is a set of three TDES keys used to manage GlobalPlatform Secure Channel Sessions between the SSD and the Application Provider using Secure Channel Protocol 01 option 05:

- PIVSSD-Kenc: Used to derive PIVSSD Session Key that will encrypt command data within a Secure Channel Session with C-DECRYPTION Security Level.
- PIVSSD-Kmac: Used to derive PIVSSD Session Key that will guarantee integrity of any data within a Secure Channel Session with C-MAC Security Level.
- PIVSSD-Kkek: Key Encryption Key used to encrypt the PIVSSD SSD Key Sets that are loaded in the CM with the PUT KEY APDU command within a Secure Channel Session.

PIV SSD Session Key Set

This CSP is a set of two TDES keys derived during the GlobalPlatform Secure Channel Session establishment from a selected PIV SSD Key Set using Secure Channel Protocol 01 option 05. These two keys are used to secure exchanges from the Application Provider to the PIV SSD:

- PIVSSD-Senc: Encryption Session Key used to encrypt data exchanged within a Secure Channel Session with C-DECRYPTION Security Level.

- PIVSSD-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 Application Provider.

RSA Private Keys

PIV Card Authentication Private Key

This CSP is the RSA Private Key that corresponds to the X.509 Certificate for PIV card authentication as defined in the PIV specifications (see [SP800-73-1]). Any Operator can use this key and only the PIV Application Provider can generate or replace this key. The CSP is not retrievable from the CM and is used by external systems to prove the identity of the CM, not the user. It is a CM Identity CSP.

RSA Public Keys

PIV Card Authentication Public 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 Provider can generate this key. This key is not stored on the card when it is generated.

RNG Seed Values

DRNG Seed and DRNG Seed Key

This CSP is an internal value computed using the NDRNG and stored in the processor RAM. These values are not accessible to any user. The hardware processor overwrites all RAM during reset which will destroy any prior values of the DRNG Seed and DRNG Seed Key. The DRNG is the only card service that uses these values.

NDRNG Seed

This CSP is an internal value computed during the initialization of the operating system. The seed value is initially placed into the NDRNG during the OS startup and is continually modified as the processor is powered. Therefore it is not possible to recover this value and is cleared during a power cycle. No user has access to this value.

5 ROLES AND SERVICES

5.1 ROLES

Cryptographic Officer Roles	
Card Administrator	This role is responsible for managing the security configuration of the module. 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 in a Secure Channel Session (see [GP] for more details).
User Roles	
PIV Application Provider	This role is responsible for managing the security configuration of a loaded application. The PIV Application Provider 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 Security Domain (SD) associated with the application. Once authenticated, the PIV Application Provider is able to execute the services provided by the application in a Secure Channel Session. This includes creating PIV RSA key pairs, putting PIV objects into the PIV applet and putting PIV RSA Private keys into the PIV applet.
No Roles	
Public Operator	No-role operator who does not know any secrets related to the ISD. This non-authenticated operator can only access non-security relevant services provided by the ISD that do not require any prior authentication. In addition the Public Operator can request authentication of the CM card, therefore requiring a signature generation request using the PIV Card Authentication Private Key. The Public Operator does not have the ability to create, modify, substitute, or disclose this key. The PIV Card Authentication Private Key is only used for CM authentication purposes, which is allowed per NIST IG3.1.
Maintenance Roles	
None	This CM does not support any maintenance role.

Table 5 - Roles description

5.2 IDENTIFICATION

This CM performs identity based authentication using cryptographic keys. A unique identifier is associated with each cryptographic key to uniquely identify the operator performing the authentication.

The ISD and PIV SSD 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 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 SSD Key Set	KVN, KID
PIV Card Authentication Key	9E

Table 6 – Identity Authentication

5.3 ROLE AUTHENTICATION

5.3.1 Card Administrator and PIV Application Provider Authentication

This CM supports identity based authentication of the Card Administrator and PIV Application Provider. For this mechanism, the two following properties stand:

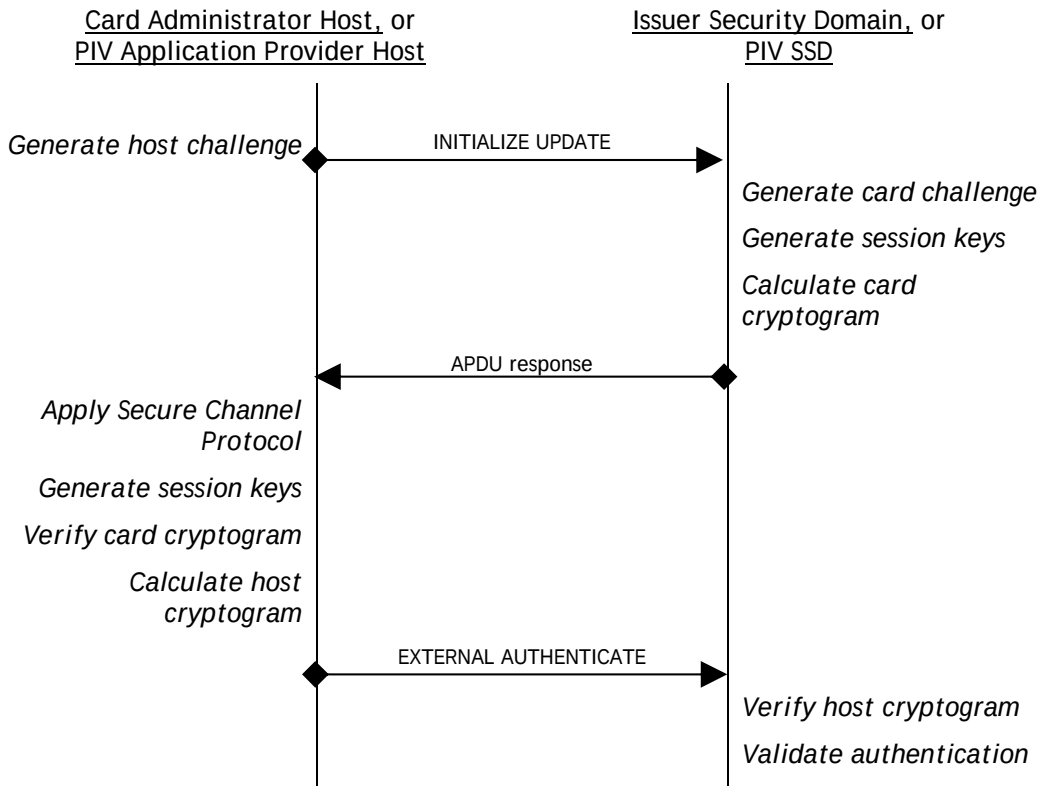
A 112 bit TDES key pair is used to authenticate to either of these roles, therefore providing a 1/2^80 probability that a single random authentication attempt will be successful.

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]).

- 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

If the authentication mechanism of the ISD is blocked the CM is irreversibly terminated (the KSSK is 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 and PIV Application Provider authenticate by opening a GlobalPlatform Secure Channel Session with the ISD and Security Domain respectively. This Secure Channel Session establishment involves two APDU commands as follows:



5.4 SERVICES

Identical services are available on the contact and contactless interfaces.

5.4.1 Card Administrator Services

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

Authentication	
INITIALIZE UPDATE	CA can initiate a GlobalPlatform Secure Channel Session, setting key set version and index.
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 CM content management.
LOAD	CA can transfer a Load File to the CM.
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.
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
DELETE (key)	CA can delete an ISD key uniquely identified by the KID and KVN.
SET STATUS	CA can modify the Card Life Cycle State or an associated Application Life Cycle State.
GET STATUS	CA can retrieve Life Cycle status information of the ISD, and all Executable Load File, Executable Module, Application or Security Domain.
STORE DATA	CA can transfer data to the ISD.

5.4.2 PIV Application Provider Services

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

Authentication	
INITIALIZE UPDATE	AP can initiate a GlobalPlatform Secure Channel Session, setting key set version and index.
EXTERNAL AUTHENTICATE	AP can open a GlobalPlatform Secure Channel Session with the PIV SSD in order to communicate with it in a secure and confidential way.
Card Content Management	
INSTALL	AP can initiate or perform the various steps required for CM content management if the APDU commands are previously signed by the Card Administrator (GlobalPlatform Delegated Management) and the content is associated with the AP.
LOAD	AP can transfer a Load File to the CM if the APDU commands are previously signed by the Card Administrator (GlobalPlatform Delegated Management) and the content is associated with the AP.
DELETE (card content)	AP 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 if the APDU commands are previously signed by the Card Administrator (GlobalPlatform Delegated Management) if it is associated with the AP.
PUT KEY	Regarding PIV SSD keys, AP can either: • Replace an existing PIV SSD key with a new key • Replace multiple existing PIV SSD keys with new keys • Add a single new PIV SSD key • Add multiple new PIV SSD keys
DELETE (key)	AP can delete a PIV SSD key uniquely identified by the KID and KVN.
SET STATUS	AP can modify the PIV SSD Life Cycle State or an associated Application Life Cycle State.
GET STATUS	AP can retrieve Life Cycle status information of the PIV SSD, and Executable Load File, Executable Module, Application or Security Domain associated with the AP.
STORE DATA	AP can transfer data to the PIV SSD.
PIV Content Management	
STORE PIV DATA	AP can store PIV data objects into the PIV applet.
GENERATE PIV KEY	AP can generate PIV RSA key pairs in the PIV applet.
PUT PIV KEY	AP can replace RSA Private keys in the PIV applet.

5.4.3 Public Operator Services

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.
GET DATA (ISD)	Operator can retrieve public data from the ISD. No CSPs can be read using this service.
GET DATA (PIV SSD)	Operator can retrieve public data from the PIV SSD. No CSPs can be read using this service.
GET DATA (PIV)	Operator can retrieve public data from the PIV applet. No CSPs can be read using this service.
GENERAL AUTHENTICATE (CHALLENGE/NO RESPONSE)	Only RSA Modular Exponentiation using the PIV Card Authentication Key.

5.4.4 Relationship between Services and Roles

	Card Administrator	PIV Application Provider	Public Operator
DELETE (card content)	X	X	
DELETE (key)	X	X	
EXTERNAL AUTHENTICATE	X	X	
GET DATA (ISD)			X
GET DATA (PIV SSD)			X
GET DATA (PIV)			X[1]
GET STATUS	X	X	
INITIALIZE UPDATE	X	X	
INSTALL	X	X	
LOAD	X	X	
PUT KEY	X	X	
SELECT			X
SET STATUS	X	X	
STORE DATA	X	X	
STORE PIV DATA		X	
GENERATE PIV KEY		X	
PUT PIV KEY		X	
GENERAL AUTHENTICATE (CHALLENGE/NO RESPONSE)			X[2]

Table 7 - Services and associated roles

[1] For the following PIV data objects only: CHUID and X.509 Certificate for Card Authentication
[2] Only RSA Modular Exponentiation using the PIV Card Authentication Private Key

5.4.5 Relationship between Services and CSPs

Relationship can be:

- Create (creation of the CSP object)
- 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

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 (card content)	Execute	AP-Smac
DELETE (key)	Execute	AP-Smac
EXTERNAL AUTHENTICATE	Execute	AP-Smac
GET DATA (ISD)	Execute	AP-Smac
GET STATUS	Execute	AP-Smac
INSTALL	Execute	AP-Smac
LOAD	Execute	AP-Smac
PUT KEY	Execute	AP-Smac
SET STATUS	Execute	AP-Smac
STORE DATA	Execute	AP-Smac

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

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

PIV SSD Key Set

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

PIV SSD Session Key Set

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

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

Service	Type of access	Key
DELETE (card content)	Execute	AP-Smac
DELETE (key)	Execute	AP-Smac
EXTERNAL AUTHENTICATE	Execute	AP-Smac
GET DATA (PIV SSD)	Execute	AP-Smac
GET STATUS	Execute	AP-Smac
INSTALL	Execute	AP-Smac
LOAD	Execute	AP-Smac
PUT KEY	Execute	AP-Smac
SET STATUS	Execute	AP-Smac
STORE DATA	Execute	AP-Smac
STORE PIV DATA	Execute	AP-Smac
GENERATE PIV KEY	Execute	AP-Smac
PUT PIV KEY	Execute	AP-Smac, PIVSSD-Kkek

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

Service	Type of access	Key
DELETE (card content)	Execute	AP-Senc, AP-Smac
DELETE (key)	Execute	AP-Smac
EXTERNAL AUTHENTICATE	Execute	AP-Senc, AP-Smac
GET DATA (PIV SSD)	Execute	AP-Senc, AP-Smac
GET STATUS	Execute	AP-Senc, AP-Smac
INSTALL	Execute	AP-Senc, AP-Smac
LOAD	Execute	AP-Senc, AP-Smac
PUT KEY	Execute	AP-Senc, AP-Smac
SET STATUS	Execute	AP-Senc, AP-Smac
STORE DATA	Execute	AP-Senc, AP-Smac
STORE PIV DATA	Execute	AP-Senc, AP-Smac
GENERATE PIV KEY	Execute	AP-Senc, AP-Smac
PUT PIV KEY	Execute	AP-Senc, AP-Smac, PIVSSD-Kkek

PIV Card Authentication Private Key

Service	Type of access
SET STATUS (TERMINATED)	Zeroize
GENERATE PIV KEY	Generate
PUT PIV KEY	Write
GENERAL AUTHENTICATE(CHALLENGE/NO RESPONSE)	Execute

PIV Card Authentication Public Key

Service	Type of access
GENERATE PIV KEY	Generate

RNG Seed Values

Service	Type of access
Card Reset	Generate
INITIALIZE UPDATE	Execute
INSTALL	Execute
GENERATE PIV KEY	Execute
GENERAL AUTHENTICATE (CHALLENGE/NO RESPONSE)	Execute

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 SSD and send a GET DATA (PIV SSD) APDU command with the tag '9F7F' and verify that the returned data contains fields as follows (other fields are not relevant here). This verifies the version of the PIV SSD applet.

Data Element	Length	Position	Value
Manufacturer code	2	2 - 3	'5453'
Interface Version	2	6 - 7	'0101'
Applet Version	2	8 - 9	'0100'

3. SELECT the PIV SSD, open a Secure Channel Session, and send the following APDU command sequence. This verifies the version and manufacturer of the PIV applet.

   Install for Personalization:

   ```
   80 E6 20 00 11 00 00 0B A0 00 00 03 08 00 00 10 00 01 00 00 00 00
   ```

   Get Version Info through Store Data

   ```
   80 E2 80 00 06 82 01 01 41 01 00
   ```

   The following information shall be returned.

   ```
   80 06 54 65 63 53 65 63 81 02 01 01 82 02 01 00
   ```

   In the data returned, the 80 tag specifies the manufacturer name, the 81 tag is the interface number and the 82 tag is the applet version number. The same information with spaces entered to show the three tags is shown below.

   ```
   80 06 54 65 63 53 65 63     81 02 01 01     82 02 01 00
   ```

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 is 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 CM is a single-chip implementation in 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 the chip that deters 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 identical 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 SSD Key Set represents the role of the PIV Application Provider

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 or PIV Application Provider: a Secure Channel Session must be open between the external operator (more precisely the middleware

the CA or AP 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 AP is responsible for application personalization and lifecycle management following GlobalPlatform.
- The AP 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 and a TDES based integrity checksum).
- PIV SSD Key Set must be loaded through a GlobalPlatform Secure Channel Session ensuring their integrity and confidentiality (112-bit TDES encryption and a TDES based integrity checksum).
- The PIV RSA keys are either generated on card or loaded through a GlobalPlatform Secure Channel Session ensuring their integrity and confidentiality (112-bit TDES encryption and a TDES based integrity checksum).
- The PIV Card Application Administration Key is loaded through a GlobalPlatform Secure Channel Session ensuring its integrity and confidentiality (112-bit TDES encryption and a TDES based integrity checksum).

7.5 KEY MANAGEMENT SECURITY RULES

Key Material

This CM supports the following CSPs:

Key name (CSP)	Type	Length	Strength
Key Secure Storage Key	TDES	112-bits	80-bits
CA ISD Key Set			
PIV SSD Key Set			
CA Session Key Set	TDES session key	112-bits	80-bits
PIV SSD Session Key Set			
PIV Card Authentication Key (Both public and private keys)	RSA	1024-bits	80-bits
DRNG Seed concatenated with DRNG Seed Key	TDES	112-bits	80-bits
NDRNG Seed	DRNG IVEC	64-bits	N/A

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

Key name (CSP)	Type	Length	Strength
TDES keys	TDES	168-bits	112-bits

AES keys	AES	128-, 192- and 256-bits	128-, 192- and 256-bits
RSA keys	RSA	1024- and 2048-bits	80- and 112-bits

Key Generation

Key Secure Storage Key

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

Key Derivation

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

Key Entry

CA ISD Key Set, PIV SSD 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 or PIVSSD-Kkek identified during the GlobalPlatform Secure Channel Session initialization, when one of the Security Domain key sets is selected.

Key Storage

Key Secure Storage Key (KSSK)

This key is stored plaintext in EEPROM.

CA ISD Key Set, PIV SSD Key Set

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, PIV SSD Session Key Set

These keys are stored plaintext in RAM.

Key Output

No keys can be output from the module.

Key Zeroization

The CM offers services to zeroize all the persistent keys:

- The KSSK is zeroized when Card lifecycle state is set to TERMINATED. The Card Administrator or PIV Application Provider 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 or keys). By zeroizing the KSSK all other keys stored in the module are made irreversibly unusable.

The CM offers services to zeroize all the session keys:

- 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.

RNG Seed Values

The CM offers services to randomize and overwrite all DRNG and NDRNG seed values and keys:

- Every time that the CM is powered up or reset, the NDRNG seed value is overwritten with random data.
- Every time that the CM is powered up, the DRNG Seed and DRNG Seed Key are randomized.
- During power up initialization, the CM computes new DRNG Seed and DRNG Seed Key values using the NDRNG. Any old seed values (which were randomized) are then overwritten with the new computed values.

7.6 ELECTROMAGNETIC INTERFERENCE/COMPATIBILITY (EMI/EMC)

The CM 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 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 Provider	TDES authentication	PIV SSD Key Set

Table 8 - Roles and Required Identification and Authentication

9.2 STRENGTH OF AUTHENTICATION MECHANISM

Authentication Mechanism	Strength of Mechanism
TDES authentication with CA ISD Key Set	2^{80}
TDES authentication with PIV SSD Key Set	2^{80}

Table 9 - Strengths of Authentication Mechanisms

All these authentication objects implement a limited retry counter.

9.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Administrator	Section 5.4.1 lists authorized services for this role
PIV Application Provider	Section 5.4.2 lists authorized services for this role

Table 10 - 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 11 - 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
[14443-1]	ISO/IEC 14443-1, First edition 2000-04-15, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics
[14443-2]	ISO/IEC 14443-2, First edition 2001-07-01, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface
[14443-3]	ISO/IEC 14443-3, First edition 2001-02-01, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision
[14443-4]	ISO/IEC 14443-4, First edition 2001-02-01, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol

Table 12 - References

11 ACRONYMS AND DEFINITIONS

Acronym	Definition
AdvX	Advance Crypto
AP	PIV Application Provider
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
PUK	PIV User PIN Unblock PIN
RNG	Random Number Generator
SSD	Supplementary Security Domain

Table 13 – Acronyms and Definitions

[END OF THE DOCUMENT]

