PKI BLADE Cosmo

(PKI BLADE Applet

On ID-One PIV (Type A))

FIPS 140-2 Security Policy

Public Version

The United States Department of State
and
Oberthur Technologies of America
4250 Pleasant Valley Road
Chantilly, VA 20151-1221 - USA

CONTENTS

TABLES

FIGURES

1 Introduction

1.1 Scope

This document defines the Security Policy for the PKI BLADE Cosmo cryptographic module, referred to below as the cryptographic module or CM. The CM is validated to overall FIPS 140-2 Level 2 with Physical Security Level 4.

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

1.2 Platform Overview

The PKI BLADE Cosmo CM defined under this Security Policy includes the addition of the PKI BLADE Applet V1.2 on the FIPS validated Oberthur ID-One PIV (Type A) cryptographic module. The PKI BLADE Applet is based on the ISO 7816 and GSC-IS command interface, and designed to be loaded on any Java card compliant with JavaCard and Global Platform specifications; this includes PIV certified Java cards. The PKI BLADE Applet leverages the Precise Biometrics Match on Card (MoC) library for biometric authentication to an authentication strength of 10^6 as required by FIPS 140-2. When deployed, the CM will provide PKI based biometric logical access to applications by leveraging strong two factor authentication using passwords and fingerprints biometrics.

The ID-One (Type A) module has been awarded Certificate #1414 and is in compliance with PIV specifications (FIPS 201 and related Special publications). The ID-One PIV (Type A) module includes the NPIVP validated PIV Applet Suite (NPIVP Certificate #25), which provides Identity proofing (storage of personal data), General Authentication Services and secure post issuance management in the PIV system. It supports all cryptographic algorithms defined in the PIV specifications (SP800-78-3) including TDEA, AES, RSA, ECDSA and ECDH with all possible key sizes. This ensures a Time Period for use of the PIV card that could go well beyond 2013.

Note that the PKI BLADE Cosmo CM described in this Security Policy contains two fingerprint Bio-Match solutions, however only the PKI BLADE Biometric Match on Card solution will be leveraged on this CM.

In addition to the above, the CM provides enhanced functionalities to extend its field of application outside the HSPD#12 program. These features include:

- **Flexible containers**: the CM allows extension of PIV card by providing feature to create any numbers of additional data containers with their own access control rules. Additional data, outside of the NIST PIV namespace are now natively supported.
- **Configurable Key slots**: New instances of keys can be added at any time by the card issuer to support additional functionalities like key history or Mutual Authentication. Access control rules to securely inject, to generate or to use the key can be configured during key creation. Applet security rules ensure that FIPS 140-2 requirements are met at all times.
- **ISO 7816-3 extended length support**: The amount of data that can be transmitted to and from the card in a single command has been extended from 256 to 32,768 Bytes. This not only removes the need for command chaining but significantly improves communication speed. For instance the PIV certificate can now be read in a single command to greatly speed up the authentication process.
- **Key Usage control**: To increase security and provide control over key usage, the CM supports Key Usage counter associated with each cryptographic key to limit the maximum number of uses of a given key. This counter is decremented each time the key is used. The key becomes unusable when the usage counter reaches zero. It is possible to disable or reinitialize this counter using secure messaging in post-issuance.

Figure 1: Sample CM cards

The following diagram shows in blue the actual module cryptographic boundary.

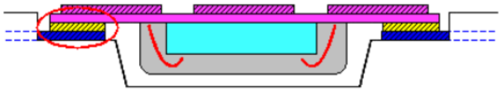

Figure 2: Cryptographic module

Only the die (in blue) is within the module cryptographic boundary. The epoxy glue and the support on which the crypto module is glued (contact plate or antenna) are not part of the crypto module boundary.

2 Security Level

The CM meets the FIPS 140-2 Level 2 overall, with Physical Security Level 4.

Security Requirements Section	Level
Cryptographic Module Specification	2
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: Module Security Level Specification

3 Cryptographic Module Specification

3.1 Overview

The CM is the addition of the PKI BLADE Applet onto the previously validated ID-One PIV (Type A) cryptographic module (FIPS 140-2 Cert. #1414, NPIVP Cert. #25).

The module operates in FIPS mode with the fingerprint authentication mechanism parameters configured as indicated in 8.6 of this Security Policy. The module provides the Get Status and Get Data commands to confirm configuration hardware and firmware version numbers.

3.2 Cryptographic Module Boundary

The cryptographic module boundary is the edge of the die. It encompasses the PKI BLADE applet, the PIV applet suite and the ID-One Cosmo V7-n platform.

The module will typically be embedded into a plastic card body and connected to an ISO 7816-2 compliant contact plate as well as to an external antenna loop.

The following sit outside of the cryptographic boundaries:

- Plastic card body or inlay into which the module may be embedded
- Contact plate
- External antenna loop

3.3 Module Configuration and Versioning

One configuration of the CM is included in this validation:

HW	FW	Op Code	Description
B0	FC10	071964	Large memory model, BIO r4 (Generic r8 + MOC 3.21 for PIV BIO)

Table 2: Part Numbers and Configuration

The above table represents the ID-One PIV (Type A). In addition to this base platform configuration, the module is delivered with the PKI BLADE Applet (FW Version 1.2).

Hardware module Part Number can be read from the Card Identification Data Object under the sub-element with tag ‘01’.

The module firmware (also called ROM code) is the module Operating System that is written in the micro-controller during chip manufacturing and cannot be subsequently changed.

The module firmware version can be read from the Card Identification Data Object under the sub-element with tag 03.

Critical patches to the module firmware may be loaded into the module EEPROM as Service Packs, called Optional Codes. They can only be loaded by Oberthur during the manufacturing stage. They are identified by one or multiple Optional Code numbers.

Module Optional Codes can be read from the Card Identification Data Object under the sub-element with tag 04.

3.4 Locks Configurations

Since the module was designed to address multiple markets, a set of non-reversible locks are activated during manufacturing to restrict the module capabilities and meet customer requirements (e.g. FIPS 140-2 validation, Common Criteria certification, etc…) or export control regulations.

Such restrictions on the module capabilities (if any) are described in the electrical profile set for each customer. See 3.6 below.

3.5 Applet Packages

The following packages are installed on the PKI BLADE Cosmo:

Package	AID	Version
Card Manager		
Card Manager (for ISD and ASD)	A0000000035350	02 03
CHV Interface Server		
com.oberthurcs.javacard.authentic.biometry.optional	A00000007701 050007 1000 00 00000014	01 00
com.oberthurcs.javacard.chv	A00000007701 080807 1000 00 00000003	01 00
com.oberthurcs.javacard.chv.cvm	A00000007701 080807 1000 00 00000002	01 00
com.oberthurcs.javacard.chv.cvm.bio	A00000007701 080807 1000 00 00000001	01 00
com.oberthurcs.javacard.chv.server.biometric	A00000007701 080807 1000 00 00000005	01 00
com.oberthurcs.javacard.chv.server	A00000007701 080807 1000 00 00000006	01 00
PIV Applet		
PIV Applet Executable Load File	A00000007701 000006 1000 00 00000024	02 32
PKI BLADE Applet		
PKI BLADE Applet Executable Load File	A0000004490064	0102
Precise BioMatch Library		
BioMatch J library Executable Load File	A000 0001320001	0302

Table 3: PKI BLADE Cosmo Applet suite packages

The exhaustive list of software packages (executable load files) present in the module as well as their version number can be retrieved using the module Issuer Security Domain GET STATUS command, using P1-P2 = ’20 02’ and a command data field set to ‘4F00’.

The above command can be used at any time to ensure that no other packages or versions than the ones that have been FIPS 140-2 validated and listed in Table 3 are present.

3.6 PKI BLADE Applet Overview

The PKI BLADE applet provides security for stored user data and credentials and an easy to use interface to PKI services. Figure 3 depicts the PKI BLADE applet context.

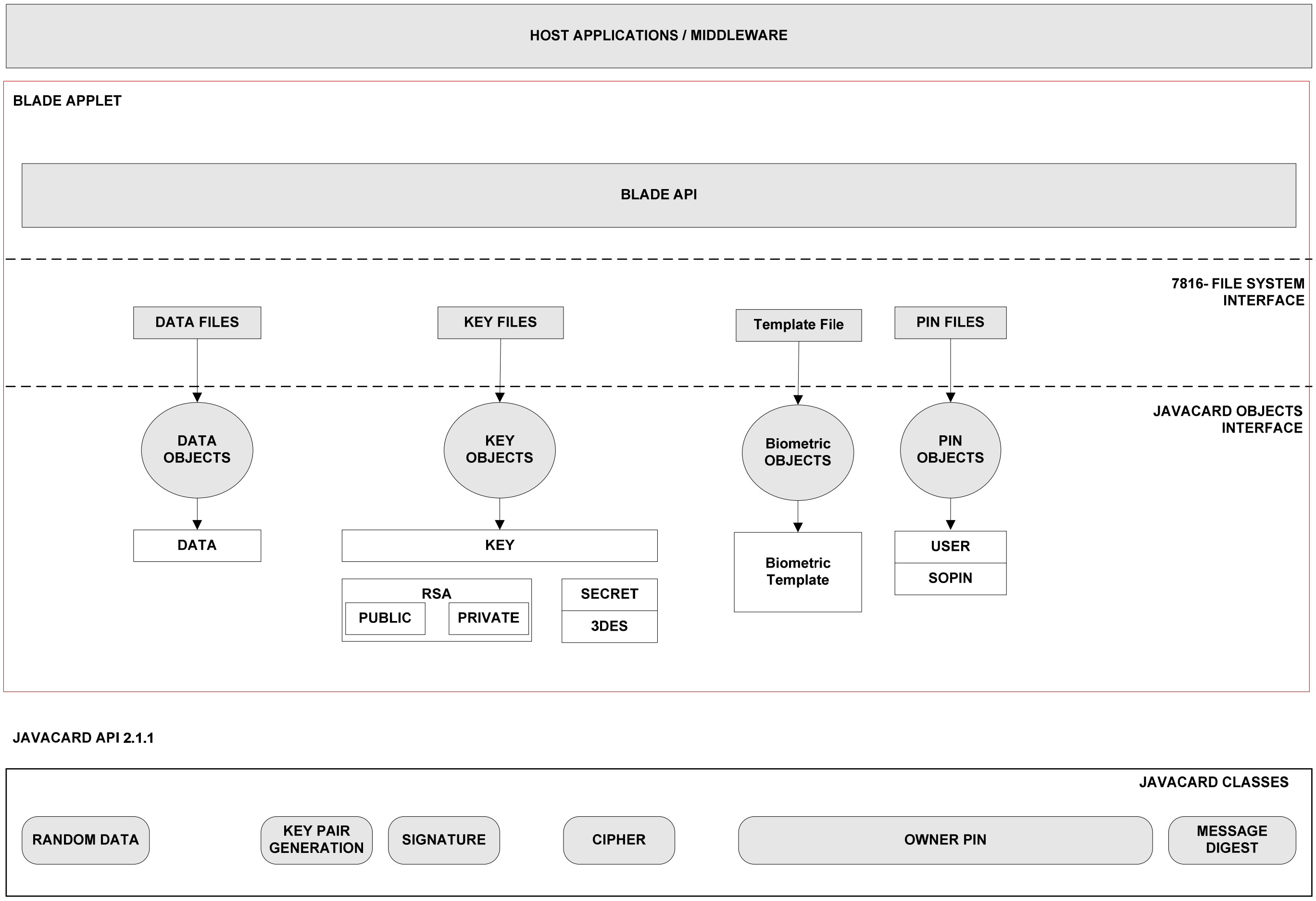

Figure 3 - PKI Blade Applet Context

The PKI BLADE applet features:

- Multi-application secure storage and retrieval of objects and digital credentials.
- Authentication of the cardholder (User) and the security officer (SO)
    - Supports PIN based authentication and / or on-token fingerprint authentication using the Precise BioMatch MOC algorithms.
- Execution of native platform cryptographic services integrated with managed objects:
    - Two-key TDES encryption and decryption.
    - SHA1 secure hashing generation.
    - RSA 1024 / 2048 key unwrap and signature.

3.6.1 PKI BLADE Applet AID and Selection

The JavaCard classes of the PKI BLADE applet are defined in a single Java package. AIDs for PKI BLADE applet and the applet package are defined in the table below:

Identifier	Value
RID	0xA0, 0x00, 0x00, 0x04, 0x49
Package PIX	0x01
Applet PIX	0x00, 0x64

Table 4 - PKI BLADE Applet AID

The applet select APDU should be coded as defined below. The data field contains the applet AID of the PKI BLADE applet.

Class	Instruction	P1	P2	Lc	Data field	Le
0x00	0xA4	0x04	0x00	0x07	0xA0, 0x00, 0x00, 0x04, 0x49, 0x00,0x64	N/A

Table 5 - PKI BLADE Applet SELECT APDU

3.7 Electrical Profile

The module can be configured during manufacturing to address multiple markets and meet different customer requirements. Every module delivery is associated with a BAP (Batch Approval Process) document that identifies the module and its specific configuration (electrical profile). The BAP document is prepared by Oberthur Technical Support staff after a discussion with the customer regarding their specific needs, and local regulations.

The BAP provides identification information (hardware, firmware, firmware extensions, locks configuration and applets) and specifies the FIPS 140-2 validation certificate number applicable to the listed configuration.

The BAP number can be retrieved from the Batch Identifier written in the card during production.

3.8 Cryptographic Algorithms

Neither the ID-One PIV Applet Suite nor the PKI BLADE Applet includes the executable code of any cryptographic algorithm. Whenever a cryptographic computation is required, the applet calls on the cryptographic API provided by the ID-One Cosmo V7-n smart card platform. Algorithms provided by the ID-One Cosmo V7-n smart card platform have been tested by CAVP during the FIPS 140-2 Level 3 validation of the smart card platform. The following table lists the algorithms used by the ID-One PIV applet suite and PKI BLADE Applet, and the associated CAVP certificate number.

Algorithm - Modes	**CAVP Cert. #**
TDES – ECB and CBC modes, 2-Key and 3-Key; TDES MAC, vendor affirmed. The use of two-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.	**698**
RSA Signature Generation and Verification, and Key Pair Generation - 1024 and 2048 bit modulus	**403**
AES 128/192/256 – ECB and CBC modes.	**840**
ECDSA Signature Generation and Key Pair Generation: Curve P-224, P-256 and P-384	**94**
ECC CDH (SP 800-56A Section 5.7.1.2)	**3**
FIPS 186-2 RNG	**480**
SHA-1	**833**

Table 6: Approved Cryptographic Algorithms

The module includes an untested implementation of AES CMAC; this component of the Global Platform operational environment is not used by the module.

3.8.1 Random Number Generators

The cryptographic module offers the services of a FIPS 140-2 approved RNG (Deterministic Random Number Generator).

The cryptographic module also offers the services of a hardware based NDRNG (Non Deterministic Random Number Generator), which can be used to generate a seed to feed the RNG and increase its entropy.

3.8.2 PKCS #1 and PSS

As per SP 800-73-3 and SP800-78-3, the ID-One PIV applet suite can generate an RSA signature on an externally generated hash. The PIV applet does not enforce the use of any specific hashing algorithm or padding scheme. It is up to the off card entity calling the RSA algorithm from the PIV applet (GENERAL AUTHENTICATE Command) to ensure that the message is hashed and padded as per SP800-78-3 prior to being sent to the card for the RSA cryptographic computation.

3.8.3 RSA Key Transport

RSA Key Transport (decryption only) performed in accordance with SP 800-73-3, SP 800-78-3 and discussion with NIST using the PIV 9D key and associated retired Key Management keys (PIV key references 83 – 95). The key establishment methodology provides 112 bits of encryption strength (determined by the use of the RSA algorithm with k = 2048.)

3.8.4 ECDSA

As per SP 800-73-3 and SP800-78-3, the ID-One PIV applet suite can generate an ECDSA signature on an externally generated hash. The PIV applet does not enforce the use of any specific hashing algorithm. It is up to the off card entity calling the ECDSA functionality from the PIV applet (GENERAL AUTHENTICATE Command) to ensure that the message is hashed and formatted as per SP800-78-3 prior to being sent to the card.

3.8.5 ECC CDH

As per SP 800-78-3 the ID-One PIV applet can generate a pre-master secret in accordance with SP 800-54A Section 5.7.12 when supplied with an external public key (ECC). Such pre-master secret can then be used by the PIV middleware to establish an encryption/decryption key. It is up to the off card entity calling the ECC CDH functionality from the PIV applet (GENERAL AUTHENTICATE Command) to ensure that the pre-master secret returned by the card is used to achieve key agreement as per SP800-78-3. The module performs ECDSA Sign and Verify self-tests, which are inclusive of point multiplication for ECDSA as required by IG 9.6 for SP 800-56A.

3.8.6 Secure Key Injection

PIV keys can be securely loaded into the module using either a TDES or an AES transport key (depending on the configuration during manufacturing). TDES transport key provides 112 bits of encryption strength and AES 128 bits of security. The key, once injected into the PIV application will have a security strength equals to the minimum between the inherent security strength of the key prior to its injection and the security strength of the transport key being used.

3.8.7 Secure Hash Algorithm

From all the secure hash algorithms (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) that have been validated in previous validations of the platform, (e.g. SHS Cert. #833), only SHA-1 may be used in the configuration subject to this Security Policy. (It is used by the DAP Verification authenticated command. However, no security claim is made for this service under FIPS 140-2.)

4 Ports and Interfaces

The CM supports two modes of communication: Contact mode and contactless mode. Contact communication is achieved through a physical connection to a smart card contact plate. Contactless communication is achieved through a physical connection to a loop antenna. Neither the contact plate nor the antenna is within the cryptographic boundary of the module. The mode of operation is determined at power-up, depending on the interface (contact or contactless) that powers the module. It cannot be changed until the module is reset.

4.1 Physical Interfaces

4.1.1 Contact Mode

In contact mode, the cryptographic module follows the standard ISO/IEC 7816 part 2 and 3 for physical and logical interfaces:

Pin	FIPS 140-2 Designation	Description
Vcc	Power supply input	Both Class A (5V) and Class B (3V) supported
RST	Control input	External Reset Signal
CLK	Control input	External Clock Signal (1 to 10Mhz) to transmit data over I/O line. Internally the card relies on an uninterrupted internal oscillator to drive the main processor and all cryptographic co-processors independently of the external clock.
I/O	Data input, Control input, Data output, Status output	See transmission parameters below
GND	Ground	Reference Voltage

Table 7: Physical Interface for contact mode

Transmission parameters

Communication with the module through the contact interface uses the half duplex block protocol defined by ISO/IEC 7816-3 as T=1.

The data communication speed on the I/O line is defined by the Values of the clock rate conversion integer (Fi) and the baud rate adjustment integer (Di) agreed upon between the reader and the module during the power on sequence. The values supported by the module are as follows (see ISO 7816-3:2006):

FI	F	**DI**	D	**I/O Communication Speed with External clock at 5MHz**
1	372	**1**	1	13,440 bauds
1	372	**2**	2	26,881 bauds
1	372	**3**	4	53,763 bauds
1	372	**8**	12	161,290 bauds
9	512	**4**	8	78,125 bauds
9	512	**5**	16	156,250 bauds
9	512	**6**	32	312,500 bauds
9	512	**7**	64	**625,000 bauds**

Table 8: Transmission parameters for contact mode

Up to 32,767 data bytes can be exchanged in each direction within a single command (using APDU with Extended Length Field).

4.1.2 Contactless Mode

In contactless mode, the cryptographic module follows the standard ISO/IEC 14443 type A, RF Interface for physical and logical interfaces:

- It uses only two electrical connections, LA and LB, which are physically different and distinct from the electrical connections used in contact mode.
- LA and LB are connected to an external antenna loop which provides power when in presence of a proximity RF field.
- Data input, control input, data output, and status output are transmitted through the antenna using signal modulation as specified in ISO 14443.

Depending on the configuration set during manufacturing, the supported bit-rates are:

- 106 Kbits/s
- 212 Kbits/s
- 424 Kbits/s
- 848 Kbits/s

Up to 32,767 data bytes can be exchanged in each direction within a single command (using APDU with Extended Length Field).

4.2 Logical Interface

The module functions as a slave processor to process and respond to the reader commands. The I/O ports of the module (two ports due to contact and contactless modes of communication) provide the following logical interfaces:

Logical Interface	Contact Mode (ISO 7816)	Contactless Mode (ISO 14443)
Data Input:	I/O Pin	LA and LB (RF Modulation)
Data Output:	I/O Pin	LA and LB (RF Modulation)
Status Output:	I/O Pin	LA and LB (RF Modulation)
Control Input:	I/O, Clock and Reset Pins	LA and LB (RF Modulation)
Power Input	VCC and GND	LA and LB (RF Modulation)

Table 9: Module Ports and Interfaces

Synchronization timing controls, provided in part by the module clock input CLK in contact mode or the modulation on the carrier in contactless mode, manages the separation of these logical interfaces that use the same physical port.

5 Roles & Services

5.1 Roles

Cryptographic Officer Roles	
CA	**Card Administrator**. This role is responsible for managing the security configuration of the module. The CA authenticates to the module through a Global Platform (GP) mutual authentication protocol with the Issuer Security Domain (ISD). A successful authentication demonstrates the knowledge of the ISD Global Platform key set and establishes a GP Secure Channel Session to execute services allowed to the CA in a secure manner. (See Global Platform Specifications for more details)
AP	**Application Provider.** This role is responsible for managing the security configuration of the PIV application. The AP authenticates to the module through a Global Platform (GP) mutual authentication protocol with the Application Security Domain (ASD). A successful authentication demonstrates the knowledge of the ASD Global Platform Key set and establishes a GP Secure Channel Session to execute services allowed to the AP in a secure manner. (See Global Platform Specifications for more details)
User Roles (excluding PKI BLADE)	
ADM	**Application Administrator.** This role is responsible for managing the content of the PIV application. The ADM authenticates to the PIV application by verifying possession of an Administrator key.
MAUTH	**Mutual Authentication User.** This role is responsible for accessing data that are protected by a Mutual Authentication Access Control Rule. The MAUTH authenticates to the PIV application by verifying possession of a Mutual Authentication key.
LPU	**Local PIN Unblock User.** The Local PIN Unblock User is responsible for unblocking the card holder local PIN and re-initialize it with a new value.
CH	**Card Holder.** The Card Holder role is responsible for ensuring the ownership of his cryptographic module, and for not communicating his PIN to other parties. An applet authenticates the Card Holder by verifying one of the following: Local PIN, Local Pin Unblocking PIN or Global PIN.
PKI BLADE Applet Roles	
User	PKI BLADE User. The authenticated cardholder.
SO	PKI BLADE Security Officer role. the authenticated PKI BLADE applet administrator
Unauthenticated Services	
AU	Anonymous User. This is not truly a role, but a convenience for listing the set of unauthenticated services, which do not permit access to cryptographic services or CSPs.
Maintenance Role	
	None – the module does not implement a maintenance role.

Table 10: Roles and required Identification and Authentication

5.1.1 Concurrent Operators

The cryptographic module offers multiple logical data in/out interface to external operators through the use of Logical Channels as defined by Global Platform.

Logical Channels facilitate the possibility of the above external entities to communicate concurrently with multiple applications on the card, each within its own secure channel session.

However, concurrent communications are not supported within the PIV application or the PKI BLADE applet, and only one authenticated communication session can be open per Security Domain.

5.2 Role Identification

The cryptographic module performs identity based authentication using application identifier and cryptographic keys.

The application identifier for the **Card Administrator** is the AID of the Issuer Security Domain (ISD).

The application identifier for the **Application Provider** is the AID of the Application Security Domain (ASD).

The application identifier for the **Application Administrator** is the AID of the PIV application (Instance) and the reference to the Administrator key (key ID plus Algorithm ID).

The application identifier for the **Mutual Authentication User** is the AID of the PIV application (Instance) and the reference to the Mutual Authentication key (key ID plus Algorithm ID).

The application identifier for the **Card Holder** is the index value associated with the reference data (Local PIN or Global PIN) used to perform the card holder verification (CHV).

The application identifier for the **Local PIN Unblock User** is the AID of the PIV application (Instance) and the index value associated with the reference data (PIN Unblocking Key) used to perform the Local PIN Unblock.

Within each application, a unique ID is associated with each cryptographic keys or reference data to uniquely identify the off-card identity performing the authentication.

See Global Platform Specifications for more details on ISD and ASD.

The application identifier for the **User (PKI BLADE applet)** is the index value associated with the reference data (PKI BLADE PIN or biometric template) used to perform the card holder verification (PKI BLADE Applet VERIFY or PB_VERIFY).

The application identifier for the **SO (PKI BLADE applet)** is the index value associated with the reference data (PKI BLADE PIN) used to perform the SO verification (PKI BLADE Applet VERIFY).

5.3 Role Authentication

All methods of authentication to the module described in this section meet the FIPS 140-2 requirements:

- The probability is less than one in one million ($<10^{-6}$) that a random authentication attempt succeeds.
- During any one minute period, the probability is less than one in one hundred thousand ($<10^{-5}$) that a random authentication attempt succeeds.

Authentication Mechanism	Probability of False Acceptance	Probability of Successful Random Attempt in 1 Minute
Platform and PIV		
Local PIN	$1/256^8$	$15/256^8$
Local PUK	$1/256^8$	$15/256^8$
Global PIN	$1/256^8$	$15/256^8$
2TDES Authentication	$1/2^{80}$	$10/2^{80}$
3TDES Authentication	$1/2^{112}$	$10/2^{112}$
AES-128 Authentication	$1/2^{128}$	$8/2^{128}$
AES-192 Authentication	$1/2^{192}$	$8/2^{192}$
AES-256 Authentication	$1/2^{256}$	$8/2^{256}$
PKI BLADE Applet		
PKI BLADE PIN	$1/255^6$	$15/255^6$
PKI BLADE Biometric	$1/10^6$	$6/10^5$

Table 11: Strength of Authentication Mechanisms

5.3.1 CA and AP

The cryptographic module supports identity based authentication of the Card Administrator and Application Provider using Global Platform EXTERNAL AUTHENTICATE function.

This mechanism includes an audit log that tracks unsuccessful authentication together with a timing mechanism that introduces an exponential delay after a failed authentication before a new attempt can be accepted. This provides a strong protection against brute force attacks as no more than a few consecutive unsuccessful authentication attempts are possible within one minute.

The authentication remains valid until one of the following conditions is initiated:

- Selection of another application on the same logical channel
- Unsuccessful authentication attempt
- Card reset (power-off)

5.3.2 ADM and MAUTH

The cryptographic module supports identity based authentication of the Application Administrator using the GENERAL AUTHENTICATE command specified in SP 800-73-3.

5.3.3 CH and LPU

The cryptographic module supports identity based authentication of the Card Holder using the VERIFY or CHANGE REFERENCE DATA commands.

The cryptographic module supports identity based authentication of the Local PIN Unblock User using the RESET RETRY COUNTER or CHANGE REFERENCE DATA commands.

In these commands, the module compares all 8 bytes of the reference data. The probability of false authentication on any given verification attempt is given by 1/(*character space* ^ *character length*). The module verification algorithm compares the full 8 bit character and all 8 characters, hence the probability is 1/256^8 = 1/1.8E+19. The module also enforces a configurable limit of unsuccessful attempts, with a maximum of 15, hence the $15/256^8$ limit to the probability of a successful random attempt in a one minute period.

The values above are those enforced by the module. FIPS 140-2 also recognizes constraints on systems and procedures external to the module – see Section 8.5 for guidance.

5.3.4 PKI BLADE PIN Authentication Mechanism and Authentication Strength

The PKI BLADE Applet Master File (MF) contains a User PIN and SO PIN file, and each Directory File (DF) can contain its own User PIN and SO PIN file. The appropriate MF or DF must be selected first prior to executing either VERIFY or CHANGE_REFERENCE_DATA command.

Each PIN instance has an associated non-volatile memory retry counter, with an initial value determined by a Configuration Data file value. A successful VERIFY resets the retry counter. Unsuccessful VERIFY or CHANGE_REFERENCE_DATA attempts decrement the associated retry count; the value persists across sessions. Exhausting the retry count disables the corresponding PIN and puts the applet in the Error state.

If allowed by the Configuration Data file, an authenticated SO may update the User PIN using the CHANGE REFERENCE DATA command in order to re-enable the User PIN and reset the associated retry counter. A limited number of 10 attempts (default 10) of unsuccessful CHANGE_REFERENCE_DATA attempts are permitted.

SO PIN exhaustion results in either reversion of the associated PIN to the Backup SO PIN value, or reset of the SO PIN to an uninitialized state, based on a Configuration Data file setting.

The probability of false authentication for PIN authentication to the module is 1/255^6, (omitting the padding character in the input string, and with applet enforcement of a 6 byte minimum PIN), meeting the FIPS minimum requirement of 1/10^6. The probability of false authentication in one minute is 15/255^6, (based on a maximum of 15 retries) meeting the FIPS minimum requirement of 1/10^5.

The SO PIN can be reset to the default SO PIN by issuing the RECYCLE command.

5.3.5 PKI BLADE Fingerprint Authentication Mechanism and Strength

Prior to enrollment, the enrollment tools have been provided to authorized users and have been configured according to agency policies.

The strength of the biometric authentication is determined by the settings applied to the biometric algorithm by the enrollment software. The biometric algorithm provider has provided a Receiver Operating Curve (ROC) characteristic curve, achieved through a large statistical sampling process, for the algorithm for use with enrollment station configuration.

The operator must select the 1/1,000,000 FAR setting when the *Bio Only* or Bio-or-PIN settings are used. This setting achieves a probability of false authentication of just less than 1/10^6 as required by FIPS 140-2.If used as a second factor to the PIN (*Bio–and-PIN*), authentication strength is met by the PIN, and the FAR may be set to a lower level as determined by the operator.

The number of allowed bad fingerprint authentication attempts is set when the fingerprint template is enrolled on the smart card. The count of bad fingerprint authentication attempts is kept internally on the applet, independent of the PIN retry counters. It is incremented with every bad fingerprint logon attempt, regardless of which fingerprint is used. Switching fingers does not clear the count. The count of bad fingerprint authentication attempts is cleared with every successful fingerprint logon.

When the internal count of bad fingerprint authentication attempts exceeds the maximum value set at enrollment, logon via the fingerprint template is locked. Once locked, no fingerprint can be used to log on until a new fingerprint template is enrolled onto the smart card.

A flag can be set during enrollment to lock this parameter. If locked, the maximum bad fingerprint limit is fixed and cannot be changed during future enrollments. Once the lock flag is set, it cannot be cleared during re-enrollment. See Section 8.6 for PKI BLADE Applet configuration and usage rules.

5.4 Platform and ID-One PIV Applet Suite Services

5.4.1 Card Administrator Services

The following table lists the services that the module makes available to the Card Administrator.

Authentication	
INITIALIZE UPDATE	This command is used by the CA to initiate a Global Platform Secure Channel Session, setting the key set version and index.
EXTERNAL AUTHENTICATE	This command is used by the CA to open a Global Platform Secure Channel Session with the Issuer Security Domain, in order to communicate in a secure and confidential way.
Card Content Management	
INSTALL	This command is used by the CA to add an application to the module.
LOAD	This command is used by the CA to load the byte-code of a new application (executable load file). For the module to remains FIPS validated, this command shall not be used to load non FIPS approved executable code.
DELETE	This command is used by the CA to delete a uniquely identifiable object. The object may be an Application, a load file, or a key set.
PUT KEY	This command is used by the CA to add or replace ISD keys. Keys are loaded protected by the encryption of the Global Platform Secure Channel Protocol (SCP) and a KCV is included in the transmission to ensure integrity of the key loading operation. This command is also used by the CA to load RSA public keys such as the Token Verification Key or the DAP Verification Key. These keys are used for Delegated Management and DAP verification as specified by Global Platform.
STORE DATA	This command is used by the CA to transfer data to the module. It is also used to clear the audit log and to modify the contactless capabilities (activate/deactivate a contactless stealth mode, or to allow only non-identifiable information to leak out of the contactless interface until the terminal can be authenticated) to increase the privacy protection of the user.
SET STATUS	This command is used by the CA to temporary lock an application, and to unlock it later on. It can also be used to terminate the crypto module.
GET STATUS	This command is used by the CA to retrieve identification and life cycle status information for all applications, executable load files, and security domains present in the module. It can also be used by the CA to verify that the module is still in the FIPS validated configuration and that only FIPS approved applications are available.
DELEGATE MANAGEMENT	Delegated Management gives a CA the possibility of empowering an AP the ability to initiate approved and pre-authorized Card Content changes (loading, installation, extradition or deletion of an applet) on his behalf.

Table 12: Card Administrator Services

5.4.2 Application Provider Services

The following table lists the services that the module makes available to the Application Provider.

Authentication	
INITIALIZE UPDATE	This command is used by the AP to initiate a Global Platform Secure Channel Session, setting the key set version and index.
EXTERNAL AUTHENTICATE	This command is used by the AP to open a Global Platform Secure Channel Session with the Application Security Domain, in order to communicate in a secure and confidential way.
Card Content Management	
DAP VERIFICATION	DAP verification allows the module to check the CA signature on an application code being loaded and abort the loading if the signature is not verified. Such verification can be made mandatory or optional.
PUT KEY	This command is used by the AP to add or replace ASD keys. Keys are loaded protected by the encryption of the Global Platform Secure Channel Protocol (SCP) and a KCV is included in the transmission to ensure integrity of the key loading operation.
DELETE	This command is used by the AP to delete a uniquely identifiable object. The object may be an Application, a load file, or a key set.
STORE DATA	This command is used by the AP to transfer data to the module.
SET STATUS	This command is used by the AP to temporary lock one of its application, and to unlock it later on.
GET STATUS	This command is used by the AP to retrieve identification and life cycle status information for all applications, executable load files, and security domains present in the module.
CREATE FILE	This command is used by the AP during personalization to add binary files support to the PIV application.
CREATE CONTAINER	This command is used by the AP during personalization to create container to store PIV application data objects.
CREATE KEY SLOT	This command is used by the AP to define the Key IDs available to the PIV application.

Table 13: Application Provider Services

5.4.3 Application Administrator Services

The following table lists the services that the module makes available to the Application Administrator.

Authentication	
GENERAL AUTHENTICATE	This command is used by the Application Administrator to authenticate to the PIV application (External Authentication).
Card Content Management	
PUT DATA	This command is used to update the content of data object in the PIV application for which the access control rules have been satisfied.
GENERATE ASYMMETRIC KEY PAIR	This command is used by the Application Administrator to generate an asymmetric key pair (RSA or ECC) in the PIV application.
PUT PIV KEY	This command is used by the Application Administrator to inject the value of a PIV application key (symmetric or asymmetric) within a secure channel opened by the Application Provider. Keys are loaded protected by the encryption of the Secure Channel Protocol (AES) and a KCV is included in the transmission to ensure integrity of the key loading operation. This command can also be used by the Application Administrator to zeroize an existing application key.
GET DATA	The GET DATA command is used to retrieve public data from the selected application and application data for which the access control rules have been satisfied. No CSP can be read using this service.
READ BINARY	The READ BINARY command is used to retrieve the content of a Binary File for which the access control rules have been satisfied. No CSP can be read using this service.
UPDATE BINARY	The UPDATE BINARY command is used to update the content of an existing file for which the access control rules have been satisfied. No CSP can be updated using this service.

Table 14: Application Administrator Services

5.4.4 Mutual Authentication User Services

The following table lists the services that the module makes available to the Mutual Authentication User.

Authentication	
GENERAL AUTHENTICATE	This command is used by the Mutual Authentication User to authenticate to the PIV application while at the same time to authenticate the PIV application (Mutual Authentication).
Card Content Management	
PUT DATA	This command is used to update the content of a data object in the PIV application for which the access control rules have been satisfied.
GET DATA	The GET DATA command is used to retrieve public data from the selected application and application data for which the access control rules have been satisfied. No CSP can be read using this service.
READ BINARY	The READ BINARY command is used to retrieve the content of a Binary File for which the access control rules have been satisfied. No CSP can be read using this service.
UPDATE BINARY	The UPDATE BINARY command is used to update the content of an existing file for which the access control rules have been satisfied. No CSP can be updated using this service.

Table 15: Mutual Authentication User Services

5.4.5 Local Pin Unblock User Services

The following table lists the services that the module makes available to the Local Pin Unblock User role.

Authentication	
CHANGE REFERENCE DATA	This command is used by the Local PIN Unblock User to authenticate to the PIV application and to change its reference data.
RESET RETRY COUNTER	This command is used by the Local PIN Unblock User to authenticate to the PIV application and Reset the Card Holder Local PIN.

Table 16: Local PIN Unblock User Services

5.4.6 Card Holder Services

The following table lists the services that the module makes available to the Card Holder.

Authentication	
VERIFY	This command is used by the Card Holder to authenticate to the PIV application.
CHANGE REFERENCE DATA	This command is used by the Card Holder to authenticate to the PIV application and to change its reference data.
GENERAL AUTHENTICATE	This command is used by the Card Holder to perform a cryptographic operation used by the off card application to authenticate the PIV application, generate a digital signature or for key management.
Card Content Management	
PUT DATA	This command is used to update the content of data object in the PIV application for which the access control rules have been satisfied.
GET DATA	The GET DATA command is used to retrieve public data from the selected application and application data for which the access control rules have been satisfied. No CSP can be read using this service.
READ BINARY	The READ BINARY command is used to retrieve the content of a Binary File for which the access control rules have been satisfied. No CSP can be read using this service.
UPDATE BINARY	The UPDATE BINARY command is used to update the content of an existing file for which the access control rules have been satisfied. No CSP can be updated using this service.

Table 17: Card Holder Services

5.4.7 Un-Authenticated Services

The following table lists the services that the platform makes available without authentication. See Table 18 for the relationship between roles and unauthenticated services. Note that Verify and General Authenticate may be used in the transition to an authenticated state, to confirm security conditions or participate in a protocol with an external system, in accordance with SP 800-73-3.

Authentication	
GENERAL AUTHENTICATE	This command is used to perform card or PIV applet authentication in accordance with SP 800-73-3 specifications and FIPS 140-2 Implementation Guidance 3.1.
Public Commands (unauthenticated)	
SELECT	This command is used for selecting an application on a specific logical channel.
MANAGE CHANNEL	This command allows opening or closing a logical channel in the card. Up to 4 logical channels may be open at a time.
PUT DATA	This command is used to update the content of data object in the PIV application that do not require authentication
GET DATA	The GET DATA command is used to retrieve public data from the selected application. No CSP can be read using this service.
READ BINARY	The READ BINARY command is used to retrieve the content of an existing file that does not require authentication. No CSP can be read using this service.
UPDATE BINARY	The UPDATE BINARY command is used to update the content of an existing file that does not require authentication. No CSP can be updated using this service.

Table 18: Platform Unauthenticated Services

5.4.8 Relationship between Roles, Services and CSP Access

Roles/Services	CA	AP	ADM	MAUTH	CH	LPU	UN-AUTH	CSP involved							CSP Access type
								CA	AP	ADM	MAUTH	CH	LPU	UN-AUTH	
SELECT							X								
INITIALIZE UPDATE	X	X													
EXTERNAL AUTH.	X	X						e	c						Execute
INSTALL	X							a							Execute
LOAD	X							a							Execute
DELETE	X	X						a	b						Execute
PUT KEY	X	X	X					d	c						Exec. Write
STORE DATA	X	X						a	b						Execute
SET STATUS	X	X						a	b						Execute
GET STATUS	X	X						a	b						Execute
DELEGATE MANAGEMENT	X							f							Execute
DAP VERIFICATION		X							g						Execute
MANAGE CHANNEL	X	X					X								
GENERAL AUTHENTICATE			X	X	X		X			j	j	j		j	Execute
GET DATA	X	X	X	X	X		X								
PUT DATA			X	X	X		X								
GENERATE ASYM. KEY PAIR			X							k					Exec. Write; Read (public key only)
PUT PIV KEY			X							j					Exec. Write
VERIFY					X		X					h	i		Execute
CHANGE REF. DATA					X	X						h	i		Exec. Write
RESET RETRY COUNTER						X									Exec. Write
CREATE FILE		X													
READ BINARY		X	X	X	X		X								
UPDATE BINARY		X	X	X	X		X								
CREATE CONTAINER		X													
CREATE KEY-SLOT		X													

Table 19: Relationship between Roles, Services and CSP Access

References to CSPs and public keys are listed in the table below:

CSP/Public Key Ref in Table 19	**List of CSP/Public Key being referred**
a	CSK
b	ASK
c	ASK, ADK
d	CSK, CDK, $K_{TOKEN,}$ K_{DAP}
e	CDK, CSK
f	CSK, $K_{TOKEN,}$ $K_{RECEIPT}$
g	K_{DAP}
h	Local and Global PINs
i	Local PUK
j	PIV Application keys with satisfied ACR
k	PIV Asymmetric application keys

Table 20: Description of the CSP/Public Key Referenced in Table 19

Note on PUT PIV KEY: PIV Key loading must always be done under the combined authentication of the Application Provider and the Application Administrator. The Application Administrator's successful authentication unlocks the updatability of the application data elements and the Application Provider's authentication provides the secure channel required to provide encrypted transport of the key from the external HSM to the module.

5.4.9 Access Control Rules

Each data object and each key has its own Access Control Rule (ACR) defined during creation.

ACR defines the access conditions under which reading (execution for a key) and updating operations are authorized on the corresponding data object (or key) for contact and for contactless modes.

The following table lists access conditions supported by the ID-One PIV Applet Suite:

Access Conditions	Notation	Meaning
Always	ALW	The flag value associated to the AC is always equal to TRUE. Meaning, the objects with this access condition (AC) is always accessible without any restriction.
Never	NEV	The flag value associated to the AC is always equal to FALSE. Meaning, the corresponding object is never accessible under any condition.
Cardholder PIN	PIN	The flag value associated to the AC is equal to TRUE when a VERIFY of the LOCAL PIN or GLOBAL PIN has been successfully performed
Cardholder PIN ALWAYS	PIN ALWAYS	The flag value associated to the AC is equal to TRUE when VERIFY of the LOCAL PIN or GLOBAL PIN has been successfully performed in the immediately preceding command.
Cardholder PIN ALWAYS	PIN ALWAYS	The flag value associated to the AC is equal to TRUE when a VERIFY of the LOCAL PIN or GLOBAL PIN1 has been successfully performed in the immediately preceding command.
Administrator Authentication	PIV_ADM	The flag value associated to the AC is equal to TRUE when a GENERAL AUTHENTICATE in mode EXTERNAL AUTHENTICATE with an Administrator Key has been successfully performed
Mutual Authentication	MUTUAL_AUTH	The flag value associated to the AC is equal to TRUE when a GENERAL AUTHENTICATE in mode MUTUAL_AUTH with a Mutual Authentication key has been successfully performed.

Table 21: Available Access conditions in PIV application

Notes:

- The presence of the Discovery Object and the value of the first byte of the PIN Usage Policy determines whether Local PIN alone or both Local PIN and Global PIN can satisfy this Access Condition. If Discovery Object is not present, only Local PIN can satisfy this Access Condition. If Discovery Object is present and the first byte of the PIN Usage Policy is ’60’, either the Local PIN or Global PIN can satisfy this access condition.

5.5 PKI BLADE Applet Services

When the PKI BLADE Applet is selected the commands listed below are available. Access control is given in parentheses; that is, SO indicates the services is accessible by the PKI BLADE Applet SO role; User indicates the services is available to the PKI BLADE Applet User; AU means the service does not require authentication, only selection of the PKI BLADE Applet.

(SO, User) CHANGE_REFERENCE_DATA – Updates the PIN of the given type if the given current PIN is valid for the currently authenticated entity.

(SO, User) CREATE_FILE – Creates an empty file of the given type.

(User) CRYPT – Performs TDES symmetric key encryption/decryption on the given data.

(SO, User) DELETE_FILE – Deletes references to a given file. When used with a DF, DELETE_FILE will remove a whole sub-directory and the files it may contain.

(SO, User) END_SESSION – Ends the current authenticated session, returning the card to the idle state.

(User) GENERATE_DES_KEY – Generates a 2 Key TDES key (DEK)

(User) GENERATE_PUBLIC_KEY_PAIR – Generates RSA 1024 or 2048 bit key pair (PSK/SVK or KUK/KWK)

(AU) GENERATE_RANDOM_NUMBER – Creates a random number of the given size, using the Oberthur platform Approved DRNG.

(AU) GETSTATUS – Returns the current status of the card. The remaining file space gives the number of bytes available for creating new files (16-bit number, MSB first). The Configuration Data format is described below.

(User) PC_CREATE_BIO_MATCH_J_TEMPLATE - Stores biometric data such as biometric headers.

(User) PB_CREATE_TEMPLATE – Creates the fingerprint template file on the token, and writes the initialized data to the file.

(AU) PB_GET_PUBLIC_TEMPLATE – Returns the public template data structure from the requested fingerprint template file. The fingerprint template file must have been previously created with the PBCreateTemplate command.

(AU) PB_VERIFY - Performs a match between a private fingerprint template and given fingerprint data.

(User) PERFORM_SECURITY_OPERATION - Dependent on the P1, P2 and data values, performs RSA key unwrap, or RSA signature operations: RSA Key unwrap - Decrypts the given ciphertext key with the private KUK in the given file. RSA Sign - Creates an RSA PKCS #1 v1.5 signature for the given data with the PSK in the given file.

(AU, SO, User) READ_BINARY - Returns the requested amount of data (at the given offset) from the active file. Use of this service is subject to access control conditions on the file specified in the command.

(AU) RECYCLE - Deletes all files and zeroes all allocated buffer space (applet zeroization).

(AU) SELECT_FILE - Makes the given file the active file (sets the current file identifier) to be used by subsequent commands. Some commands will operate on the selected file if no file identifier is provided with the command.

(AU) SHA1_DIGEST - Initiates, continues, or completes a SHA-1 hash of the given data.

(AU) VERIFY - Hashes the given PIN and compares the result to the appropriate MF or DF hashed PIN value. A successful comparison updates the applet security state for SO or User authentication.

(AU, SO, User) WRITE_BINARY - Writes the given data (at the given offset) to the active file. Use of this service is subject to access control conditions on the file specified in the command.

The Table below lists all services provided by the PKI BLADE Applet, the access control for the function by each PKI BLADE Applet role, and the relationship of each service to each CSP. The services are described further below the table. CSPs are defined in a later section. The PKI BLADE Applet has no access to platform CSPs.

Service	**PINs**			**Bio**	**Symmetric**		**Asymmetric**	
	SO	**User**	**Backup SO**	**PFT**	**DEK**	**IV**	**PSK**	**KUK**
CHANGE_REFERENCE_DATA	E,W	E, W	W	N	N	N	N	N
CREATE_FILE	N	N	N	N	N	N	N	N
CRYPT	N	N	N	N	E	E,W	N	N
DELETE_FILE	D	D	D	D	D	D	D	D
END_SESSION	N	N	N	N	N	N	N	N
GENERATE_DES_KEY	N	N	N	N	W	N	N	N
GENERATE_PUBLIC_KEY_PAIR	N	N	N	N	N	N	W	W
GENERATE_RANDOM_NUMBER	N	N	N	N	N	N	N	N
GETSTATUS	N	N	N	N	N	N	N	N
PB_CREATE_BIO_MATCH_J_TEMPLATE	N	N	N	W	N	N	N	N
PB_CREATE_TEMPLATE	N	N	N	W	N	N	N	N
PB_GET_PUBLIC_TEMPLATE	N	N	N	N	N	N	N	N
PB_VERIFY	N	N	N	E	N	N	N	N
PERFORM_SECURITY_OPERATION	N	N	N	N	E	E	E	E
READ_BINARY	N	N	N	N	R	R	R	R
RECYCLE	D	D	D	D	D	D	D	D
SELECT_FILE	N	N	N	N	N	N	N	N
SHA1_DIGEST	N	N	N	N	N	N	N	N
VERIFY	E	E	N	N	N	N	N	N
WRITE_BINARY	W	W	W	N	W	W	W	W

Table 22 – PKI BLADE Applet Services, Access Control and Relationship to CSPs

D = Destroy (zeroizes the CSP as a result of command execution)
E = Execute (uses the CSP in the execution of the command)
R = Read (the value of the CSP exits the module as a result of command execution)
W = Write (the value of the CSP is written into the module as a result of command execution)
U = Update
N = No access

6 Critical Security Parameters and Public Keys

The following describes CSPs and public keys that are available to an operator as a service from the ISD or ASD.

There is no interface to retrieve any of these CSPs or public keys.

6.1 Card Administrator Keys in Issuer Security Domain

1. **CDK**: This CSP is a set of three Keys, called CDK_{ENC} CDK_{MAC} and CDK_{KEK} of 16 bytes each. Depending on the initialization of the Issuer Security Domain, these keys are Two-Key TDES or AES 128 keys. The first two, CDK_{ENC} and $CDK_{MAC,}$ are only used to derive Secure Channel session keys (CSK_{ENC} and CSK_{MAC}) during the initiation of a Global Platform Secure Channel, and the last one, CDK_{KEK} is used to encrypt CDK keys to be loaded into the Issuer Security Domain using the PUT KEY command.

   The process used to generate a unique CDK per cryptographic module takes place outside of the crypto module.

   The loading of a new CDK key is done with a PUT KEY command and is protected by a Global Platform Secure Messaging using another CDK.

2. **CSK**: Card Administrator Session Keyset: Set of two transient Keys (called CSK_{ENC} and CSK_{MAC}) generated by diversification of the CDK per Global Platform specifications CSK_{ENC} is used for Secure Channel Encryption, and CSK_{MAC} is used for Secure Channel MAC verification and to authenticate the operator. CSK keys are used with the same algorithm (Two-Key TDES or AES 128) as the CDK from which they derived.

3. **K_{TOKEN}**: Key Token (Public Key): Public RSA Key (1024 bits) used to verify the tokens included in Delegated Management commands that embed the signature of these commands as per Global Platform specifications. This key may or may not be loaded into the module. It is an added feature and is not intended to satisfy any of the FIPS 140-2 requirements for applet loading.

4. **$K_{RECEIPT}$:** Key Receipt: Two-Key TDES key used to compute a receipt on Delegated Management Commands as per Global Platform Specifications. This key may or may not be loaded into the module. It is an added feature and is not intended to satisfy any of the FIPS 140-2 requirements for applet loading.

6.2 Application Provider Keys in Application Security Domains

1. **ADK**: This CSP is a set of three Keys, called ADK_{ENC} ADK_{MAC} and ADK_{KEK} of 16 bytes each. Depending on the initialization of the Application Security Domain, these keys are Two-Key TDES or AES 128 keys. The first two, ADK_{ENC} and $ADK_{MAC,}$ are only used to derive Secure Channel session keys (ASK_{ENC} and ASK_{MAC}) during the initiation of a Global Platform Secure Channel, and the last one, ADK_{KEK} is used to encrypt ADK keys to be loaded into the Application Security Domain using the PUT KEY command.

   The process used to generate a unique ADK per cryptographic module takes place outside of the crypto module.

   The loading of ADK keys set is done with a PUT KEY command and is protected by a Global Platform Secure Messaging using another ADK.

2. **ASK**: Applet Provider Session Keyset: Set of two transient Keys (called ASK_{ENC} and ASK_{MAC}) generated by diversification of the ADK per Global Platform specifications. ASK_{ENC} is used for Secure Channel Authentication and optionally Encryption, and ASK_{MAC} is used for Secure Channel MAC verification and to authenticate the operator. ASK keys are used with the same algorithm (Two-Key TDES or AES 128) as the ADK from which they derived.

3. **K_{DAP}**: DAP Key (Public Key): Public part of the Card Administrator RSA DAP Key (1024 bits) used verify the signature of an executable load file being loaded by the Application Provider. This key may or may not be loaded into the module. It is an added feature and is not intended to satisfy any of the FIPS 140-2 requirements for applet loading. This key is present only in Security Domain with DAP Verification. See Global Platform Specification for more information on the use of DAP.

6.3 PIV Keys

The ID-One PIV Applet Suite supports the following keys:

Key Name	Supported Algorithms
Administrator Keys	TDES (2-Key and 3-Key); AES 128/192/256
Mutual Authentication Keys	TDES (2-Key and 3-Key); AES 128/192/256
Internal Authentication Symmetric Key	TDES (2-Key and 3-Key); AES 128/192/256
General Authenticate Asymmetric Keys	RSA 1024, 2048; ECC P-224, P-256, P-384

Table 23 : Supported algorithms for PIV keys.

Multiple instances of each of the above keys, (each with a different key ID) can coexist in the module. This allows the module to support new PIV functionalities like key history.

6.3.1 Administrator Keys

A successful external authentication using an Administrator key with the GENERAL AUTHENTICATE command grants the Application Administrator privilege.

An Administrator key can only be used to perform an external authentication or a Mutual Authentication.

6.3.2 Mutual Authentication Keys

A successful mutual authentication using a Mutual Authentication key with the GENERAL AUTHENTICATE command grants the Application Mutual Authentication privilege.

6.3.3 Internal Authenticate Symmetric Keys

The Internal Authenticate Symmetric Key is used by the off-card application to authenticate the card using a challenge response mechanism described in SP800-73-3.

It does not grant any specific privilege internal to the module.

6.3.4 General Authenticate Asymmetric keys

The General Authenticate Asymmetric Key is used to perform one of the following:

1. Internal authentication using public key cryptography
2. Digital Signature
3. Key Establishment. (Key Transport for RSA and ECC CDH for ECC)

Digital signature and key establishment are not actually performed by the ID-One PIV Applet Suite. The module is merely providing a cryptographic service that is used by the off-card application to complete the digital signature or key establishment protocol. Such completion is done outside of the cryptographic boundaries of the module.

For RSA keys the same command is used to perform any of the above three functionalities, and the cryptographic computation performed by the module is always the same: Compute $c = m^d$ mod n where d is the secret exponent and n the modulus. What makes this computation an internal authentication, a digital signature or a key establishment depends on how the input message is constructed by the off-card application, and is outside the cryptographic boundaries of the module.

For ECC keys, the same command is used to perform internal authentication and digital signature. In both cases, the cryptographic computation performed by the module is an ECDSA computation. For key establishment with ECC, the command sent to the module is different and the module returns the pre-master secret of the ECDH algorithm in accordance with SP 800-56A Section 5.7.1.2 instead of an ECDSA signature. Completion of the key establishment protocol is performed by the off card application and is outside the cryptographic boundaries of the module.

6.4 Card Holder Verification Reference data

6.4.1 Local PIN

The local PIN is an 8 Byte binary value that is used to authenticate the CH role. Such authentication is valid only within the currently selected application. The local PIN is an optional CSP that may not be present when the Global PIN is already present.

The local PIN is created during personalization by loading its initial value over a secure channel. Once created, it can then be loaded into the module over a secure channel or in plaintext using the VERIFY and CHANGE REFERENCE DATA commands. It is destroyed using the Change Reference Data Command, or upon deletion of the application.

6.4.2 Local PUK

The local PUK is an 8 Byte binary value that is used to authenticate the LPU role. Such authentication is valid only for the duration of one APDU. The local PUK is an optional CSP that may not be present when the Local PIN does not need to be unblocked.

The local PUK is created during personalization by loading its initial value over a secure channel. Once created, it can then be loaded into the module over a secure channel or in plaintext using the RESET RETRY COUNTER and CHANGE REFERENCE DATA commands. It is destroyed using the Change Reference Data Command, or upon deletion of the application.

6.4.3 Global PIN

The Global PIN is an 8 Byte binary value that is used to authenticate the CH role. Such authentication is valid for any application within the module that recognizes the Global PIN as an acceptable CH verification method (see PIN Discovery Data object from SP800-73-3). The Global PIN is an optional CSP used according to the Discovery Object policy.

The Global PIN is created during personalization by loading its initial value over a secure channel. Once created, it can then be loaded into the module over a secure channel or in plaintext using the Verify and Change Reference Data commands. It is destroyed using the Change Reference Data Command, or upon deletion of the CHV Interface Server.

6.4.4 Fingerprint biometric template

PKI BLADE Applet fingerprint biometric methodology uses Precise Match-on-Card technology. The biometric process is divided into two separate functions: enrollment and verification.

During the *enrollment* process using PB_CREATE_BIO_MATCH_J_TEMPLATE service, biometric reference template is extracted and stored on the card. The reference fingerprint template is split into two different data objects: less than 850 bytes reference data and 128 bytes biometric header. The reference data contains the characteristic information extracted from the original fingerprint image. The biometric header contains public information associated with the reference data. The highly sensitive information contained in the reference data is security stored on the card and is not accessible outside the card. The biometric header, however, shall be stored on the card in such a way that it is accessible by the host application at any time using the PB_GET_PUBLIC_TEMPLATE service.

During the *verification* process using PB_VERIFY service, a user's fingerprint image from one of the user's enrolled fingers is scanned and the corresponding biometric header information is uploaded from the smart card. The fingerprint image is processed using the biometric header, and the characteristic features are extracted and converted into verification data. This data is then is sent to the card for the on card matching algorithm to compare the two data sets and according to the outcome of the on card verification, the internal card state may transition to the user authenticated state.

6.5 Other Platform CSPs

6.5.1 RNG Seed

The seed used by the RNG is a 20 byte value generated by the Hardware NDRNG. To get the best possible entropy, only 40 bytes are retrieved from the RNG before it is re-seeded from the Hardware NDRNG.

6.6 PKI BLADE Applet CSPs

All CSPs, summarized in the table below, are stored in plaintext form in EEPROM. Keys are protected against unauthorized modification, substitution and disclosure by the PKI BLADE applet file access control system. Authenticated Users or the SO may enter or output keys in key files in plaintext form.

CSP Name	Length and type
SO PIN	20 byte SHA-1 hashed value of 20 byte data string for SO authentication. The PKI BLADE applet requires 1 instance in the MF and allows an additional instance in each possible DF.
Backup SO PIN	6-20 byte data string for SO authentication; the Backup SO PIN is an optional copy of the previous SO PIN value. See Section 5.1.6 for additional context. The reference value is stored hashed by SHA-1 in EEPROM. The PKI BLADE applet requires 1 instance in the MF and allows an additional instance in each possible DF.
User PIN	20 byte SHA-1 hashed value of 20 byte data string for User authentication. The PKI BLADE applet requires 1 instance in the MF and allows an additional instance in each possible DF.
PFT	Private portion of fingerprint template. Up to four fingerprint templates per user, stored under the MF or under any DF.
DEK	2-Key TDES (112 bit) Data Encryption Key. The applet allows up to 64 instances, determined by available space and maximum number of files.
PSK	RSA 1024 or 2048 Private Signature Key. The applet allows up to 64 instances, determined by available space and maximum number of files.
KUK	RSA 1024 or 2048 private Key Unwrap Key, used by the PERFORM_SECURITY_OPERATION for RSA key unwrapping. Up to 64 instances, determined by available space and maximum number of files.

Table 24 - PKI BLADE Applet CSPs

A key file can be zeroized by issuing the DELETE_FILE command. Additionally, the RECYCLE command will zeroize all applet files including all key and PIN files.

Only an authenticated User can generate keys on the card. No internally generated secret or private keys can be read, written or updated. The PKI BLADE Applet uses the ID-One Cosmo platform services to generate keys:

- 16 byte 2 Key TDES (using the Oberthur platform Approved DRNG)
- 1024 or 2048-bit RSA public and private key pairs (using the Oberthur platform Approved RSA key pair generation with conditional test)

6.7 PKI BLADE Applet Public Keys

CSP Name	Length and type
SVK	RSA 1024 or 2048 Public Signature Verification Key (the public key associated with PSK). This public key is an output of key pair generation and is not used by the module.
KWK	RSA 1024 or 2048 public Key Wrap Key. This public key is an output of key pair generation and is not used by the module.

Table 25 - PKI BLADE Applet Public Keys

7 Self Tests

7.1 Power on Self Tests

Each time the module is powered by a reader (contact or contactless), a “reset” signal is sent from the reader to the module. The module then performs a series of GO/NO-GO tests to validate that the cryptographic module is in good working order before it answers subsequent card commands.

The Power-up self-tests include:

- EEPROM code integrity check
- Cryptographic algorithm tests (KAT)
  - Random Number Generator
  - TDES – Encryption and Decryption
  - AES Encryption and Decryption
  - RSA – Signature and Verification
  - SHA-1 Known Answer Test
  - Elliptic Curves Engine – ECDSA Signature and verification

Critical function tests including system tests and CRC algorithms tests as well as additional tests to protect against new types of attacks such as SPA, DPA, “flash gun”, EMI etc, are also performed at this stage. The module also performs Environmental Failure Protection; during code execution light sensors and numerous logical controls are set such as any discrepancies detected leads to a Kill Card mechanism. Furthermore, other environmental sensors (frequency, abnormal voltages and temperature) are continuously enabled to detect any discrepancy leading to a card cold reset.

The module does not respond to any commands while self-tests are being performed.

If any of the above tests fail, the card returns an error status before entering an error state in which further commands are not processed.

7.2 Conditional Self-Tests

7.2.1 Key Pair-Wise Consistency Tests

RSA Key Generation: After generating an RSA key pair, the module performs a double pair-wise consistency check to validate that the newly generated key pair for both signature/verification and encryption/decryption.

Elliptic Curve Key Generation: After generating an ECC key pair, the module performs a pair-wise consistency check to validate the newly generated key pair for signature/verification using ECDSA algorithm.

7.2.2 Continuous Random Number Generator Test

Continuous testing is performed on every output of the Random Number Generators. (Both Deterministic and Non Deterministic) RNGs. Additional statistical testing is also performed to ensure the highest possible quality of the generated random numbers.

7.2.3 CSP Integrity Tests

Each time a CSP is used, its integrity is verified using either a 16 bit CRC polynomial on its value or a KAT.

7.2.4 Firmware Load Test

Application loading follows the Global Platform specifications. A TDES MAC for each packet of the executable load file is verified each time an applet is loaded onto the cryptographic module.

8 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

8.1 Authentication Security Rules

- For the Card administrator (CA), the secret is the CDK and the identifier is a combination of the ISD AID (Application Identifier) and the key set ID within the ISD.
- For the Application Provider (AP), the secret is the ADK and the identifier is a combination of the ASD AID (Application Identifier) and the key set ID within the ASD.
- For the Application Administrator (ADM), the secret is the PIV key 9B and the identifier is a combination of the Application AID (Application Identifier) and the algorithm to be used by key 9B.
- For the Mutual Authentication User (MAUTH), the secret is the PIV key 9F and the identifier is a combination of the Application AID (Application Identifier) and the algorithm to be used by key 9B.
- For the Local PIN Unblock User (LPU), the secret is the local PUK and the identifier is a combination of the Application AID (Application Identifier) and the index value associated with the reference data (PIN Unblocking Key) used to perform the PIN Unblock User verification (CHV).

- For the Card Holder (CH), the secret is the value of either the local or Global PIN and the identifier is the index value associated with the reference data (Local PIN or Global PIN) used to perform the card holder verification (CHV).

8.2 Application Life Cycle Security Rules

Additional application can be loaded in the module in post issuance under specific conditions. Application loading is one of the services provided by the module operating system that is restricted to the Card Administrator or the Application Provider: It can be performed only within a GP secure channel that provides authentication of the role and integrity of the application executable code (Applet) being loaded.

The loading and installation of FIPS validated applications may occur before, during, or after card issuance.

For the module to run in a validated FIPS 140-2 Level 2 mode of operation, all applets must be validated to the same level prior to being loaded into the module. It is the responsibility of the Cryptographic Officer to insure that applets loaded post-validation have been FIPS 140-2 Level 2 validated.

The module validation to FIPS is no longer valid once a non-validated applet is loaded.

The command described in Section 3.5 allows an authorized operator to check, at any time, both identity and version number of all packages (applets) present in the module.

8.3 Access Control Security Rules

All cryptographic keys must be loaded through a secure channel session ensuring their integrity and confidentiality.

8.4 Key Management Security Policy

8.4.1 Crypto Officer Cryptographic keys

The module uses the following CSPs for the Crypto-Officers:[1]

Key Name (CSP)	Type	Length	Strength
CDK $_{DES}$	TDES	128-bits	80-bits
ADK $_{DES}$			
CSK $_{DES}$	TDES Session Keys	128-bits	80-bits
ASK $_{DES}$			
CDK $_{AES}$	AES	128-bits	128-bits
ADK $_{AES}$			

[1] PKI BLADE Applet CSPs are described separately.

CSK $_{AES}$	AES Session Keys	128-bits	128-bits
ASK $_{AES}$			
K$_{RECEIPT}$	TDES	128-bits	80-bits

Table 26: CSP used for Crypto-Officers

In addition, the PIV applet from the module supports the following CSP available to users (PIV Keys):

Key Name	Type	Length	Strength
TDES Secret Keys	TDES ECB and CBC	128-bits 192-bits	80-bits 112-bits
AES Secret Keys	AES ECB and CBC	128-bits 192-bits 256-bits	128-bits 192-bits 256-bits
RSA Private Keys	RSA 1024 and 2048 Signature Generation and & Key Unwrapping	1024 to 2048 bits	80 to112 bits
ECC Private Keys	ECDSA and ECDH with the following curves P-192, P-224, P-256, P-384	192, 224, 256, 384	80 112 128 192

Table 27: CSP available to users

8.4.2 Cryptographic key generation

- TDES and AES Session key generation using SCP and FIPS 186-2 approved RNG for secure channel opening.
- RSA key pair generations (up to 2048 bit key length) fully compliant with ANSI X9.31 and using a FIPS140-2 approved RNG. Both standard RSA key and RSA Chinese Remainder Keys can be generated.
- ECC key pair generations (on GF(P) curves with “f” up to 384)

8.4.3 Cryptographic key entry

Keys can only be input in encrypted format, using the Put Key command within a secure channel. During this process, the keys are encrypted using the Key Encryption Key of the ASD and optionally the encryption session key of the secure channel.

Regardless of the inherent cryptographic strength of the key algorithm used, the cryptographic strength of the key once loaded in the module will not exceed the cryptographic strength of the transport key being used during the key entry process.

Keys can never be output by the platform. The PKI BLADE Applet permits entry and output of PKI BLADE Applet CSPs in plaintext, as determined by PKI BLADE Applet file access controls.

8.4.4 Cryptographic key storage

The Keys are structured to contain the following parameters during storage:

- Key set version
- Key Index, which is the ID of the key
- Algo ID, which determines which algorithm to be used
- Integrity Mechanisms

8.4.5 Cryptographic Key Zeroization

All platform cryptographic keys stored in non-volatile memory can be zeroized using the **DELETE** command (package deletion).

Session cryptographic keys (CSK and ASK) are stored in volatile memory and are zeroized upon termination of the session, i.e. when the secure channel is closed or when the module is powered off.

User keys (PIV application keys) can also be zeroized using the delete mode of the **PUT PIV KEY** command.

Cryptographic Officer keys (Card Administrator keys and Application Provider keys) stored in non-volatile memory are also zeroized using a procedural overwrite (reloading another value using the **PUT KEY** command).

8.5 ID-One PIV Applet Suite Guidance

In addition to the above guidance, the issuer and end-users must observe the following rules:

The ID-One PIV Applet Suite PIN and Global PIN value must use a length and character set combination that meets the FIPS 140-2 authentication strength requirement (probability of false acceptance 1/1,000,000). Note that SP 800-73-3 calls for numeric-only PIN values; in this case, at least six characters must be used.

8.6 PKI BLADE Applet Guidance

When or before the card is issued, the end-user should be made aware that the card is an extension of the user’s ID and is capable of generating a digital signature for the user, which is as valid and legal as a written signature on a paper document. For this reason the user should also understand that he /she should keep the card on their person or under lock and key when not in use, and to protect their secret pass phrase from observation when logging on.

At the time the card is issued, an initial user pass phrase is in the card. The issuer should be urged to immediately change the initial pass phrase to one which the user can easily remember but one which others cannot easily guess.

Users must ensure RSA key transport services are used only for key wrap and unwrap; these operations limit use to data input of the appropriate size as a safeguard against usage for bulk encryption.

The SO is responsible for ensuring that cards are issued with a card configuration file as well as file permissions in accordance with organization security policy.

The following rules must be observed:

1. The 1/1,000,000 FAR setting must be selected when the Bio Only or Bio-or-PIN settings are used.
2. A value between 1 and 10 inclusive for the number of allowed bad fingerprint authentication attempts must be selected when the Bio Only or Bio-or-PIN settings are used.
3. The SO must change the default SO PIN as soon as the card is in possession of the SO and must not communicate his/her PIN to any entity.
4. When the Recycle command is issued the EXF file is deleted. This command must only be used when the card is destroyed.
5. The SO must unblock User PIN only for legitimate Users.
6. Use of DEK keys must be restricted to 2^20 encrypt or decrypt operations.

9 Physical Security

The Oberthur ID-One Cosmo V7-n is a production quality single chip cryptographic module that meets FIPS 140-2 Level 4 Physical Security Requirements.

The Oberthur ID-One Cosmo V7-n employs a NXP SmartMX single chip secure microprocessor cryptographic module with approved contactless interface functionality. This SmartMX and its OS incorporate a range of both hardware and software-based security features as counter measures against attempted attacks. The SmartMX combines handshaking circuit technology, a very dense 5-metal-layer 0.14 µm technology, glue logic and active shielding methodology for optimum security results. SmartMX card ICs also features - beyond exception sensors for voltage, frequency, temperature - dedicated countermeasures against Differential Failure Analysis, Single/Double Power Analysis and dangerous locally focused/well-timed laser light attacks . This makes the entire family extremely resistant to any kind of physical analysis and forced malfunction during operation. A hardware memory management unit (Firewall) provides additional protection for PKI controllers. The SmartMX has achieved best-in-class Common Criteria EAL5+ certification on the basis of the rigorous BSI-PP-0002-2001 Protection Profile (CC# BSI-DSZ-CC-0410-2007).
Key features include:

- Secure_MX51 high performance CPU using 0,14 µm CMOS technology based on power saving, self-timed asynchronous technology
- 32 bit high speed and attack-hardened PKI crypto engine for RSA and ECC
- (RAM-supported RSA key length up to 4096 bit) direct 32 bit access to crypto RAM
- 8 bit parallel processing attack-hardened AES engine
- 64 bit parallel processing 2/3 keys attack-hardened TDES engine
- 25 years minimum data retention
- 500k EEPROM erase/program cycles endurance
- Data protection (true encryption and physical measures) for RAM, EEPROM and ROM
- State of the art security sensors (V, f, T, light),
- Complex and dynamic active shielding, Single Fault Injection (SFI) attack detection
- NXP Semiconductors signed CRI license for legal use of DPA countermeasures

A visual inspection system used during manufacturing automatically sorts out damaged chips.

10 Mitigation of Other Attacks

10.1 Power Analysis (SPA/DPA)

Power analysis attacks use information gathered from non-invasive measurements to crypto analyses and extract keys from tamper resistant devices.

Simple Power Analysis (SPA) attacks use direct observation of a device's power consumption. Because power consumption often varies significantly with computations performed by the crypto module, SPA observations can identify sensitive computational processes, reveal the presence of cryptographic sub-routines, and significantly accelerate reverse engineering.

Differential Power Analysis (DPA) attacks use statistical analysis and error correction techniques to extract information leaked across multiple operations. This aggregation of data allows extremely small differences in power consumption to be isolated, including effects that are many orders of magnitude smaller than "noise".

The Oberthur ID-One Cosmo V7 cryptographic module has been designed to mitigate both Simple Power Analysis (SPA) and Differential Power Analysis (DPA).

The module includes protections against SPA and DPA attacks for all embedded cryptographic algorithms involving secret elements. The chip protection level was evaluated against state-of-the art attacks (at the time of design).

The cryptographic module mitigates Simple Power Analysis (SPA) and Differential Power Analysis (DPA) attacks using a combination of hardware and software design that makes differentiation of key values impractical by equalizing or scrambling current consumption of the card during algorithm cryptographic computation.

Based on the algorithm used, the defense mechanisms vary, as the internal hardware implementations of these algorithms do not use the same underlying hardware.

10.2 Timing Analysis

Timing attacks are non-invasive attacks that rely on the variation in computation time required for the microprocessor to perform its secret calculation.

All cryptographic algorithms as well as Java Card API comparison functions offered by the chip are designed to be protected against Timing Analysis.

This is done by enforcing the fact that any sensitive operation is achieved in a constant time regardless of the value of keys or data involved.

10.3 Fault Induction

This type of attack is based on the theoretical possibility of flipping some random bits of the secret key, stored in RAM or EEPROM, before or during the computation done by the module (Bellcore attack). Another fault induction attack is to induce decoding error during the execution of one instruction.

The Oberthur ID-One Cosmo V7 cryptographic module includes a combination of software and hardware protections in order for the chip not to operate in extreme conditions that may cause processing errors that could lead to revealing the values of cryptographic keys or secret elements. Extreme Conditions refer to abnormal temperature, external power supply and external clock supply.

In addition, every keys and PINs are protected by a signature that is checked prior to every use of the keys or PINS. See Section 7.2 Conditional Self-Tests.

10.4 Flash Gun

The Oberthur ID-One Cosmo V7 cryptographic module includes a combination of software and hardware protections in order to detect “Flash Gun” type of attacks and abort any current processing before becoming mute.

10.5 Electromagnetic Attacks

The Oberthur ID-One Cosmo V7 cryptographic module includes a combination of software and hardware protections in order to detect “EMI” type of attacks and abort any current processing before becoming mute.

10.6 Card Tearing

The Oberthur ID-One Cosmo V7 cryptographic module includes a combination of software and hardware protections in order to protect the card against damages potentially caused by a discontinued power (or RF for contactless) supply during an operation. Roll back mechanisms restore the card memory to a safe previous stable state during the next power-on sequence.

11 References

The Oberthur ID-One Cosmo V7 cryptographic module complies with the following specifications:

[1] ISO/IEC 7816-3 – Information Technology – Identification Cards – Integrated Circuit(s) with Contacts – Part 3: Electronic Signals and Transmission Protocols, December 1997 – Amendment, June 2002.

[2] ISO/IEC 7816-4 – Information Technology – Identification Cards – Integrated Circuit(s) with Contacts – Part 4: Inter-industry Commands for Interchange, September 1995 – Amendment, December 1997.

[3] ISO/IEC 7816-5 – Information Technology – Identification Cards – Integrated Circuit(s) with Contacts – Part 5: Numbering system and registration procedure for application identifiers, June 1994 - Amendment, December 1996.

[4] ISO/IEC 14443-3 – Information Technology – Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 3: Initialization and Anti-collision, February 2001.

[5] ISO/IEC 14443-4 – Information Technology – Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 4: Transmission Protocols, February 2001.

[6] GlobalPlatform Card Specification, version 2.1.1, March 2003.

[7] GlobalPlatform Card Specification, Amendment A, February 2004.

[8] Visa Open Platform Card Implementation requirements 3 – Multiple Security Domains with DAP Capability, October 2001.

[9] Visa GlobalPlatform 2.1.1 Card Implementation Requirements, May 2003.

[10] JavaCard 2.2.2 Application Programming Interface, March 2006.

[11] JavaCard 2.2.2 Run-time Environment Specification, March 2006.

[12] JavaCard 2.2.2 Virtual Machine Specification, March 2006

[13] "Integrated Circuit Card Specifications for Payment Systems" – EMV 2000

Part 1: Electromechanical Characteristics, Logical Interface, and Transmission Protocols (version 3.0)
Part 2: Data Elements and Commands (version 3.0)
Part 3: Application Selection (version 3.0)
Part 4: Security Aspects (Version 3.0)

[14] " Biometric data interchange formats – part 2 – Finger minutiae data " ISO/IEC 19794-2 (2005)

[15] FIPS-201-1-v5 FIPS Publication 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors (March 14, 2006)

[16] FIPS-201-1-chng1 FIPS 201-1 Change Notice 1 - June 23, 2006

[17] SP 800-73-3 Interfaces for Personal Identity Verification, September 2008

[18] SP 800-76-1 Biometric Data Specification for Personal Identity Verification, January 2007

[19] SP 800-78-3 Cryptographic Algorithms and Key Sizes for Personal Identity Verification, August 2007

[20] SP 800-104 A Scheme for PIV Visual Card Topography, June 2007

[21] SP 800-85A-2 PIV Card Application and Middleware Interface Test guidelines, March 2009.

[22] PKCS 1 PKCS #1: RSA Encryption Standard, Version 1.5, November 1993

12 Definitions and Acronyms

12.1 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ACR	Access Control Rules
ADM	Application Administrator
AID	Application Identifier
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASD	Application Security Domain
ATR	Answer To Reset (contact mode)
ATS	Answer to Select (contactless mode)
BAP	Batch Approval Process (First article validation from Production line)
CA	Card Administrator
CBC	Cipher Block Chaining
CH	Card Holder
CHV	Card Holder Verification
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DF	Directory File (PKI BLADE Applet)
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman

ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
ISD	Issuer Security Domain
ISO	International Standard Organization
JC	Java Card
JCRE	Java Card Runtime Environment
LPU	Local PIN Unblock User
MAC	Message Authentication Code
MAUTH	Mutual Authentication User
MF	Master File (PKI BLADE Applet)
MOC	Match on Card (PKI BLADE Applet)
NDRNG	Non Deterministic Random Number Generator
OP	Open Platform
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
RAM	Random Access Memory
ROM	Read only Memory
RSA	Public key cryptographic algorithm invented by Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
SCP	Secure Channel Protocol
TDES	Triple DES