Oberthur ID-One Cosmo 128 v5.5 for DoD Common Access Card (CAC)

FIPS 140-2 Level 2
Security Policy
Public Version
Version 1
June 5, 2009

Oberthur Technologies of America Corp.
4250 Pleasant Valley Road
Chantilly, VA 20151-1221
USA
+1 (703) 263-0100

Document Version Information

Table 1 lists the version history of this Security Policy.

Version - Date	Description
V 1 June 2009	Official Release

Table of Contents

1 Introduction

This document defines the Security Policy for the "Oberthur ID-One Cosmo 128 v5.5 for DoD CAC' cryptographic module, submitted for validation in accordance with FIPS 140-2 Level 2 security requirements. Included are, a description of the security requirements of the module, and a qualitative description of how each security requirement is achieved. In particular, this security policy specifies the security rules under which the cryptographic module must operate.

2 Module Overview

The module is the combination of the ActivIdentity JavaCard Applet suite v2.6.2B running on the Oberthur ID-One Cosmo 128 v5.5 smart card.

2.1 ID-One Cosmo 128 v5.5

The ID-One Cosmo 128 v5.5 Java Card Chip Platform, hereafter referred to as the module, is a single chip multi-application Smart Card micro-controller, with two communication interfaces (contact ISO 7816, and Contactless ISO 14443) that provides secure data storage and processing capabilities specifically designed for identity and government market needs.

The module state of the art security architecture benefits from Oberthur's extensive expertise as a smart card world leader since the inception of smart cards in the late 70's. It includes software and hardware countermeasures against the latest cryptographic attacks (both passive and active).

The module loads and runs applications written in Java™ programming language and includes a native implementation of Java Card™ version 2.2.2 and Open Platform version 2.1.1.A specifications, with full support for Delegated Management and DAP / Mandated DAP, that defines a secure infrastructure for post-issuance programmable platforms. Its micro-controller provides the loaded applications with all the low-level services such as memory management, I/O control, cryptographic algorithms and physical security.

This new generation Oberthur Smart Card programmable module offers a highly secure architecture with state of the art on board cryptographic services that include in some aspect and even exceed NSA SUITE-B cryptography with Advanced Encryption Standard (AES 256) for symmetric encryption; Secure Hash Algorithm (SHA up to 512) for message digest; Elliptic-Curve Diffie-Hellman (ECDH compatible mode) for key agreement and Digital Signature Algorithm (ECDSA with up to 384-bit prime modulus) for digital signatures.

Additional cryptographic features for legacy systems include Triple DES (128 and 192) and RSA (up to 2048) with a true ANSI X9.31 on-board key generation, ISO 9796, ISO 9797, PKCS#1.5, OAEP, PSS, and a FIPS 186-2 Random Number Generators.

Additional features include biometric extensions as defined by the Java Card Forum and a built-in on card fingerprint matching engine using standard ISO 19794-2 for finger minutia data format.

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

To complement the large memory size of this new module, ADPU management has been upgraded to include support for extended length fields, removing limitations of previous generation cards to a payload per APDU of 256 bytes max. With this new generation module, a single APDU can transmit up to 32767 bytes of data in each direction (In/Out). Photo ID, a fingerprint images and X509 certificates can now be read in a single APDU without requiring chaining.

The ID-One Cosmo 128 v5.5 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, two security firewalls have been implemented, the first one allows application developers to disable contactless access for sensitive operations within their application (applet instance), and the second one allows card issuer to temporarily or permanently disable all contactless activity at the card level or to restrict contactless activity to prevent the leaking over the contactless interface of identifiable information. This greatly improves the privacy protection of the card holder.

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).

The Card Manager provides the Open Platform services that are both internal (accessible by applet instances) and external services (accessible by external or non-chip applications).

In addition, whether embedded into a plastic card, or into an electronic passport, the ID-One Cosmo 128 v5.5 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 module is available with one or two communication interfaces (ISO 7816 for contact and ISO 14443 for contactless).

2.1.1 Common Criteria Protection Mechanisms

In addition to the security requirements from FIPS 140, the module has been independently tested to meet the requirements often asked in Common Criteria Certification, such as:

- Erase transient data on completion of operation execution.
- Prevent unauthorised data leakage to non-volatile memory
- Prevent data release *(cryptographic keys, PINs),* by physical/logical means.
- Prevent unauthorised data storage, or data overwrite.
- The card unlock function can only be performed by an authorised administrator.

2.1.2 Product Form Factors

The module is designed to be encased into different form factors such as a plastic card, an Electronic Passport, or any other support to produce the ID-One Cosmo 128 v5.5 Java Card Chip Platform, on which FIPS 140-2 Level 2 validated applets may be loaded and instantiated at post issuance.

The following figures show a few examples of various form factors available from Oberthur.

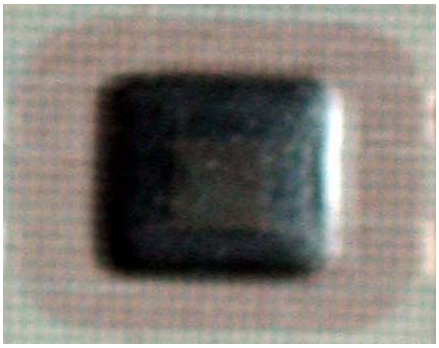

Figure 1
Stand alone module

Figure 2:
Module embedded into a
PIV Dual Interface Smart Card

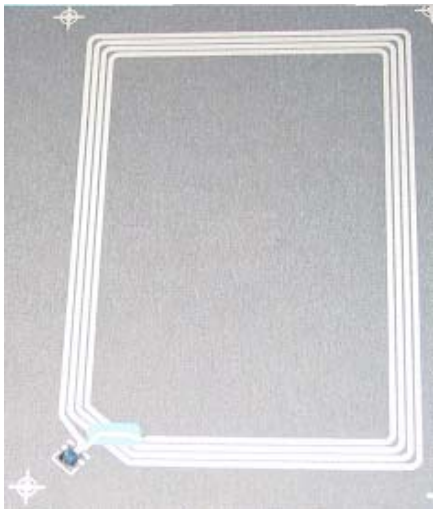

Figure 3:
Module embedded in the
cover of an **e-Passport**

2.1.3 Product Terminology

In the remaining of this document, the cryptographic module described above will be referred indifferently as ID-One Cosmo 128 v5.5 or as module, regardless of whether the form factor is a actually a smart card module, a full ID-1 smart card, an e-Passport book cover or any other form factor Oberthur may come up with to answer specific market needs.

2.2 ActivIdentity Digital Identity Applet Suite V2 for Extended PIV

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV supports execution of services via contact and contacless interfaces. Only a few services are contactless enabled, while all applet commands can execute with a contact reader.

The v2 applet suite consists of six applets:

- **Access Control Applet (ACA)** – This applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. Three off-card entity authentication methods – GP secure messaging, PIN, and ActivIdentity External Authentication are included by default in the ACA applet.
- **PKI/Generic Container/ SKI (PKI/GC/SKI) Applet** – The PKI/GC/SKI Applet can be used to provide secure storage for PKI credentials, and other data that are required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based cryptographic operations using the RSA private key stored in the PKI buffers. The applet also exposes services for OTP (One Time Password) through a synchronous or asynchronous authentication
- **ASC Library package** – This is the library package that implements functions required by other applets. The library functions are not directly accessible via the cryptographic module command interface.
- **PIV EP Wrapper Applet** – This Applet implements the Personal Identity Verification services from NIST SP800-73-1. It exposes the End Point (EP) APDU commands from this specification. The Applet is a wrapper on top of v2.6.2B applets (ASC Lib, ACA and GC/PKI/SKI above). Its purpose is to access PIV Card-Edge and objects although objects are stored in v2.6.2B applet instances. This PIV Applet cannot operate in a standalone mode; it must link with ACA and GC/PKI/SKI(s) applet to operate properly. This applet can only be instantiated in a strictly compliant mode to SP800-73-1 and data model
- **PIV EP Extended (Ext) Applet** – This Applet implements SP800-73-1 (both at card-edge and data model levels) and is extended to support additional features on top of native PIV such as support of additional PKI RSA keys (example for administrator login. PKI Key Encryption Key, SSO (single sign-on) storage, support of SKI authentication mechanisms, etc. This applet can be instantiated in PIV EP mode (native PIV features) or in PIV Ext mode (extensions are accessible through the 800-73-1 card edge.).
- **Secure Messaging Anonymous (SMA) plug-in Applet** – This is an authentication and secure messaging plug-in to the ACA applet (for card authentication to the off card application). It provides PKI (RSA) based card authentication and secure messaging (using 3DES) to secure the

communication between an off-card entity and any card applications. This protocol is not used during issuance or post-issuance operation but rather during usage of the card. The SMA session is opened between the middleware and the card if the Access Control Rule for some services in the card has SMA registered. SMA protocol comprised 2 operations PKI-based key exchange and 2TDEA secure messaging (DES3 with Double Key Length)

- Key Exchange Protocol
  - Card creates seeds
  - Off card application generates 2TDEA pre-session keys (MAC, ENC)
  - Off card application wraps pre-session keys with RSA 1024 (or 2048) bit RSA_PKCS_1 (key establishment methodology provides 80 or 112 bits of encryption strength)
  - Card unwraps 2TDEA pre-session keys
  - 2TDEA Session keys (MAC, ENC) are derived from both Off Card generated pre-session keys and card seeds
- Secure messaging Protocol
  - Based on secure messaging of Global Platform Secure Messaging (ENC, MAC)
  - Separate 2TDEA session keys for encryption and MAC
  - Chained APDU with DES3_CBC for MAC
  - Can wrap and/or MAC card command in both directions using Session keys

3 Security Level

The Oberthur ID-One Cosmo 128 v5.5 for DoD CAC has been designed and implemented to meet the overall Level 2 requirements of FIPS140-2.

Security Requirements Section	Level
Cryptographic module specification	2
Cryptographic module ports and interfaces	2
Roles, services, and authentication	3
Finite state model	2
Physical security	3
Operational environment	N/A
Cryptographic key management	2
EMI/EMC	3
Self tests	2
Design assurance	2
Mitigation of other attacks	2

Table 1 - Module Security Level Specification

4 Cryptographic Module Specifications

The Cryptographic Boundary is defined to be the "module edge' of the Oberthur ID-One Cosmo 128 v5.5 for DoD CAC crypto module.

4.1 Target of validation

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

The module submitted for validation consists of the ID-One Cosmo 128 v5.5 Chip Platform with an instantiated ActivIdentity applet in addition to the Card Manager (CM) and built-in Security Domains (SD).

In the scope of this document, the cryptographic module is a single chip Integrated Circuit with its embedded firmware. It is designed to be embedded into different form factors such as a plastic card, an Electronic Passport, or any other support to produce the ID-One Cosmo 128 v5.5 Java Card Chip Platform, on which FIPS 140-2 Level 2 validated applets may be loaded and instantiated at post issuance.

The "Cryptographic Boundary" for the ID-One Cosmo 128 v5.5 module vis-à-vis the FIPS 140-2 validation is the "module edge". The module is the encapsulated chip and is constructed to provide tamper resistance and tamper evidence required in the FIPS 140-2 physical Level 3 validation. The following diagram shows the actual module cryptographic boundaries.

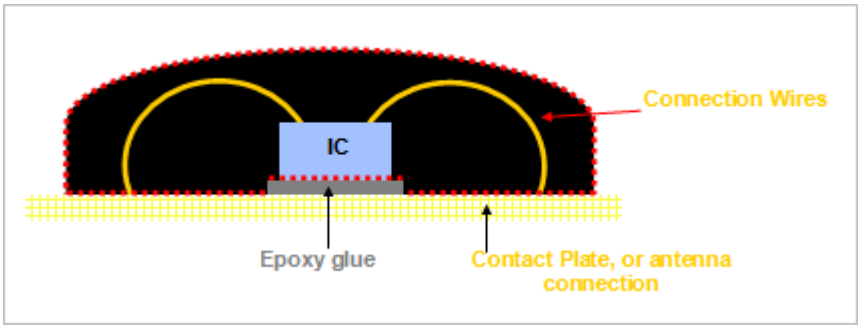

Figure 4

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.

4.2 ID-One Cosmo 128 v5.5

The cryptographic module supports a command-set aimed at allowing the mutual authentication of identities using strong cryptography with "card acceptance devices" or terminals that they might be connected to. Specifically, the TDES algorithm is used within authentication commands between the cryptographic module and the "card acceptance device" environment for strong authentication of identities. Establishment of identities using these commands is then used to fulfill "access conditions" which limit the ability of the external world to access information and/or commands on the module.

The Oberthur Card Systems ID-One Cosmo 128 v5.5 is a single chip implementation of a cryptographic module. The module comprises the following elements:

- Secure micro controller Integrated Circuit with:
    - A 32 bit crypto coprocessor optimized for public key cryptographic calculations (ECC and RSA)
    - A Triple DES (Data Encryption Standard) Co-Processor
    - An AES (Advanced Encryption Standard) Co-Processor
    - High reliability 144 KB EEPROM for both customer applications and Operating System data
    - System firmware, consisting of the operating system installed in Read Only Memory (ROM)
    - Firmware extension (Optional Code) loaded in EEPROM to fine tune OS capabilities
- Applets (Applications) that are to be installed onto the module: ActivIdentity Applets v2.6.2B.
- Critical Security Parameters stored in EEPROM as part of the Chip Platform personalization operation.

4.2.1 Module Hardware

The Integrated Circuit used for the ID-One Cosmo 128 v5.5 is identified by its Hardware Part Number B0.

Part number B0 comes in different customizations depending on the communication interface(s) needed by the end customer (i.e. ISO 7816 contact and/or ISO 14443 Contactless). This Security Policy applies to the above listed hardware part number, regardless of the communication interfaces that have been activated.

Module hardware Part Number can be read from the Card Identification Data Object under tag 04.

4.2.2 Module Firmware

The firmware (hard mask) is the ROM code that is written in the micro-controller during manufacturing and cannot be subsequently changed.

The firmware version of the ID-One Cosmo 128 v5.5 is F310.

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

4.2.3 Module Firmware Extensions

The functionality of the module operating system can be extended through the use of firmware extensions called optional codes. Such optional codes can be loaded in the EEPROM only during manufacturing and cannot be subsequently removed or modified. Examples of functionality that can be added through such firmware extension include critical patches on the card OS as well as support for additional cryptographic algorithms, additional biometric match on card algorithms, etc.

This document addresses the submission for validation of the module with the following firmware Extension(s):

Firmware Extension	Note
067733	Generic Codop R3.0

Table 2: Firmware Extension(s) included in this validation

4.2.4 Locks Configuration

The module includes several locks that can be set by Oberthur during the manufacturing phase to configure the module in a specific electrical configuration to meet customer requirements (e.g. FIPS 140-2, FIPS 140-3, CC, etc). Some of the locks could also be set by the Security Officer during the life of the module to 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 card (or e-Passport) holder.

However, the locks that could have an impact on the FIPS mode of operation of the module are non reversible and always set during the manufacturing phase.

4.2.5 Module Identification

Every module delivery is associated with a BAP 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. The BAP provides identification

information (hardware, firmware, and firmware extension, and locks configuration) and specifies if the electrical profile set the module in FIPS mode of operation when it leaves Oberthur factory.

Please make sure you specify at the time of ordering that you want the product to be validated to FIPS 140-2 as it may not be the default configuration from all Oberthur factories. (Modules in non FIPS mode of operation are usually faster and may be preferred by some customers). Oberthur technical support staff is fully trained to discuss your needs in terms of level of security and mode of operation and can make sure the electrical profile prepared for you sets the module in a FIPS mode of operation.

Modules in FIPS validated mode are listed as such in the BAP document associated with your delivery.

4.2.6 FIPS Approved Security Functions

The following table gives the security functions that have been FIPS validated on the ID One Cosmo 128 v5.5.

Security Function	Details	FIPS Validation #
2 Key Triple DES (128)	ECB and CBC in both Encryption and Decryption	**606**
3 Key Triple DES (192)	ECB and CBC in both Encryption and Decryption	**606**
Triple DES MAC (128)	CBC mode	**606, vendor affirmed**
AES 128	ECB and CBC in both Encryption and Decryption	**657**
AES 192	ECB and CBC in both Encryption and Decryption	
AES 256	ECB and CBC in both Encryption and Decryption	
SHA-1	Byte-oriented messages	**688**
SHA-224 & SHA-256		
SHA-384 & SHA-512		
RNG	FIPS 186-2	**377**
RSA (Modulus sizes: 1024, 1536 and 2048)	GenKey 9.31	**304**
	SigGenPKCS1.5	
	SIgGenPSS	
	SigVerPKCS1.5	
	SigVerPSS	
ECDSA (P192, P-224, P-256, P-384)	Key Pair Generation	**70**
	SigGen	

	SigVer	

4.3 Actividentity Applet V2 for Extended PIV

The ActivIdentity Digital Identity Applet Suite V2.6.2B for Extended PIV supports identity-based authentication of the Card Holder, Application Operators, and Cryptographic Officers, using PIN/ PUK or TDES 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 machines, Card Manager application, and ActivIdentity 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 checks all validated applets, and will not load any applets that do not have the correct MAC.

The ActivIdentity Digital Identity Applet Suite V2 for PIV is composed of the following elements:

Applet V2.6.2B:

- ASC library version 2.6.2B.3
  - Executable Load File AID= A0.00.00.00.79.11.FE.02.06
  - Load File Version: 02.06
- ACA applet version 2.6.2B.4
  - Executable Load File AID= A0.00.00.00.79.10.FE.02.06
  - Load File Version: 02.06
- PKI/GC/SKI applet version 2.6.2B.4
  - Executable Load File AID= A0.00.00.00.79.01.FE.02.06
  - Load File Version: 02.06
- PIV End Point Wrapper module 2.6.2B.4
  - Executable Load File AID= A0.00.00.00.79.20.FE.02.06
  - Load File Version: 02.06
- PIV End Point Extended module 2.6.2B.4
  - Executable Load File AID= A0.00.00.00.79.21.FE.02.06
  - Load File Version: 02.06
- SMA applet version 2.6.2B.3
  - Executable Load File AID= A0.00.00.00.79.05.FE.02.06
  - Load File Version: 02.06

The applet and library package byte code is loaded in the cryptographic module memory. Note that the ASC library package consists of static utility classes only accessed by the applet, and the library cannot be accessed directly by off-card entity.

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.

Applets depend on a unique security domain (SD) for the 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.

The ownership of a key set allows for establishing a Secure Channel (SC) between the host and either the security domain or the security domain applets. 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 replacement key set, can take control of the personalization of all applet instances belonging to a security domain.

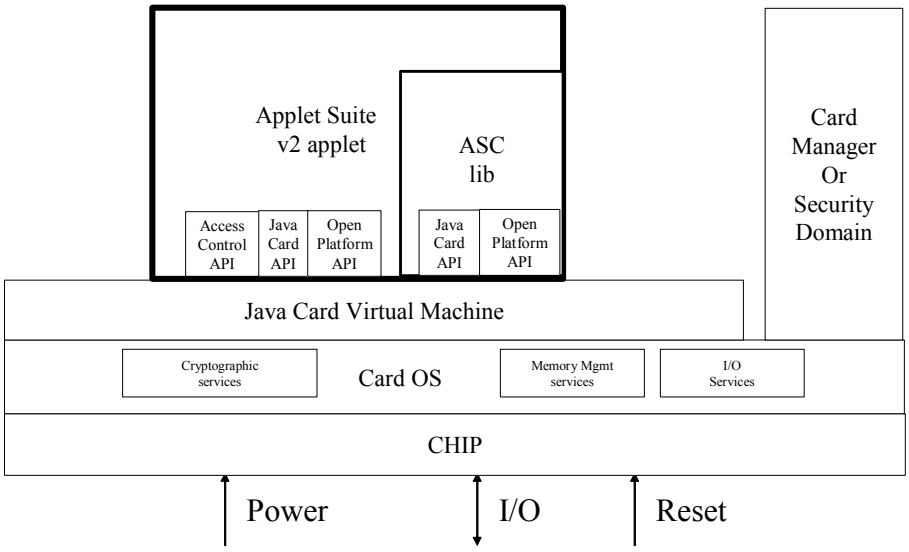

Figure 5: Functional block diagram

5 Ports and Interfaces

The integrated circuit used in the module is a single chip that supports both a contact and a contactless communication interface. Contact communication is achieved through a physical connection to a smart

card contact plate. Contactless communication is achieved through physical connection to an antenna. Neither the contact plate, nor the antenna, are within the cryptographic boundaries of the module.

The following sections, describe each of these three communication interfaces.

5.1 Physical Port: Smart Card Contact Plate

5.1.1 Interface Physical Specifications

In this contact mode, communication to and from the cryptographic module is done through an ISO/IEC 7816-21 smart card contact plate (also called printed circuit) that provides the electrical connection required by ISO/IEC 7816-32.

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 here only for illustration purposes.

5.1.2 Interface Electrical Specifications

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

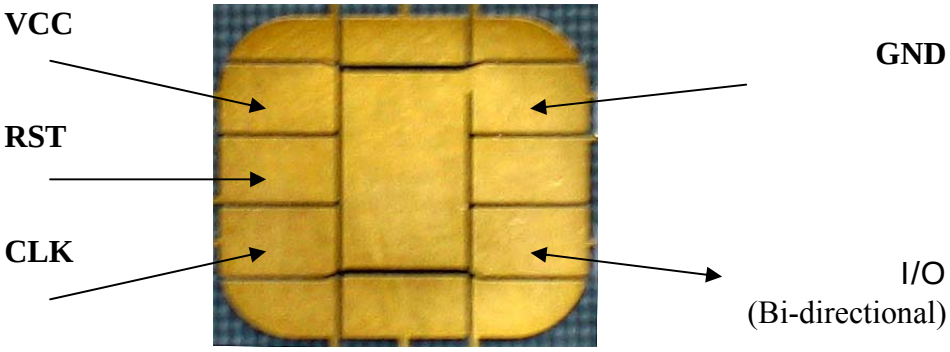

Figure 6: Example of an ISO 7816-2 compliant contact plate used to provide ISO 7816-3 electrical communications with the cryptographic module

The five 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)

[1] ISO/IEC 7816 Part 2: Identification Cards — Integrated Circuit Cards with contacts — Dimensions and location of the contacts (Second Edition – 2007)
[2] ISO/IEC 7816 Part 3: Identification Cards — Integrated Circuit Cards with contacts — Electrical interface and transmission protocols (Third Edition – 2006)

- **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 five electronic signals are in full compliance with ISO/IEC 7816-3 standard.

5.1.3 Condition of use

5.1.3.1 Power Supply

The Oberthur PIV EP card operates in both ISO 7816-3 class A and class B. This opens new ranges of application using lower voltage portable readers.

- 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.

5.1.3.2 Frequency

The card supports an external clock Frequency from 1MHz to 10MHz

5.1.3.3 Speed

The card support communication speed up to 625,000 bits/sec in contact mode with an external clock of only 5Mhz as per the latest (2006) edition of ISO 7816-3.

Values of the clock rate conversion integer (Fi) and the baud rate adjustment integer (Di) supported by the module are as follows:

FI	F	**DI**	D	**Maximum communication speed**
1	372	**1**	1	13,440 bauds at 5Mhz and 9,600 bauds at 3.576MHz
1	372	**2**	2	26,881 bauds at 5Mhz
1	372	**3**	4	53,763 bauds at 5Mhz
1	372	**8**	12	161,290 bauds at 5Mhz
9	512	**4**	8	78,125 bauds at 5Mhz
9	512	**5**	16	156,250 bauds at 5Mhz
9	512	**6**	32	312,500 bauds at 5Mhz
9	512	**7**	64	**625,000 bauds at 5Mhz**

5.1.3.4 Transmission Protocol

The transmission protocol complies with ISO/IEC 7816-3:2006 with full support for extended length APDU.

Depending on the electrical profile defined in the BAP, the module can be configured in manufacturing to support any of the following ISO/IEC 7816-3 transmission protocols:

- Character oriented transmission protocols (T=0) only
- Block oriented transmission protocols (T=1) only
- Both T=0 and T=1

However, from an APDU-TPDU management level, the Block oriented transmission (T=1) is the only one that behaves identically on all three interfaces. Therefore if the module is to be used also in contactless mode, it is recommended to disable T=0 and develop only in T=1 to allow the middleware to be fully transparent to the communication ports being used.

Characters can be exchanged in direct convention (Z level corresponds to a logical 1 and LSB is sent first) or in inverse convention (Z level corresponds to a logical 0 and LSB is sent first).

The Oberthur ID-One Cosmo 128 v5.5 supports the Protocol and Parameter Selection to select a new protocol type or change transmission baud rate.

Up to 32767 data bytes can be exchanged in each direction within a single command (using APDU with Extended Length Field).

5.2 Physical Port: Contactless Mode

In contactless mode, the cryptographic module follows the standard ISO/IEC 14443 RF Interface.

5.2.1 Interface Physical Specifications

In this mode, the 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 and distinct from the electrical connections used in contact mode.

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

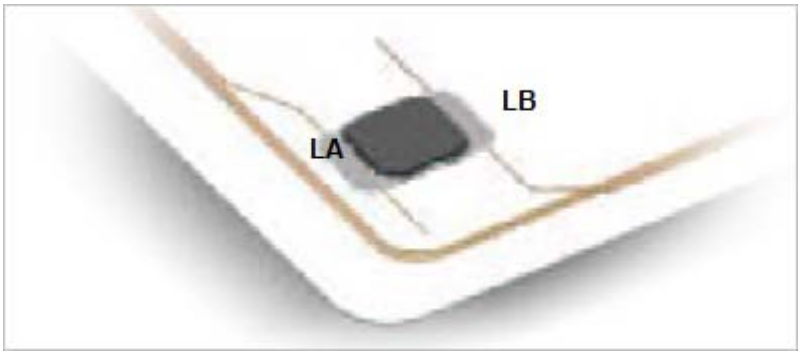

Figure 7: Example of connection of the cryptographic module to the antenna for a contactless mode.

5.2.2 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 128 v5.5 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 cryptographic co-processors 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 14443-23

An anti-collision mechanism compliant with 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.

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

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

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 standards.

5.2.3 Condition of use

5.2.3.1 Operating Field

The operating field depends on the form factor of the final product in which the module is embedded.

When the module is embedded into an ISO 7810 ID-1 Oberthur contactless smart card, the card can operate under a field between 1.5 A/m to 7.5 A/m rms

5.2.3.2 Frequency

The module nominal frequency for contactless communication is 13.56 MHz

[3] ISO/IEC 14443 part 2: Radio frequency power and signal interface for contactless integrated circuit cards – Proximity cards.

5.2.3.3 Speed

The supported bit rates of the Oberthur ID-One Cosmo 128 v5.5 are:

- 106 Kbits/s
- 212 Kbits/s
- 424 Kbits/s
- 847 Kbits/s

5.2.3.4 Transmission protocol

Communications with the module in contactless mode is based on a fully standardized (ISO/IEC 14443), half-duplex transmission protocol, called T=CL.

From an APDU-TPDU translation level, this protocol is similar to the T=1 Block transmission protocol used in the contact mode.

Up to32767 data bytes can be exchanged in each direction within a single command (using APDU with Extended Length Field).

5.3 Logical Interface Description

Once communication is established between the reader and the module, the module functions as a "slave" processor to implement and respond to the reader commands. The module adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible. The I/O ports4 of the module (either physical in contact mode or virtual in the case of RF transmission) provide the following logical interfaces:

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

Synchronization timing controls, provided in part by the module CLK clock input 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.

5.3.1 APDU Commands

The data exchange protocol between the cryptographic module and the outside world follows ISO/IEC 7816-4 standard. The cryptographic module acts as a slave device, receiving and executing APDU commands from the host.

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

An application protocol data unit is either a command APDU or a response APDU. A step in application protocol consists of transmitting a command APDU, processing it in the receiving entity and returning the response APDU. This pair of APDUs is called a command-response pair.

A command APDU consists of a mandatory header of four bytes denoted CLA INS P1 P2, followed by a conditional body of variable length.

Command header	Command body
CLA INS P1 P2	[Lc field] [Data field] [Le field]

A response APDU consists of a conditional body of variable length followed by a mandatory trailer of two bytes denoted SW1 SW2 and encoding the status of the receiving entity after processing the command.

Response body	Response trailer
[Data field]	SW1 SW2

5.3.2 API Interface

The Oberthur module provides trusted applets with internal services through its APIs. The cryptographic module performs the requested services according to its roles and services Security Policy.

6 Roles and Services

6.1 Identification

The Oberthur ID-One Cosmo 128 v5.5 for DoD CAC 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.

6.2 Roles

The Oberthur ID-One Cosmo 128 v5.5 for DoD CAC defines three distinct roles that are supported by the on-module cryptographic system; the Card Security Controller (CSC) role, the Application Operator role, and the Card Holder role.

6.2.1 User Roles

Card Holder Role (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 his PIN.

Application Operator Role (AO): The Application Operator role represents an external application requesting the services offered by the applets. An applet authenticates the Application Operator role by verifying possession of the Application External Authenticate (XAUT) TDES key. The AO is also able to provide the PUK credential to unblock the PIN (SP800-73-1).

6.2.2 Cryptographic Officers roles

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 GP secure channel TDES key set stored within the Card Manager. By successfully executing the GP secure channel mutual authentication protocol, the CSC role establishes a secure channel to the Card Manager and execute services allowed to the CSC role in a secure manner. The CSC role can also be responsible for unblocking the PIN using a specific unblock PIN XAUT key with ActivIdentity external authentication protocol. Note: CSC doesn't operate SMA.

6.2.3 Identity based Authentication

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV cryptographic module supports identity based role authentication using the following scheme.

6.2.4 User Role Authentication

- The Card Holder role is authenticated with a PIN
  - **PIN**: The Card Holder role must send a VERIFY APDU to the module to access services protected with PIN access control rules (PIN once for session or PIN-Always). The APDU corresponding to the applet service protected by the PIN, can access the service before the cryptographic module is removed or a reset command is sent to the cryptographic module. The PIN object is identified through a unique identifier (both values 00 or 80h are accepted)
- The Application Operator role is authenticated by the possession of a TDES key or a 8 bytes-string for PIN Unblocking Key (PUK).
  - **Application External Authentication (XAUT) key**: The Application Operator role must prove the possession of a particular TDES key to access the PKI/GC/SKI buffer read, or update service protected with the External Authentication protocol using this particular key. An 8-byte challenge is first obtained from the applet. The application controlled by the operator encrypts the challenge with a 128-bit or 192-bit TDES key, and submits the resulting cryptogram to the module for verification. The APDU corresponding to the particular applet service protected by the XAUT key, can access the service before the cryptographic module is removed or a reset command is sent to the cryptographic module. Each Key has a unique identifier in the card called KeyID [01-08 for XAUTH key]
  - **Unblock with PUK:** The AO can also complete the PIN unblock operation with the PUK (which is loaded under the CSC role). The PUK object is identified through a unique identifier 81h.

6.2.5 Cryptographic Officer Role Authentication

- The Cryptographic Officer role is authenticated by a TDES key set in the case of secure channel key set, or a TDES key in the case of XAUT key.
    - **Secure Channel key set:** The Cryptographic Officer (CSC) role must prove the possession of a key set composed of three TDES keys. Two keys (K_{MAC}, K_{ENC}) are used to generate session keys according to Global Platform specification. The session keys ensure the confidentiality of the command payload, allow the mutual authentication of the parties and protect the APDU command integrity. A third key (K_{KEK}) is used to wrap keys transported within the APDU command. Each Key Set is identified by a unique identifier in the card called Key Set Version [00-FF]
    - **Unblock PIN with XAUT key:** The Cryptographic Officer (CSC) role performs the ActivIdentity external authentication protocol using the XAUT TDES key. The PIN is unblocked if the CSC role is successfully authenticated. Each Key has a unique identifier in the card called KeyID [01-08 for XAUTH key]

6.3 Services

6.3.1 Cryptographic Officer Services

Several services are made available to an authenticated Cryptographic Officer (CSC) only. They are primarily used to manage Security Domains, allow the creation of additional applications (applet instances of already FIPS approved executable byte code present in the card) and/or allow the loading of applets into the card.

- ***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 remain FIPS validated, 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.

- ***STORE DATA:*** This command is used by the CSC to clear the audit log and load Data Objects at the module level. It is also used 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 APDU is used by the CSC to temporary lock an application, and to 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 the FIPS validated configuration 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.

- ***PIN CHANGE/UNBLOCK:*** The Pin Change/Unblock instruction is used to change the value of the Global PIN or to unblock the current Global PIN. The command is used with GP Secure Messaging in the context of a Secure Channel; its level of security must so match the security level of the current Secure Channel.

- ***DAP VERIFICATION:*** DAP verification allows an Applet Provider to own a Security Domain which can be requested to check application code integrity and authenticity before the application code is loaded by the Card Security Controller (Crypto-Officer).

The following APDUs are sent to ActivIdentity applets:

- ***CHANGE REFERENCE DATA:*** This APDU intends to create the PIN and PUK in the card. It is also used to update the PUK value.

- ***INITIALIZE UPDATE***: Similar to command set to Card manager/Security Domain

- ***EXTERNAL AUTHENTICATE***: Similar to command set to Card manager/Security Domain

- ***GENERATE ASYMMETRIC RSA KEY PAIR:*** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications

- ***GENERATE KEY PAIR:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.

- ***GET DATA***: This command is used to retrieve a single data object

- ***PRIVATE SIGN/DECRYPT***: This APDU uses the RSA private key in the PKI buffer to sign data

- ***PUT DATA:*** This APDU intends to set the applet properties, load keys as well as personalize the container managed under the PIV Ext applet. This APDU is present for compliance with PIV specifications.

- ***PUT KEY***: This APDU is used to either enter the XAUT keys (like used to unblock the PIN), the RSA private key component or the SKI key for One Time Password generation. The APDU must be used with a secure channel established by CSC role. The APDU format is compliant with GP specifications.

- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.

- ***REGISTER ACR:*** This APDU manages the mapping between ACRID and actual APDU instruction as well as record the ACR definition for the applet services.

- ***REGISTER APPLET:*** This APDU is to register applet instances to the ACA instance so that the access control and GP secure message service can be provided.

- ***RESET RETRY COUNTER:*** This APDU is used to unblock the Card Holder PIN and restore the VERIFY service with a new counter value if the CSC role is authenticated successfully. The command operates as long as the unblock counter has not expired.

- ***SET APPLICATION UID***: This APDU is sent when the UID associated with the applet instance needs to be changed

- ***SET PROPERTIES:*** This APDU creates and sets the object properties for GC/PKI/SKI applet.

- ***SET STATUS***: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, and PERSONALIZED

- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.

- ***UPDATE PROPERTIES:*** This command updates the ACA properties

6.3.2 Application Operator Services

The following APDUs are sent to ActivIdentity applets only:

- ***AC EXTERNAL AUTHENTICATE***: This APDU is used in combination with a Get Challenge to authenticate the Application Operator using the AC external authenticate protocol.

- ***GENERATE ASYMMETRIC RSA KEY PAIR:*** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications. This APDU is present for compliance with PIV specifications.

- ***GENERATE KEY PAIR:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.

- ***GET DATA***: This command is used to retrieve a single data object like PIV object content

- ***PUT DATA:*** This APDU is present for compliance with PIV specifications and it is used to personalize containers managed under the PIV Ext applet

- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.

- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.

- ***RESET CARD:*** This command resets the card content (buffer content, PKI credentials, SKI keys as well the PIN/PUK)

- ***RESET RETRY COUNTER:*** This APDU is used to unblock the PIN with PUK string.

6.3.3 User Services (Card Holder)

The following APDUs are sent to ActivIdentity applets:

- ***CHANGE REFERENCE DATA:*** This APDU is used to change the Card Holder PIN if the Card Holder is correctly authenticated.

- ***GENERATE ASYMMETRIC RSA KEY PAIR:*** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications.

- ***GENERAL AUTHENTICATE***: The APDU is for PKI operations (via the PIV EP wrapper and PIV EP Ext)

- ***GENERATE KEY PAIR:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.

- ***GET DATA***: This command is used to retrieve a single data object like PIV object content

- ***INTERNAL AUTHENTICATE (GENERAL AUTHENTICATE command)***: The APDU is for SKI operations (One Time Password) and to generate a cryptogram from the card for verification by the calling application.

- ***PRIVATE SIGN/DECRYPT:*** This APDU uses the RSA private key in the PKI buffer to sign data.

- ***PUT DATA:*** This APDU intends to personalize the card objects. This APDU is present for compliance with PIV specifications.

- ***PUT KEY***: This APDU is used to either enter the XAUT keys, the RSA private key component or the SKI key for One Time Password generation. In a Card Holder role, the APDU must be used with a SMA channel to encrypt the key component.

- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.

- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.

- ***UPDATE PROPERTIES:*** This command updates the ACA properties

- ***VERIFY***: This APDU checks the PIN presented by the Card Holder against the current PIN.

6.4 No Role

The following services are available without authentication

- ***MANAGE CHANNEL:*** **T**his command allows the terminal to open or close a logical channel in the card. Up to 4 logical channels may be open at a time. Logical channel is not used by the ActivIdentity Applet.

- ***GET DATA:*** The GET DATA command is used to retrieve a non protected data object available from the selected application. Example of data retrievable includes Identification Data, configuration data, Issuer Identification Number, Card Image number, Audit log, and a few others described in the module programmer's guide.

- ***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 it's previously loaded executable code.

- ***ENVELOPE:*** This command transmits [part of] either a command APDU or a BER-TLV data object that otherwise could not be transmitted by the available transmission protocol. See examples in ISO/IEC 7816-3.

The following APDUs are sent to ActivIdentity applets:

- ***GET CHALLENGE:*** This APDU is used in combination with AC external authenticate to perform an external authentication of the Application Operator in order to unblock the PIN. It is also involved when opening a SMA session.

- ***GENERAL AUTHENTICATE***: The APDU is for PKI operations (via the PIV EP wrapper and PIV EP Ext) as well as when opening a SMA session

- ***GET ACR:*** This APDU is used to retrieve the ACR definition for the services.

- ***GET DATA***: This command is used to retrieve a single data object, such as the Card Identification data.

- ***GET PROPERTIES***: This APDU is used to obtain information about applet instance configuration.

- ***GET RESPONSE***: This command is restricted to T=0 ISO protocol for an incoming command which has data to send back. That data is received with the GET RESPONSE command sent immediately after the command to which it is related.

- ***LOGOUT:*** To logout all authenticated roles.

- ***UPDATE PROPERTIES:*** This APDU modifies the applet properties The APDU is accessible from ACA applet.

- ***READ BINARY:*** This APDU reads binary data stored on the card.

- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.

- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.

- ***SELECT***: This command is used for selecting an application (Card Manager, security domain or Applet). The Card Manager may be selected either for the loading of a Load File or for installing a previously loaded application (or security domain)

- ***PRIVATE SIGN/DECRYPT:*** This APDU uses the RSA private key in the PKI buffer to sign data (involved with PIV Card Authentication Key)

- ***MANAGE SMA***: The APDU is used to explicitly close the SMA secure session

6.5 Relationship between Roles, Services and CSP Access

For the Card Manager services, the access rules are listed in the following table:

Roles/Services	CSC	No Role	CSP involved		CSP Access type
			From CSC	From AP	
INSTALL	X		CSK		Execute
LOAD	X		CSK		Execute
DELETE	X		CSK		Execute
PUT TDES KEY	X		CSK, CDK	ASK, ADK	Execute, Write
PUT PUBLIC KEY	X		CSK, $\mathbf{K}_{TOKEN}$, $\mathbf{K}_{DAP}$		Execute, Write
STORE DATA	X		CSK	ASK	Execute
SET STATUS	X		CSK	ASK	Execute
GET STATUS	X		CSK	ASK	Execute
INITIALIZE UPDATE	X				
EXTERNAL AUTHENTICATE	X		CDK, CSK	ADK, ASK	Execute
DELEGATE MANAGEMENT	X		CSK, $\mathbf{K}_{TOKEN}$, $\mathbf{K}_{RECEIPT}$		Execute
PIN CHANGE/UNBLOCK	X		PIN, CSK		Write and Execute
DAP VERIFICATION	X			$\mathbf{K}_{DAP}$	Execute
MANAGE CHANNEL		X			
GET DATA		X			
SELECT		X			
ENVELOPE		X			

Table 4: Role and possible ACR configuration for Card Manager

For ActivIdentity applets suite v2, the access rules are listed in the following table.

Role / Authentication Method Vs. Services	**No Role / None**	**Cryptographic Officer (CSC) / SECURE CHANNEL**	**Application Operator / XAUT (or PUK)**	**Card Holder / PIN**	**CSP Involved**	**Applet V2.6.2b**	
						ISO 7816	**ISO 14443**
AC EXTERNAL AUTHENTICATE			X		XAUT	X	
CHANGE REFERENCE DATA (change PIN)				X	PIN	X	
CHANGE REFERENCE DATA (Create PIN/PUK + Update PUK)		X			PIN PUK	X	
EXTERNAL AUTHENTICATE		X			CDK, CSK (from CSC)	X	
GENERATE KEY PAIR		X	X	X	RSA Private Key RSA Public Key	X	
GENERATE ASYMMETRIC RSA KEY PAIR		X	X	X	PIV RSA Private Key RSA Public Key	X	
GENERAL AUTHENTICATE	X			X	XAUT PIV RSA Private Key RSA Public Key	X	X
GET ACR	X					X	
GET CHALLENGE	X					X	X
GET DATA	X	X	X	X		X	X
GET PROPERTIES	X					X	X
GET RESPONSE	X					X	X
INITIALIZE UPDATE		X				X	
INTERNAL AUTHENTICATE				X	Secret Key for OTP	X	X
LOGOUT	X					X	
MANAGE SMA	X					X	X
PRIVATE SIGN/DECRYPT	X	X		X	RSA Private Key RSA Public Key	X	X
PUT KEY		X		X (SMA-ENC minimum)	RSA Private Key RSA Public Key	X	
PUT DATA		X	X	X	RSA Private Key PIV RSA Private Key RSA Public Keys XAUT Secret Key for OTP	X	

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC) / SECURE CHANNEL	Application Operator / XAUT (or PUK)	Card Holder / PIN	CSP Involved	Applet V2.6.2b	
						ISO 7816	ISO 14443
READ BINARY	X					X	X
READ CERTIFICATE / STATIC BUFFER	X	X	X	X		X	X
REGISTER APPLET		X				X	
REGISTER ACR		X				X	
RESET CARD			X			X	
RESET RETRY COUNTER (with PUK)			X (PUK)		PUK PIN	X	
RESET RETRY COUNTER (without PUK)		X			CDK, CSK (from CSC)	X	
SET APPLICATION UID		X				X	
SELECT	X					X	X
SET PROPERTIES		X				X	
SET STATUS		X				X	
UPDATE CERTIFICATE / STATIC BUFFER	X	X	X	X		X	
UPDATE PROPERTIES	X	X		X		X	
VERIFY				X	PIN	X	X

Table 5: Role and possible ACR configuration for Applet

7 Cryptographic Key Management

The cryptographic module handles various keys and PINs:

- Global PIN and ActivIdentity ACA PIN
- PIN Unblocking Key (PUK)
- Card Manager and Security Domain Keys
- Symmetric and asymmetric Keys for One Time Password, External Authentication and PKI operations (signature, encryption…)

7.1 Global PIN

The Global PIN (Personal Identification Number) supported by the ID-One Cosmo 128 v5.5 can be a sequence of 6-254 digits max. It may be used through a standard GP 2.1.1 API to authenticate the future Card Holder to the module with a probability of false authentication of less than 1/1,000,000. By successfully entering a PIN sequence, a Card Holder can prove knowledge of a shared secret (the PIN) and thereby authenticate to the module.

The Cryptographic Officer has the capability to unlock a cryptographic module that has been locked after reaching a predefined number of consecutive errors on PIN verification. However, PIN setting and verification are available only through API to be called by an applet. Until such applet gets FIPS 140-2 validated, the Global PIN feature cannot be used.

7.2 ACA PIN

The ACA PIN (Personal Identification Number) supported by the Actividentity Applet can be a sequence of 6 to 254 characters max. The ACA PIN relies on Java Card PIN management service It also authenticates the Card Holder to the module with a probability of false authentication of less than 1/1,000,000. By successfully entering a PIN sequence, a Card Holder can prove knowledge of a shared secret (the PIN) and thereby authenticate to the module.

The Cryptographic Officer has the capability to unlock a cryptographic module that has been locked after reaching a predefined number of consecutive errors on PIN verification. The PIN setting and verification are authorized from the ActivIdentity applet v2.6.2B.

The initial PIN is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set, and can be changed later by the user after a successful user authentication event.

The PIN is assigned with an identifier: 00h or 80h in the card.

Note: ACA PIN and GP Global PIN are two different PIN objects. GP Global PIN is not called by ActivIdentity Applets.

7.3 PUK

The PIN Unblocking Key (PUK) is managed inside the ACA Applet too. It is used to authenticate the AO and the command CHANGE REFERENCE DATA initializes the PUK. Its role is to unblock the PIN. The PUK is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set. The PUK pattern is 8 bytes long in the card and it contains a static byte sequence unique in each card issued.

PUK is assigned with identifier 81h in the card. Maximum PUK value is 15 in decimal.

7.4 Cryptographic Keys

Two categories of keys coexist in the module. The keys exposed by the Card Manager/Application Provider Security Domain and keys exposed by the ActivIdentity applets. Each key is identifier by a Key Identifier.

The FIPS validated ID-One Cosmo 128 v5.5 (i.e. in Card Manager OP-Secured) includes the following keys that conform to Global Platform Specifications v2.1.1:

7.4.1 Initial Issuer Transport Key

1. **KDC**: Initial Issuer Key set: Set of three Triple DES Keys (called KDC_{ENC} KDC_{MAC} and KDC_{KEK}) of 16 bytes each. The first two, KDC_{ENC} and $KDC_{MAC,}$ are only used to generate Secure Channel session keys during the initiation of a Global Platform Secure Channel, and the last one, KDC_{KEK} is used as a key transport key within a secure channel.

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

2. **KSC**: Initial Issuer Session Transport Keyset: Set of two transient Triple DES Keys (called KSC_{ENC} KSC_{MAC}) of 16 bytes each. KSC_{ENC} is used for Secure Channel Encryption, and KSC_{MAC} is used for Secure Channel MAC verification.

KDC_{ENC} and KDC_{MAC} are used to derive KSC_{ENC} and KSC_{MAC} keys that are used to authenticate the secure sessions with the card Manager.

KDC_{KEK} does not derive any keys but is used directly to wrap the CO CDK key set and the User ADK key set when they are entered into the module for the first time. As a result this Triple DES KDC can only be used to wrap/unwrap other Triple DES keys of the same size.

7.4.2 Crypto-Officer keys in Card Manager

1. **CDK**: Crypto-Officer Keyset: Set of three Triple DES Keys (called CDK_{ENC} CDK_{MAC} and CDK_{KEK}) of 16 bytes each. 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 as a key transport key within the secure channel to wrap only other Triple DES keys of the same size.

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

2. **CSK**: Crypto-Officer Session Keyset: Set of two transient Triple DES Keys (called CSK_{ENC} and CSK_{MAC}) of 16 bytes each. CSK_{ENC} is used for Secure Channel Encryption, and CSK_{MAC} is used for Secure Channel MAC verification.

3. $\mathbf{K}_{TOKEN}$: 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.

4. **$K_{RECEIPT}$:** Key Receipt: Triple DES Key (16 bytes) used to compute a receipt on Delegated Management Commands. See the Delegated Management section. 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.

7.4.3 Keys in Security Domains

1. **ADK**: Applet Provider Keyset: Set of three Triple DES Keys (called ADK_{ENC} ADK_{MAC} and ADK_{KEK}) of 16 bytes each. 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 as a key transport key within the secure channel to wrap only other Triple DES keys of the same size. This keyset is present in both type of Security Domain, Security Domain with Delegated Management, and Security Domain with DAP Verification. The process used to generate a unique ADK per cryptographic module takes place in the cryptographic HSM outside of the crypto module.
2. **ASK**: Applet Provider Session Keyset: Set of two transient Triple DES Keys (called ASK_{ENC} and ASK_{MAC}) of 16 bytes each. ASK_{ENC} is used for Secure Channel Authentication and optionally Encryption, and ASK_{MAC} is used for Secure Channel MAC verification.
3. **K_{DAP}**: Key DAP: Public RSA Key (1024 bits) used to verify the DAP on an application code to be loaded into the module and authorize or not its loading. (See the DAP Verification section). 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. More information on how this key is used can be found in the DAP Verification section.

7.4.4 Keys from ActivIdentity Applets

1. **External Authentication Keys (XAUT)**: TDES keys that enable the authentication of either Application Operators or Cryptographic Officers (RESET RETRY COUNTER command for Unblocking the PIN). These keys are generated out side of the cryptographic module in an HSM, and then are loaded protected with a Global Platform secure channel using the CSC Card Manager / Security Domain key set. Key Identifier is [01-08].
2. **RSA private keys**: managed (generated or unwrapped) from the PKI/GC/SKI applet using the Java Card cryptographic services. These keys are used to generate signatures. They are either generated on the card or outside of the cryptographic module in an HSM, and then loaded protected with a Global Platform secure channel using the CSC Card Manager / Security Domain key set. It also includes the PKI key for SMA. Object identifier is encoded on 2 bytes [0000-FFFF].

3. **RSA public keys** : Public keys are stored under the form of public key certificate and recorded in GC buffers that belongs from the GC/PKI/SKI applet. There is a certificate slot booked for each RSA private key defined in the card. Object identifier is the same as for the corresponding private key, it is encoded on 2 bytes [0000-FFFF]
4. **PIV private key objects**: Four RSA keys are managed in the Applet PIV. Those keys are defined in the PIV specification (SP800-73-1) and are attached with key Identifiers: 9Ah (PIV Authentication Key), 9Ch (PIV Digital Signature Key), 9Dh (PIV Key Management Key), 9Eh (PIV Card Authentication Key).
5. **Secret Key for OTP:** TDES key is involved during generation of the One Time Password and then authentication from the card to the calling application. Key Identifier is [01-08]

7.4.5 Keys Exchange

The following key exchange takes place with the Cryptographic Officer and with the User prior to the module being initialized by Oberthur.

The values of the root secrets used to retrieve a module unique CDK, (with optionally KRECEIPT) and ADK are securely exchanged between Oberthur production HSM and respectively the Cryptographic Officer HSM and the User HSM using a well defined and highly secure key ceremony described in a separate document.

The values of the RSA public Keys KTOKEN and KDAP, are provided respectively by the Cryptographic Officer and the User using a method that guarantees the integrity but not necessarily the confidentiality of the transmission.

In this FIPS configuration, the CSK and the ASK are the only keys that are not loaded but generated automatically by the module whenever needed. The keys are generated via the Open Platform Card Specification Secure Session Key Generation Process that was approved by NIST/CSE during the first Java based smart card validation. All Java-based smart cards use this process to generate session keys.

7.4.6 Key Loading

During the card manufacturing and initialization process, an initial set of Open Platform Keys called KDC is securely loaded into the Card Manager (Crypto-Officer) Security Domain. This key set is generated by a derivation process using a master secret key called KMC and card specific information such as chip serial number.

The KDC keyset is used to open a Secure Channel that will protect the loading of the initial value of Crypto-Officer and User Keys (except for the transient session keys ASK and CSK that are not loaded but generated automatically by the module whenever needed).

Crypto-Officer and User Key Loading is done using an authentication followed by a PUT TDES KEY or PUT PUBLIC KEY command depending on the type of key being loaded. Keys are valid until replaced

Both the Crypto-Officer and the User can replace their own keys at anytime during the active life of the module or whenever they feel a key may be compromised. This is done using an authentication with

the current keyset (CDK or ADK) followed by a Put Key command with "Key update" as parameter. Depending on the key to replace, the PutKey command is actually a PUT TDES KEY or a PUT PUBLIC KEY command. The new value is loaded into the card encrypted with the old key-set value using the TDES algorithm.

7.4.7 EEPROM encryption Key

Security relevant data stored in the EEPROM like cryptographic keys and PINs are automatically encrypted using DES algorithm with a unique secret key generated by the module using an Oberthur proprietary5 key generation algorithm.

In addition all EEPROM cells regardless of their content, are encrypted using a low level routine of the chip to protect against direct reading of the cells content. This mechanism is outside of the scope of this security policy.

8 Module Cryptographic Functions

The purpose of the cryptographic module is to provide a FIPS approved module for applets that may in turn provide cryptographic services to end-user applications. The keys represent the identity of the roles involved in controlling the module.

A variety of FIPS 140-2 validated algorithms are used in the ID-One Cosmo 128 v5.5 to provide cryptographic services. (see the FIPS Approved Security Functions section)

Some of these cryptographic services are made available only to applets and through Java APIs. Since the module described in this security policy does not include any instantiated applets other than the Card Manager and Security Domains, security services not used by either the Card Manager or by the Security Domain are not available to any of the current operator of the module.

The following describes cryptographic functions that are available to an operator as a service from the Card Manager, Security Domain and Applet.

- **2 Key TDES, (128):** The TDES (CBC mode) algorithm is used:
    - For authenticating the Crypto-Officer (EXTERNAL AUTH command)
    - For encrypting data flow from the off module to the on-module environment. The reverse direction is not encrypted; i.e. the status words returned in response to an APDU are not encrypted.
    - As a TDES MAC to authenticate the originator and to the verification the integrity of the message.

[5] This is not a FIPS approved implementation

TDES is also used to sign receipts from Delegated Management.

- **3 Key TDES, (192):** TDES (CBC mode) algorithm is used:
  - For authenticating the Crypto-Officer during PIN unblock request
  - For Application Operator for external authentication
  - During One Time Password operations

- **RSA (1024 up to 2048 bit keys):** RSA functions are provided as services to Card Manager (see Delegated Management below) and to Security domain (see the DAP Verification section below). Those keys lengths are also available at the Application Level (GC/PKI./SKI applet). RSA is also used with SMA protocol.

The module makes also use of the FIPS validated Random number generator (RND). Others cryptographic algorithms exposed by the smart card (section FIPS Approved Security Functions) are not called by the module.

8.1 Random Number Generators (RND)

The cryptographic module offers the services of a FIPS 140-2 approved DRNG (Deterministic Random Number Generator). The random generation algorithm has been validated to be compliant with the FIPS PUB 186-2 standard.

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 DRNG and increase its quality.

8.2 Delegated Management

The design of the Oberthur ID-One Cosmo 128 v5.5 module takes into account the possibility that the Card Issuer (Cryptographic Officer) may not necessarily want to manage all Card Content changes, especially when the Card Content does not belong to the Card Issuer. The concept of Delegated Management defined by Global Platform gives the Card Issuer the possibility of empowering partnered Applet Providers the ability to initiate approved and pre-authorized Card Content changes (loading, installation, extradition6 or deletion). This approval, which is central to the concept of Delegated Management, ensures that only Card Content changes that the Card Issuer (Cryptographic Officer) has authorized will be accepted and processed by the module. This delegation of control in the Card Content changes gives the Applet Provider more flexibility in managing its Application.

[6]Application Extradition allows an Application that is already associated with a Security Domain to be extradited and associated with another Security Domain

The Security Domain with the delegated management privilege allows making:

- Delegated loading (requires a pre-authorization)
- Delegated installation (requires a pre-authorization)
- Delegated extradition (requires a pre-authorization)
- Delegated deletion (no pre-authorization required)

The Delegated Management is based on the use of Token. A token is a cryptographic value provided by a Card Issuer (Cryptographic Officer) as proof that a specific Delegated Management operation has been authorized.

Delegated Management Tokens are RSA PKCS1 signatures of one or more Delegated Management functions and a hash of associated data (loading application code, installing Applications and extraditing Applications) generated by the Card Issuer (Cryptographic Officer) outside of the crypto module and transmitted to a user with Delegated Management privilege. The public RSA key KTOKEN, associated with the Crypto-Officer token signature private RSA key, must be present in the Card Manager.

When the User wants to perform the pre-authorized function, it appends to the function's data transmitted through a secure channel with its Security Domain inside the ID-One Cosmo 128 v5.5 Chip Platform the associated token. The User security domain will then decrypt and verify the secure channel communication using its ASK. The function and its associated Token are then automatically transmitted to the Crypto-Officer Card Manager for token verification using the Card Manager KTOKEN Public RSA key. If the signature is verified, the function is authorized to complete. Otherwise, it is aborted and cleared for memory.

The Card Issuer's security policy may require the generation of Receipts for Delegated Management operations. A Receipt is a cryptographic value (Triple DES signature on the receipt data) generated by the Card Manager KRECEIPT key to provide confirmation from the card that a successful card content management function has occurred through the delegated installation process. The Install Receipt is comprised of data related to the delegated card content management function including Card Unique Data generated by the Card Manager. The card manager also keeps track of a Confirmation Counter value that is incremented when generating each Receipt.

The receipt is computed by the Card Manager using the KRECEIPT, an ICV of binary zeroes and the signature method described in Global Platform 2.1.1, Appendix B.1.2.2 - Single DES Plus Final Triple DES MAC.

8.3 DAP Verification

If the Applet Provider does not have a Security Domain capable of Delegated Management to load application code to the card, it may rely on the loading services of the Card Issuer (Cryptographic Officer) and require a check of application code integrity and authenticity before the application code is loaded by the Crypto-Officer. Likewise, a Controlling Authority may mandate a check of application code integrity and authenticity before the application code is loaded, installed and made available to the Card Holder by the crypto-Officer or by a User with Delegated Management. The DAP Verification

privilege for a User Security Domain provides this service on behalf of an Applet Provider. The mandated DAP Verification privilege provides this service on behalf of a Controlling Authority.

The way it works is as follows: The user first computes a SHA-1 message digest of the application that is to be subsequently loaded into the module. He then uses his DAP RSA private key (matching the public key KDAP in the user security domain) to sign the previously calculated hash. The result, called DAP, is sent to the personalization entity together with the application code itself. When the application must be loaded into the card, the User Security Domain with DAP verification uses its DAP public key KDAP to check the DAP signature. The application code can be loaded into the module only if the verification succeeds.

9 Self Tests

9.1 Power Up 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 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
  - Triple DES – Encryption and decryption in CBC and ECB mode
  - AES – Encryption and decryption in CBC mode
  - SHA1 Hashing
  - SHA 256 Hashing
  - SHA 512 Hashing
  - RSA signature generation and signature verification
  - RSA Key wrapping and unwrapping
  - ECDSA signature generation and signature verification
  - 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", EMI etc, are also performed at this stage.

The module does not respond to any commands while 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 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.

9.2 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.

Elliptic Curve Key generation: After generating an ECC key pair, the module performs a pair wise consistency check to validate that the generated key pair is correct for signature and verification. 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. (Both Deterministic and Non Deterministic) RNGs. Other statistical testing is also performed to ensure the highest possible quality of the generated random numbers. Detailed description of the module Random Number Generator and associated tests is provided in a separate document (IRS).

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 be 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.

9.3 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.

10 Finite State Machine

The Open Platform Card Manager manages the states of the Java Card platform and applets life cycle. The cryptographic module has its Card Manager in OP-Secured phase when issued to a user.

The Finite State Machine diagrams applicable to the module are provided as separate documents (one for the module and one for the Applets).

11 Physical Security

The Oberthur ID-One Cosmo 128 v5.5 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 epoxy resin, that is resistant to commonly available solvents, is used to encapsulate the module into an opaque support.

The chip is usually in possession of the Card Security Controller or of the 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

12 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."

13 Operational Environment

It is the responsibility of the Cryptographic Officer to insure that only FIPS validated instances are created.

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable.

14 Security Rules

14.1 Approved mode of Operation

The ID-One Cosmo 128 v5.5 described in this security policy does not include any non-FIPS validated applet instances. As such, the cryptographic module is always in an approved mode of operation. The security services described in this document can be used to load any kind of applets into the ID-One Cosmo 128 v5.5 Java Card Chip Platform. However, it is the responsibility of the Cryptographic Officer to insure that only FIPS validated instances are created.

The FIPS approved mode of operation for the validation described in this Security Policy starts from the instantiation of the Card Manager and Security Domains and ends with the instantiation of any non-FIPS validated applets.

The Cryptographic Officer can determine whether the card is still in the FIPS validated configuration by authenticating to the Card Manager and issuing a Get Status command to list all the applications instances currently installed in the card. However, with Java card, an application can be given any AID (application Identifier) during instantiation, regardless of the identity of the underneath executable load file. To prevent a non FIPS approved applet to be instantiated and given the AID of an approved applet, Oberthur has implemented a special Get Status command that returns not only the AID given to the applet instance, but also, and more important, the AID and version number of the underlying executable load file (ie the binary of the applet being loaded on the card; Executable Load File AID and package version are found in the Actividentity Applet V2 for Extended PIV section). The Cryptographic Officer can then at any time check that only FIPS approved executable load files have been instantiated.

Additionally, the ACA Applet returns the FIPS Security Level (here FIPS L2) in which the module is running. This information is found in the ACA applet properties by sending the GET PROPERTIES command, reading tag 24.

14.2 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.

14.2.1 Cryptographic Officer Identification & Authentication

The operator that wishes to authenticate into the Cryptographic Officer Provider role must first identify him/herself by providing both information to uniquely select the Card Manager, and a Key Set ID. The authentication is then done by proving the possession of the particular keyset identified in the identification phase. This Key Set is composed of 3 TDES keys. One key is used to encrypt the

command data, one key to authenticate the user, and the third key is used to encrypt keys transported within the APDU command.

14.3 Applet Loading Security Rules

Applets can only be loaded through a secure channel; i.e. they pass from the off-module to the on-module environment in a MACed form. An additional applet encryption is also available as an option. To activate that option, the Cryptographic Officer would have to request the encryption option when opening the secure channel with the module.

In the ID-One Cosmo 128 v5.5 Chip Platform, the applet is always loaded by the Card Issuer (Cryptographic Officer). The optional mechanism designated as "DAP" in GP 2.1.1 enables the applet provider to check, independently of the Card Issuer (Cryptographic Officer), that his applet has been correctly loaded. This check is done by verifying a RSA PKCS #1 signature on the Hash of the applet code being loaded. This process is described in detail in the GP 2.1.1 document.

For the ID-One Cosmo 128 v5.5 to run in a validated FIPS 140-2 Level 3 mode of operation, all applet instances must be validated to the same level. Although any applet can be loaded during post issuance, it is the responsibility of the Cryptographic Officer to insure that only FIPS 140-2 Level 3 validated instances are created. Instantiation of non-validated applets within the FIPS 140-2 validated cryptographic module, or instantiation of a FIPS 140-2 validated applet with a different security level, will invalidate the original validation.

FIPS 140-2 Level 3 validated applets may be loaded and instantiated at post issuance.

14.4 Key Management Security Policy

14.4.1 Cryptographic key generation

TDES Session key derivation for Secure Channel Opening, conforming to Open Platform Card Specification v2.1 (SCP01) using FIPS186-2 approved ANSI X9.31 DRNG.

RSA key pair generations (up to 2048 bit key length) fully compliant with ANSI X9.31 and using a FIPS140-2 approved DRNG. Both standard RSA key and RSA Chinese Remainder Keys can be generated. This cryptographic service is made available through Java APIs only.

14.4.2 Cryptographic key entry

Keys shall always be input in encrypted format, using the Put Key (TDES or Public) command within a secure channel. During this process, the keys are encrypted using the Key Encryption Key and optionally the encryption session key of the secure channel.

Keys can never be output by the module.

14.4.3 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.

14.4.4 Key Destruction

The ID-One Cosmo 128 v5.5 destroys cryptographic keys by reloading another key-set with the same version number for Crypto-Officer/Card Security Controller Keys and User Keys, using the PUT **TDES KEY** or **PUT PUBLIC KEY** command.
User Keys can also be zeroized by deleting the Security Domain that hosts the keys, using the **DELETE** command.
Closing of the secure channel has also the effect of zeroizing the associated session keys stored in RAM memory.

Key zeroization is achieved by the Oberthur Garbage Collector that overwrites with binary zeros the deleted key value in its memory zone (whether in RAM or in EEPROM).

15 Mitigation of Other Attacks Policy

15.1 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.

15.2 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.

15.3 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 the section “Conditional Tests”.

15.4 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.

15.5 ElectroMagnetic Attacks

The Oberthur PIV EP card includes a combination of software and hardware protections in order to detect "EMI" type of attacks and abort any current processing before becoming mute.

16 Security Policy Check List Tables

16.1 Roles and required Identification and Authentication

Role	Type of Authentication	Authentication Data
Crypto-Officer/Card Security Controller (CSC)	TDES Authentication	TDES Keys (Crypto-Officer Security Domain)
Application Operator	AC External Authenticate protocol PUK verification	Application XAUT TDES key PUK
Card Holder	Verify service	PIN

16.2 Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
TDES Authentication	The strength of the authentication mechanism is equal to or greater than 80 bits. Therefore the probability that a random authentication attempt succeeds is less than 1 in 1,000,000.
RSA Authentication	The strength of the authentication mechanism is equal to or greater than 80 bits. Therefore the probability that a random authentication attempt succeeds is less than 1 in 1,000,000
PIN	2^{48} if PIN is encoded on 6 characters (each character uses 1 byte in the card)
PUK	2^{64}

16.3 Services Authorized for Roles

Role	Authorized Services

Crypto-Officer/Card Security Controller (CSC)	All Crypto-Officer Services are listed in the Services section.
Application Operator	All Application Operator Services are listed in the Services section.
Card Holder	All User Services are listed in the Services section.

16.4 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
Electro magnetic Interferences	Counter Measures against EMI	N/A

17 Cryptographic Algorithms

17.1 Cryptographic Algorithms

The following cryptographic services are provided by the ID-One Cosmo 128 v5.5 Java Card API along with the subset of algorithms used by the operators accessing the cryptographic module. In the future, other algorithms can be called by other applications loaded on the card; those applications will have to be FIPS140-2 as well (re-validation process to be involved).

The implementation of the following algorithms is fully compliant with JavaCard specifications:

Cryptography	Characteristics	Key size	Accessed by module operator	Remarks
Triple DES	Encrypt/decrypt operations ECB/CBC modes FIPS 46-3 compliant	112/ 168 bits	√	Single DES (Key size 56) is disabled during module manufacturing when the module is a validated FIPS module
MAC with Triple DES	MAC generation and verification (Triple DES in CBC mode)	112 bits	√	Triple DES triple length key is not supported in this version

Cryptography	Characteristics	Key size	Accessed by module operator	Remarks
RSA	Signature/verification operations CRT/SFM modes Key generation ANSI X9.31 compliant	1024/ 1280/ 1536/ 1792/ 2048 bits	√ (1024 / 2048)	The following key sizes can be enabled during module manufacturing when the module is not a validated FIPS module: 512/576/640/704/768/832/896/960/ 1088/1152/1216/ 1344/1408/1472/ 1600/1664/1728/ 1856/1920/1984 bits
Elliptic Curves ALG_ECDSA_SHA	GF(p) algorithm Signature/verification operations Key generation IEEE P1363-2000 compliant	192/ 224/ 256/ 384 bits		
Elliptic Curves DH (Diffie-Hellman) ALG_EC_SVDP_DH, ALG_EC_SVDP_DHC	key agreement algorithms IEEE P1363-2000 compliant	192/ 224/ 256/ 384 bits		
AES	Encrypt/decrypt operations ECB/CBC modes	128/ 192/ 256 bits		
RNG ALG_PSEUDO_RANDOM, ALG_SECURE_RANDOM	Base on HW True Random Number Generator FIPS 186-2 compliant		√	
ALG_SHA, ALG_SHA_256, ALG_SHA_384, ALG_SHA_512	Message Digest operations			SHA-1 SPA resistant

17.2 Additional Cryptographic Algorithms

The following algorithms are not part of JavaCard Specifications and therefore use an Oberthur Proprietary implementation. None of those algorithms are called by the module described here.

Cryptography	Characteristics
ALG_SHA_224 (0x08)	Message Digest operations
ALG_SHA_CHAIN (0x81)	
ALG_SHA2_CHAIN (0x82)	
Elliptic Curves ALG_ECDSA_SHA224(0x21)	GF(p) algorithm Signature/verification operations
Elliptic Curves ALG_ECDSA_SHA256(0x22)	
Elliptic Curves ALG_ECDSA_SHA384(0x23)	

ALG_ECDSA_SHA_LDS (0x25)	
ALG_ECDSA_SHA256_LDS(0x26)	
ALG_ECDSA_SHA384_LDS(0x27)	
Diffie-Hellman KEYAGREEMENT_ALGO_RSA(0x81)	Key Agreement Operations
Diffie-Hellman ALG_EC_SVDP_DH_GK (0x82)	
Diffie-Hellman ALG_EC_SVDP_DHC_GK (0x83)	
Non-Deterministic Random Number Generator (NDRNG)	Hardware Seed Generation for the Deterministic RNG
Oberthur proprietary key generation algorithm	Key Generation for non FIPS approved encryptions

18 Applicable Documents

- "Java Card 2.2.2 - API"
  Application Programming Interfaces Version 2.2.2 March, 2006, Sun Microsystems
- "Java Card 2.2.2 – JCRE "
  Runtime Environment Specification Version 2.2.2 March, 2006, Sun Microsystems
- "Java Card 2.2.2 - Virtual Machine Specifications"
  Version 2.2.2 March, 2006, Sun Microsystems
- "Global Platform 2.1.1"
  Card Specification v2. 1, 01 Mars 2003
- ISO/IEC 7816-3 (2006)
  Identification cards - "Integrated circuit(s) cards with contacts - Part 3 Electronic signal and transmission protocols."
- ISO/IEC 7816-4 (2005)
  Identification cards - "Integrated circuit(s) cards with contacts - Part 4: Inter industry commands for interchange."
- ISO/IEC 7816-5 (2004)
  Identification cards - "Numbering system and registration procedure for application identifiers"
- EMV 2000
  "Integrated Circuit Card Specifications for Payment Systems"
  - 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)

- "Java Card 2.2 Biometry API proposal "
  Javadoc version (4-4-02) on JCF web site
- ISO/IEC 14443-3 (2001-02-01)
  "Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision"
- ISO/IEC 14443-4 (2001-02-01)
  "Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol"
- [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.

19 Definitions and Acronyms

19.1 Definitions

19.1.1 Card Manager

The Card Manager, also called Issuer Security Domain, is the on-card representative of the Card Issuer (Cryptographic Officer). It is the most privileged entity of the cryptographic module as it is the only entity that performs Card Content management without having been explicitly delegated previously. Privileges of the Card Manager include but are not limited to card locking, card termination and CVM (Card Holder Verification Method) management.

The Issuer Security Domain shall have the following set of privileges clearly identifying its functionality (i.e. a Security Domain with card lock, card terminate and CVM management privileges and possibly the Default Selected privilege) in addition to its implied unrestricted Card Content management privilege.

19.1.2 Security Domains

Security Domains allow a number of distinct identities to be established on the ID-One Cosmo 128 v5.5 Chip Platform. These are identities that control access to the various applets stored on the module. A Security Domain represents the identity of an application (applet) operator.

19.1.3 Applets

"Applets" are applications that can be executed on the Chip Platform. They come in two parts; the applet executable code, which defines all the functions that could be executed on the Chip Platform, and the Applet Instance, that provides the environment (i.e. variables) and an interface to the functions present in the applet executable code. An applet can have several instances, each with its own variables, but all sharing the same functionality as defined in the underlying executable code. The Applet Instance is the mandatory communication path between the applet Executable Module and the outside world.

In order for an application to be activated and provide its high level services to the outside world, two prerequisites must have been fulfilled:

- The Applet Executable Load File, that contains the actual Java code (Executable Module) of the application, must be present on the Chip Platform. This can be achieved by physically downloading the load file into the Chip Platform EEPROM, or by activating a pre-loaded Executable Load File present in ROM.
- At least one applet instance of the executable module must have been created.

The services described in this Security Policy allow the security officer to load and unload (delete) any applets. This allows the loading of executable load files, which can take up to 30 seconds depending of the size of the file, to take place during pre-issuance. Until the time they are instantiated, the executable load files can be considered as "dead code". The actual applet activation, which is done through instantiation, takes only a few milliseconds and could take place in post issuance, under the control of the Security Officer, and after the applet has been FIPS 140-2 validated.

For the cryptographic module to be correctly operated according to this Security Policy, applets instantiated into the Chip Platform must be validated to FIPS 140-2.

19.2 Acronyms

AES	Advanced Encryption Standard
AID	Application Identifier
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
BAP	Batch Approval Process (First article validation from Production line)
CBC	Cipher Block Chaining
CRC	Cyclic Redundancy Check
CSP	Cryptographic Security Parameter
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
HCL	Hardware Compatibility List
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
ISO	International Standard Organization
JC	Java Card ™
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
OP	Open Platform
OTP	One Time Password
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PUK	PIN Unblocking Key
RAM	Random Access Memory
RND	Random Number Generator (Non Deterministic and Deterministic)
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
WHQL	Microsoft Windows Hardware Quality Lab