Oberthur PIV EP v1 on ID-One Cosmo 64 v5 D

FIPS 140-2 Level 2

Security Policy

Public Version

Version 1.1

April 27, 2006

Oberthur Card Systems
4250 Pleasant Valley Road
Chantilly, VA 20151-1221 USA
+1 (703) 263-0100

Version Control

Table 1 shows the version history of this Security Policy.

Version - Date	Description
V1.0 - March 31, 2006	First Submission to NIST
V1.1 – April 27, 2006	Changes per NIST comments

Table 1 - Document Version History

TABLE OF CONTENTS

1 Introduction

This document defines the Security Policy for Oberthur PIV EP v1 on ID-One Cosmo 64 v5 D which is a dual interface single chip cryptographic module hereafter referred to as Oberthur PIV EP card, submitted for validation in accordance with FIPS 140-2 Level 2 requirements.

Included are a description of the security requirements of the module and a qualitative description of how each security requirements is achieved. In particular, this security policy specifies the security rules under which the cryptographic module must operate.

This document describes the security policy when the module is configured for FIPS 140-2 Level 2 operation.

2 Module Overview

The Oberthur PIV EP card is made up of the Oberthur PIV EP (End Point) Applet Suite on Oberthur ID-One Cosmo 64 v5 chip platform.

The following section provides an overview of both components.

2.1 Oberthur ID-One Cosmo 64 v5 Chip Platform

The Oberthur Card Systems ID-One Cosmo 64 v5 chip platform is a single chip multi-application cryptographic Java Card module with optional dual interface (contacts & contactless) specifically designed for identity and government market needs. It contains a microprocessor and EEPROM to provide processing capabilities and data storage and offers Java Card™ Technology and Open Platform services to applets on the chip.

The chip platform directly provides all the low-level services such as memory management, I/O control, cryptographic algorithms and physical security. It loads and runs applets written in Java programming language and includes a native implementation of Java Card™ version 2.2 and Open Platform version 2.1.1A specifications, with full support for Delegated Management and DAP / Mandated DAP, that define a secure infrastructure for post-issuance programmable platforms.

Additional features include biometric extensions as defined by the Java Card Forum and an on card fingerprint matching using matching algorithms from various third parties.

The built in management of Logical Channels allows the platform to support multiple applications simultaneously, each with their own Security Domain.

The ID-One Cosmo 64 v5 Chip Platform combines the advantages of the Java programming language and cryptographic services with those of a dual interface micro module. The same security level can be achieved with both contact (ISO 7816) and contactless (ISO 14443) interfaces thanks to carefully designed hardware and software features. And to protect against skimming, a built-in firewall allows application developers to disable contactless access for sensitive operations.

All the above services can be accessed by the applets instantiated from code loaded onto the chip EEPROM or ROM using the Java Card™ Application Programming Interface (API).

In addition, whether embedded into a plastic card; a USB token or into an electronic passport, the ID-One Cosmo 64 v5 Chip Platform hardware module provides tamper-resistance and tamper evidence features that meet FIPS 140-2 LEVEL 3 physical requirements.

The module requires a lower voltage than traditional smart cards to operate making it the perfect cryptographic module for a new range of application using lower voltage portable readers. The cryptographic module operates under either 5 Volt power supply (ISO 7816-3 Class A) or 3 Volt power supply (ISO 7816-3 Class B).

The ID-One Cosmo 64 v5 Cryptographic Module has already achieved FIPS 140-2 Level 3 validation as a Chip Platform, and the platform implements all the security requirements required by such validation. NIST Certificate 548 provides detail information on the FIPS validation: http://csrc.nist.gov/cryptval/140-1/1401val2005.htm#548.

This document slightly increases the cryptographic boundaries of the above module by adding the Oberthur PIV EP v1 Applet Suite to the list of approved applications that can run while the module is in FIPS mode. An overview of the Oberthur PIV EP Applet Suite is provided in the next section.

2.2 Oberthur PIV EP v1 Applet Suite

The Oberthur PIV EP Applet Suite has been developed to provide a Personal Identity Verification Card (PIV) validated to FIPS 140-2 and FIPS 201.

More precisely, the Oberthur PIV EP card solution is an implementation of the PIV "end point" card services described in NIST Special Publication 800-73-1. See http://csrc.nist.gov/piv-program/fips201-support-docs.html for supporting documents.

The applet offers Identity proofing (storage of personal data), User authentication, Card authentication, digital signature, and secure post issuance management.

The Oberthur PIV EP Applet Suite also comes with support for a Global PIN management application, to allow multiple on card applications to share the same Card Holder Verification Method (Global Pin).

2.3 Target of Evaluation

The module submitted for validation consists of the ID-One Cosmo 64 v5 Chip platform on which the Oberthur PIV EP Applet Suite has been loaded.

This document addresses the submission for validation of the module in accordance with FIPS 140-2 Level 2 standard.

The target of evaluation can be embedded into different form factors. Below are some sample packaging for the cryptographic module; one as a FIPS 201 compliant dual interface smart card, and one as a contactless USB token that provides in a smaller form factor the same electrical functionalities (i.e. FIPS functionality from contact and contactless interfaces.

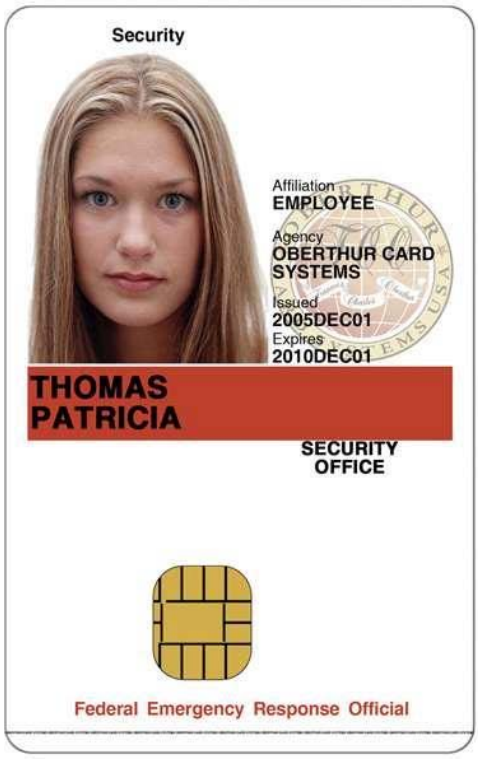

Figure 1: **PIV Dual Interface Smart Card**

Figure 2: **PIV Token**
Includes a smaller antenna for contactless communications and replaces the golden contact plate with a USB plug to remove the need of a smart card reader.

The following diagram shows the actual module cryptographic boundaries.

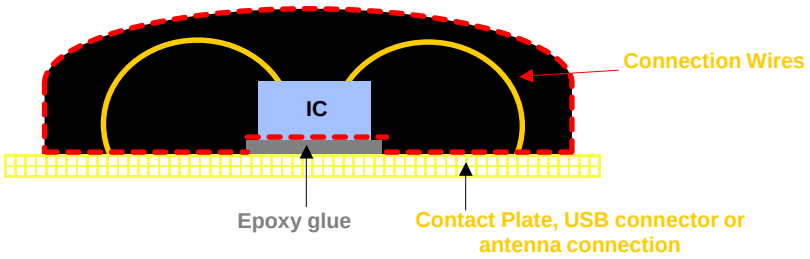

Figure 3

The red dotted line shows 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.

2.4 Product Terminology

In the remaining of this document, the cryptographic module described above will be referred to as Oberthur PIV EP card, regardless of whether the form factor is a actually a smart card, a USB token or any other form factor Oberthur may come up with to answer specific market needs.

3 Security Level

The Oberthur PIV EP card meets the overall requirements applicable to Level 2 security of FIPS 140-2.

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

Table 2 - Module Security Level Specification

4 Cryptographic Module Specifications

The Oberthur PIV EP card supports Identity-based authentication of the Card Holder, Application Operators, and Cryptographic Officers, using PIN or TDES or RSA keys. All services provided by the cryptographic module are protected by an identity-based access control policy following the result of the authentication.

This validation effort is aimed at the Systems Software, Virtual Machine, Card Manager/Security Domain applications, and Oberthur applets. If additional applets are loaded into this cryptographic module, then these additional applets require a separate validation, and they must be FIPS 140-2 validated.

The cryptographic module prevents the loading of unauthorized applet by restricting the applet loading to the Cryptographic Officer only, and by enforcing applet integrity verification by mandatory MAC or DAP verification.

The Cryptographic Module submitted for this validation includes:

1. The Oberthur ID-One Cosmo 64 v5 D Chip Platform
2. The Oberthur PIV EP v1 Applet Suite composed of the following elements:
   - OCS PIV Applet for PIV EP functionalities
   - OCS SSO Applet for Global PIN functionalities.

The applets offer services to external applications, relying on key management, secure memory management and cryptographic services, provided by the cryptographic module. The services are activated with “APDU commands” sent to the cryptographic module.

Each applet is associated to a unique Security Domain (SD) for its security configuration. This SD can be either the Card Manager or a separate Security Domain. The Card Manager is itself a security domain with additional services.

Every security domain holds one or more security domain key sets composed of TDES keys and optional RSA public Key for signature verification.

The ownership of a key set allows for establishing a Secure Channel (SC) between the host and either the security domain or an applet associated with the SD. Generally, the SC is used for administrative operations such as entering the application keys in the applet instances belonging to the security domain, or entering new key sets in the security domain itself. Note that a security domain key set can be used to enter a replacement key set in the same security domain – the replacement involves the deletion of the original key set. This is how a Card Security Controller role (CSC), which solely owns the Security Domain key set, can take control of the personalization of all applet instances belonging to a security domain.

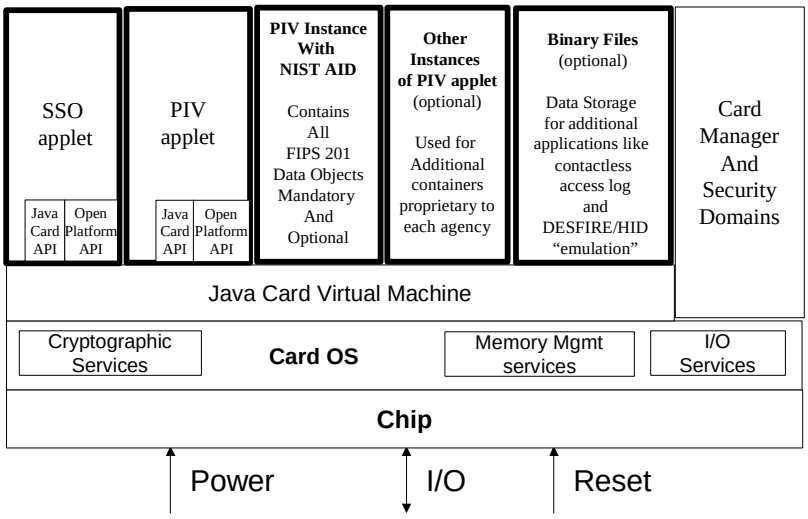

Figure 3: Functional block diagram

4.1 Module Identification

This document addresses the submission for validation of the module Oberthur PIV EP v1 on ID-One Cosmo 64 v5 D based on the following configuration:

- Hardware Platform # '77' with Firmware 'E303-063684' and PIV EP v1 Applet Suite.

Oberthur PIV EP v1 Applet Suite is made up of the following two applets:
- o PIV Applet Version 1.08
- o SSO Applet Version 1.08

For the purpose of this validation the Oberthur PIV EP card should be viewed as a whole and indivisible entity. Although it is technically based on the ID-One Cosmo 64 v5 Java Card platform, the system software of the said platform requires a special customization to support the Oberthur PIV firmware application. When delivered to the customer the module is already in FIPS mode with the PIV EP Applet Suite loaded and instantiated.

The hardware module complete Identification and configuration can be retrieved at any time using the Get Data services described in paragraph 6.4.1 and in the product user guide.

5 Ports and Interfaces

The integrated circuit used in the Oberthur PIV EP card is a single chip that supports both a contact and a contactless communication interfaces.

Depending on the form factor used in manufacturing, the contact interface can be either a smart card contact interface as per ISO/IEC 7816 parts 2 and 3, or a USB contact interface. In either case, the module remains a single chip cryptographic module as the management of the USB communication protocol is fully integrated into cryptographic module and does not require any external controller.

From an APDU management level, all 3 communication interfaces above use the same communication protocol, i.e. ISO/IEC 7816-3 T=1 (half duplex block oriented transmission protocols). This allows the middleware to be fully transparent to the communication ports being used.

The following sections, describe each of these interfaces.

5.1 Physical Interface for Contact Mode: ISO/IEC 7816 Parts 2 and 3

5.1.1 Interface Physical Specifications

In this contact mode, communication to and from the cryptographic module is done through a printed circuit (contact plate) that provides the electrical connection required. Five electric wires connect the module to the printed circuit, and from there, to the outside world. The printed circuit itself is outside of the module cryptographic boundaries and mentioned only for illustration purposes.

The Oberthur PIV EP card operates in both ISO 7816-3 class A and class B. Class A requires a power supply voltage between 4.5 Volt and 5.5 Volt. Class B requires a power supply voltage between 2.7 Volt and 3.3 Volt. This opens new ranges of application using lower voltage portable readers.

5.1.2 Interface Electrical Specifications

The following picture shows an example of printed circuit and the location were the five electrical connections from the module are wire bonded to the contact plate.

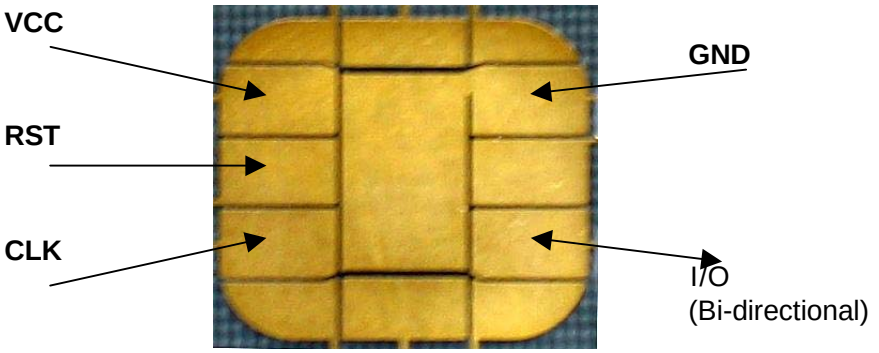

Figure 4: Example of contact plate used to provide 7816-3 electrical communications with the cryptographic module

The 5 electrical signals transmitted to the module through the contact mode wires coming from the contact plate are the following:

- **VCC**: Supply Voltage Power supply input. (1.62V to 5.5V)
- **GND**: Ground (reference voltage)
- **RST**: External reset signal from the interface device (card read / write device)
- **CLK**: External clock (1MHz to 10MHz). This clock is just for data transmission as both processor and coprocessors are driven independently by an internal oscillator at a much higher frequency.
- **I/O**: Input or output for serial data to / from the processor

These 5 electronic signals are in full compliance with ISO/IEC 7816-3 standard.

5.1.3 Transmission protocol and speed

The transmission protocol with the Oberthur PIV EP card complies with ISO/IEC 7816-3 T=1 (half duplex block oriented transmission protocols).

The Oberthur PIV EP card supports the Protocol and Parameter Selection to select a new protocol type or change transmission baud rate.

Up to 256 data bytes can be exchanged within one command.

The maximum communication speed in contact mode is 614,400 bauds (with a clock of 4.9Mhz).

5.2 Physical Interface for Contact Mode: USB

In this contact mode, communication to and from the cryptographic module is done through a Series “A” USB connector that provides the electrical connection required. Four electric wires connect the module to the connector, (two for power and two for signal) and from there, to the outside world. The connector itself is outside of the module cryptographic boundaries and mentioned only for illustration purposes.

5.2.1 Interface Electrical Specifications

Four electrical signals are wire bonded between the module and the USB type A connector to allow communication with the outside world. These are:

- **VBUS**: Supply Voltage Power supply input.
- **D-**: Signal
- **D+**: Signal
- **GND**: Ground (reference voltage)

These 4 electronic signals are in full compliance with USB standard from http://www.usb.org. Please refer to USB specifications for further details.

5.2.2 Transmission protocol and speed

The transmission protocol with the Oberthur PIV EP card complies with ISO/IEC 7816-3 T=1 (half duplex block oriented transmission protocols).

The lower level interface used in this mode is a USB 2.0 LS interface. This is a standard USB physical interface. Please refer to USB specifications for details on this interface.

5.3 Physical Interface for Contactless Mode: ISO/IEC 14443 RF Interface

5.3.1 Interface Physical Specifications

In this optional contactless mode, the cryptographic module uses only two electrical connections, LA and LB, to close the loop of an external antenna, as illustrated in the following picture. The two electrical connections LA and LB, used in contactless mode are physically different from the electrical connections used in contact mode.

The antenna is not within the cryptographic boundaries of the module.

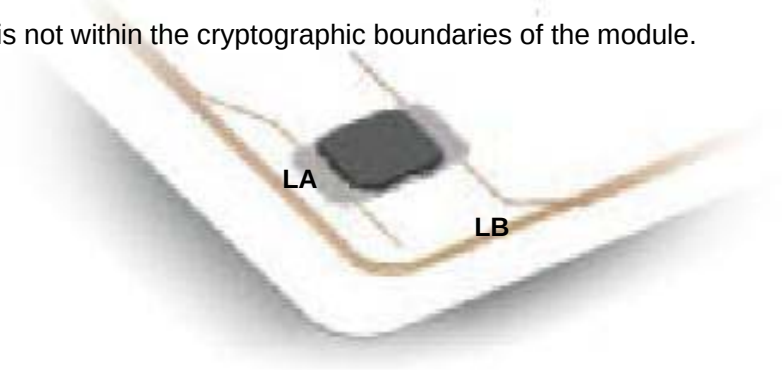

Figure 5: Example of connection of the cryptographic module to the antenna for a contactless mode

5.3.2 Interface Electrical Specifications

Power and data are transmitted to the module from the antenna using a modulation signal at 13.56 MHz.

The Proximity coupling device (reader) produces an energizing RF field that couples to the Proximity Mounted Chip Assembly (ID-One Cosmo 64 v5 module) to transfer power.

Data communication is achieved through a modulation of the energizing RF field, using amplitude shift keying (ASK) type of modulation.

The module operates independently of the external clock applied on the interfaces. The main processor and all three cryptographic co-processors (TDES and RSA) are driven independently of the external clock by an uninterrupted internal oscillator.

During contactless communications, an on-chip capacitor provides all power to the internal oscillator.

A low frequency sensor monitors the external frequency applied to the interfaces. If the frequency is out of the specified range, the chip is reset.

RF signal and Power interface are fully compliant with ISO/IEC 14443 part 2: Radio frequency power and signal interface for contactless integrated circuit cards – Proximity cards.

Initialization and anti-collision that define start of communication and card select are fully compliant with ISO/IEC 14443 part 3

A transmission protocol that defines data exchange between reader and cards are fully compliant with ISO/IEC 14443 part 4.

An anti-collision mechanism compliant with ISO/IEC 14443 is provided by the interface to insure trouble free communication with the cryptographic module, and to protect from interference due to the presence of multiple modules or readers within the communication range.

The contactless communication range of the Oberthur PIV EP card is about 10 cm.

More information on this interface can be found in the above-mentioned ISO/IEC standard.

5.3.3 Transmission protocol

Communications with the Oberthur PIV EP card in contactless mode is based on a fully standardized (ISO/IEC 14443), half-duplex transmission protocol, called T=CL. From an APDU level, this protocol is similar to the T=1 Block transmission protocol used in the contact mode.

5.4 Logical Interface Description

Once communication is established between the reader and the platform, the platform functions as a "slave" processor to implement and respond to the reader commands. The platform adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible. The I/O ports[1] of the platform (either physical in contact mode or virtual in the case of RF transmission) provide the following logical interfaces:

Logical Interface	**Contact Mode (ISO 7816)**	**Contact Mode (USB)**	**Contactless Mode (ISO 14443)**
Data Input:	I/O Pin	D+ and D-	LA and LB
Data Output:	I/O Pin	D+ and D-	LA and LB
Status Output:	I/O Pin	D+ and D-	LA and LB
Control Input:	I/O, Clk and Reset Pins	D+ and D-	LA and LB
Power Input	VCC and GND	VBUS and GND	LA and LB

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

[1] Two ports due to contact and contactless mode of communications.

6 Roles & Services

6.1 Roles

The Oberthur PIV EP defines three distinct roles that are supported by the internal cryptographic system: the Card Security Controller (CSC), The Application Administrator (ADM) and the Card Holder (CH).

6.1.1 Cryptographic Officer Role

- ***Card Security Controller (CSC) Role***: This role is responsible for managing the security configuration of the card manager and security domains. The CSC role authenticates to the cryptographic module by demonstrating to the Card Manager application that he possesses the knowledge of a Global Platform (GP) secure channel TDES key set stored within the Security Domain. By successfully executing the OP secure channel mutual authentication protocol, the CSC role establishes a secure channel to the Security Domain and executes services allowed to the CSC role in a secure manner.

6.1.2 User Roles

- ***Application Administrator (ADM) Role*** – The Application Administrator role represents an external application requesting the administrative services offered by the applets. An applet authenticates the Application Administrator role by verifying possession of the Application Administrator key.
- ***Card Holder (CH) Role*** - 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 his PIN or Pin Unblocking PIN.

6.2 Identification

The Oberthur PIV EP performs identity-based authentication using PIN and cryptographic keys. A unique index value is associated with the PIN or the cryptographic key to uniquely identify the off-card entity performing the authentication.

6.3 Authentication

The Oberthur PIV EP cryptographic module supports identity based role authentication using the following scheme.

6.3.1 User Role Authentication

6.3.1.1 Card Holder

The Card Holder role is authenticated with a PIN: The Card Holder role must send a Verify CHV APDU to the module to access services protected with PIN access control rules.

The authentication remains valid until one of the following happens:

1. Another application is selected on the same logical channel (except if the authentication was done with the Global PIN).
2. A new authentication attempt with a failed result.
3. The module is powered-off, receives a reset command, or is removed from the reader.

Authentication of the Card Holder can be performed only through the contact interface

6.3.1.2 Application Administrator

The Application Administrator role is authenticated by the possession of the Application Administrator Key. This is done through either an External Authentication or a Mutual Authentication using the GENERAL AUTHENTICATE command from ISO 7816-4. A successful authentication unlocks the administrative rights until one of the following happens:

1. Another application is selected on the same logical channel.
2. A new authentication attempt with a failed result.
3. The module is powered-off, receives a reset command, or is removed from the reader.

Authentication of the Application Administrator can be performed only through the contact interface.

6.3.2 Cryptographic Officer Role Authentication

6.3.2.1 Card Security Controller

The Card Security Controller authenticates himself using a mutual authentication comprising two commands: INITIALIZE UPDATE immediately followed by EXTERNAL AUTHENTICATE. During this mutual authentication the Card Security Controller has to encrypt a random message sent by the card, proving knowledge of the TDES key set that was referenced during the identification.

The authentication remains valid until one of the following happens:

1. Another application is selected on the same logical channel.
2. The module is powered-off, receives a reset command, or is removed from the reader.

6.4 Services

6.4.1 Card Security Controller Services

Several services are made available to an authenticated Cryptographic Officer only. They are primarily used to manage Security Domains and allow the creation of additional application (applet instances of already FIPS approved executable byte code present in the card) and to load encrypted cryptographic keys into the newly created applications.

- ***INSTALL:*** this APDU is used to add an application from an executable byte code already present in the module.
- ***LOAD:*** this APDU is used to load the byte-code of a new application. For the module to remains in FIPS mode, this command shall not be used to load non FIPS approved executable code.

- ***DELETE:*** this APDU is used by the CSC role to delete an application from the cryptographic module. Load File (package) or an applet (applet instance).
- ***PUT TDES KEY:*** this APDU is used to add or replace security domain key sets (TDES). Keys are loaded protected by the double encryption of the global Platform Secure Channel and a KCV is included in the transmission to ensure integrity of the key loading operation.
- ***PUT PUBLIC KEY***: this APDU is used 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.
- **PUT PIV_TDES KEY**: This command is used to load cryptographic keys (TDES128 ECB and CBC, TDES192 ECB and CBC) into the selected instance of the PIV applet. Keys are loaded protected by the encryption (TDES) and integrity verification (TDES MAC) of the Global Platform Secure Channel. This command is also used to set or reset the optional usage counter associated to a given key.
- **PUT PIV_RSA KEY_PAIR**: This command is used to load RSA Key Pairs (1024 and/or 2048) into the selected instance of the PIV applet. Keys are loaded protected by the encryption and integrity verification of the Global Platform Secure Channel. Private (CRT) and public parts of the key are transmitted together and the module checks the success of the key loading by performing a pairwise consistency check on the newly loaded key pair. This command is also used to set or reset the optional usage counter associated to a given key.
- **PUT DATA**: This command is used by the CSC to clear the audit log and load Data Objects at the platform level.
- **GET DATA**: The GET DATA command is used to retrieve a non protected data object available from the selected application. Example of data retrievable by the CSC using get Data includes Identification Data, configuration data, Issuer Identification Number, Card Image number, Audit log, and a few other described in the module programmer's guide.
- ***SET STATUS***: This APDU is used by the CSC to temporary lock an application, and unlock it later on. It can also be used to terminate the crypto module.
- ***GET STATUS:*** this APDU is used to get the life cycle state of the cryptographic module or the life cycle state of an application. It can also be used by the CSC to verify that the module is still in FIPS Mode and that only FIPS approved applications are instantiated.
- ***INITIALIZE UPDATE***: this APDU is used by the CSC to exchange with the crypto module data needed to establish the session keys and initiate a GP Secure Channel with a given Security Domain in the crypto module.
- ***EXTERNAL AUTHENTICATE***: this APDU is used by the CSC to authenticate to the crypto module and to finalize the establishment of the GP Secure Channel by providing the level of security required for all subsequent commands within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.
- ***DELEGATE MANAGEMENT***: Delegated Management gives a CSC the possibility of empowering another CSC the ability to initiate approved and pre-authorized Card Content changes (loading, installation, extradition or deletion) on his behalf.
- **CREATE FILE**: This command is used to create a new binary file to be used as a scratch pad to store non-security relevant data. It is only authorized during personalization. The size of the binary file is set during creation and cannot be modified afterwards.
- **All Services under "No Role"**

6.4.2 Application Administrator Services

The following services (commands) are made available to an authenticated Application Administrator:

- **GENERAL AUTHENTICATE (Internal):** This ISO 7816-4 smart card command is used to authenticate the crypto module (Internal Authenticate) using a challenge response mechanism if a symmetric key is used, or a signature process if an asymmetric key is used. The Host generates a challenge that is encrypted/signed by the module and returned to the Host for verification.
- **GENERAL AUTHENTICATE (External)**: This ISO 7816-4 smart card command is used to authenticate the Application Administrator to the crypto module (External Authenticate) using a challenge response mechanism. The module generates and outputs a challenge that is TDES encrypted by the Host and returned to the module for verification.
- **GENERAL AUTHENTICATE (Mutual):** This ISO 7816-4 smart card command is used to perform a mutual authentication between the Application administrator and the crypto module, where the command is used for both sides to identify each other simultaneously. This process is functionally equivalent to performing both a General Authenticate (Internal) and a General Authenticate (External) at the same time.
- **PUT DATA**: This command is used to store or update the value of a Data Object within the application, including X509 certificate. It can also be used by the application administrator to temporary disable any contactless communication with the application. This prevents the application from leaking personal data without the cardholder knowledge when located in an unsecured area. Only Data Objects with access control rules set to “Administrative rights” for update can be updated.
- **GENERATE ASYMMETRIC KEYPAIR:** This command initiates the generation of an asymmetric cryptographic key pair by the security module and its secure storage within the module itself. A double pairwise consistency check (Sign/Verify and Encrypt/Decrypt) is automatically performed by the module to validate the generated key pair. Only the public value of the key pair is made available to the outside world.
- **GET DATA**: This command is used to retrieve a single data object from the selected application. Some data objects are available only to the Application Administrator and require previous authentication. Data objects that can be retrieved by the Application Administrator include PIV data objects specified in NIST Special Publication 800-73-1 for the PIV application as well as additional proprietary data objects. Please refer to Oberthur PIV EP programmer’s guide for further details.
- **All Services under “No Role”**

6.4.3 Card Holder Services

- **VERIFY PIN**: This command checks the PIN presented by the Card Holder against the current PIN associated with the selected application, or associated with the Card PIN applet instance (Card Global PIN). It is used to authenticate the card Holder.
- **PUT DATA**: This command is used to store or update the value of a Data Object within the application. Only Data Objects with access control rules set to “Card Holder rights” for update can be updated.
- **GET DATA**: This command is used to retrieve a single data object from the selected application. Some data objects are available only to the Card Holder and require previous PIN verification. Data objects that can be retrieved by the cardholder include PIV data objects specified in NIST Special Publication 800-73-1 for the PIV application as well as additional proprietary data objects. Please refer to Oberthur PIV EP programmer’s guide for further details.

- **GENERAL AUTHENTICATE (Internal):** This ISO 7816-4 smart card command is used to authenticate the crypto module (Internal Authenticate) using a challenge response mechanism if a symmetric key is used, or a signature process if an asymmetric key is used. The Host generates a challenge/SHA-based hash that is encrypted/signed by the module and returned to the Host for verification.
- **CHANGE REFERENCE DATA:** This command is used to verify the Card Holder PIN and replace it with a new value if the verification succeeds.
- **RESET RETRY COUNTER:** The VERIFY PIN instruction is automatically disabled for an application after a predefined number of consecutive failed verification is reached. (That predefined number is set by the crypto officer during applet instantiation with a value between 1 and 15.) The RESET RETRY COUNTER allows unlocking the VERIFY PIN command for the selected application, resetting its associated Retry Counter to its initial value, and replaces the value of the current PIN. The RESET RETRY COUNTER required the cardholder to authenticate himself using the PIN Unblocking PIN (or Card Global PIN Unblocking PIN if the Retry counter to reset is the Card Global PIN retry counter).
- **GET DATA**: The GET DATA command is used to retrieve a non protected or PIN protected data object available from the selected application.
- **All Services under "No Role"**

6.4.4 No Role

The following services are available without authentication

- **PUT DATA**: This command is used to store or update the value of a Data Object within the application. Only Data Objects with access control rules set to "Always" for update can be updated.
- **GET DATA**: The GET DATA command is used to retrieve a non protected data object available from the selected application.
- **SELECT**: This command is used for selecting an application (Card Manager, Security Domain or Applet Instance). The Card Manager may be selected either for the loading of an application executable code (Load File) or for activating an application by instantiation of its previously loaded executable code.
- **GET RESPONSE:** This command is used to retrieve the remaining data that the card wanted to respond with but could not fit in the response buffer of the initial command.
- **GENERAL AUTHENTICATE (Internal):** This ISO 7816-4 smart card command is used to authenticate the crypto module (Internal Authenticate) using a challenge response mechanism if a symmetric key is used, or a signature process if an asymmetric key is used. The Host generates a challenge that is encrypted/signed by the module and returned to the Host for verification.
- **READ BINARY**: This command is used to read the content of the above created scratch pad. It is not subject to any Access Control Rule (Free Access) but it does not allow access to module CSP or PIV data objects.
- **UPDATE BINARY**: This command is used to update the content of the above-created scratch pad. It is not subject to any Access Control Rule (Free Access) but it does not allow access to module CSP or PIV data objects.

6.4.5 Relationship between Roles and Services

Roles/Services	Card Security Controller	Application Administrator	Card Holder	Un-authenticated (No Role)	CSP[2]	Type of Access to CSP
INSTALL	X					
LOAD	X					
DELETE	X					
PUT TDES KEY	X				CM/ Security Domain key set	Write
PUT PIV_TDES KEY	X (see note)	X (see note)			9B, A0, A1, A2, B0, B1,B2	Write
PUT PIV_RSA_KEY_PAIR	X (see note)	X (see note)			9D, 9E D0, D1, D2	Write
PUT PUBLIC KEY	X				$\mathbf{K}_{TOKEN,}$ $\mathbf{K}_{DA,}$	Write
GET STATUS	X					
INITIALIZE UPDATE	X					
EXTERNAL AUTHENTICATE	X				K_{ENC} K_{MAC} K_{KEK}	Execute
DELEGATE MANAGEMENT	X				$\mathbf{K}_{TOKEN,}$ $\mathbf{K}_{DA,}$	Execute
SET STATUS	X					
GENERAL AUTHENTICATE (Internal)			X		9A, 9C, 9D, 9E, A0, A1, A2, B0, B1, B2 D0, D1, D2	Execute
	X	X		X	9E, A0, A1, A2,	
GENERAL AUTHENTICATE (External)		X			9B	Execute

[2] See Section 7.4 Critical Security Parameters: for further CSP pointer details.

Roles/Services	Card Security Controller	Application Administrator	Card Holder	Un-authenticated (No Role)	CSP[2]	Type of Access to CSP
GENERAL AUTHENTICATE (Mutual)		X			9B	Execute
PUT DATA	X	X	X	X		
GENERATE ASSYMMETRIC KEY PAIR		X			9A, 9C, 9D, 9E, D0, D1, D2	Read (Public Key only)
VERIFY PIN			X		App. PIN, Global PIN	Execute
GET DATA	X	X	X	X		
SELECT	X	X	X	X		
GET RESPONSE	X	X	X	X		
CHANGE REFERENCE DATA			X		App. PIN, Global PIN, App. PUP, Global PUP	Execute & Write
RESET RETRY COUNTER			X		App. PUP, Global PUP	Execute & Write
CREATE FILE	X					Write
READ BINARY	X	X	X	X		Read
UPDATE BINARY	X	X	X	X		Write

Note on PUT_PIV_TDES_KEY and PUT_PIV_RSA_KEY_PAIR: Key loading must always be done under the combined authentication of the Cryptographic Officer and the Application Administrator. The Application administrator successful authentication unlocks the updatability of the application data elements and the Cryptographic Officer authentication provides the secure channel required to provide encrypted transport of the key from the external HSM to the PIV EP card.

7 Module Cryptographic Functions

The purpose of the Oberthur PIV EP card is to provide a FIPS approved platform that in turn, provides cryptographic services to end-user applications. The key ID identifies the role involved in controlling the cryptographic module, and the key value authenticates operators into their roles. A variety of FIPS 140-2 validated algorithms are used in the Oberthur PIV EP v1 on ID-One Cosmo 64 v5 D to provide cryptographic services.

7.1 Cryptographic algorithms, mode and key length

These include:

- TDES128, (2 keys TDES CBC/ECB)
- TDES192, (3 keys TDES CBC/ECB)
- SHA-1
- RSA PKCS#1 v2.1 (RSA-PSS (SigGen and SigVer) and RSA PKCS #1 v1.5 (SigGen)) (1024 and 2048 bit keys)
- DRNG

The TDES128 (CBC mode) algorithm is used to authenticate the CSC (EXTERNAL AUTH command) and to encrypt data flow from the external application to the cryptographic module environment. The reverse direction is not encrypted (i.e. the status words returned in response to an APDU are not encrypted).
The TDES192 and TDES128 are also used for mutual authentications.
The RSA key is used to authenticate the application and to perform electronic signature.

7.2 Random Number Generators

The cryptographic module offers the services of a FIPS 140-2 approved DRNG (Deterministic Random Number Generator). The random number generation algorithm is compliant with the FIPS PUB 186-2 standard. More precisely, the method used is “Constructing the function G from the DES,” taken from the FIPS 186-2 appendix 3, section 3.4.

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

7.3 Self Tests

7.3.1 Power Up Self Tests

Each time the Oberthur PIV EP card 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 to the reset signal with an Answer To Reset (ATR) packet of information as specified by ISO/IEC 7816 (for contact mode) or with an Answer To Select (ATS) as defined in ISO/IEC 14443 for contactless mode.

The Power-up self-tests include:

- EEPROM integrity check using CRC16 algorithm for:
  - System Data
  - Optional codes (firmware extensions), if any
  - Uploaded application packages (Executable Load files), if any
- Cryptographic Known Answer Tests for
  - DES – Encryption and decryption in ECB mode
  - Triple DES – Encryption and decryption in CBC mode
  - SHA Hashing
  - RSA signature generation and signature verification
  - RSA encryption and decryption
  - Deterministic Random Number Generator (DRNG)
- Critical Function Tests
  - CRC-16 KAT
  - RAM functional test
  - Sensor bit test
  - Audit log scan
  - Resident applet life cycle

Additional tests to protect against new types of attacks such as SPA, DPA, “flash gun”, etc, are also performed at this stage.

No data of any type (except error status) is transmitted from the cryptographic module to the reading device while the self-tests are being performed.

If any of the above tests fail, the card will enter an error state in which further APDU’s are not processed. Depending on the test that fails, the module may return the ATR/ATS with an error status before becoming mute.

More details about all the power-up self-tests and their implementation are provided in a separate confidential document.

7.3.2 Conditional Tests

RSA Key generation: After generating an RSA key pair, the module performs a double pair wise consistency check to validate that the generated key pair is correct for both signature/verification and encryption/decryption. Description of the implementation of this test is provided in a separate document.

Random Number Generators: Continuous testing is performed on every output of the Random Number Generators. Checks on the non-deterministic (Hardware) component are made on 16 bits and checks on deterministic part (FIPS approved) are made on 160 bits. Description of the implementation of this test is provided in a separate document.

Credentials: Keys and PINs: Each time a credential is used, whether a TDES, or RSA key or a PIN, its integrity is checked by an EDC. Description of the implementation of these checks is provided in a separate document.

Software (Applet) load tests: A TDES128 CBC MAC on the applet executable load file is verified each time an applet is loaded onto the cryptographic module since applet loading always takes place within a Secure Channel. An optional DAP verification can also made. The algorithm used is RSA1024 signature verification.

If TDES MAC or DAP verification fails, the package load is terminated and the module built-in garbage collector cleans the EEPROM of any traces of the aborted download.

Description of the implementation of this test is provided in Global Platform 2.1.1 Specifications.

7.3.3 Key Load Tests:

- **Symmetrical Keys** (TDES) are transmitted encrypted together with a KCV (Key Check Value) that is checked by the module to verify correct decryption of the key. The KCV is the first 3 bytes of the cryptogram generated when encrypting 8 bytes of '00' with the symmetrical key.

- **Asymmetrical Keys** (RSA) are transmitted encrypted as key pairs, with both private (CRT) and public components. The KCV value is replaced by a pair wise consistency check performed by the module to verify integrity of the decrypted key.

7.4 Critical Security Parameters:

- **Initialization key set K_{init}**: used to secure the card during its transportation from the manufacturer site to the issuance site. This TDES128 key set is generated outside of the cryptographic module and then loaded into the card manager security domain during the card manufacturing and initialization process.
- **CSC Card Manager / Security Domain key set:**
  - K_{ENC}: used to generate session keys for the encrypted mode of the secure channel
  - K_{MAC}: used to generate session keys for CSC authentication and MAC mode of the secure channel. This key is used to authenticate the CSC to the card
  - K_{KEK}: used to wrap keys to be loaded onto the cryptographic module

  This TDES128 key set is generated outside of the cryptographic module in an HSM, and then loaded protected with a Global Platform secure channel using the key set that already exists in the card manager security domain (for example, K_{init}).
- **PIV Authentication Key (9A)**: RSA (1024 or 2048) key pair that enables the outside world to authenticate the Oberthur PIV EP card (or token) as a genuine PIV card (or token). This key is generated by the module itself during application personalization. This key is available only to the Card Holder Role and is used by the General Authenticate command to perform external authentication. This key is protected by an optional usage counter that can be set by the Crypto Officer during personalization up to 65537 and can be reset at any time by a combined authentication of the Cryptographic Officer and the Application Administrator.
- **PIV Card Administrator Key (9B):** TDES192 key or TDES128 that enables the authentication of an application administrator. This key is generated outside of the cryptographic module in an HSM, and then loaded protected with the double encryption of a Global Platform secure channel using K_{enc} and K_{kek} of the CSC Card Manager / Security Domain key set via the PUT_TDES_KEY command. This key can only be used by the General Authenticate command and is the only key that can authenticate the Application Administrator Role. This key is protected by an optional usage counter that can be set by the Crypto Officer during personalization up to 65537 and can be reset at any time by a combined authentication of the Cryptographic Officer and the Application Administrator.
- **PIV Digital Signature Key (9C)**: RSA (1024 or 2048) key pair that is used by the card Holder to sign the hash of a message. This key is generated by the module itself during activation. This key is used by the General Authenticate command to generate a signature on an externally generated/input SHA-based hash of a message. This key is protected by an optional usage counter

that can be set by the Crypto Officer during personalization up to 65537 and can be reset at any time by a combined authentication of the Cryptographic Officer and the Application Administrator.

- **PIV Management Key (9D)**: RSA (1024 or 2048) key pair that is used to provide additional management services to a FIPS 201 application. This key is generated outside of the cryptographic module in an HSM, and then loaded protected with the double encryption of a Global Platform secure channel using K_{ENC} and K_{KEK} of the CSC Card Manager / Security Domain key set via the PUT_RSA_KEY_PAIR command. This key is used by the General Authenticate command to authenticate the PIV application to an external Card Management System. This key is protected by an optional usage counter that can be set by the Crypto Officer during personalization up to 65537 and can be reset at any time by a combined authentication of the Cryptographic Officer and the Application Administrator.
- **PIV Card Authentication Key (9E)**: TDES192 key or TDES128 or RSA (1024 or 2048) key pair that enables the outside world to authenticate the Oberthur PIV EP card (or token) over the contact or contactless interface and without requiring prior PIN verification. This key is generated by the module itself during application personalization or is generated outside of the cryptographic module in an HSM, and then loaded protected with the double encryption of a Global Platform secure channel using K_{ENC} and K_{KEK} of the CSC Card Manager / Security Domain key set via respectively the PUT_TDES_KEY command or the PUT_RSA_KEY_PAIR command. This key can only be used by the General Authenticate command to perform external authentication. This key is protected by an optional usage counter that can be set by the Crypto Officer during personalization up to 65537 and can be reset at any time by a combined authentication of the Cryptographic Officer and the Application Administrator.
- **Additional TDES Keys**: Each instance of the application can contain up to 6 additional TDES keys **(A0 through A2 and B0 through B2)** for each of the 4 TDES algorithms (TDES128 ECB, TDES128 CBC, TDES192 ECB, TDES192 CBC). These keys are not used to authenticate into the module but provide cryptographic services to authenticate the card to the back end system. These keys can only be used by the General Authenticate command. This key is protected by an optional usage counter that can be set by the Crypto Officer during personalization up to 65537 and can be reset at any time by a combined authentication of the Cryptographic Officer and the Application Administrator.
- **Additional RSA Keys**: Each instance of the application can contain up to 6 additional RSA key pair (3 of 1024 and 3 of 2048 bits) named **D0 through D2** that can be used to provide additional authentication services with non-PIV application. The keys are protected by the PIN and are generated by the module itself or outside of the cryptographic module in an HSM, and then loaded protected with the double encryption of a Global Platform secure channel using K_{enc} and K_{kek} of the CSC Card Manager / Security Domain key set. These keys are not used to authenticate into the module but provide cryptographic services to authenticate the card to the back end system or provide additional signature functionalities. These keys can only be used by the General Authenticate command. This key is protected by an optional usage counter that can be set by the Crypto Officer during personalization up to 65537 and can be reset at any time by a combined authentication of the Cryptographic Officer and the Application Administrator.
- **PIV Application PIN** used for Card Holder Authentication. The initial PIN is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set, via the CHANGE REFERENCE DATA Command and can be changed later by the Card Holder after a successful user authentication event, using the same command.
- **PIV PIN Unblocking PIN (PUP)** used for Card Holder Authentication during the RESET RETRY COUNTER Command. The initial value is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set, via the CHANGE REFERENCE DATA Command and can be changed later by the user after a successful Card Holder authentication event, using the same command.

- **Card Global PIN** used for Card Holder Authentication. The initial PIN is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set, via the CHANGE REFERENCE DATA Command and can be changed later by the Card Holder after a successful user authentication event, using the same command.
- **Card Global PIN Unblocking PIN** used for Card Holder Authentication during the RESET RETRY COUNTER Command. The initial value is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set, via the CHANGE REFERENCE DATA Command and can be changed later by the user after a successful Card Holder authentication event, using the same command.

7.5 Public Keys

- K_{TOKEN}: Key Token: Public RSA Key (1024 bits) used to verify the tokens included in Delegated Management commands that embed the signature of these commands. 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.
- K_{DAP}: Key DAP: Public RSA Key (1024 bits) used to verify the DAP on an application code to be loaded into the Oberthur ID-One Cosmo 72K RSA D chip platform and authorize or not its loading. (See section 7.2.3 on DAP verification). 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.
- **Public components of key 9A.** Output automatically at the completion of the Generate Asymmetric key pair command if internally generated or input through the Put RSA_Key_Pair command.
- **Public components of key 9C.** Output automatically at the completion of the Generate Asymmetric key pair command if internally generated or input through the Put RSA_Key_Pair command.
- **Public components of key 9D.** Output automatically at the completion of the Generate Asymmetric key pair command if internally generated or input through the Put RSA_Key_Pair command.
- **Public components of key 9E.** Output automatically at the completion of the Generate Asymmetric key pair command if internally generated or input through the Put RSA_Key_Pair command.
- **Public components of key D0.** Output automatically at the completion of the Generate Asymmetric key pair command if internally generated or input through the Put RSA_Key_Pair command.
- **Public components of key D1.** Output automatically at the completion of the Generate Assymmetric key pair command if internally generated or input through the Put RSA_Key_Pair command.
- **Public components of key D2.** Output automatically at the completion of the Generate Assymmetric key pair command if internally generated or input through the Put RSA_Key_Pair command.

8 Physical Security

The Oberthur PIV EP card is a single chip cryptographic module. It is designed to meet FIPS 140-2 Level 3 requirements for physical security.

The module is a production quality IC. It meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. It uses standard passivation techniques for the entire chip.

In addition to the passivation material, a hard, opaque epoxy, that is resistant to commonly available solvents, is used to encapsulate the module into an opaque support.

The chip is usually in possession of either a Cryptographic Officer (CSC) or of the User (Card Holder).

In order to physically attack the module, an attacker will have to take possession of the module and use extraordinary means such as electronic probe or electronic microscope.

As the chip module is covered with a hard, tamper-evident resin, that resin must be removed to attempt any physical attack on the chip.

In this event, the absence of the chip is easily detected by its owner. Once the chip has been attacked through extraordinarily physical means, the attack leaves permanent evidence and is consequently detected by the owner.

In addition to the above passivation material, the following active features available in the module provide increased protection against physical attacks:

- Low / high supply voltage sensor
- Low / high clock frequency sensor
- Low / high temperature sensor
- Light sensor
- Single fault injection (SFI) attack detection
- Programmable “Card Disable” feature

9 EMI/EMC

The cryptographic module meets the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements specified by United States Standards 47 CFR Part 15, Subpart B: “Unintentional Radiators, Digital Devices, Class B”.

It is also in compliance with the electromagnetic compatibility requirements defined in European Standard EN 55022, Class B: “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment.”

10 Security Rules

10.1 Approved mode of Operation

When the PIV EP module leaves Oberthur factory it is already in FIPS mode and the PIV application already initialized with the PIV application instantiated and in personalized state. To maintain the module in approved mode of operation, the operator must restrict usage of the module as follows:

- The cryptographic Officer shall not instantiate any additional applets that are not validated to FIPS 140-2.
- Key loading must always be done under the combine authentication of the Cryptographic Officer and the Application Administrator. The Application administrator successful authentication unlocks the updatability of the application data elements and the Cryptographic Officer authentication provides the secure channel required to provide encrypted transport of the key from the external HSM to the PIV EP card.
- Key loading and usage shall comply with the restriction specified in sections 6.4.5 Relationship between Roles and Services and 7.4 Critical Security Parameters:
- All PIV Application instances must be in a personalized state, per the requirements in this Security Policy.
- The module follows all security rules outlined in section 12 Security Policy Check List Tables to remain in FIPS mode.

10.2 Identification & Authentication Security Rules

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of the binding of an Identity-based Access Control Rule to each service. The ID is used to identify the roles, operators, and the PINs and keys are used to authenticate those operators into their roles.

The operator who wishes to authenticate into a given role must first identify him/herself by providing a Key (or PIN) ID. The authentication is then done by proving the possession of the particular keyset (or PIN) identified in the identification phase.

- The PIN or the Global PIN ID represents the identity of the Card Holder role.
- The Application Administrator Key ID represents the identity of the Application Administrator role.
- The Key set ID of the Security Domain associated to the application represents the identity of the Cryptographic Security Controller role.

10.3 Applet Life Cycle Security Rules

As mentioned before the Oberthur PIV EP applet is always loaded during card manufacturing. However the Oberthur PIV EP module permits loading of additional applet but only applets validated to FIPS140-2. The following security rule applies to such additional applets.
Applets can only be loaded through a GP secure channel (i.e. they pass from the external application to the cryptographic module in an encrypted and MACed form).

- The Card Holder must take the necessary measures to ensure that the terminal and/or Card Acceptance Device are controlled by a valid role; Card Holder, Application Administrator or CSC.
- Management of applet life cycles (load, install, delete, personalize keys), follows the Global platform standard.
- Applet and key APDU command management (i.e. download, install, delete, put key) are protected by secure channel MAC (TDES-CBC). Their origin is authenticated, and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post-issuance.
- The download of validated applet packages, and the installation of applet instances, may occur either at pre-issuance, issuance or post-issuance.
- There may be as many instances of each applet as there are cryptographic module resources available.

10.4 Access Control Security Rules

- Keys must be loaded through a GP secure channel. Consequently, keys are always loaded in the encrypted and MACed form.
- The password or PIN that is used by the applet to authenticate the Card Holder must not be divulged to parties other than the Card Holder.
- Each instance of the application must be configured by the cryptographic officer so that:
    - After 1 <= N <= 15 consecutive unsuccessful PIN/PIN-Unblocking-PIN code validation attempts, the Card Holder services must be disabled. (e.g. the PIN is blocked)
    - The PIN length L verifies the following rules:
        - The card does not enforce any specific format for PIN, PIN-Unblocking-PIN, Global PIN and Global PIN Unblocking PIN.
        - PIV Application PIN and PIV PIN Unblocking PIN are both checked as binary strings of 8 Bytes each.

Global PIN and Global PIN Unblocking PIN are both checked as binary strings of 8 to 127 Bytes each. The length of the Global PIN and Global PIN Unblocking PIN are set during card personalization.

10.5 Key Management Security Policy

10.5.1 Cryptographic key generation

TDES Session key generation for Secure Channel Opening, conforming to Open Platform Card Specification v2.1.1 (SCP01) using FIPS186-2 approved ANSI X9.31 DRNG.

PKCS v1.5 compliant RSA key pair generations (1024 and 2048 bit key length) with strong prime numbers (ANSI X9.31) using FIPS140-2 approved DRNG.

10.5.2 Cryptographic key entry and output

Symmetrical Keys shall always be input in wrapped format, using the PUT TDES KEY command within a GP secure channel. During this process, the keys are double wrapped (using the Session Key and the K_{KEK} Key).

Symmetrical keys (TDES) are transmitted encrypted together with a KCV (Key Check Value) that is checked by the module to verify correct decryption of the key.

Asymmetrical Keys shall always be input in wrapped format, using the PUT RSA KEY_PAIR command within a GP secure channel. During this process, all key pair components are double wrapped (using the Session Key and the K_{KEK} Key).

Asymmetrical Keys (RSA) are transmitted encrypted as key pairs, with both private (CRT) and public components. The KCV value is replaced by a pair wise consistency check performed by the module to verify integrity of the decrypted key.

Keys can never be output by the module (except the public part of a newly generated RSA key).

The strength of the key loading mechanism is 80 bits.

10.5.3 Cryptographic key storage

The Keys are structured to contain the following parameters:

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

The cryptographic key storage integrity mechanism is described in a separate confidential document called Self Test Description.

10.5.4 Destruction of Keys & PINs

The Oberthur PIV EP destroys cryptographic keys/PINs by reloading another key-set/PIN with an all zero value.

RSA Key Pairs can also be zeroized independently without replacing the old value with a new one. This is done with the PUT PIV RSA KEY_PAIR command using a special parameter. This offers the additional benefit of freeing up the EEPROM memory that was previously used to store the RSA Key Pair.

Keys and PINs can also be zeroized by deleting the Security Domain or applet instance that hosts them, using the **DELETE** command.

Closing of the secure channel has also the effect of zeroizing the associated session keys stored in RAM memory.

11 Mitigation of Other Attacks Policy

11.1 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 PIV EP card 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.

11.2 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.

11.3 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 PIV EP card 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 7.3.2 Conditional Tests

11.4 Flash Gun

The Oberthur PIV EP card 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.

12 Security Policy Check List Tables

12.1 Roles and required Identification and Authentication

Role	Type of Authentication	Authentication Data
Card Security Controller	TDES Authentication	TDES128 Keys (Card Security Controller Security Domain)
Application Administrator	TDES Authentication	TDES192 or TDES128 Administrator Key
Card Holder	Verify PIN	PIN

12.2 Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
TDES Authentication	2^{80}
Application PIN	2^{64}
Application PIN-UNBLOCKING-PIN	2^{64}
Card Global PIN	2^{64} to 2^{80}
Card Global PIN-UNBLOCKING-PIN	2^{64} to 2^{80}

12.3 Services Authorized for Roles

Role	Authorized Services
Card Security Controller	The Card Security Controller role services are listed in section 6.4.1
Application Administrator	The Application Administrator role services are listed in section 6.4.2
Card Holder	The Card Holder role services are listed in section 6.4.3

12.4 Access Right within Services

Service	CSP	Type of Access (i.e. Read; Write, Execute)
Crypto Officer (Card Security Controller) Service	OP Secure Channel with TDES key set	Execute (Encrypt), Write (Put Key)
Application Administrator Service	General Authenticate	Execute (Encrypt, Decrypt), Write (Put Data)

Card Holder Service	TDES Key Encryption (during key loading)	Execute (Verify PIN), Write (Change Reference Data); Read (Get Data)

12.5 Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A
Timing Analysis	Counter Measures against TA	N/A
Fault Induction	Counter Measures against FI	N/A
Flash Gun	Counter Measures against FG	N/A

13 Applicable Documents

- Open Platform Card Specification - Version 2.1.1 – Mars 2003, Global Platform
- Open Platform Card Specification - Version 2.1.1 Amendment A – February 2004, Global Platform
- Java Card™ 2.2 Virtual Machine Specification – June 2002, Sun Microsystems
- Java Card ™ 2.2 Application Programming Interface – revision 1.1- September 2002, Sun Microsystems
- Java Card™ 2.2 Runtime Environment Specification - June 2002, Sun Microsystems
- Global Platform 2.1 Card Implementation Requirements –May 2002, Visa International
- Visa Open Platform Card Implementation Requirements Configuration 3 – Multiple Security Domains with DAP Capability October 2001
- Visa Open Platform Card Implementation Requirements Configuration 3 – Multiple Security Domains with DAP Capability Version 2 – Errata February 2002
- [FIPS140-2] National Institute of Standards and Technology, FIPS 140 -2 standard.
- [FIPS140-2A] National Institute of Standards and Technology, FIPS 140 -2 Annex A: Approved Security Functions.
- [FIPS140-2B] National Institute of Standards and Technology, FIPS 140 -2 Annex B: Approved Protection Profiles,
- [FIPS140-2C] National Institute of Standards and Technology, FIPS 140 -2 Annex C: Approved Random Number Generators
- [FIPS140-2D] National Institute of Standards and Technology, FIPS 140 -2 Annex D: Approved Key Establishment Techniques
- [DES] National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publication 46-3, October 25, 1999.
- [DES Modes] National Institute of Standards and Technology, DES Modes of Operation, Federal Information Processing Standards Publication 81, December 2, 1980.
- JC2.2 API SRS revision issuee1-AC, Oberthur Card Systems
- Basic Input/Output System (BIOS) SRS, revision 1-AA, Oberthur Card Systems
- Java Card Virtual Machine V2.2 SRS, revision 1-AB, Oberthur Card Systems
- "Integrated circuit(s) cards with contacts - Part 2 Dimension and Location of the contacts." ISO/IEC 7816-2 (1999)
- "Integrated circuit(s) cards with contacts - Part 3 Electronic signal and transmission protocols." ISO/IEC 7816-3 (1997), ISO/IEC 7816-3 AMD1 (2002)
- "Integrated circuit(s) cards with contacts - Part 4: Inter industry commands for interchange." ISO/IEC 7816-4 (1995), ISO/IEC 7816-4 AMD1 (1997)
- "Numbering system and registration procedure for application identifiers" ISO/IEC 7816-5 (1994), ISO/IEC 7816-5 AMD1 (1996)
- “Information technology – Security techniques – Digital signature scheme giving message recovery - Part 2: Mechanism using a hash function.” ISO/IEC 9796-2 (1997)

- "Information technology – Security techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher" ISO/IEC 9797-1 (1999)
- Contactless integrated circuit(s) cards – Proximity cards — Part 2: Part 2: Radio frequency power and signal interface, ISO/IEC 14443-2 (2001)
- Contactless integrated circuit(s) cards – Proximity cards — Part 3: Initialization and anti-collision, ISO/IEC 14443-3 (2001)
- Contactless integrated circuit(s) cards – Proximity cards — Part 4: Part 4: Transmission protocol, ISO/IEC 14443-4 (2001)
- "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)
- "API File System Library" Ref: 055731 00 SRS revision-issue 1-AA, Oberthur Card Systems
- "API Utils File System" Ref: 055901 00 SRS revision-issue 1-AA, Oberthur Card Systems
- "Java Card 2.2 Biometry API proposal" Javadoc version (4-4-02) on JCF web site
- "Format des templates biométriques" FQR 110 1767 Ed 1, Oberthur Card Systems
- [FIPS_201] FIPS Publication 201-1 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (March 14, 2006)
- [SP800_73_01] NIST Special Publication 800-73-1 Interfaces for Personal Identity Verification, 2006 Edition (March 24, 2006)
- [SP800_73_SI] Special Publication 800-73 Supplemental Information: *Namespace Management for Personal Identity Verification(PIV) Applications and Data Objects (October 6, 2005)*
- [SP800_76] Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification* [SP800_78] NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification (April 25, 2005)*
- [SP800_78] NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification (April 25, 2005)*
- [SP800_85] NIST Special Publication 800-85, *PIV Middleware and PIV Card Application Conformance Test Guidelines*
- [IR_7284] NIST InterAgency Report (NIST IR) 7284 *Personal Identity Verification Card Management Report* (January 18, 2006)

14 Definitions and Acronyms

14.1 Acronyms

- AID Application Identifier
- AP Application Provider
- APDU Application Protocol Data Unit
- API Application Programming Interface
- ATR Answer To Reset (contact mode)
- ATS Answer to Select (contactless mode)
- API Application Programming Interface
- CBC Cipher Block Chaining
- CRC Cyclic Redundancy Check
- DAP Data Authentication Pattern
- DES Data Encryption Standard
- DPA Differential Power Analysis
- DM Delegated Management
- DRNG Deterministic Random Number Generator
- ECB Electronic Code Book
- EEPROM Electrically Erasable and Programmable Read Only Memory
- EMI Electromagnetic Interference
- EMC Electromagnetic Compatibility
- GP Global Platform
- ICAO International Civil Aviation Organization
- ISO International Standard Organization
- JC Java Card ™
- JCRE Java Card ™ Runtime Environment
- MAC Message Authentication Code
- NDRNG Non Deterministic Random Number Generator
- OP Open Platform
- PIN Personal Identification Number
- PKCS Public Key Cryptographic Standards
- 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
- TDES Triple DES
- TLV Tag Length Value