Security Policy

for

TECSEC ARMORED CARD – CONTACT CRYPTOGRAPHIC MODULE

August 7, 2013

Software Release:	See Section 1.4
Document Version:	2
Document Revision:	H
Document Number:	DEV_32_082_

Providing the Transition
from Communication Security
to Information Security

Approval Sheet

Document Title: Security Policy for TecSec Armored Card - Contact	**Original Date**: August 7, 2013
Document Number: DEV_32_082	**Revision Date**: August 7, 2013
Author: Roger D. Butler Jr.	**Revision**: 2H
Approval Authority: Configuration Control Board	**Approval**:

Revision History

DATE	VERSION REVISION NO.	REVISION/CHANGE DESCRIPTION	AREA(S) AFFECTED
March 11, 2009	1.0	Original Issue – Title: TecSec PIV Eagle Card – Contact [FIPS 140] Cryptographic Module Security Policy; $ > Documentation > Certifications > EagleCard_Certification > OriginalPIVCard > TecSec PIV [FIPS 140] Documentation Set > Security Policy > Contact	All
February 16, 2010	1.1	Title: TecSec PIV Eagle Card – Contact [FIPS 140] Cryptographic Module Security Policy; $ > *Documentation > EagleCard > FIPS > Eagle card 2*	
December 3, 2010	1.2	Title: TecSec PIV Eagle Card – Contact [FIPS 140] Cryptographic Module Security Policy; *Based version of document rolled into new template.*	All
February 2, 2011	A	Document reformatted in preparation for the developer updating the information	All
May 12, 2011	B	Headers and Footers put into place, format checked. None of the comments or track changes that are related to content were addressed. Electronic title updated after putting back onto Visual Studios to correspond to the new document title.	All

October 31, 2011		Research and added version history of document only.	Revision History Only
August 6, 2012	2	InfoGard team update in preparation for certification	All
August 7, 2012	A	SILO changed to Attribute Container; Figure 1.2-.1 Updated with text box for No Connect items; Figure 1.3-1 Updated changing Silo to Attribute Container and BMOC to BOCC; Formatting of key numbers; searched for all document references and added them to the Reference Table 11.1-1	All
August 7, 2012	B	Brought into this document the specific segments of an Athena SP (provided by Infogard) where our documents could benefit from their language.	Specific noted areas
August 21, 2012	B	This version was written onto the primary document in TFS as a new version. Rogers's latest changes are included in this version. No changes made to the document, only this note added for clarity.	
August 21, 2012	C	By direction of Dean B I have accepted the track changes only. All comments have been left active, no wording changes or content changes made. Issues with document number resolved, this is Dev_32_082. Cryptographic Module words were taken out of the title as instructed by Roger B. The format was checked for consistency only.	All
August 22, 2012	C	Validated that the CKM Attribute Container Applet Version was 1.2	
August 28, 2012	D	Patent list updated. Changes to the document made by Wai have been incorporated	All
August 30,2012	D	Updated PIV Applet version number to match the PIV Applet Man	Page 4
September 9, 2012	E	Compared the most recent version of SP with the changes received from Steve Weymann and updated our most recent version to reflect those changes. Where his changes did not comply with our document template and CM policy (first use acronym and labeling tables) the changes were not implemented.	All
October 2, 2012	F	Updated with missing information	All
December 14, 2012	G	Updated due to SP800-133 completion status affecting section references. Also updated the CSP list due to missing items found in the contactless review	3.4, 3.8, 3.9.4
August 7, 2013	H	Updated with comments from CMVP	All

Table of Contents

List of Figures

List of Tables

1 Introduction

The purpose of this document is to define the ***Security Policy for the TecSec Armored Card – Contact Cryptographic Module (CM)*** as part of the [FIPS 140] certification process. The CM, validated to [FIPS 140] overall Level 2, is a single-chip embodiment with the GlobalPlatform Java Card operating system, the contact interface subset of a dual-chip PIV [FIPS 201] solution, Biometric On Card Comparison (BOCC) and CKM® Data Attribute Container functionality.

The [FIPS 140] security levels for the CM are as follows:

Table 1.0-1 Security Level of Security Requirements

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

1.1 Scope

The TecSec Armored Card – Contact Cryptographic Module is the product defined. This document is part of a set of documents documenting the cryptographic module embedded in the card. There is also a set of documents for the Contactless chip.

1.2 Hardware

The CM is specifically designed for smart cards and targets ID applications. The physical form of the CM is depicted in figure 1.2-1 below. A block diagram of the CM is depicted in Figure 1.2-2 below.

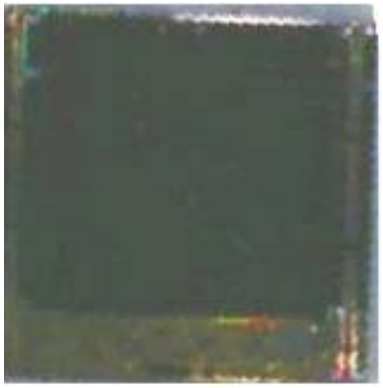

Figure 1.2-1 - CM Physical Image

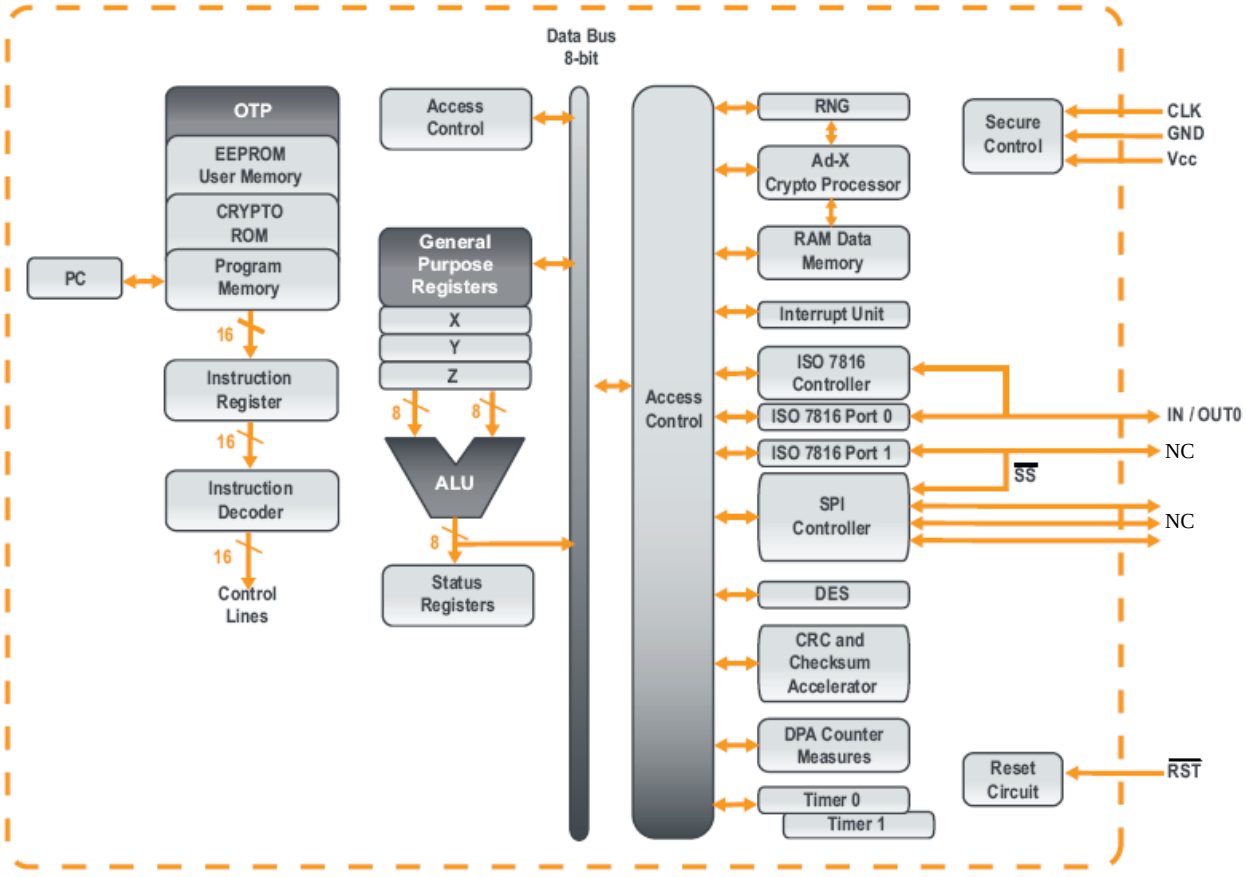

Figure 1.2-2 TecSec Armored Card – Logical Block Diagram

The CM Processor is a low-power, high-performance, 8/16-bit microcontroller with ROM program memory, EEPROM memory, based on the RISC architecture. The CM Processor features the Ad-X cryptographic accelerator for fast computation and low-power operation, based on a 32-bit multiplier-accumulator architecture designed to accelerate encryption and authentication functions.

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

The CM will typically be embedded into a plastic smart card body and connected to an ISO 7816 compliant contact plate. The CM boundary separates the chip from the card and contact plate. The cryptographic boundary is the surface of the chip and associated bond pads, and not the entire smart card.

1.3 Firmware

CM firmware comprises five Java Card applets implementing PIV contact features, the Biometric On Card Comparison (BOCC) applet and the CKM Attribute Container applet (one applet, potentially with multiple instances) and the CKM Info applet (for reporting on free resources) running on a GlobalPlatform Java Card operating system. Assembled onto a smart card with a companion module for Contactless functionality, the CM has been validated for conformance to [SP 800-73] – see NPIVP PIV Card Application Cert. #35.

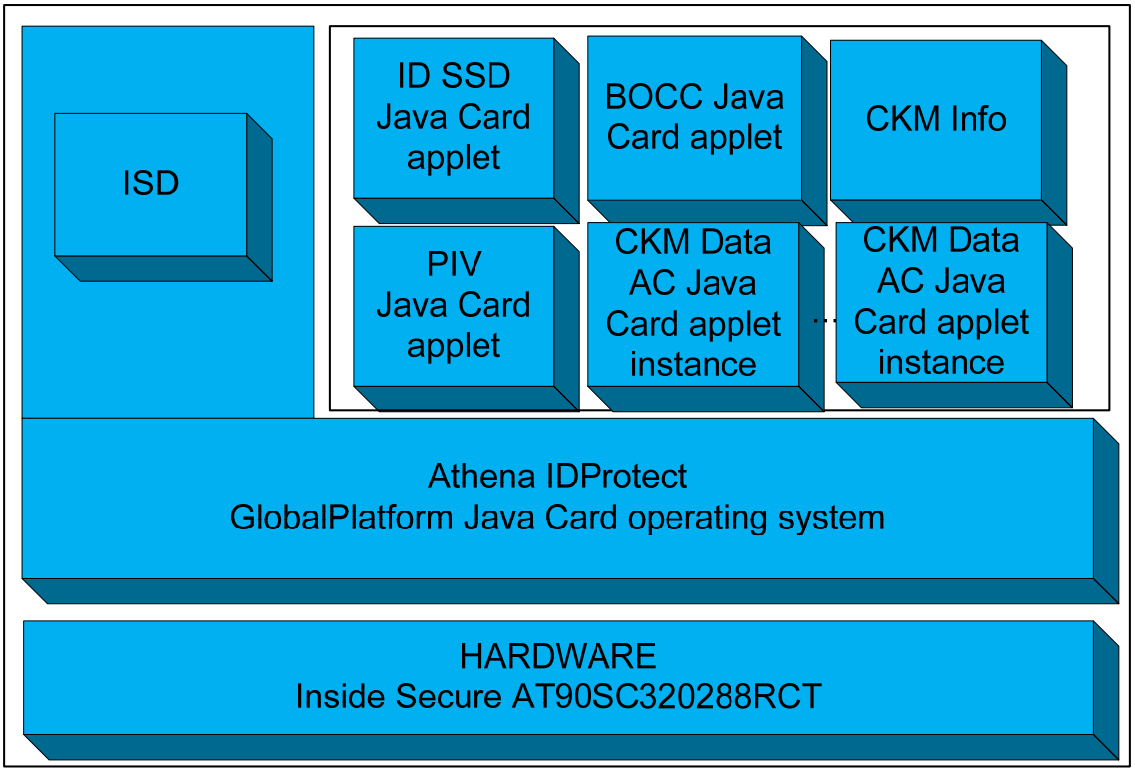

Figure 1.3-1 Crypto Module Block Diagram

The ISD applet is also known as the Global Platform Card Manager. ISD and SSD applets have identical functionality but distinct roles, differentiated by Security Domain keyset.

The embedded operational environment implementation is compliant with:

- GlobalPlatform, Card Specification, Version 2.1.1, March 2003
- GlobalPlatform, Card Specification 2.1.1, Amendment A, March 2004
- GlobalPlatform, Card Specification 2.2, Amendment D Secure Channel Protocol 03, Version 1.1, September 2009
- 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

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

The Java Card API provides a large set of cryptographic services. Some of these services rely on hardware. All applets are written in Java (as limited by the Java Card standards).

1.4 Versions and Mode of Operation

Hardware: P/N Inside Secure AT90SC320288RCT Revision E

Firmware

- P/N Athena IDProtect Version 0108.0264.0001
- P/N TecSec SSD Applet Version 1.001
- P/N TecSec PIV Applet Version 1.007
- P/N TecSec BOCC Applet Version 1.001
- P/N TecSec CKM Attribute Container Applet Version 1.002
- P/N TecSec CKM Info Applet Version 1.000

The module is always in the Approved mode of operation. To verify that a module is in the Approved mode of operation, the Card Issuer must:

1. Send GET DATA to the ISD applet with the CPLC Data tag and verify that the OS version matches 0108.0264.0001.
2. Validate that the SSD and PIV applets are in the FIPS mode as per [PIVAPP]. The SSD shall be version 1.001 and the PIV shall be 1.007.
3. Select the BOCC applet and verify that the File Control Information (FCI) returned from the BOCC applet indicates version 1.001. (See [BOCCAPP] for more details.)
4. Use the Configuration service (Get TecSec Information command) on the CKM Attribute Container applet. The version shall be 1.002. See [CKMAPP] for details.

2 Ports and Interfaces

The CM functions as a slave processor, accessed via a smart card reader over an ISO/IEC 7816 compliant interface. The CM supports both the T=0 and T=1 half-duplex transmission protocols.

Table 2.0-1 Ports and Interfaces

PIN	DESCRIPTION	LOGICAL INTERFACE TYPE
CLK	External Clock signal 1 – 10.1MHz	Control in
GND	Ground	Power
VCC	Supply Voltage Power 1.62 – 5V	Power
In/Out 0	Input/Output	Data in, data out, control in, status out
NC	Unused	No Connect
RST	External Reset signal	Control in

3 Cryptographic Functionality

The CM operating system implements the FIPS Approved and Non-FIPS Approved cryptographic function listed in Table 3.0-1 and Table 3.0-2 below.

Table 3.0-1 FIPS Approved Cryptographic Functions

FUNCTION	ALGORITHM	DESCRIPTION	CERT #
Random Number Generation	[SP 800-90] Hash_DRBG	[SP800-90] DRBG. The Module supports a SHA-256 based Hash_DRBG.	98
Message Digests	SHA-1[1]	[FIPS 180-2] Secure Hash Standard compliant hashing algorithms	1465
	SHA-256		
	SHA-512		
Message Authentication Codes	HMAC-SHA-512	[FIPS 198] Keyed Hash Message Authentication Code. Uses the Cert. #1465 SHA-512 primitive.	1354 (HMAC)
	AES CMAC	[SP 800-38B] AES CMAC. Uses the Cert. #1654 AES-256 primitive.	2226 (AES)
Digital Signature	RSA PKCS#1.5	[FIPS186-2] RSA signature generation and verification. The Module supports [PKCS#1] RSASSA-PSS and RSASSA-PKCS1-v1_5 with 1024- and 2048-bit RSA keys.	824
	ECDSA	[FIPS186-3] Elliptic Curve Digital Signature Algorithm. The Module supports the NIST defined P-256, P-384 and P-521 curves for signature generation and verification, and key pair generation.	214
Encryption and decryption	Triple-DES	[SP800-67] Triple Data Encryption Standard Algorithm. The Module supports the 2-Key[2] and 3-Key options; in ECB and CBC modes.	1087
	AES	[FIPS197] Advanced Encryption Standard algorithm. The Module supports AES-128, AES-192 and AES-256; in ECB and CBC modes.	1654
Key Generation	ECDSA	[FIPS186-3] Elliptic Curve Digital Signature Algorithm. The Module supports the NIST defined P-256, P-384 and P-521 curves for key pair generation.	214
Key Agreement	ECC CDH	[SP800-56A] The Section 5.7.1.2 ECC CDH Primitive only. The module supports the NIST defined P-256, P-384 and P-521 curves.	2 (CVL)
Key Derivation	KDF CTR	[SP 800-108] KDF in Counter Mode, using the Cert. # 1354 HMAC-SHA-512 and Cert. #2226 AES-CMAC primitives and the Cert.#98 DRBG.	4 (KDF)

[1] Per NIST SP 800-131A: Through December 31, 2013, the use of SHA-1 is deprecated for digital signature generation. *SHA-1 shall not be used for digital signature generation after December 31, 2013.*

[2] Per NIST SP 800-131A: Through December 31, 2015, the use of 2-key Triple DES for encryption is restricted: the total number of blocks of data encrypted with the same cryptographic key shall not be greater than 2^{20}. *After December 31, 2015, 2-key Triple DES shall not be used for encryption.* Decryption using 2-key Triple DES is allowed for legacy-use.

Table 3.0-2 Non-FIPS Approved But Allowed Cryptographic Functions

CATEGORY	ALGORITHM	DESCRIPTION
Random Number Generation	NDRNG	Hardware RNG; minimum of 64 bits per access. The HW RNG output is used to seed the FIPS approved DRBG.
Key Decapsulation	RSA	The module implements a non-SP 800-56B-compliant Key Transport primitive (RSA key decapsulation). This operation follows the PIV specification [SP 800-73] mechanism and does not establish a key or CSP into the module.
RSA Key Generation	RSA	ANSI X9.31 RSA key pair generation (untested, non-compliant). The Module supports 1024- and 2048-bit RSA key generation. Per IG 7.12, the non-Approved RSA key generation method is allowed for use in the Approved mode until the transition end date of 12/31/2013.
AES Key Wrap	AES	[AESKeyWrap] AES Key Wrap. The Module supports AES key wrapping with AES-256. (Used for key output, not key establishment.)
MAC	AES CMAC	AES CMAC (untested, non-compliant). The Module supports AES CMAC with AES-128, AES-192 and AES-256 for GlobalPlatform SCP03. The AES CMAC implementation is embedded within the SCP functionality and was not CAVP validated, but is not required for secure operation of the module or to meet FIPS requirements.
ECC Key Agreement	EC Diffie-Hellman	Non-SP 800-56A compliant EC Diffie-Hellman. Uses the CAVP tested ECC CDH primitive. (Key establishment methodology provides between 128 and 256 bits of encryption strength.)

The CM implements GlobalPlatform Secure Channel Protocol 03 (SCP03) for authentication and the establishment of session keys for use in secure channel data encryption and data integrity functions for the CI and IDI roles.

The CM implements a Supplemental Security Domain to administer the PIV and BOCC applets, associated with the IDI role.

The PIV applet provides the cryptographic end-point services specified in [SP 800-73] for the contact interface. The CKM Attribute Container applet provides CKM® Combiner / Recombiner and CKM Data Attribute Container functionality, described further below. The BOCC applet provides cryptographic services to securely transport authentication data.

3.1 Critical Security Parameters

All CSPs used by the CM are described in this section. All usage of these CSPs by the CM, including all CSP lifecycle states, is described in Section 0, cross referenced to roles and services.

3.1.1 Operating System and Security Domain CSPs

CSPs used by the CM's operating system are prefixed with OS.

Table 3.1.1-1 CM Operating System and Security Domain CSPs

KEY	DESCRIPTION / USAGE
Operating System CSPs	
OS-DRBG-SEED	384 bit random value from HW RNG used to seed the DRBG (entropy input)
OS-DRBG-STATE	880 bit value of current DRBG state, inclusive of V and C
OS-MKEK	AES-256 key used to encrypt all secret and private keys stored in the EEPROM
OS-PKEK	AES-256 key used to encrypt all PINs stored in the EEPROM
Global Platform SCP03 – Security Domain Keyset	
SD-KENC	AES-256 key used by the CI and IDI roles to establish SD-SENC.
SD-KMAC	AES-256 key used by the CI and IDI roles to establish SD-SMAC and SD-SRMAC.
SD-KDEK	AES-256 data decryption key used by the CI and IDI roles to decrypt CSPs
SD-SENC	AES-256 session encryption key used by the CI and IDI roles to encrypt/decrypt Secure Channel Session data
SD-SMAC	AES-256 session MAC key used by the CI role to verify inbound Secure Channel Session data integrity MAC
SD-SRMAC	AES-256 session MAC key used by the CI role to generate outbound Secure Channel Session data integrity MAC

The CM supports two sets of security domain keys, ISD and SSD.

3.2 BOCC Applet CSPs

BOCC applet CSP names are prefixed with "BOCC".

Some key identifiers permit different algorithms for a given key identifier; correspondingly, in the table below, BOCC-KEAK is shown with multiple key types.

Table 3.2-1 BOCC Applet CSPs

KEY	DESCRIPTION / USAGE
BOCC-BIO	Private portion of biometric authentication data, 1-n instances
BOCC-KDK	RSA 1024, 2048 RSA key transport private key; an optional* key used to decapsulate BOCC-SENC. This key may be used by the Sign Certificate Request until a valid certificate is loaded into the module.
BOCC-KAK	ECDH P-256, P-384 key agreement key; an optional* ECC private key used for ECDH establishment of BOCC-SENC. This key may be used by the Sign Certificate Request until a valid certificate is loaded into the module.
BOCC-SENC	AES-128/192/256 session data decryption key; established using ECDH or using RSA key transport.

3.3 PIV Applet CSPs

PIV applet CSP names are prefixed with "PIV".

[SP 800-73] defines the operations performed by the PIV applet and [SP 800-78] defines the cryptographic requirements for the PIV applet. Some key identifiers described in these specifications permit different algorithms for a given key identifier; correspondingly, in the table below, PIV-APSK, PIV-CMENC, PIV-DSPSK and PIV-CAPS are shown with multiple key types.

The [SP 800-73] draft specification defines a different usage for the [SP 800-78] 9D key when used with RSA or EC DH algorithms, hence the separation of PIV-KMKDK and PIV-KMKGK below.

Table 3.3-1 PIV Applet CSPs

KEY	DESCRIPTION / USAGE
PIV-LPIN	PIV Local PIN, per [SP 800-73]. 6-8 char plaintext string. The module enforces use of numeric ('0' – '9') values only.
PIV-GPIN	Global PIN 6-8 char plaintext string. The module enforces use of numeric ('0' – '9') values only.
PIV-LPUK	Local PIN unblocking key, per [SP 800-73]. 8 byte plaintext string. 0xFF reserved for padding.
PIV-A-PSK	[SP 800-78] 9A (FIPS 201-1 PIV Authentication Key) private signature key. RSA 1024, RSA 2048; ECDSA P-256.
PIV-CM-ENC	[SP 800-78] 9B (FIPS 201-1 Card Management Key) secret key. 3-Key Triple-DES; AES-128, AES-192, AES-256.
PIV-DS-PSK	[SP 800-78] 9C (FIPS 201-1 Digital Signature Key) private signature key. RSA 2048; ECDSA P-256, P-384.
PIV-KM-KDK	[SP 800-78] 9D (FIPS 201-1 Key Management Key) private key when used for RSA key decryption. RSA 2048.
PIV-KM-KGK	[SP 800-78] 9D (FIPS 201-1 Key Management Key) private key when used for the ECC CDH shared secret (Z value) generation function. ECDH P-256 and P-384 curves.
PIV-CAK	[SP 800-78] 9E (FIPS 201-1 Card Authentication Key). The PIV specifications permit both symmetric and asymmetric algorithms to be used for card authentication. This module supports all defined options: 3-key Triple-DES; AES-128, AES-192, AES-256; RSA 1024, RSA 2048; ECDSA P-256 and P-384 curves.

3.4 CKM Attribute Container CSPs

Table 3.4-1 Critical Security Parameters

KEY	DESCRIPTION / USAGE
CKM-CRD-MKn	CKM Credential Master Key n: 128 byte secret key material (0 to 10 instances). A constituent of CKM Symmetric and Asymmetric Credentials.
CKM-CRD-PAKn	CKM Credential Private Authorization Key n: Private component of an ECC P-521 key pair (0 to 10 instances). A constituent of a CKM7 Asymmetric Credential.
CKM-CRD-PSKn	CKM Credential Private Signature Key n: Private component of an ECC P-521 key pair (0 to 10 instances). A constituent of a CKM7 Asymmetric Credential.
CKM-EHS-PSK	CKM Ephemeral-Header-Signature Private Signature Key: Private component of an ECC P-521 key pair. Optional key used to sign the CKM header.
CKM-AUTH-SYM	CKM symmetric authentication key: optional AES-128, AES-192 or AES-256 key used for authentication, 0-24 instances.
CKM-USER-PSK	CKM user signing key: optional RSA 2048, ECDSA P-256, P-384 or P-521 key used for digital signature, 0-n instances
CKM-USER-SYM	CKM user symmetric key: optional AES-128, AES-192 or AES-256 key used for key wrap, encryption and decryption, 0-n instances.
CKM-USER-KAK	CKM user Key Agreement key: optional EC-CDH P-256, EC-CDH P-384 or EC-CDH P-521 key used for Key Agreement, 0-n instances
CKM-WK-DEK	CKM Working Key: AES-256 data encryption key used to protect CKM data.
CKM-WK-KWK	CKM Working-Key Key Wrapping Key: AES-256 key used to wrap CKM-WK-DEK for protected storage in the CKM header.
CKM-WK-SMK	CKM Working-Key Static Master Key: 128 byte secret key material, used as input to SP 800-108 KDF for derivation of the working key.
CKM-WK-EKGK	CKM Working-Key Ephemeral Key Generating Key: AES-256 key used as the key to the SP 800-108 PRF function for derivation of the working key.

3.5 Platform Public Keys

Table 3.5-1 Platform Public Keys

KEY	DESCRIPTION / USAGE
SD-DAP	RSA 1024 new firmware signature verification key.

3.6 PIV Applet Public Keys

The PIV Applet public keys are generated using the PIV Applet GENERATE ASYMMETRIC KEYPAIR service. An entity external to the CM packages these public keys in a certificate and is expected to store them back onto a card container using the PIV applet PUT DATA operation. The CM supports the PIV Applet GET DATA command to retrieve these certificates. Only the ID Issuer role can generate these keys.

These public keys are:

- Returned by the card when the matching RSA Private Key is generated.
- Not used for any other purpose or service on the CM

Table 3.6-1 PIV Public Keys

KEY	DESCRIPTION / USAGE
PIV-A-SVK	[SP 800-78] 9A (FIPS 201-1 PIV Authentication Key) public signature verification key. RSA 1024, RSA 2048; ECDSA P-256.
PIV-DS-SVK	[SP 800-78] Digital Signature Key (9C). RSA 2048; ECDSA P-256, P-384.
PIV-KM-KWK	[SP 800-78] Key Management Key (9D). RSA 2048.
PIV-KM-KZG	[SP 800-78] Key Management Key (9D), ECC CDH variant. ECDH P-256, P-384.
PIV-CA-PUB	[SP 800-78] Card authentication key (9E), RSA or ECDSA variant. RSA 1024 and 2048, ECDSA P-256, P-384.

3.7 BOCC Public Keys

Table 3.7-1 BOCC Public Keys

KEY	DESCRIPTION / USAGE
BOCC-KDK-PUB	RSA 1024, 2048 RSA key transport public key; an optional key provided to the external host for it to use to encapsulate BOCC-SENC.
BOCC-KAK-PUB	ECDH P-256, P-384 key agreement key; an optional ECC public key used for ECDH establishment of BOCC-SENC.

3.8 CKM Attribute Container Public Keys

Table 3.8-1 CKM Public Keys

KEY	DESCRIPTION / USAGE
CKM_CRD_PBAKn	CKM CReDential PuBlic Authorization Key n: 0 to 10 instances of the public component of an ECC P-521 key pair. A constituent of a CKM7 Asymmetric Credential.
CKM_CRD_SVKn	CKM CReDential public Signature Verification Key n: 0 to 10 instances of the public component of an ECC P-521 key pair. A constituent of a CKM7 Asymmetric Credential.
CKM-EHS-SVK	CKM Ephemeral-Header-Signature Signature Verification Key: an optional ECC P-521 key pair, used to generate or verify a signature header.
CKM-USER-SVK	User defined public signature verification keys for data attribute containers. The CM supports as many instances as will fit in the attribute container.
CKM-USER-KAK-PUB	User defined public key agreement keys for data attribute containers: EC-CDH P-256, EC-CDH-P-384, EC-CDH P-521. The CM supports as many instances as will fit in the attribute container.

3.9 Key Generation and Key Establishment

3.9.1 Random Bit Generation

The DRBG is implemented in accordance with the **Hash_DRBG** method described in [SP 800-90] Section 10.1. 1. All DRBG parameters are in accordance with Table 2 of [SP 800-90].

3.9.2 Key Generation

The CM uses the [SP 800-90] DRBG to generate keys in accordance with applicable standards.

3.9.3 ECC Key Agreement Primitives

The CM implements a non-SP 800-56A compliant (untested) ECC Key Agreement scheme C (1,1, ECC-CDH). The ECC-CDH primitive is implemented in accordance with [SP 800-56A] Section 5.7.1.2 (ECC-CDH primitive – CAVP tested, CVL Cert. #2) and the Section 5.8.1 concatenated Key Derivative Function (KDF).

3.9.4 CKM Key Construction

The CM implements CKM Key Construction in accordance with [ANSI X9.73] Annex D and [ANSI X9.69]. CKM is a method of key establishment using the methods described in [SP 800-133] Section 7.4 and Section 7.6, with the exception that in CKM the key agreement primitives are used to protect data at rest rather than data in motion. That is, the primitives are used to derive a key value at different times: when the key is needed for storage and when the key is needed for retrieval. A given data protection scenario uses a configurable set of pre-shared keys, comprised of symmetric, asymmetric and shared secret (ECC CDH) key constituents. These keys are concatenated and digested by a SHA-512 in a configurable sequence to form a CKM Working-Key Key Wrapping Key (CKM-WK-KWK).

The CKM Working Key (CKM-WK-DEK) is derived from the CKM Working-Key Static Master Key (CKM-WK-SMK) and the CKM Working-Key Ephemeral Key Generating Key (CKM-WK-EKGK) using [SP 800-108]. The [SP 800-90] DRBG is used to derive or generate any key or random value required for this process. All primitives used in this process are Approved and CAVP validated, with the requisite self-tests. All elements of the process employ 256-bit security strength functions and key lengths: AES-256 symmetric keys, p521 ECC CDH and SHA-512.

4 Roles, Authentication and Services

Table 4.0-1 lists all operator roles supported by the module. This CM does not support a maintenance role. The CM does not support concurrent operators and clears previous authentications on power cycle.

Table 4.0-1 Roles Description

ROLE ID	DESCRIPTION
CI	Card Issuer (the Cryptographic Officer role for [FIPS 140] purposes). This role is responsible for managing the security configuration of the module. The Card Issuer authenticates to the module through the GlobalPlatform (GP) mutual authentication protocol. This protocol is based on the sharing of an AES key set between the Card Issuer operator and the CM ISD. Once authenticated, the Card Issuer is able to execute the services provided by the ISD in a Secure Channel Session (see [GP] for more details).
IDI	ID Issuer. This role is responsible for managing the security configuration of a loaded application. The ID Issuer authenticates to the module through the GlobalPlatform mutual authentication protocol. This protocol is based on the sharing of AES key sets between the ID Issuer operator and the CM embedded SSD. Once authenticated, the ID Issuer is able to execute the services provided by the application over an SCP03 secure channel session. This includes putting PIV objects into the PIV applet, putting PIV RSA and EC Private keys into the PIV applet, putting BOCC data into the BOCC applet and managing putting BOCC RSA and EC Private keys into the BOCC applet via the CS SSD.
PA	PIV Application Administrator. This role is responsible for managing PIV applet container content using the PIV applet PUT DATA command and invoking asymmetric key pair generation using the PIV applet GENERATE ASYMMETRIC KEY PAIR command. Authenticates to the module using the external authentication sequence of the GENERAL AUTHENTICATE command with the PIV-CM-ENC (9B) key.
PC	PIV Cardholder (the User role for [FIPS 140] purposes). This role is responsible for interaction with the cardholder PIV applet card command functions. The operator in this role has knowledge of the PIV User local PIN (PIV-LPIN) and/or global PIN (PIV-GPIN) and can perform cryptographic operations using the keys stored in the PIV applet as well as retrieve applet containers restricted to the cardholder. The PIV User authenticates to the module through the PIV applet by presenting the PIV User local or global PIN.
PP	PIV PIN Administrator. This role is responsible for interaction with the PIN administrator PIV applet card command functions. The operator in this role has knowledge of the PIV PIN Unblocking Key (PIV-LPUK) 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 LPUK in the CHANGE REFERENCE DATA or RESET RETRY COUNTER APDU commands.
CU	CKM User: CKM Attribute Container role used to grant or deny access to objects or CSPs. This role can be authenticated with multiple combinations of authentication data in accordance with the CKM access control scheme.
ACO	CKM Attribute Container Owner: CKM Attribute Container role used to grant or deny access to

ROLE ID	DESCRIPTION
	objects or CSP's. This role can be authenticated with multiple combinations of authentication data in accordance with the CKM access control scheme. This role is used to maintain the CSPs (loading/generating, …) and to create/destroy data objects in the attribute container.
PO	Public Operator. A 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 use the PIV Card Authentication service, which in accordance [SP 800-73] does not require authentication. The Public Operator does not have the ability to create, modify, substitute, or disclose any CSP.

4.1 SCP03 Authentication

The CM supports the [SCP03] mutual authentication handshake, providing identity based authentication of the Card Issuer (CI) and ID Issuer (IDI) roles. Authentication is associated to a security domain, which is in turn implicitly associated with a role as described above: the CM ISD Key Set corresponds to the CI role; the PIV SSD, BOCC SSD and CKM SSD key sets correspond to the ID Issuer role.

The [SCP03] mutual authentication verifies possession of a secret shared between the CM and the external operator. Access control restrictions are listed by service in the tables in Section 4.5. Each service available to the CI or IDI roles requires successful [SCP03] mutual authentication as described in this section.

This authentication 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 OS-MKEK and OS-MPEK 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 [SCP03] interaction utilizes the 256 AES session key associated with the domain to authenticate to the associated role. The authentication strength for this method is as follows:

- The probability that a random attempt at authentication will succeed is 1/2^128 (2.94E-39).
- 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 255/2^128 (7.49E-37).

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

4.2 PIV Authentication Methods

The CM implements cardholder verification as defined by [SP 800-73]. Briefly, the PIV cardholder or PIV PIN Administrator provides a shared secret string value in plaintext to the module via commands sent by an external application through a card reader. The CM compares the provided value to the corresponding stored authentication data, PIV-LPIN, PIV-GPIN, or PIV-LPUK, as identified by a parameter in the command. Each of these methods has an associated retry count. The retry counts are definable as card personalization parameters, with a maximum retry of 10.

[SP 800-73] defines the PIN and PUK parameters in the commands as described above. The CM PIV applet enforces a six numeric character minimum length. The authentication strength for this method is as follows:

- The probability that a random attempt at authentication will succeed is 1/10^6 (1.0E-6). This calculation is based on the PIV-LPIN and PIV-GPIN variants of this mechanism; the PIV-LPUK permits a larger character set (all values except 0xFF).
- 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 10/10^6 (1.0E-5).

The CM also implements the GENERAL AUTHENTICATE service in the PIV Applet for internal, external or mutual authentication as defined by the protocols described in [SP 800-73]. Only the internal authenticate and the internal portion of mutual authenticate are relevant to [FIPS 140] authentication requirements. Briefly, a random challenge of at least eight bytes is sent to the CM; the CM responds with the value of the challenge encrypted with the PIV-CMENC key (the [SP 800-78] ‘9B’ key, described in [FIPS 201] as the *Card Management Key*). The minimum equivalent strength of the possible PIV-CMENC key types is 112 bits. The CM enforces a maximum retry of 255 attempts. The authentication strength for this method is as follows:

- The probability that a random attempt at authentication will succeed is 1/2^64 (5.4E-20) at minimum, when the 3-Key Triple-DES variant of 9B is used. The CM implements all [SP 800-73] algorithm and strength options for this key; the AES variants are stronger (a lower probability of false authentication).
- 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 255/2^112 (1.38E-17)

All PIV PIN, PUK and cryptographic keys are identified by a one-byte value as defined in [SP800-78].

4.3 Biometric On Card Comparison

Biometric authentication strength is set by a biometric threshold parameter when the fingerprint is enrolled. The biometric algorithm provider has provided a Receiver Operating Curve (ROC) characteristic curve, achieved through a large statistical sampling process, to be used by the algorithm within the CM and by the corresponding enrollment software. To comply with [FIPS 140] authentication strength, the operator must select the 1/1,000,000 FAR setting when validating fingerprint minutiae.

Biometric On Card Comparison may also be used as a second factor to the PIN (the *Fingerprint and PIN* option). In this configuration, authentication strength is met by the PIN, and the FAR may be set to a lower level (See 4.4 CKM Authentication).

4.4 CKM Authentication

The CKM Authentication can be configured to use basic authentication mechanisms in an And/Or combination. For instance one CU role can be configured to be "(Pin and Bio) or SecureChannel." The valid authentication mechanisms are:

- Secure Channel
- External Authentication (Challenge Response)
- Biometric Match using the BOCC applet

NOTE: If the BOCC mechanism is used alone then it must be configured for the 1:1,000,000 FAR by the Identity Issuer (IDI role).

Both the Secure Channel and External Authentication use keys stored in the CM for the validation.

The CKM Attribute Container applet uses the proprietary file system described in detail in [CKMAPP] to securely store key information. The applet file system enhances the Global Platform file system. Every file (MF, DF, EF, Object) has 5 security indicators that describe who can perform 5 types of actions on the files. The actions are ***Read***, ***Write***, ***Delete***, ***Crypto***, and Life Cycle State Identifier (***LCSI)***. ***Read*** controls the reading of non-internal file types. Internal file types cannot be returned to the card edge. ***Write*** controls the writing/updating/PutKey/GenerateKey operations. ***Delete*** specifies who can delete the file. ***Crypto*** specifies that the card may perform cryptographic operations with this file assuming that the command and file type match. The ***LCSI*** security setting controls who can perform the ActivateEF, DeactivateEF and TerminateEF commands on that file. It is also used in some special cases like the resetRetryCounter to specify which authentications are required in order to

perform that command. Each security setting indicates which of the 6 CU roles, the Attribute Container Owner (ACO) role or Public role that are needed to perform the specified services.

If the CKM Attribute Container Applet is configured to support the PKCS #11 standard then 2 of the CU roles are predefined for the PKCS #11 User and PKCS #11 Security Officer (SO).

For the Secure Channel and External Authentication mechanisms the associated key files should be created as internal keys which prevent all access to the keys by the card edge (the keys cannot be read).

The type of the key file determines the type of authentication mechanism that is to be used and how many support files will also be needed. Here is a table of the supported authentication key file types and the mechanism used to authenticate the file.

Table 4.4-1 Supported Authentication Key File Types

FILE TYPE	AUTHENTICATION MECHANISM DESCRIPTION
AES Keyset	Secure Channel type 03 or Verify command using the first key
CKM Credential	Secure Channel type F2
AES key	Verify command (performs External Authentication mechanism)
Biometric Template	Global Biometric applet is authenticated

Note: The file types in the above table also include the internal file types. Therefore AES Keyset also matches Internal AES Keyset.

4.5 Services

All services implemented by the CM are listed in the tables below. Each service description also describes all usage of CSPs by the service. The following security rules also apply to the CM:

- No additional interface or service is implemented by the CM 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 SET STATUS (TERMINATED) zeroization service in the CI role.
- The module does not support manual key entry, output plaintext CSPs or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

4.5.1 General Purpose and Unauthenticated Services

The services listed next do not require authentication, and may be performed by any role, including the unauthenticated PO role.

Table 4.5.1-1 General Purpose and Unauthenticated Services and CSPs

SERVICE	DESCRIPTION
Card reset	Power cycle the CM by removing and reinserting it into the contact reader slot, or by reader assertion of the RST signal. On the first instance of card reset, the CM generates OS-MKEK (global component) and OS-MPEK. On any card reset, the CM overwrites OS-DRBG-STATE On any card reset, the card zeroizes SD-S-ENC, SD-S-MAC, SD-S-RMAC.
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	When used by unauthenticated PO or by the authenticated PA or PC, to retrieve public data. No CSPs are accessed this service in this context.
GET RESPONSE	Retrieves additional bytes buffered by the CM from the previous command. As a low level transport protocol, does not access any CSPs.
INITIALIZE UPDATE	Initiate a GlobalPlatform Secure Channel Session, setting key set version and index. When used in the ISD, executes using OS-MKEK, ISD-KENC, ISD-KMAC and generates ISD-SENC; ISD-SMAC. When used in the SSD, executes using SSD-KENC, SSD-KMAC and generates SSD-SENC and SSD-SMAC.

4.5.2 Security Domain Administrative Services

The CI and IDI roles are active only when the applicable domain is currently selected following successful authentication.

The ISD, ID SSD and BOCC SSD key sets and the PIV-CA key are loaded within a GlobalPlatform Secure Channel Session to ensure confidentiality (256-bit AES encryption) and integrity (AES CMAC).

Application loading (utilizing several of the above services) is an operating system function available before and after card issuance, but restricted to the Card Issuer or ID Issuer: an SCP03 Secure Channel Session must be open between the external operator (more precisely the middleware the CI or IDI is using to manage card content) and the ISD. Application loading is protected by an AES CMAC on every block of data.

The IDI is responsible for application personalization and lifecycle management in accordance with [GP].

Table 4.5.2-1 Domain Administrative Services

SERVICE	DESCRIPTION	CI	IDI
DELETE (card content or key)	Delete a uniquely identifiable object such as an Executable Load File (package), an Application (applet) or an Executable Load File and its related Applications. The DELETE (key) service deletes a key uniquely identified by the KID and KVN within the applicable domain: SD-Key-ENC, SD-Key-MAC, SD-Key-	X	X

SERVICE	DESCRIPTION	CI	IDI
	DEK. The IDI role is permitted to execute the DELETE service only if the APDU commands are previously signed by the Card Issuer (GlobalPlatform Delegated Management). When invoked within an [SCP03] secure channel session executes using SD-S-MAC, SD-S-ENC SD-S-RMAC, determined by security level.		
EXTERNAL AUTHENTICATE	Open a GlobalPlatform Secure Channel Session with the ISD to communicate with confidentiality and integrity, inclusive of operator authentication.. Executes using OS-MKEK. When invoked within an [SCP03] secure channel session executes using SD-S-MAC, SD-S-ENC, SD-S-RMAC, SD-Key-ENC, SD-Key-MAC, SD-Key-DEK.	X	X
Personalize Applet	Personalize the PIV applet or BOCC applet. Executes using OS-DRBG-STATE. Writes BOCC-KEAK. PIV-LPIN, PIV-GPIN, PIV-LPUK, BOCC-BIO, PIV-KMKDK, PIV-KMKGK Generates BOCC-KEAK. PIV-APSK, PIV-CMENC, PIV-DSPSK, PIV-KMKDK, PIV-KMKGK , PIV-CAK Outputs public key for BOCC-KEAK, PIV-APSK, PIV-DSPSK, PIV-KMKDK, PIV-KMKGK, PIV-CAK		X
GET STATUS	Retrieve Life Cycle status information of the ID SSD, and Executable Load File, Executable Module, Application or associated Security Domain. When invoked within an [SCP03] secure channel session executes using SD-S-MAC, SD-S-ENC SD-S-RMAC, determined by security level.	X	X
Install and Load Applet	Initiate or perform the various steps required for CM applet management. The IDI role is permitted to execute this service only if the APDU commands are previously signed by the Card Issuer (GlobalPlatform Delegated Management). Executes using OS-DRBG-STATE, SD-S-MAC, SD-S-ENC, SD-S-RMAC, SD-Key-ENC, SD-Key-MAC, SD-Key-DEK.	X	X
PUT KEY	The service can: Replace an existing key with a new key Replace multiple existing keys with new keys Add a single new key Add multiple new keys Writes SD-Key-ENC, SD-Key-MAC, SD-Key-DEK. Executes using OS-DRBG-STATE, OS-KSSK, SD-S-MAC, SD-S-ENC, SD-S-RMAC, SD-Key-ENC, SD-Key-MAC, SD-Key-DEK.	X	X
SET STATUS	Modify the Card Life Cycle State or an associated Application Life Cycle State. The IDI role can modify the ID SSD Life Cycle State or an associated Application Life Cycle State. When invoked with the TERMINATED status in the CI role, zeroizes OS-KSSK and OS-PSSK, effectively destroying all other CSPs. Executes using SD-S-MAC, SD-S-ENC, SD-S-RMAC, SD-Key-ENC, SD-Key-MAC, SD-Key-DEK.	X	X
STORE DATA	Transfer data to the SD.	X	X

SERVICE	DESCRIPTION	CI	IDI
	Executes using SD-S-MAC, SD-S-ENC, SD-S-RMAC, SD-Key-ENC, SD-Key-MAC, SD-Key-DEK.		

4.5.3 PIV Applet Card Command Services

Table 4.5.3-1 Services, Roles, and Associated CSP Usage

SERVICE	DESCRIPTION	PA	PC	PP
CHANGE REFERENCE DATA	Change the PIV-LPIN or PIV-GPIN. Requires the correct current value		X	
GENERAL AUTHENTICATE	As defined in [SP 800-73] for the Contact function, has several different usages depending on the operator and on command tags. When invoked with a challenge or witness tag by the PC operator, executes the specified algorithm using PIV-APSK, PIV-DSPSK, PIV-KMKDK, or PIV-KMKGK as specified in the command. When invoked with a challenge or witness tag by the PC or PO operator, executes the specified algorithm using PIV-CAPS. When invoked with a challenge or witness tag by the PA operator, executes the specified algorithm using PIV-CMENC. When invoked for nonce generation in a challenge executes using OS-DRBG-STATE	X	X	
GENERATE ASYMMETRIC KEY PAIR	The PIV Application Administrator can cause any of the PIV RSA key pairs (9A, 9C, 9D, 9E) to be created and stored in the PIV applet.	X		
GET DATA	The GET DATA card command retrieves the data content of the single data object whose tag is given in the data field.		X	
PUT DATA	The PIV Application Administrator can replace the contents of PIV Data objects using this APDU command.	X		
RESET RETRY COUNTER	Resets the retry counter of the PIN to its initial value and changes the PIN's reference data			X
VERIFY	Authenticate the PIV cardholder using PIV-LPIN or PIV-GPIN.		X	

4.5.4 CKM Attribute Container Applet Services

CKM Attribute Containers are a 7816 File/Data Object system with PKCS 11 extensions. Each Attribute Container has an MF with at least some EFs; and may have a credential set. Commands are permitted to an authorized operator; command access control is based on both file/data object type and file / data object permissions.

CKM Attribute Containers offer Cryptographic Services and Authentication Services as shown in the tables in this section.

Authentication for file / data object is any and/or combination of

- External / Mutual authentication
- SCP03
- Biometric

5 8-bit words per file/object: Read Write Delete Crypto LCSI

8 bits represent public + 6 general operator roles (CU) and the ACO role

One specialized operator type is Attribute Container owner. Attribute Container Owner has additional capability on some commands: e.g. retrieve a file map for all files, delete any file.

Table 4.5.4-1 CKM Attribute Container Applet Services

SERVICE	DESCRIPTION	CU	ACO
File / data object	This service is the general purpose file and object read/write functionality that is derived from ISO/IEC 7816-4 and ISO/IEC 7816-9	X	X
Authentication	This service contains commands that are used to authenticate a role or validate that a role is authenticated	X	X
Encrypt / decrypt	These commands are used to encrypt or decrypt user provided data using an on-card CSP	X	X
RSA Wrap/Unwrap	These commands are used to wrap or unwrap caller specified data using on card RSA CSPs	X	X
Sign / verify	These commands are used to create or validate a signature using a user provided hash value and an on-card CSP	X	X
Key management	These commands are used to establish keys (CSPs) on card	X	X
Configuration	These commands are used to configure the attribute container or to retrieve configuration information about the attribute container		X

4.5.5 CKM Info Applet

The CKM Info applet has no CSPs and no defined roles. All services are available to the unauthenticated role.

Table 4.6-1 CKM Info Applet Services

SERVICE	DESCRIPTION	PUBLIC
Query	Returns the free card resources, specifically available EEPROM, and RAM in bytes.	X

5 Self Test

Table 5.0-1 Power-On Self-Tests

TEST TARGET	DESCRIPTION
Firmware integrity	A CRC 16 EDC is used to test firmware integrity.
SHS	Performs separate SHA-1, SHA-256 and SHA-512 KATs.
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in CBC mode.
AES	Performs separate encrypt and decrypt KATs using an AES-128 in CBC mode.
RSA	Performs a KAT (RSA PKCS#1 sign and verify) using an RSA 2048 bit key pair.
ECDSA	Performs a KAT (ECDSA sign and verify) using an ECC P-256 key pair.
ECC-CDH	Performs an ECC-CDH KAT using an ECC P-256 key pair.
Ctr KDF HMAC	Performs HMAC SP 800-108 KDF in Counter mode; incorporates self-test of the embedded HMAC-SHA-512 algorithm.
Ctr KDF AES-CMAC	Performs AES-CMAC SP 800-108 KDF in Counter mode; incorporates self-test of the embedded AES-CMAC algorithm.
DRBG	Performs a KAT of the DRBG functions.

Table 5.0-2 Conditional Self-Tests

TEST TARGET	DESCRIPTION
HW RNG	On every generation of 64 bits of random data by the HW RNG the Module performs a stuck fault test to assure that the output is different from the previous value. In case of failure the Module enters the “CM is mute” error state.
DRBG	Each time the Module is powered on it performs the DRBG health test monitoring functions. On every generation of 256 bits of random data by the DRBG, the Module performs a stuck fault test to assure that the output is different from the previous value. In case of failure the Module enters the “CM is mute” error state.
Key Gen PCT	When an asymmetric key pair is generated (for RSA or ECC) the Module performs a Pairwise Consistency Test (PCT). In case of failure the invalid key pair is zeroized and the Module enters the “CM is mute” error state.
Key pair integrity	When a signature is generated (for RSA or ECDSA) the Module performs a PCT using the associated public key. This PCT is also performed during the RSA and ECDSA KAT.
Firmware Load	When new firmware is loaded into the Module using the LOAD command, the Module verifies the integrity of the new firmware by verifying a signature of the new firmware using the ISD-DAP public key; the new firmware in this scenario is signed by an external entity using the private key corresponding to ISD-DAP. If the signature verification fails the Module returns an error and does not load the firmware.
CSP Usage	Every CSP is protected with a 16 bit CRC. The integrity is checked when a CSP is used. In case of failure the Module enters the “ISD is terminated” error state.

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 Physical Security and Mitigation of Other Attacks

The CM is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The CM uses standard passivation techniques and is protected by a hard opaque tamper-evident metal active shield. The CM hardware is designed to meet Common Criteria EAL5+.

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.

The CM chip is coated with opaque, hard tamper-evident materials to deter direct observation within the visible spectrum and to provide 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.

The CM has passed Level 4 physical security testing for hardness, opacity and tamper evidence.

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 PIN and Keys by monitoring the module power consumption and timing of operations or bypass sensitive operations.

This Cryptographic Module is protected against SPA, DPA, Timing Analysis and Fault Induction by combining State of the Art 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. This chip is

Common Criteria certified; more information is available her http://www.commoncriteriaportal.org/products/.

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

9 Security Rules and Guidance

The Module implementation enforces the following security rules:

- The Module does not output plaintext CSPs. The Module does not support manual key entry.
- The Module does not output intermediate key values.
- 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 CSPs are zeroized by the zeroization service.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.

Additional applications can be loaded in the Module after issuance as specified in GlobalPlatform. However, any other firmware loaded into this Module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Application loading is one of the services provided by the operating system that is restricted to the Card Manager: a Secure Channel Session must be open between the external operator (more precisely the middleware the CM is using to manage content) and the ISD. Application loading is protected by ISD-DAP.

The application loading service is available before and after Module issuance.

The CM is responsible for application personalization and lifecycle management following GlobalPlatform. The application loading service uses RSA 1024 for Data Authentication Pattern (DAP) operations. DAP is used for firmware load integrity and is deprecated per SP800-131A but may be used through 12/31/2013 for digital signature verification. All other uses of RSA 1024 are there for legacy operations and should not be used for new signatures. The user of the CM shall not use RSA 1024 for any other purpose as all other uses are disallowed per SP800-131A.

Since the BOCC can be used as a form of authentication in the CKM Attribute Container applet, it shall be configured by the Identity Issuer (IDI Role) for 1:1,000,000 FAR when the

fingerprints are enrolled. If a lesser FAR is used the BOCC either cannot be used or must be used in an AND condition with either the external authentication (Verify command) or a secure channel. The process to set the FAR is described in [PIVAPP].

10 References

The documents listed in this section form a part of this document to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this document, the contents of this document, upon final approval, are considered the superseding authority. The latest versions of these documents are assumed to be applicable unless otherwise specified by including the specific version. Refer to the master list of documents, or equivalent, for the latest revision and date.

The following standards are referred to in this Security Policy.

Table 10.0-1 References

ACRONYM	FULL SPECIFICATION NAME
[FIPS140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-2]	SECURE HASH STANDARD
[FIPS 198]	The Keyed-Hash Message Authentication Code (HMAC), March 6, 2002
[FIPS201]	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006 (Change Notice 1, June 23, 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
[ANSI X9.69]	ANSI X9.69-2006 Framework for Key Management Extensions.
[ANSI X9.73]	ANSI X9.73-2010 Cryptographic Message Syntax ASN.1 and XML
[ANSI X9.96]	ANSI X9.64-2004 XML Cryptographic Message Syntax (XCMS)
[SCP03]	GlobalPlatform Card Technology Secure Channel Protocol 03 Card Specification v 2.2 – Amendment D Version 1.1 September, 2009
[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
[GP]	GlobalPlatform Card Specification v2.1.1
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography

ACRONYM	FULL SPECIFICATION NAME
[SP 800-73]	Interfaces for Personal Identity Verification –Part 1: End-Point PIV Card Application, Namespace, Data Model and Representation, September 2008 Interfaces for Personal Identity Verification –Part 2: End-Point PIV Card Application Card Command Interface, September 2008
[SP 800-78] 9A	(FIPS 201-1 *PIV Authentication Key*) Private signature key
[SP 800-78] 9B	(FIPS 201-1 *Card Management Key*) Secret key
[SP 800-78] 9C	(FIPS 201-1 *Digital Signature Key*) Private signature key
[SP 800-78] 9D	(FIPS 201-1 *Key Management Key*) Private key when used for RSA key decryption
[SP 800-78] 9D	(FIPS 201-1 *Key Management Key*) Private key when used for the EC DH shared secret (Z value) generation function
[SP 800-78] 9E	(Card Authentication) key. The PIV specifications permit both symmetric and asymmetric algorithms to be used for this purpose
[SP 800-90]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
[PIVAPP]	TecSec PIV Application Provider Manual
[BOCCAPP]	Bio Cardholder Verification Module (CVM) APDU List
[CKMAPP]	CKM® Attribute Container Applet Manual

Table 10.0-2 Abbreviations and Acronyms

ACRONYM	DEFINITION
AC	Attribute Container
AdvX	Advance Crypto
AES	Advanced Encryption Standard
AID	Application Identifier
AP	ID Issuer
APDU	Application Protocol Data Unit (IS0 7816/14443 data packet)
API	Application Programming Interface
AVR	Automatic Voltage Regulation
BOCC	Biometric On Card Comparison
CA	Certificate Authority
CI	Card Issuer
CM	Cryptographic Module
CSP	Critical Security Parameter
DAP	Data Authentication Pattern
DES	Data Encryption Standard

ACRONYM	DEFINITION
DF	Directory File (per 7816-4)
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
ECC-CDH	Elliptic Curve Cryptography - Cofactor Diffie-Hellman
ECDSA	Elliptic Curve Digital Signing Algorithm
EEPROM	Electronically Erasable Programmable Read Only Memory
EF	Element File (per 7816 -4)
EMI/EMC	ElectroMagnetic Interference, ElectroMagnetic Compatibility
GP	GlobalPlatform
HRNG	Hardware Random Number Generator
ID	Identity
IDI	Identity Issuer
ISD	Issuer Security Domain
KSSK	Key Secure Storage Key
KID	Key Identifier, see [GP]
KVN	Key Version Number, see [GP]
LCSI	Life Cycle State Identifier
MF	Master File (per 7816-4)
PIV	Personal Identity Verification
PIV-LPIN	PIV User local PIN
PIV-GPIN	PIV Global PIN
PKCS	Public Key Cryptography Standard
PUK	PIV User PIN Unblock PIN
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman
SO	Security Officer
SSD	Supplementary Security Domain