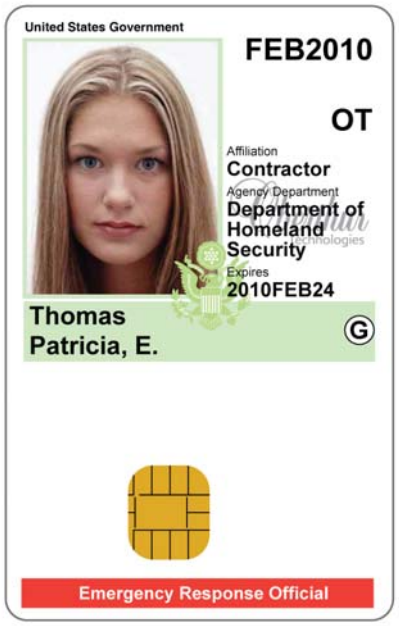
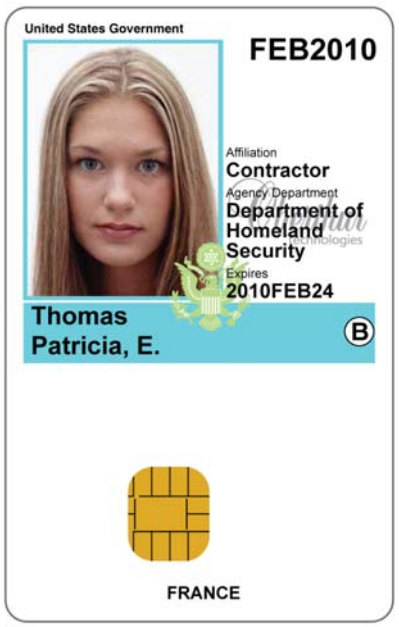
ID-One PIV (Type A)

(PIV Applet Suite on ID-One Cosmo V7-n)

FIPS 140-2 Security Policy

Public Version





Oberthur Technologies of America
4250 Pleasant Valley Road
Chantilly, VA 20151-1221 - USA

Change Record

Revision	***Date***	***Author***	***Description of Change***
1	June 30, 2010	C. GOYET	First Public version

Table 1: Document Version History

CONTENTS

TABLES

FIGURES

1 Introduction

1.1 Scope

This document defines the Security Policy for the ID-One PIV (Type A) cryptographic module from Oberthur Technologies.

The module 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.

The ID-One PIV (Type A) cryptographic module is composed of the Oberthur ID-One PIV applet suite that has been loaded on the ID-One Cosmo V7-n smart card cryptographic module.

The ID-One PIV applet suite is available under two commercial configurations called ID-One PIV BIO and ID-One PIV ECC. Except for the Fingerprint On-Card Comparison that is activated only on the "BIO" version, both versions share the same functionalities and the description of the ID-One PIV in the remainder of this document applies to both the ID-One PIV BIO and the ID-One PIV ECC unless explicitly stated otherwise.

The ID-One PIV (Type A) is also available in multiple memory sizes to better meet marketing requirements.

Depending on the hardware platform being used, the ID-One PIV supports either the Type A or Type B contactless communication described in ISO/IEC 14443. This document defines the Security Policy for the Oberthur ID-One PIV (Type A) cryptographic module.

1.2 Module Overview

ID-One PIV (Type A) is the latest Oberthur Technologies Card offering validated by NIST to comply with PIV specifications (FIPS 201 and related Special publications). ID-One PIV (Type A) has received NPIVP Certificate #18. It offers Identity proofing (storage of personal data), General Authentication Services and secure post issuance management in the PIV system.

It supports all the strongest cryptographic algorithms defined in the PIV specifications (SP800-78-2) 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.

The ID-One PIV BIO includes a Fingerprint On-Card Comparison that delivers exceptional performances in terms of interoperability, accuracy and speed, while maintaining an error rate lower than the thresholds defined by the US Government's PIV program. The Fingerprint On-Card Comparison algorithm has been independently tested by NIST, and was found to comply to the PIV interoperability specifications, with an error rate of under 0.55% regardless of the (MINEX Approved) fingerprint vendor being used to extract the biometric data. It was also the fastest to date with an average of 0.28 seconds per positive match.

The main advantage of Fingerprint On-Card Comparison is to enhance security and user privacy since the reference biometric data never leaves the card. It provides a very secure way of authenticating the card holder. The ID-One PIV BIO works with any fingerprint reader that can output a minutia template compliant with the ISO/IEC 7816-11 BIT retrieved from the module.

In addition to the above, the ID-One PIV from Oberthur provides enhanced functionalities to extend its field of application outside the HSPD#12 program. These features include:

- **Flexible containers**: the ID-One PIV 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.
- **AES Based secure messaging:** the ID-One PIV implements an optional secure messaging based on AES cryptographic algorithm. This enhances security in communication of sensitive data with the card.
- **Key Usage control**: To increase security and provide control over key usage, the ID-One PIV Card 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 ID-One PIV cards

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

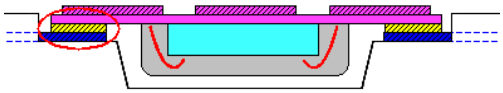


Figure 2: Cryptographic module

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 ID-One PIV applet suite when loaded on the ID-One Cosmo V7-n smart card cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2, with Physical Security being validated against Level 4 requirements.

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

Table 2: Module Security Level Specification

3 Cryptographic Module Specification

3.1 Overview

The ID-One PIV applet suite is loaded onto the ID-One Cosmo V7-n smart card cryptographic module that has been independently FIPS 140-2 Level 3 validated (FIPS 140-2 Cert. #1236).

The module is always in a FIPS 140-2 Approved mode of operation. 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 PIV applet suite and the ID-One Cosmo V7 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 Hardware

The ID-One PIV (Type A) inherits the hardware platform identifiers of the ID-One Cosmo V7-n smart card cryptographic module on which it has been loaded.

The following hardware platforms may be used by the ID-One Cosmo V7-n cryptographic module to offer a wider range of EEPROM memory sizes:

- For ID-One PIV loaded on ID-One Cosmo V7-n Large:
    - HW P/N B0 with FW Version FC10 (with optional code 069778)
    - HW P/N B0 with FW Version FC10 (with optional code 071964)
- For ID-One PIV loaded on ID-One Cosmo V7-n Standard:
    - HW P/N BA with FW Version FC10 (with optional code 069778)
    - HW P/N BA with FW Version FC10 (with optional code 071964)

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

3.4 Module Firmware

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 firmware version supported by the module described in this security policy is: **FC10**

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

The complete firmware identification is achieved by putting together the firmware version and the firmware extension below.

3.5 Service Packs

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

The ID-One PIV (Type A) cryptographic module has been validated with the following optional codes:

FW	Optional Code	Note
FC10	069778	Generic r8 (for PIV ECC)
FC10	071964	BIO r4 (Generic r8 + MOC 3.21 for PIV BIO)

Table 3: Optional Codes included in this validation

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

3.6 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 3.8 below.

3.7 Applets

The ID-One PIV applet suite version 2.3.2 is composed of the following packages:

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 02
com.oberthurcs.javacard.chv.cvm	A00000007701 080807 1000 00 00000002	01 02
com.oberthurcs.javacard.chv.cvm.bio	A00000007701 080807 1000 00 00000001	01 02
com.oberthurcs.javacard.chv.server.biometric	A00000007701 080807 1000 00 00000005	01 02
com.oberthurcs.javacard.chv.server	A00000007701 080807 1000 00 00000006	01 02
PIV Applet		
PIV Applet Executable Load File	A00000007701 000006 1000 00 00000024	02 32

Table 4: ID-One PIV 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 4 are present.

3.8 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.

3.9 Cryptographic Algorithms

The ID-One PIV applet suite does not include 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 that are available through the ID-One PIV applet suite, and the associated CAVP certificate number.

Algorithm ID	Algorithm - Modes	Reference	Key Size	Bits of Security	CAVP Cert. #
'00'	3 Key Triple DES – ECB	SP 800-78-2	192 bits	**112**	**698**
'01'	2 Key Triple DES – ECB	SP 800-78-2	128 bits	**80**	
'02'	2 Key Triple DES – CBC	SP 800-78-1[1]	128 bits	**80**	
'03'	3 Key Triple DES – ECB	SP 800-78-2	192 bits	**112**	
'04'	3 Key Triple DES – CBC	SP 800-78-1	192 bits	**112**	
'06'	RSA 1024 bit modulus	SP 800-78-2	1024 bits	**80**	**403**
'07'	RSA 2048 bit modulus	SP 800-78-2	2048 bits	**112**	
'08'	AES-128 – ECB	SP 800-78-2	128 bits	**128**	**840**
'09'	AES-128 – CBC	SP 800-78-1	128 bits	**128**	
'0A'	AES-192 – ECB	SP 800-78-2	192 bits	**192**	
'0B'	AES-192 – CBC	SP 800-78-1	192 bits	**192**	
'0C'	AES-256 – ECB	SP 800-78-2	256 bits	**256**	
'0D'	AES-256 – CBC	SP 800-78-1	256 bits	**256**	
'0E'	ECC: Curve P-224	SP 800-73[2]	NIST Curve P-224	**112**	**94**
'11'	ECC: Curve P-256	SP 800-78-2	NIST Curve P-256	**128**	
'14'	ECC: Curve P-384	SP 800-78-2	NIST Curve P-384	**192**	
N/A	RNG	FIPS 186-2	N/A	N/A	**480**
N/A	RSA Key Pair Generation	ANSI X9.31	1024 + 2048	N/A	**403**
N/A	ECC Key Pair Generation	FIPS 186-2	NIST Curves P224, P256, P384	N/A	**94**

[1] CBC algorithms have been removed from SP 800-78-2 but remain supported by Oberthur to enable backward compatibility.
[2] Algorithm '0E', as defined in the original SP800-73, although no longer specified in SP-800-78-1, remains supported by Oberthur to enable backward compatibility.

N/A	Triple-DES MAC	Global Platform	128 bits	80	**698, vendor affirmed**
N/A	AES MAC	Global Platform	128 bits	128	**840, vendor affirmed**

Table 5: Supported Cryptographic Algorithm

Note that as per SP800-78-2, both the '00' and '03' algorithm identifiers correspond to 3 Key Triple DES – ECB.

3.9.1 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.

3.9.2 PKCS #1 and PSS

As per SP 800-73-3 and SP800-78-2, the ID-One PIV applet can generate an RSA signature on an externally generated hash. The PIV applet does not enforce the use of any specific hashing algorithm (SHA1, SHA 256 or SHA 384) and padding scheme (PKCS #1 v1.5 or PSS). 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 SP800-78-2 prior to being sent to the card for the RSA cryptographic computation.

3.9.3 RSA Key Transport

RSA Key Transport (decryption only) performed in accordance with SP 800-73-3, SP 800-78-2 and discussion with NIST using the PIV 9D key. The key establishment methodology provides 112 bits of encryption strength (determined by the use of the RSA algorithm with k = 2048.)

3.9.4 ECDSA

As per SP 800-73-3 and SP800-78-2, the ID-One PIV applet 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 SP800-78-2 prior to being sent to the card.

3.9.5 ECDH

As per SP800-78-2, the ID-One PIV applet can generate a pre-master secret using Elliptic Curve Diffie-Hellman (ECDH) 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 ECDH 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 SP800-78-2.

3.9.6 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 80 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.

3.9.7 Secure Hash Algorithm

From all the secure hash algorithms (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) that have been validated on the ID-One Cosmo V7 platform (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 ID-One PIV (Type A) card 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 6: Physical Interface for contact mode

4.1.1.1 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.

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

The module also supports the PPS to negotiate communication speed with the reader (Interface Device). Data communication speed on the I/O line is defined by the Values of the clock rate conversion integer “F” and the baud rate adjustment integer “D” 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):

F	D	f (max.) MHz	I/O Communication Speed with External clock at 5MHz (default max value as per ISO 7816-3:2006)
372	1	5	13,440 bauds
372	2	5	26,881 bauds
372	4	5	53,763 bauds
372	12	5	161,290 bauds
512	8	5	78,125 bauds
512	16	5	156,250 bauds
512	32	5	312,500 bauds
512	64	5	625,000 bauds

Table 7: Transmission parameters for contact mode

4.1.2 Contactless Mode

In contactless mode, the ID-One PIV (Type A) 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 8: 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	
Card Administrator (CA)	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)
Application Provider (AP)	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	
Application Administrator (ADM)	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
Mutual Authentication User (MAUTH)	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
Local PIN Unblock User (LPU)	The Local PIN Unblock User is responsible for unblocking the card holder local PIN and re-initialize it with a new value.

Card Holder (CH)	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 or more of the following: Local PIN; Local Pin Unblocking PIN; Global PIN; Fingerprint On-Card Comparison
Maintenance Roles	
None	The module does not support any maintenance role.

Table 9: 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, 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, Global PIN, or Fingerprint Template) 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.

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	Strength of Mechanism	Probability of Successful Random Attempt in 1 Minute
Local PIN	2^{11}	$15/2^{11}$
Local PUK	2^{11}	$15/2^{11}$
Global PIN	2^{11}	$15/2^{11}$
Fingerprint On-Card Comparison	$> 10^{6}$ *	$< 1/10^{5}$ *
2TDES Authentication	2^{80}	$10/2^{80}$
3TDES Authentication	2^{112}	$10/2^{112}$
AES-128 Authentication	2^{128}	$8/2^{128}$
AES-192 Authentication	2^{192}	$8/2^{192}$
AES-256 Authentication	2^{256}	$8/2^{256}$

Table 10: Strength of Authentication Mechanisms

* See Authentication Security Rules – biometric parameters are set to comply with FIPS 140-2 requirements as stated above.

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 – Using VERIFY or CHANGE REFERENCE DATA

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 in accordance with the SP 800-73-3 specifications ($2^{11} = 2^3$ (eight characters) * 2^8 (8 bits per Byte)). The module also enforces a configurable limit of unsuccessful attempts, with a maximum of 15, hence the $15/2^{11}$ limit to the probability of a successful random attempt in a one minute period.

5.3.4 CH – Using Fingerprint On-Card Comparison

The cryptographic module supports Fingerprint On-Card Comparison using the VERIFY command. False match rates for the biometric algorithm are determined through empirical studies which yield a characteristic curve for False Match Rate (FMR). The threshold and maximum retry count are set in the enrollment phase by Application Provider using the PUT DATA command as described in the module's Reference Guide [22]. Please see the Authentication Security Rules section for FIPS 140-2 compliant module initialization.

5.4 Services

Unauthenticated services that can be performed at any time independent of role are listed in Table 17. The relationship between roles, services and CSP is summarized in Table 18.

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 11: 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 Application Security Domain within 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.
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 always loaded protected by the encryption of the Secure Channel Protocol (AES). For symmetric keys a KCV is included in the transmission to ensure integrity of the key loading operation. For asymmetric key pairs, the integrity of the key loading operation is ensured by the module performing an automatic pairwise consistency check of the decrypted key pair. This command can also be used by the Application Administrator to zeroize an existing application key.
RESET RETRY COUNTER	This command is used by the Application Provider during personalization to create Local PIN, Local PUK and Global PIN if needed. It is also used during the life of the application to Reset existing reference data (Local PIN, Local PUK, or Global PIN) and update their associated maximum try limit (from 1 to 15).

Table 12: 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.
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. It is also used to update the Card Holder biometric reference template to be used by the Fingerprint On-Card Comparison function.
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.
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.
CREATE KEY SLOT	This command is used by the AP to add Key IDs, and their associated security parameters (e.g. ACRs), available to the PIV application.

Table 13: 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.
GENERATE ASYMMETRIC KEY PAIR	This command is used by the Mutual Authentication User to generate in the PIV application a new asymmetric key pair value (RSA or ECC) for a key ID for which he has been granted write access by the Application Provider or by the Application Administrator during Key Slot creation.

Table 14: 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 15: 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 and to update the Card Holder biometric reference template to be used by the Fingerprint On-Card Comparison function.
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.
GENERATE ASYMMETRIC KEY PAIR	This command is used by the Card Holder to generate in the PIV application a new asymmetric key pair value (RSA or ECC) for a key ID for which he has been granted write access by the Application Provider or by the Application Administrator during Key Slot creation.

Table 16: Card Holder Services

5.4.7 Un-Authenticated Services

The following table lists the services that the module 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	
VERIFY	This command is used to request the module to compare Local PIN or Global PIN, or the biometric data being sent through that command against up to 10 fingerprint reference templates previously enrolled (usually the 10 fingers of the card holder).
GENERAL AUTHENTICATE	This command is used by the Public User to perform a cryptographic operation used by the off card application to authenticate the card using a cryptographic key that can be used by the unauthenticated role.
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 17: Public User 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						d	c						Exec. Write
STORE DATA	X	X						a	b						Execute
SET STATUS	X							a	b						Execute
GET STATUS	X							a	b						Execute
DELEGATE MANAGEMENT	X							f							Execute
DAP VERIFICATION		X							g						Execute
MANAGE CHANNEL							X								
GENERAL AUTHENTICATE			X	X	X		X			j	j	j		j	Execute
GET DATA			X	X	X		X								
PUT DATA			X	X	X		X		l						Exec. Write
GENERATE ASYM. KEY PAIR			X	X	X					k					Exec. Write; Read (public key only)
PUT PIV KEY		X								j					Exec. Write
VERIFY					X		X					h, l	i		Execute
CHANGE REF. DATA					X	X						h	i		Exec. Write
RESET RETRY COUNTER		X				X									Exec. Write
CREATE FILE		X													
READ BINARY			X	X	X		X								
UPDATE BINARY			X	X	X		X								
CREATE CONTAINER		X													
CREATE KEY-SLOT		X	X												

Table 18: 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 18**	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
l	Fingerprint minutia template

Table 19: Description of the CSP/Public Key Referenced in Table 18

5.4.9 Access Control Rules

The ID-One PIV application suite supports an almost unlimited number of data objects and application keys.

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 application 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 OR Biometric Data	PIN ^ BIO	The flag value associated to the AC is equal to TRUE when a VERIFY of the LOCAL PIN or GLOBAL PIN or BIOMETRIC DATA has been successfully performed
Cardholder PIN AND Biometric Data	PIN & BIO	The flag value associated to the AC is equal to TRUE only when a VERIFY of the LOCAL PIN or GLOBAL PIN and BIOMETRIC DATA 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 immediate previous command.
Cardholder PIN ALWAYS OR BIO ALWAYS	PIN ALWAYS ^ BIO ALWAYS	The flag value associated to the AC is equal to TRUE when a VERIFY of the LOCAL PIN or GLOBAL PIN or BIOMETRIC DATA has been successfully performed in the immediate previous 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 20: 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.
- A verified Biometric Data (e.g. fingerprint) can satisfy this Access Condition if Biometric option is not deactivated.
- When the access condition is set to ‘PIN ^ BIO’ or ‘PIN ALWAYS ^ BIO ALWAYS’, a successful PIN verification gives access to authenticated services and a successful verification of the card holder fingerprint template give access to un-authenticated services.
- ‘PIN ^ BIO’, ‘PIN & BIO’, ‘PIN ALWAYS ^ BIO ALWAYS’ Access control rules (ACR’s) default to corresponding PIN ACR when Biometrics verification option has been explicitly disabled or is not available in the card configuration. Please see the Authentication Security Rules section for FIPS 140-2 compliant module initialization.

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 Triple DES 128 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.

2. **CSK**: Card Administrator Session Keyset: Set of two transient Keys (called CSK_{ENC} and CSK_{MAC}) of 16 bytes each generated by diversification of the CDK as per Global Platform 2.1 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 (Triple DES 128 or AES 128) as the CDK from which they derived.

3. $\mathbf{K}_{TOKEN}$: 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. $\mathbf{K}_{RECEIPT}$**:** Key Receipt: Triple DES 128 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 Triple DES 128 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.

2. **ASK**: Applet Provider Session Keyset: Set of two transient Keys (called ASK_{ENC} and ASK_{MAC}) of 16 bytes each generated by diversification of the ADK as per Global Platform 2.1 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 (Triple DES 128 or AES 128) as the ADK from which they derived.

3. $\mathbf{K}_{DAP}$: 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 Oberthur PIV application supports the following keys:

Key Name	Supported Algorithms (see Table 5)
Administrator Keys	00; 01; 02; 03; 04; 08; 09; 0A; 0B; 0C; 0D
Mutual Authentication Keys	00; 01; 02; 03; 04; 08; 09; 0A; 0B; 0C; 0D
Internal Authentication Symmetric Key	00; 01; 02; 03; 04; 08; 09; 0A; 0B; 0C; 0D;
General Authenticate Asymmetric Keys	06; 07; 0E; 11; 14

Table 21 : 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 ECDH for ECC)

Digital signature and key establishment are not actually performed by the module. 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 $c = m^d \bmod n$ 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 instead of an ECDSA signature. Completion of the key establishment protocol is performed by the off card application and is 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 minutia template

A ISO/IEC 19794-2 compact size Finger Minutiae Format data object is used to verify the biometrics of the card holder. Strength is based on the characteristic curve for the biometric algorithm – see Section 5.3.4.

6.5 Other CSP

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.

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
    - Elliptic Curves 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. At a minimum, a MAC of the executable load file is verified each time an applet is loaded onto the cryptographic module as part of the security offered by the Global Platform Secure Messaging when the ISD is in OP-SECURED.

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).
- The module supports configuration of the PIN and Fingerprint On-Card Comparison mechanisms for use in access control. Configuration is performed at the PIV Application initialization phase by Application Provider. For FIPS 140-2 conformant use of Fingerprint On-Card Comparison, the operator is required to configure the module to use Bio threshold value 0x1EDE (or higher), and BioTry Limit value 10 (or less).

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 3.7 allows 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:

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}			
CSK_{AES}	AES Session Keys	128-bits	128-bits
ASK_{AES}			
$\mathbf{K}_{RECEIPT}$	TDES	128-bits	80-bits

Table 22: 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 23: 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 (or ISD for CDK) 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 module.

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

User keys (PIV application keys) can 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 zeroized using a procedural overwrite. (Reloading another value using the **PUT KEY** command)

ADK can also be zeroized by deleting the Application Security Domain that hosts the keys, using the **DELETE** command.

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.

9 Physical Security

The Oberthur ID-One PIV (Type A) 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 PIV (Type A) 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 PIV (Type A) 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 PIV (Type A) 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 PIV (Type A) 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 PIV (Type A) 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 PIV (Type A)- 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, February 2010

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

[19] SP 800-78-2 Cryptographic Algorithms and Key Sizes for Personal Identity Verification, February 2010

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

[21] SP 800-85A-1 PIV Card Application and Middleware Interface Test guidelines, March 2009.

[22] ID-One PIV FIPS 201 Validated Dual Interface Smart Card Reference Guide.

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
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
FMR	False Match Rate (biometric on card verification)
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
NDRNG	Non Deterministic Random Number Generator
OP	Open Platform
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PPS	Protocol Parameter Selection
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