Entrust Securing Digital Identities & Information

Entrust IdentityGuard PIV Credential
FIPS 140-2 Cryptographic Module Security Policy

Version: 1.0

Date: January 24, 2013

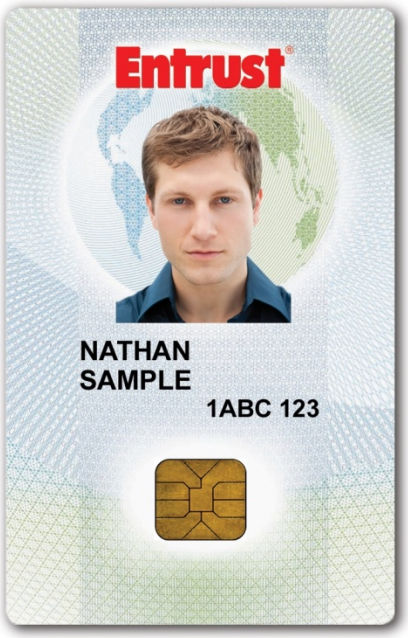

Table of Contents

Table of Tables

Table of Figures

1 Introduction

This document defines the Security Policy for the Entrust IdentityGuard PIV Credential cryptographic module, hereafter denoted *the Module*. The Module, validated to FIPS 140-2 overall Level 2, is a single chip smartcard module implementing the Global Platform operational environment, with Card Manager and PIV applets.

The Module is intended for use by US Federal agencies and other markets that require smartcards with a [SP 800-73-3] conformant PIV applet. The module can also be configured for use in markets where the set of keys and data objects, or the access control rules governing their use, differ from the PIV data model. The cryptographic boundary is the surface of the chip and the pads.

The FIPS 140-2 security levels for the Module are as follows:

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	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 1 – Security Level of Security Requirements

The Module implementation is compliant with:

- [ISO 7816] Parts 1-4
- [ISO 14443] Parts 1-4
- [JavaCard]
- [GlobalPlatform]

1.1 Hardware and Physical Cryptographic Boundary

The Module is designed to be embedded into plastic card bodies, with a contact plate and contactless antenna connections. The physical form of the Module is depicted in Figure 1 (to scale); the red outline depicts the physical cryptographic boundary, representing the surface of the die and the bond pads. The cross-hatching indicates the presence of active and passive tamper shields. In production use, the module is wire-bonded to a frame connected to a contact plate, enclosed in epoxy and mounted in a card body. The contactless ports of the module are electrically connected to an antenna embedded in the card body. The Module relies on [ISO7816] and [ISO14443] card readers as input/output devices.

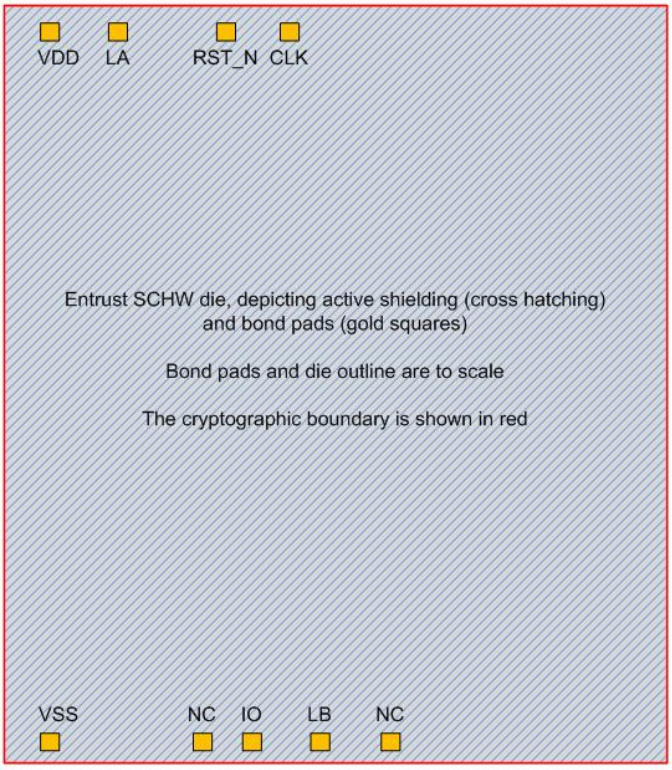

Figure 1 – Entrust IdentityGuard PIV Credential: Physical Form

Pad	Description	Logical interface type
VSS, VDD	ISO 7816: Power and ground	Power
CLK	ISO 7816: Clock	Control in
RST_N	ISO 7816: Reset	Control in
IO	ISO 7816: Serial interface	Data in, data out, control in, status out
LA, LB	ISO 14443: Antenna	Data in, data out, control in, status out
NC	No connect	Not used

Table 2 – Ports and Interfaces

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment and applets. Any number of PIV Applet instances can be instantiated on a single Module, depending on resource availability. Each PIV Applet instance has its own administration subcomponent, labeled "PIV Admin" in the diagram.

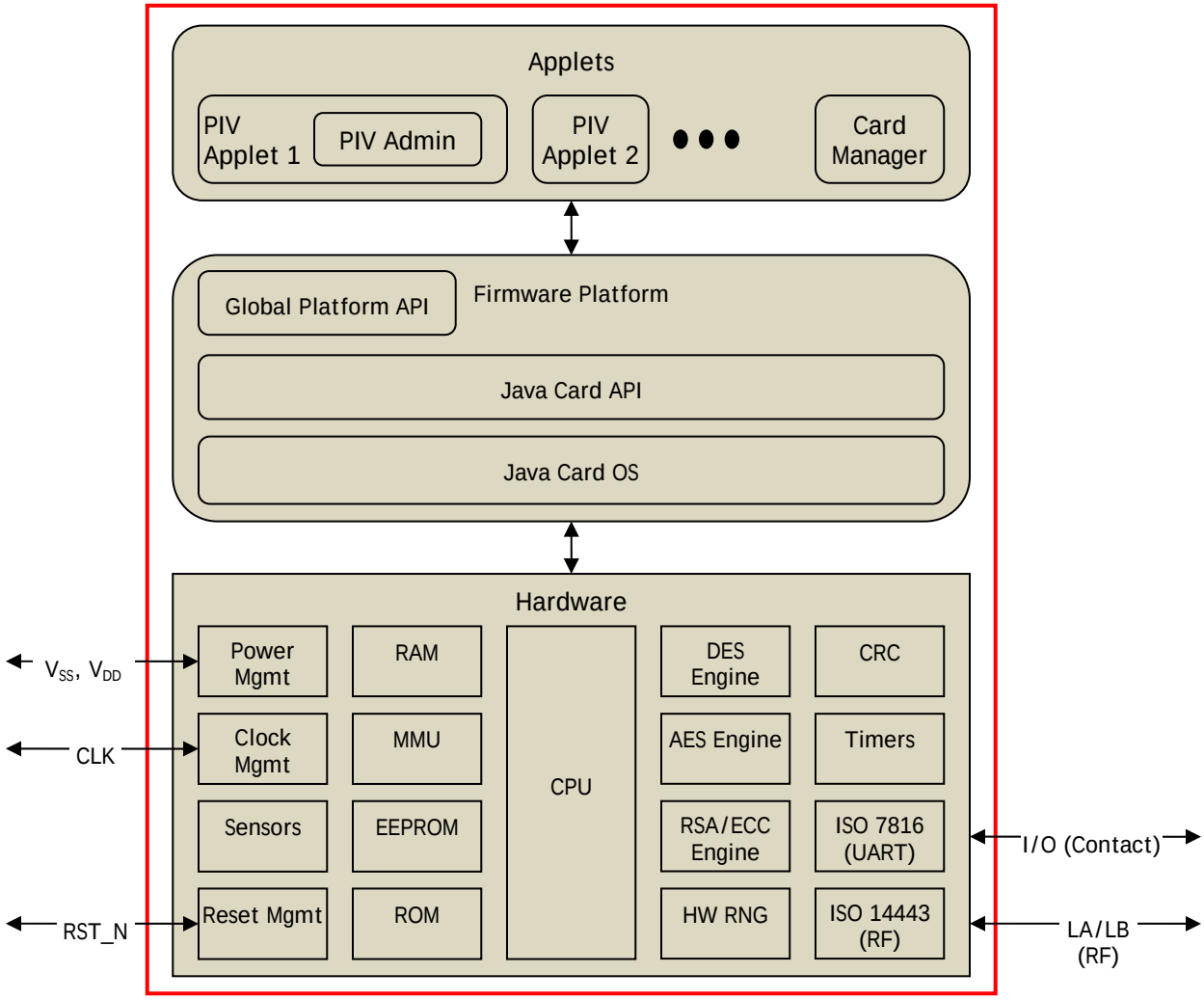

Figure 2 - Module Block Diagram

- The ISO 7816 UART supports the T=0 and T=1 communications protocol variants
- The ISO 14443 communications block supports 13.56 MHz Type A signaling (106 kbps; 212 kbps; 424 kbps; 848 kbps and the T=CL protocol
- 144 KB EEPROM; 264 KB ROM; 7.5 KB RAM

Section 3 describes applet functionality in greater detail. The Java Card and Global Platform APIs are internal interfaces available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

1.3 Versions and mode of operation

Hardware: SCHW 1.0
Firmware (OS): SCOS 1.0
Firmware (applet): Entrust IdentityGuard PIV Applet 1.0.1 Patch 172799

Configuring the module so that it is in the FIPS approved mode of operation is in two parts:

- The firmware platform is initialized into the FIPS approved mode of operation at the time of module production. This mode is fixed at production time and cannot be reversed.
- The default-selected PIV Applet instance is configured for FIPS mode by sending a specific installation parameter to the instance as it is installed. This is performed after card production by the IdentityGuard Print Module (which must be configured specifically to do so).

An operator can confirm that the firmware platform is initialized into the FIPS approved mode of operation by retrieving the CPLC data from the card using the GET DATA command and confirming the following values:

Data Element	Length (bytes)	Value
IC Module Fabricator	2	36 62
ICC Manufacturer	2	80 00

Table 3 – Portion of CPLC Data Confirming Firmware in FIPS Mode

An operator can confirm that a PIV Applet instance is configured for FIPS mode by authenticating with secure channel then sending the GET INFO command to the instance's administration subcomponent. The module responds with the following information:

Data Element	Length (bytes)	Value
Internal component 1 version info	8	00 01 00 00 00 01 01 1e
Internal component 2 version info	8	00 01 00 00 00 01 01 1e
Internal component 3 version info	8	00 01 00 02 00 00 00 fb
Internal component 4 version info	8	00 01 00 02 00 00 00 fb
Internal component 5 version info	8	00 01 00 02 00 00 00 fb
Internal component 6 version info	8	00 01 00 02 00 00 00 fb
Platform identifier	1	01
Vendor identifier	1	02
Persistent memory available	2	Varies
Reserved	8	00 00 00 00 00 00 00 00
Reserved	1	00
FIPS flag	1	01
Attack counter	2	Varies

Table 4 - Information Returned by the PIV Applet's GET INFO Command

All of the information returned by the card must match the data specified in Table 4. The "FIPS flag" indicator in Table 4, when it has value 01, indicates that the PIV Applet instance is configured in FIPS mode.

2 Cryptographic functionality

The Module operating system implements the FIPS Approved and Non-FIPS Approved but Allowed cryptographic functions listed in Table 5 and Table 6 below.

Algorithm	Description	Cert #
RNG	[ANSI X9.31] 2-Key TDEA DRNG.	942
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports the 2-Key and 3-Key options; CBC and ECB modes.	1144
Triple-DES MAC	[FIPS113] TDEA Message Authentication Code. Vendor affirmed, based on the validated TDEA above.	1144
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports 128-, 192- and 256-bit key lengths and ECB and CBC modes.	1769
AES-CMAC	[SP800-38B] AES CMAC is used with 128 and 256 bit keys.	1769
RSA-CRT	[PKCS#1] RSA CRT signature generation. The module supports 1024- and 2048-bit RSA keys. PKCS#1 is followed except in cases where raw RSA decryption/signing is required by [SP800-73-3].	885
ECDSA	[FIPS 186-2] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-256 curve for key pair generation and signing.	237
ECC CDH	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive only. The module supports the NIST defined P-256 curve.	5

Table 5 – FIPS Approved Cryptographic Functions

Algorithm	Description
HW RNG	Hardware RNG; minimum of 8 bits per access. The HW RNG output used to seed the FIPS approved DRNG.
RSA Key Gen	RSA CRT key pair generation, 1024- and 2048-bit keys.
RSA Key Decrypt	The module supports non-SP 800-56B compliant RSA key decryption using 1024- and 2048-bit keys. Key wrapping; key establishment methodology provides 80-112 bits of encryption strength.
TDEA Symmetric key wrap	Symmetric key wrapping. Using 2-Key TDEA, key establishment methodology provides 112 bits of encryption strength.
AES Symmetric key wrap	Symmetric key wrapping. Using AES-256, key establishment methodology provides 256 bits of encryption strength (see Sections 2.3 and 2.4).

Table 6 – Non-FIPS Approved But Allowed Cryptographic Functions

2.1 Critical Security Parameters

All critical security parameters (CSPs) used by the Module are described in this section. All usage of these CSPs by the Module, including all CSP lifecycle states, is described in the services detailed in Section 3.

The following critical security parameters are present:

Key	Description / Usage
OS-SEED	64 bit random value; Seed from Fast RNG used for ANSI X9.31 DRNG seed.
OS-SEED-KEY	192 bit seed key; Seed key used for ANSI X9.31 DRNG
OS-RNG-STATE	320 bit value; Current RNG state
OS-MKEY	2-Key TDEA Master key used to encrypt all key and PIN data stored in the EEPROM.
ISD-SENC	2-Key TDEA Master key used to generate ISD-SESSION-SENC
ISD-SMAC	2-Key TDEA Master key used to generate ISD-SESSION-SMAC.
ISD-DEK	2-Key TDEA Master key used to generate ISD-SESSION-DEK.
ISD-SESSION-SENC	2-Key TDEA Session encryption key used to encrypt / decrypt secure channel data.
ISD-SESSION-SMAC	2-Key TDEA Session MAC key used to verify inbound secure channel data integrity.
ISD-SESSION-DEK	2-Key TDEA Session data decryption key used to decrypt sensitive data.
ISD-PIN-GLOBAL	Global Platform global PIN.
PIV-PIN-APP	8 character string; PIV application PIN
PIV-PIN-PUK	8 character string; PIV PIN Unblocking Key
PIVA-KTK-PRI	RSA 2048 key transport private key; this key is ephemeral; it is used to transport PIV-DEK and PIV-MACK then deleted.
PIV-DEK	AES 256 bit data encryption key, used to decrypt sensitive data imported into the PIV applet.
PIV-MACK	AES-256 data MACing key, used to verify the MAC on sensitive data imported into the PIV applet.
PIV-KP-PRI	RSA 1024, RSA 2048, or ECC P-256 asymmetric private key. Any number of PIV-KP-PRI keys can exist (including 0) on the card, limited by available memory on the card. This key is used for the asymmetric private key functions of the PIV model. The PIV Authentication Key (9A), the Digital Signature Key (9C), the Key Management Key (9D, including retired 9D keys) and the Card Authentication Key (9E, asymmetric variant) are instances of this key.
PIV-SK-CRK	2/3 Key Triple DES, AES 128/192/256 challenge-response key. Any number of PIV-SK-CRK keys can exist (including 0) on the card, limited by available memory on the card. The key is used for symmetric challenge-response. The symmetric variant of PIV Card Authentication Key (9E) is an instance of this key.
PIV-SK-CRK-UA	2/3 Key Triple DES, AES 128/192/256 challenge-response key that can authenticate a Cardholder to the card. Any number of PIV-SK-CRK-UA keys can exist (including 0) on the card, limited by available memory on the card.
PIV-SK-CRK-AA	2/3 Key Triple DES, AES 128/192/256 challenge-response key that can authenticate a PIV Applet administrator to the card. Any number of PIV-SK-CRK-AA keys can exist (including 0) on the card, limited by available memory on the card. The PIV Card Management (9B) key is an instance of this CSP.
PIV-SK-CRK-UPU	2/3 Key Triple DES, AES 128/192/256 challenge-response key that can be used to unblock PIV-PIN-APP. Any number of PIV-SK-CRK-UPU keys can exist (including 0) on the card, limited by available memory on the card.
PIV-SK-GP	2/3 Key Triple DES, AES 128/192/256 general purpose key, decrypted by GENERAL AUTHENTICATE using a PIV-KP-PRI key (such as the 9D key) and the RSA algorithm.

Table 7 - Module Critical Security Parameters

2.2 Public keys

The following public keys are present:

Key	Description / Usage
PIVA-KTK-PUB	RSA 2048 key transport public key; this key is ephemeral; it is used to transport PIV-DEK and PIV-MACK then deleted.
PIV-KP-PUB	RSA 1024, RSA 2048, or ECC P-256 public key. Any number of PIV-KP-PUB keys can exist (including 0) on the card, limited by available memory on the card. This public key component is the counterpart to PIV-KP-PRI; the number of PIV-KP-PUB keys is equal to the number of PIV-KP-PRI keys. The role of public keys in the PIV model is described below.

Table 8 - Public Keys

[SP800-73-3] Part 2 defines the command issued to the card to initiate the generation of asymmetric key pairs. When the GENERATE ASYMMETRIC KEY PAIR service is called, the generated public key is output by the PIV applet. An external entity (e.g., a card management system) is responsible for packaging the public key in an X.509 certificate and storing it in the corresponding X.509 certificate container in the PIV applet. The public key is also separately stored by the applet. For RSA keys, the public key is used to verify the result of RSA CRT private key operations.

2.3 Security Strength of 2-Key TDEA

[SP 800-131A] Section A.1 provides the NIST rationale for 2-Key TDEA security strength. The module claims 100 - 112 bits security strength for its 2-key TDEA operations based on the NIST rationale and the following Module characteristics:

- ISD-SENC, ISD-SMAC, and ISD-DEK are long term keys used in GlobalPlatform Secure Channel to derive the session keys ISD-SESSION-SENC, ISD-SESSION-SMAC, and ISD-SESSION-DEK. No data encrypted or decrypted using these keys is ever revealed. 2-Key TDEA key establishment provides 112 bits of security strength.
- The Module uses the ISD-SESSION-DEK key to decrypt critical security parameters, and does not perform encryption with this key or output data decrypted with this key. This usage of TDEA provides 112 bits of security strength.
- ISD-SESSION-SMAC and ISD-SESSION-SENC are used in Global Platform Secure Channel for authentication and decryption and integrity protection of APDU data. The operator must ensure that no more than 2^20 TDEA blocks are processed with these keys. This usage of TDEA provides 100 bits of security strength.
- This security policy requires that the module be configured to disallow use of 2-key TDEA keys other than for Secure Channel.

2.4 Security Strength of Key Establishment

The module establishes 2-key TDEA keys in the Secure Channel protocol. See the discussion in Section 2.3 above.

The module implements RSA 2048 bit key transport to import the PIV-DEK and PIV-MACK keys. This key transport mechanism is limited to 112 bit security strength. The PIV-DEK key is used to import PIV Applet and PIV Administration subcomponent sensitive data, including keys. Although the PIV-DEK key is an AES-256 key, this method of key establishment provides 112 bits of security strength because PIV-DEK is established into the module using RSA 2048 bit key transport.

3 Roles, authentication and services

3.1 Roles

Table 9 lists all operator roles supported by the module. This Module does not support a maintenance role. The Module does not support concurrent operators and clears previous authentications on power cycle.

Role ID	Role Description
AN	Anonymous. This role is associated with the user before authentication is complete.
CM	Card Manager (the Cryptographic Officer role for FIPS 140-2 validation purposes). This role is responsible for card issuance and management of card data via the Card Manager and PIV applets. Authenticated using the SCP authentication method with ISD-SESSION-SENC. This role also has the privileges associated with the PIV Administrator (PA) role.
CH	Card Holder (the User role for FIPS 140-2 validation purposes). This role is associated with the PIV applet, and by extension, the PIV Administration subcomponent; the Card Holder uses the Module for an identity token. Authenticated to the PIV applet using the VERIFY service with PIV-PIN-APP or ISD-PIN-GLOBAL, or with the GENERAL AUTHENTICATE service with a PIV-SK-CRK-UA symmetric key.
PA	PIV Administrator – this role is associated with the PIV applet, and by extension, the PIV Administration subcomponent. The PA role is responsible for configuration of the PIV data using the PIV Administration Subcomponent and the PIV applet PUT DATA and GENERATE ASYMMETRIC KEY PAIR services. The PIV Administrator authenticates with a card management key (PIV-SK-CRK-AA).
PU	PIN-unblocking User – this role is associated only with the RESET RETRY COUNTER and CHANGE REFERENCE DATA PIV services. This role is not associated with the PIV Administration subcomponent because the authentication mechanism is valid for only the duration of the single service invocation. Authenticated to the PIV applet using the RESET RETRY COUNTER service with the PIV-PIN-PUK or a PIV-SK-CRK-UPU symmetric key. Authenticated to the PIV applet using the CHANGE REFERENCE DATA service with the PIV-PIN-PUK.

Table 9 - Role Descriptions

3.2 Authentication

Secure Channel Protocol (SCP) Authentication

The GlobalPlatform Secure Channel Protocol authentication method is performed when the EXTERNAL AUTHENTICATE service is invoked after successful execution of the INITIALIZE UPDATE command. These two commands operate as described next.

The ISD-SENC, ISD-SMAC, and ISD-DEK keys are used along with other information to derive the ISD-SESSION-SENC, ISD-SESSION-SMAC, and ISD-SESSION-DEK keys, respectively. The ISD-SESSION-SENC key is used by the Module to create a cryptogram; the external entity participating in the mutual authentication also creates a cryptogram. Each participant compares the received cryptogram to the expected value and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module in the CM role).

As discussed in Section 2.3, the Module's 2-Key TDEA security strength is determined to be 100 bits. The Module blocks attempts to use the Card Manager authentication keys within 2^10 consecutive failed attempts. Based on this strength, ignoring the additional security provided by a MAC in the EXTERNAL AUTHENTICATE message, and assuming a 64 bit authentication datum block size:

- The probability that a random attempt at authentication will succeed is 1/2^64 or 5.42E-20, meeting the FIPS 140-2 probability requirement of 1.00E-6.
- Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is (2^10)/(2^64) = 5.55E-17, meeting the FIPS 140-2 probability requirement of 1.00E-5.

PIV Applet Application PIN, Global PIN and PUK Comparison Authentication

This authentication method compares a PIN value sent to the Module to the stored PIV-PIN-APP, ISD-PIN-GLOBAL or PIV-PIN-PUK values; if the two values are equal, the operator is authenticated. This method is used in the VERIFY and CHANGE REFERENCE DATA services to authenticate to the CH role, and by the RESET RETRY COUNTER service to authenticate to the PU role.

The strength of authentication for this authentication method depends on how the PIN is generated, the maximum try count, and the character set permitted for the PIN. The PIV Applet of the module can be configured to enforce minimum length and character set requirements on the PIN when the PIN is set through the CHANGE REFERENCE DATA and RESET RETRY COUNTER services. The maximum try count enforced by the VERIFY, CHANGE REFERENCE DATA, and RESET RETRY COUNTER services can also be configured. All of the rules are configured separately for each PIN.

The default rules configured for all PINs by the Module are (note that a Card Management System may apply different defaults):

- Minimum length of 7
- Maximum try count of 3
- Digits only

The operator can change these defaults, but must ensure that the rules meet the strength requirements described below.

Based on these defaults and assuming that the PINs are generated uniformly at random, the strength of this authentication method is as follows:

- The probability that a random attempt at authentication will succeed is at most 1.00E-7, meeting the FIPS 140-2 probability requirement of 1.00E-6.
- The probability that a random attempt will succeed over a one minute period is at most 3.00E-7, meeting the FIPS 140-2 probability requirement of 1.00E-5.

[SP800-73-3] does not define a service to define the initial value of ISD-PIN-GLOBAL, PIV-PIN-APP or PIV-PIN-PUK. These values are set (and can be updated at any time) through the PIV Applet administration subcomponent SET PIN INFO service, which does not enforce any restrictions on the PIN value except a maximum length of 8 characters. The PIV Administrator must ensure that the PINs provided through this service meet the password rules specified for the CHANGE REFERENCE DATA and RESET RETRY COUNTER services.

Please see Section 9 for guidance on required external security procedures associated with the PIV Applet PIN Comparison authentication method.

PIV Applet Symmetric Cryptographic Authentication

In this authentication method the module encrypts (using PIV-SK-CRK-UA, PIV-SK-CRK-AA, or PIV-SK-CRK-UPU) a generated challenge, reveals the plaintext or the ciphertext, and compares the unrevealed data to the response sent to the module by an external entity.

The strength of authentication for this authentication method is based on the strength of the symmetric key in use; only AES-128, AES-192, AES-256, and 3-Key TDEA are allowed for these keys in the approved mode of operation, with a minimum security strength of 112 bits; assuming a 64 bit authentication datum block size the associated strength of this authentication method is:

- The probability that a random attempt at authentication will succeed is 1/2^64 or 5.42E-20, meeting the FIPS 140-2 probability requirement of 1.00E-6.
- The maximum communication speed of the module is 848 kbps. Based on this communication speed, and because more than 13 bytes must be transmitted in each authentication attempt, the

probability that a random attempt will succeed over a one minute period is at most 848*1024*60/(8*13*2^64) = 2.72E-14, meeting the FIPS 140-2 probability requirement of 1.00E-5.

3.3 Policies and permissions controlling access to services

Policies associated with PIV PIN CSPs

Associated with each of the PIN critical security parameters is a set of policies dictating the conditions under which the PIN can be used or managed. These policy values are specified below:

Policy	Policy Description
ACCEPT ON CONTACT INTERFACE	A bit indicating whether or not the VERIFY, CHANGE REFERENCE DATA, and RESET RETRY COUNTER services should accept the PIN when presented on the contact interface of the card.
ACCEPT ON CONTACTLESS INTERFACE	A bit indicating whether or not the VERIFY, CHANGE REFERENCE DATA, and RESET RETRY COUNTER services should accept the PIN when presented on the contactless interface of the card.
ALLOW PIN UPDATE	A bit indicating whether or not the CHANGE REFERENCE DATA service should allow the PIN to be updated.
MINIMUM PIN LENGTH	The minimum length that is required for a new PIN.
MAX AUTHENTICATIONS AFTER ADMIN RESET	The number of PIN authentications allowed following a PIN change with the SET PIN INFO service. After the specified number of authentications the PIN must be changed through the CHANGE REFERENCE DATA service. This parameter is ignored for ISD-PIN-GLOBAL and PIV-PIN-PUK.
MAX ATTEMPTS	The maximum number of authentication attempts, after which the PIN is blocked.
DIGIT POLICY	Specifies whether digit characters are allowed, required, or rejected.
UPPER ALPHA POLICY	Specifies whether uppercase characters are allowed, required, or rejected.
LOWER ALPHA POLICY	Specifies whether lowercase characters are allowed, required, or rejected.
SPECIAL CHAR POLICY	Specifies whether ASCII printable characters are allowed, required, or rejected.
NONPRINTABLE POLICY	Specifies whether ASCII non-printable characters are allowed, required, or rejected.

Table 10 – Policies Associated with PIN CSPs

Until configured through the SET PIN INFO service, the ACCEPT ON CONTACT INTERFACE and ACCEPT ON CONTACTLESS INTERFACE policy settings are set to false, effectively disabling the PIN. The character policy and pin length policy settings are ignored when the SET PIN INFO service is used.

Permissions and policies associated with PIV Key CSPs

Associated with each of the PIV Applet key critical security parameters is a set of permissions dictating the conditions under which the CSP can be used. Six permission bit collections are associated with each PIV Key CSP:

- Permissions for CM and PA when a command is received over the contact interface.
- Permissions for CM and PA when a command is received over the contactless interface.
- Permissions for CH after successful authentication when a command is received over the contact interface.

- Permissions for CH after successful authentication when a command is received over the contactless interface.
- Permissions for AN when a command is received over the contact interface.
- Permissions for AN when a command is received over the contactless interface.

Within each permission collection are permission bits for granting the following permissions:

Permission	Permission Description
KEY GENERATION	Allows the key to be generated using the GENERATE ASYMMETRIC KEY PAIR service. Key generation is not supported for symmetric keys.
KEY IMPORT	Allows the key to be imported using the IMPORT KEY service.
ONE USE AFTER FRESH AUTHENTICATION	Allows the key to be used once immediately after a successful authentication using a PIN. This permission must be granted when the USE permission is granted.
USE	Allows the key to be used.

Table 11 – Permissions Associated with PIV Key CSPs

3.4 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service. Note that once a secure channel has been established through the INITIALIZE UPDATE and EXTERNAL AUTHENTICATE services, all services (both of the Card Manager and PIV Applet) may use ISD-SESSION-SMAC and ISD-SESSION-SENC in accordance with SCP-02 [GlobalPlatform] to integrity check and decrypt commands. This use is not explicitly listed in the tables below. The columns to the right of the description indicate which roles are allowed access to the service. In the FIPS-approved configuration, no service allows the export of CSPs from the card.

Service	Description
Card Reset (Self-test)	This service is activated by power cycling the Module. On the contact interface, this is done by removing and reinserting the Module into the contact reader slot, or by reader assertion of the RST signal. On the contactless interface, this is done by removing and re-inserting the Module into the contactless reader's field or by transmitting an ISO 14443 DESELECT then activating the Module. The *Card Reset* service will invoke the power on self-tests described in Section 4.1. On any card reset, the Module overwrites OS-SEED, OS-SEED-KEY and OS-RNG-STATE. On any card reset, the card clears all volatile memory.
EXTERNAL AUTHENTICATE	Complete the initiation of the secure channel protocol. Must be preceded by a successful INITIALIZE UPDATE. Uses ISD-SMAC, ISD-SENC, ISD-DEK and other information to generate ISD-SESSION-SMAC, ISD-SESSION-SENC, and ISD-SESSION-DEK. Uses all of these CSPs in accordance with SCP-02 [GlobalPlatform]. Upon successful completion, the operator is authenticated in the CM role.
INITIALIZE UPDATE	Initiate the Secure Channel protocol; to be followed by EXTERNAL AUTHENTICATE. Uses ISD-SMAC, ISD-SENC, ISD-DEK and other information to generate ISD-SESSION-SMAC, ISD-SESSION-SENC, and ISD-SESSION-DEK. Uses all of these CSPs in accordance with SCP-02 [GlobalPlatform].
GET DATA	Retrieve a single data object. No CSPs are used except as required for secure channel.
GET STATUS	Retrieve information about the card. No CSPs are used except as required for secure channel.
SELECT	Select an applet or the PIV Applet administration subcomponent or retrieve

Service	Description
	card identification data (IDENTIFY). No CSPs are used except as required for secure channel.

Table 12 - Unauthenticated Operating System and Card Manager Services and CSP Usage

Service	Description	CM
DELETE	Uninstall an applet instance or delete a Java Card package from EEPROM. No CSPs are used except as required for secure channel.	X
INSTALL	Install an applet instance. No CSPs are used except as required for secure channel.	X
LOAD	Load a load file (e.g. an applet). No CSPs are used except as required for secure channel.	X
STORE DATA	Transfer data to an application. No CSPs are used except as required for secure channel.	X
PUT KEY	Load Card Manager keys. This command updates the ISD-SENC, ISD-SMAC, and ISD-DEK. The new key values are unwrapped with ISD-SESSION-DEK.	X
SET STATUS	Modify the card or applet life cycle status. Moving the card to the TERMINATED state with this command causes all CSPs to be destroyed.	X

Table 13 – Card Manager Services and CSP Usage

Service	Description	AN	CH	PA	CM
GET INFO	Retrieves PIV Applet package and runtime information. No CSPs are used except as required for secure channel.				X
SET ATR HISTORICAL BYTES	Sets the ATR historical bytes that should be returned by the card on power up. No CSPs are used except as required for secure channel.				X
CREATE DATA CONTAINER	Creates a PIV data container and associates it with a specific BER-TLV tag. No CSPs are used except as required for secure channel.				X
DELETE DATA CONTAINER	Deletes a specified PIV data container or all PIV data containers. No CSPs are used except as required for secure channel.				X
CREATE KEY CONTAINER	Creates a PIV key container and associates it with a specific key reference and permission bits. No CSPs are used except as required for secure channel.				X
DELETE KEY CONTAINER	Deletes a specified PIV key container or all PIV key containers. Any PIV-KP-PRI, PIV-SK-CRK, PIV-SK-CRK-UA, PIV-SK-CRK-AA or PIV-SK-CRK-UPU CSPs associated with a deleted key container are deleted.				X
IMPORT KEY	Imports a PIV symmetric or asymmetric key into the specified key container. The command data, which includes the raw key data, is encrypted. The service decrypts the data using AES-CBC with the PIV-DEK key and verifies the MAC using PIV-MACK. The key data is loaded into a PIV-KP-PRI, PIV-SK-CRK, PIV-SK-CRK-UA, PIV-SK-CRK-AA or PIV-SK-CRK-UPU CSP. PIV-KP-PUB is updated when PIV-KP-PRI is updated.		X	X	X

Service	Description	AN	CH	PA	CM
SET PIN INFO	Sets the PIN policy and optionally also the PIN value associated with the specified PIN key reference. When a PIN value is specified, the retry counter associated with the PIN is reset. This command can update ISD-PIN-GLOBAL, PIV-PIN-APP, and PIV-PIN-PUK.				X
SET APPLICATION TEMPLATE	Sets the data returned by the PIV Applet in response to a SELECT command that selects the PIV Applet. No CSPs are used except as required for secure channel.				X
CREATE DATA PROTECTION KEYS	Generates PIVA-KTK-PUB and PIVA-KTK-PRI and returns the public key portion. Accepts the concatenation of two AES-256 keys wrapped with PIVA-KTK-PUB using PKCS1 V1.5 padding. Decrypts the key data using PIVA-KTK-PRI importing it into the PIV-DEK and PIV-MACK keys. PIVA-KTK-PRI is deleted after the import.		X	X	X
GET DATA CONTAINER INFO	Returns information about a set of data containers (permissions, capacity, current data length), or the list of data containers present on the card. No CSPs are used except as required for secure channel.	X	X	X	X
GET KEY CONTAINER INFO	Returns information about a set of key containers (permissions, key type), or the list of key containers present on the card. No CSPs are used except as required for secure channel.	X	X	X	X
GET PIN POLICY	Returns the policy associated with a specific PIN. No CSPs are used except as required for secure channel.	X	X	X	X
SET DATA CONTAINER INFO	Sets the permission bits associated with an existing data container. No CSPs are used except as required for secure channel.				X
SET KEY CONTAINER INFO	Sets the permission bits associated with an existing key container. No CSPs are used except as required for secure channel.				X
GET FORCED PIN CHANGE STATE	Returns an indication of whether a PIN change is required (this would be the case if the PIN has been set by an administrator and the policy indicates that the user must then change it). No CSPs are used except as required for secure channel.	X	X	X	X
SET ALGORITHM USE LIMITS	Configures on a per-algorithm basis the number of times that a key can be used. No CSPs are used except as required for secure channel.				X
GET ALGORITHM USE LIMITS	Retrieves the configuration settings set through the SET ALGORITHM USE LIMITS service. No CSPs are used except as required for secure channel.				X
TERMINATE CARD	Places the card in the Global Platform TERMINATED state. This command requires no authentication but can be invoked only when the power-on self-tests fail. This causes all CSPs to be destroyed.	X	X	X	X

Table 14 – PIV Administration Subcomponent Services and CSP Usage

Service	Description	AN	CH	PU	PA	CM
CHANGE REFERENCE DATA	Changes the value of a PIN CSP (ISD-PIN-GLOBAL, PIV-PIN-APP, or PIV-PIN-PUK). This service requires authentication with the current PIN value. Successful execution of this service with either ISD-PIN-GLOBAL or PIV-PIN-APP is an instance of the VERIFY authentication method; that is, the CH role has been authenticated. Whether or not a PIN can be updated with this service depends on the policy settings associated with the CSP.		X	X		
GENERAL AUTHENTICATE	As defined in [SP 800-73], this service has several different usages depending on the tags embedded in the APDU data, and also on the prior execution of other commands in a protocol. Depending on the permissions configured in the key container referenced in the APDU and the type of CSP, the following operations can be performed: • Sign (decrypt) a message using the CSP (for PIV-KP-PRI) • Encrypt a challenge (for PIV-SK-CRK) • Decrypt a witness (for PIV-SK-CRK) • Generate a random challenge (for PIV-SK-CRK, PIV-SK-CRK-UA, PIV-SK-CRK-AA, PIV-SK-CRK-PUK) • Validate a challenge response (for PIV-SK-CRK, PIV-SK-CRK-UA, PIV-SK-CRK-AA). For PIV-SK-CRK-UA mark the CH role as authenticated. For PIV-SK-CRK-AA mark the PA role as authenticated. • Generate a random witness (for PIV-SK-CRK, PIV-SK-CRK-UA, PIV-SK-CRK-AA) • Validate a witness response and, if it is correct, encrypt and return the provided challenge (for PIV-SK-CRK, PIV-SK-CRK-UA, PIV-SK-CRK-AA). For PIV-SK-CRK-UA mark the CH role as authenticated. For PIV-SK-CRK-AA, mark the PA role as authenticated. • Perform the ECC CDH primitive (for PIV-KP-PRI when the key is an elliptic curve key). Depending on the permissions associated with the key container referenced in the APDU, authentication may be required for the service to process the command.	X	X	X	X	X
GENERATE ASYMMETRIC KEY PAIR	Generates new RSA or ECC key pairs. Updates the PIV-KP-PRI CSP and PIV-KP-PUB associated with the key container specified in the command. Depending on the permissions associated with the key container referenced in the APDU, authentication may be required for the service to process the command.		X		X	X
GET DATA (PIV Variant)	Retrieve a single data object managed by the PIV applet access control conditions. Depending on the permissions associated with the data container referenced in the APDU, authentication may be required for the service to process the command. This service does not use any CSPs except as required for secure channel.	X	X	X	X	X
PUT DATA	Replace the contents of a PIV data container. Depending on the permissions associated with the data container referenced in the APDU, authentication may be required for the service to process the command. This service does not use any CSPs except as required for secure channel.	X	X	X	X	X
RESET RETRY COUNTER	Reset the PIV-PIN-APP CSP. This service requires authentication with the current PIV-PIN-PUK value (i.e. authentication of the PU			X		

Service	Description	AN	CH	PU	PA	CM
	role) or authentication with PIV-SK-CRK-UPU to succeed. Updates the counter associated with PIV-PIN-APP and the PIV-PIN-APP value.					
VERIFY	Performs VERIFY authentication; executes using PIV-PIN-APP or ISD-PIN-GLOBAL as specified in the APDU.		X			

Table 15 – PIV Applet Services and CSP Usage

4 Self-test

4.1 Power-on self-test

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data has not been damaged. Power-on self–tests are available on demand by power cycling the module and sending an APDU command.

On power on or reset, the Module performs the self-tests described in Table 16 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the system enters an error state and will start again after a reset. The self-tests complete during processing of the first command APDU.

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code located in EEPROM. This integrity test is not required or performed for code stored in masked ROM code memory.
ANSI X9.31	Performs a fixed seed KAT.
TDEA	Performs separate encrypt and decrypt KATs using 3-Key TDEA in ECB and CBC modes.
AES	Performs separate encrypt and decrypt KATs using an AES 128 key in ECB mode.
AES-CMAC	Performs separate AES-CMAC generation and verification KATs using AES-128 CMAC.
RSA	Performs an RSA signature KAT using an RSA 1024 bit key.
ECC	Performs an ECDH KAT using P-256.
ECDSA	Performs a pairwise consistency test using P-256.

Table 16 – Power-On Self-Test

4.2 Conditional self-tests

On every call to the HW RNG and ANSI X9.31 DRNG, the Module performs the FIPS 140-2 AS09.42 continuous RNG test to assure that the output is different than the previous value.

When any asymmetric key pair is generated (for RSA or ECC keys) the Module performs a pairwise consistency test.

When new firmware is loaded into the module using the LOAD command, the module when used in the FIPS approved mode of operation verifies the integrity and authenticity of the new firmware using a TDEA MAC process and the ISD-SESSION-SMAC key.

5 Physical security policy

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques and is protected by passive shielding (metal layer coverings opaque to the circuitry below) and active shielding (a grid of top metal layer wires with tamper response). A tamper event detected by the active shield causes the Module to become unusable.

The Module is intended to be mounted in a plastic smartcard; physical inspection of the module boundary is not practical after mounting. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process. The module also provides a key to protect the module from tamper during transport.

6 Operational environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

7 Electromagnetic interference and compatibility (EMI/EMC)

The 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 policy

The Module implements defenses against:

- Light attacks
- Invasive fault attacks
- Side-channel attacks (SPA/DPA)
- Timing analysis
- Differential fault analysis (DFA)

9 Security Rules and Guidance

The Module implementation also enforces the following security rules:

- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support manual key entry.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

In addition, the following guidance must be followed to operate the Module in accordance with this security policy:

- PIV Applet administrators are required to configure PIN policies such that PIN values meet the FIPS 140-2 security strength of 1/1,000,000 and 1/100,000.
- PIV Applet administrators, when setting PIN values through the SET PIN INFO service, must procedurally ensure that PIN values comply with the configured PIN policies.
- PIV Applet administrators are required to limit the use of GlobalPlatform Secure Channel such that at most 2^20 TripleDES blocks are processed before the Secure Channel keys are replaced.
- Users of the module must configure it to disallow use of 2-key TripleDES keys except for their use in Secure Channel.

- When configuring key containers with either the CREATE KEY CONTAINER or SET KEY CONTAINER INFO services, the operator must not grant any permissions to the anonymous role except for keys used solely for authentication. Key import and key generation permissions must never be granted to the anonymous role.
- When firmware is loaded into the module, an integrity-protected Secure Channel mode must be used.
- PIV Applet administrators desiring FIPS 201 compliance are required to configure key lengths as specified in SP800-78-3.

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
[FIPS201-1]	*Personal Identity Verification (PIV) Of Federal Employees and Contractors*, March 2006
[ISO 7816]	ISO/IEC 7816 series; Information technology – Identification cards – Integrated circuit(s) cards with contacts
[ISO 14443]	ISO/IEC 14443-1:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics ISO/IEC 14443-2:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 2: Radio frequency power and signal interface ISO/IEC 14443-3:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision ISO/IEC 14443-4:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol
[JavaCard]	Sun Microsystems: Java Card 3.0.1 http://www.oracle.com/technetwork/java/javacard
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1,* March 2003, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP800-73-3]	*Interfaces for Personal Identity Verification - Part 1: End-Point PIV Card Application Namespace, Data Model and Representation,* February 2010 *Interfaces for Personal Identity Verification - Part 2: End-Point PIV Card Application Card Command Interface,* February 2010
[SP800-78-3]	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, December 2010

Table 17 – References

11 Acronyms and definitions

Acronym	Definition
APDU	Application Protocol Data Unit
ISD	Issuer Security Domain
PIV	Personal Identity Verification
SCP	Secure Channel Protocol
SPA/DPA	Simple Power Analysis / Differential Power Analysis (side channel attack techniques).

Table 18 – Acronyms and Definitions