Oberthur
ID-One Cosmo 64 v5.4 D

FIPS 140-2 Level 3

Security Policy

Public Version

Version 1.0

May 22, 2007

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

Version Control

Table 1 shows the version history of this Security Policy.

Version - Date	Description
V1.0 – May 22, 2007	Initial Release

Table 1 - Document Version History

TABLE OF CONTENTS

1 Introduction

This document defines the Security Policy for the Oberthur Card Systems ID-One Cosmo 64 v5.4 D Java Card platform submitted for validation in accordance with FIPS 140-2 Level 3 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

2.1 Product Overview

The ID-One Cosmo 64 v5.4 D Java Card platform, hereafter referred to as the module, is a single chip multi-application Smart Card micro-controller, with up to three communication interfaces (contact ISO 7816, Contact USB 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 2.2.1 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.

The module offers a highly secure architecture with on board cryptographic services such as Triple DES (128 and 192), AES (up to 256 bits), RSA (up to 2048) with a true ANSI X9.31 on-board key generation, ECDSA, SHA-1 & SHA-256, ISO 9796, ISO 9797, PKCS#1.5, OAEP, PSS, FIPS 186-2 Random Number Generator, etc.

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 platform to support multiple applications simultaneously, each with their own Security Domain.

The ID-One Cosmo 64 v5.4 D 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/or USB) 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.

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, a USB token or into an electronic passport, the ID-One Cosmo 64 v5.4 D 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).

2.2 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.

2.3 Cryptographic Algorithms

The following cryptographic services are provided by the ID-One Cosmo 64 D v5.4 D Java Card API.

- Triple DES encryption and decryption (ECB & CBC modes) using 128-bit and 192-bit key sizes:
  - In Raw mode (no formatting)
  - With formatting and padding automatically added by the card OS:
    - ISO/IEC 9797 padding, methods 1.
    - ISO/IEC 9797 padding, methods 2.
- Triple DES Message Authentication Code generation and verification:
  - In Raw mode (no formatting)
  - With formatting and padding automatically added by the card OS:
    - ISO/IEC 9797 padding methods 1,
    - ISO/IEC 9797 padding methods 2,
    - ISO/IEC 9797 padding methods 2 with MAC algorithm 3,

- AES[1] encryption and decryption (ECB & CBC modes) using 128, 192 and 256-bit key sizes,
- AES Message Authentication Code generation and verification,
- ANSI X9.31 RSA key generation (up to 2048-bit key size)
- RSA key Wrapping/Unwrapping:
  - In Raw mode (no formatting)
  - With formatting and padding automatically added by the card OS:
    - PKCS#1 padding,
    - PKCS#1-OAEP padding,
- RSA signature and verification:
  - In Raw mode (no formatting)
  - With message formatting and padding automatically added by the card OS:
    - PKCS#1 padding,
    - PKCS#1-PSS padding,
    - ISO/IEC 9796 padding,
- SHA-1 digest computation
- SHA-256 digest computation
- FIPS 186-2 RNG
- ECDSA Key Generation GF(p) from 161 to 192[2]
- ECDSA Signature generation and verification[3]

Please be aware that in this FIPS configuration, there are no applets to exercise cryptography besides the Security Domains. As a result the only available service which utilizes the RSA algorithm is one that uses a 1024 bit RSA public key for DAP verification, and no services use AES, ECDSA, or Triple DES with on card formatting.

[1] AES is available only in firmware version E910-065972
[2] ECDSA is available only as prototype and cannot be run as a FIPS Approved algorithm in this module because an ECDSA KAT is not performed
[3] See previous footnote

2.4 Product Form Factors

The module is designed to be encased in a hard opaque resin which can be embedded into different form factors such as a plastic card, a USB token, an Electronic Passport, or any other support to produce the ID-One Cosmo 64 v5.4 D Java Card Chip Platform, on which FIPS 140-2 Level 3 validated applets may be loaded and instantiated at post issuance.

The photo, Figure # 1, shows an example of the module in its opaque resin.

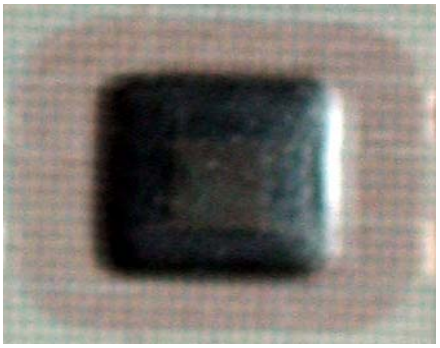


Figure 1

The module, after encapsulation into its opaque tamper resistant resin, can be embedded into different form factors, such as a smart card, a token, or a paper document.

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

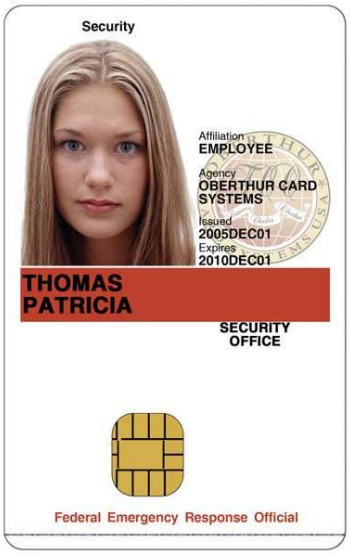


Figure 2:
Module embedded into a
PIV Dual Interface Smart Card

Figure 3:
Module embedded into a
PIV Contactless & USB Token.
Includes a smaller antenna for contactless communications and replaces the golden contact plate with a USB plug to remove the need of a smart card reader.

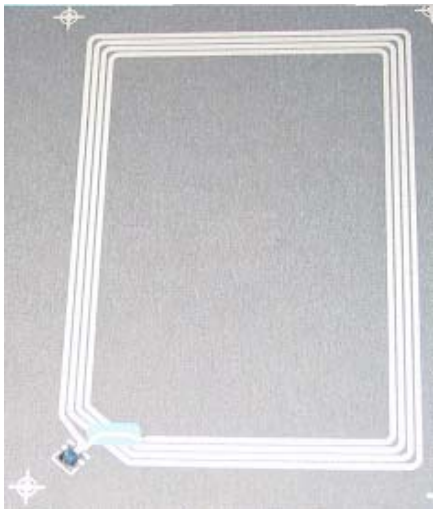


Figure 4:
Module embedded in the
cover of an **e-Passport**

2.5 Product Terminology

In the remaining of this document, the cryptographic module described above will be referred indifferently as ID-One Cosmo 64 v5.4 D or as module, regardless of whether the form factor is a actually a smart card module, a full ID-1 smart card, a USB token, an e-Passport book cover or any other form factor Oberthur may come up with to answer specific market needs.

3 Security Level

The Oberthur ID-One Cosmo 64 v5.4 D meets the overall requirements applicable to Level 3 security of FIPS 140-2.

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

Table 2 - Module Security Level Specification

4 Cryptographic Module Specifications

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 64 v5.4 D 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
  - A Triple DES (Data Encryption Standard) Co-Processor
  - An AES (Advanced Encryption Standard) Co-Processor
  - High reliability 72 KB EEPROM for both customer applications and Operating System data
  - System firmware, consisting of the operating system installed in Read Only Memory (ROM)
  - Optional Code as identified in section 4.2 Module Hardware
- Applets (Applications) that are to be installed onto the module.
- Critical Security Parameters stored in EEPROM as part of the Chip Platform personalization operation.

The following figure demonstrates a logical block diagram of the module.

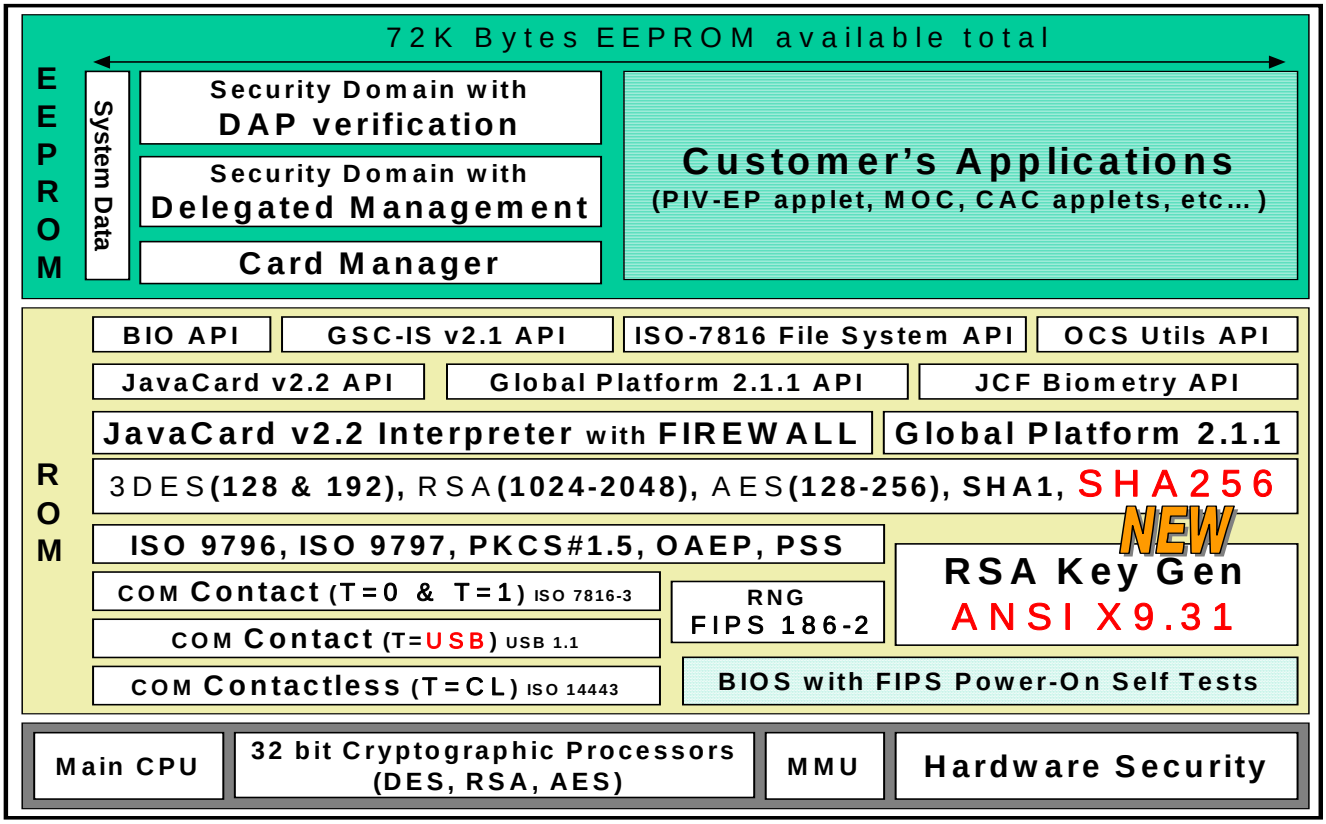


Figure 5: Logical Block Diagram of the Oberthur ID-One Cosmo 64 v5.4 D

4.1 Target of Validation

This document addresses the submission for validation of the module in accordance with FIPS 140-2 Level 3 standard.

The module submitted for validation consists of the ID-One Cosmo 64 v5.4 D Chip Platform without any instantiated applet other than the Card Manager (CM) and built-in Security Domains (SD).

This validation is aimed at the Systems software, virtual machine, and Card Manager/Security Domains applets without any other instantiated applets.

Instantiating a (security relevant) applet will require a re-validation and the issuance of a new certificate, even if the applet itself was validated to FIPS 140-2.

In the scope of this document, the cryptographic module is a single chip Integrated Circuit with its embedded firmware. It is designed to be encased in a hard opaque resin which can be embedded into different form factors such as a plastic card, a USB token, an Electronic Passport, or any other support to produce the ID-One Cosmo 64 v5.4 D Java Card Chip Platform, on which FIPS 140-2 Level 3 validated applets may be loaded and instantiated at post issuance.

The "Cryptographic Boundary" for the ID-One Cosmo 64 v5.4 D 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.

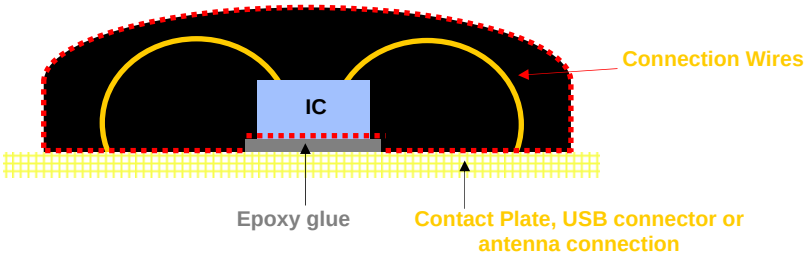


Figure 6

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 Module Hardware

The Integrated Circuit used for the ID-One Cosmo 64 v5.4 D is identified by its part number 77. Part number 77 comes in different customizations depending on the communication interface(s) needed by the end customer (i.e. ISO 7816 contact, ISO 14443 Contactless, and USB). This Security Policy applies to hardware part number 77, regardless of the communication interfaces that have been activated on the Integrated Circuit.

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

4.3 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 64 v5.4 D is E910

Module hardware can be read from the Card Identification Data Object under tag 00.

4.4 Module Firmware Extensions

The ID-One Cosmo 64 v5.4 D functionality can be extended through the use of a firmware extension called optional code. Such optional code 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 support for additional cryptographic algorithms, WHQL, additional biometric match on card algorithms, etc.

Module Firmware Extension can be read from the Card Identification Data Object under tag 03.

This document addresses the submission for validation of the module “ID-One Cosmo 64 v5.4 D” with any one of the following firmware Extensions (These firmware extensions cannot be combined on the module, so only one value shall be returned under tag 03 of the Card Identification Data Object):

Firmware Extension (only one value authorized)	**Note**
066491	Basic configuration, FIPS
065972	FIPS + AES Support
066421	FIPS + WHQL[4] USB interface

Table 3: Firmware Extensions included in this validation

4.5 Locks configuration

The ID-One Cosmo 64 v5.4 D includes several locks that can be set by Oberthur during the manufacturing phase to put the module in a specific electrical configuration. Such locks are primarily used to activate a low power consumption mode, enable elliptic curve cryptography, or disable a communication interface (USB, Mifare, ISO14443) when that mode is not needed by the customer. But these locks can also be used to disable some of the features of the module operating system for prototyping and test purposes.

For the module to be in FIPS mode, there is only two locks that need to be checked:

- FIPS lock that enables FIPS specific security features: That lock must be set to 00 to enable all FIPS checks.
- CVM lock that enables restriction on the length of the Global PIN: That lock must be set to 'F9' to set the Global PIN minimal length to 6 digits.

Lock configuration can be read from the Card Identification Data Object under tag 02. The return value to check for FIPS mode should be: XX **00 F9** XX XX XX XX

4.6 Module Identification

Module identification and configuration (complete firmware version, including optional code extension as well as the status of the locks set during module pre-issuance that allow to activate FIPS mode) can be retrieved at any time using the Get Data services as described in section 6.2.3. The associated tag is 'DF52' and the return value includes a TLV structure with the above tags. Other tags may be returned as well but are outside the scope of this validation.

[4] The version of USB interface provided by this firmware extension has been submitted to Microsoft Windows Hardware Quality Labs (WHQL) for participation in the Windows Logo Program. Successful passage of the WHQL tests results in both the "Designed for Windows" logo and a listing on the Microsoft Hardware Compatibility List (HCL).

4.7 FIPS Approved Security Functions

The following table gives the security functions that have been FIPS certified on the ID One Cosmo 64 D v5.4.

Security Function	Details	FIPS Certification #
2 Key Triple DES (128)	ECB Mode in Encryption	**454**
	ECB Mode in Decryption	
	CBC Mode in Encryption	
	CBC Mode in Decryption	
3 Key Triple DES (192)	ECB Mode in Encryption	**455**
	ECB Mode in Decryption	
	CBC Mode in Encryption	
	CBC Mode in Decryption	
AES 128	ECB Mode in Encryption	**425**
	ECB Mode in Decryption	
	CBC Mode in Encryption	
	CBC Mode in Decryption	
AES 192	ECB Mode in Encryption	
	ECB Mode in Decryption	
	CBC Mode in Encryption	
	CBC Mode in Decryption	
AES 256	ECB Mode in Encryption	
	ECB Mode in Decryption	
	CBC Mode in Encryption	
	CBC Mode in Decryption	
SHA-1	Byte-oriented messages	**496**
SHA-256	Byte-oriented messages	
RNG	FIPS 186-2	**219**
RSA (Modulus sizes: 1024, 1536 and 2048)	GenKey 9.31	**160**
	SigGenPKCS1.5	
	SIgGenPSS	
	SigVerPKCS1.5	
	SigVerPSS	
ECDSA (P-192)	Key Pair Generation	**32**
	SigGen	
	SigVer	

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 either a smart card contact plate or a USB connector. Contacless communication is achieved through physical connection to an antenna. Neither the contact plate, the USB connector, 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 7816-2 (Dimensions and contact location) smart card contact plate (printed circuit) that provides the electrical connection required by ISO 7816-3 (Electrical interface and transmission protocols). 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.

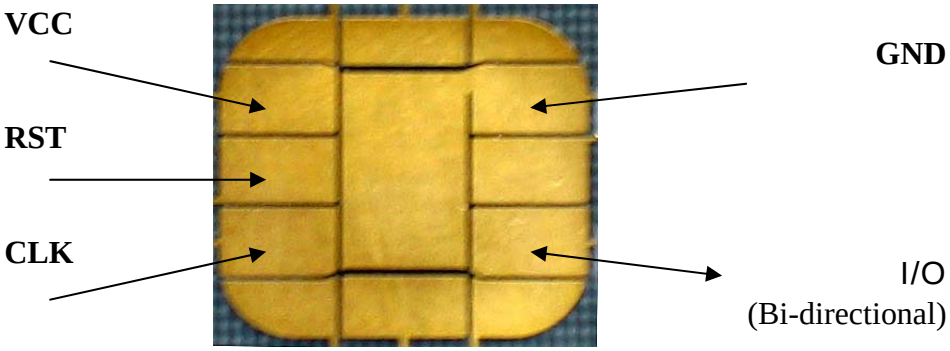


Figure 7: Example of an ISO 7816-2 complaint contact plate used to provide ISO 7816-3 electrical communications with the cryptographic module

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

- **VCC**: Supply Voltage Power supply input. (1.62V to 5.5V)

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

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

5.1.3 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 maximum communication speed in contact mode is **614,400 bits/sec** (with an external clock of 4.9Mhz) as per ISO 7816-3: 2006.

The maximum communication speed can be reduced at manufacturing stage to meet the capabilities of the customer existing infrastructure (Card readers).

5.1.3.4 Transmission protocol

The transmission protocol complies with ISO/IEC 7816-3

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 USB or

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.

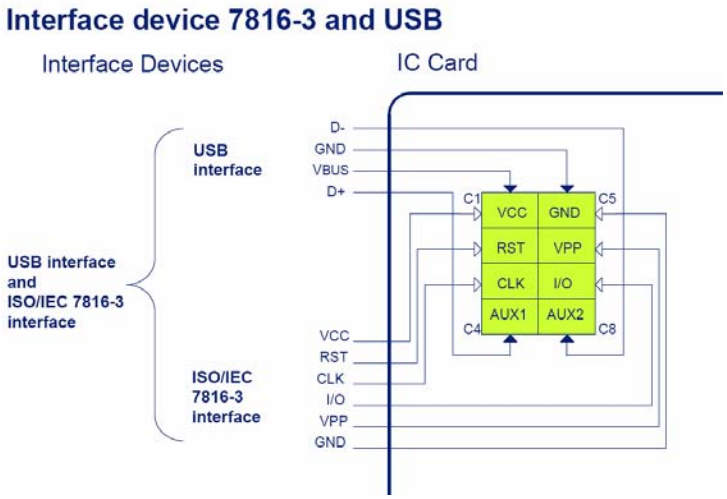
Characters can be exchanged in direct convention (Z level corresponds to a logical 1 and LSB is sent first) or in inverse convention (Z level corresponds to a logical 0 and LSB is sent first).

The Oberthur ID-One Cosmo 64 D v5.4 D supports the Protocol and Parameter Selection to select a new protocol type or change transmission baud rate.

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

5.1.4 7816-3 and USB Contact Plate

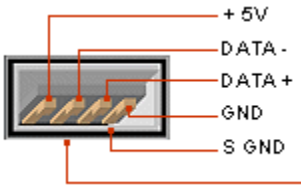
The printed Circuit can support both 7816 and USB interfaces. In this case two additional signals, AUX1 and AUX2 are wired to the contact plate to carry USB data signals D- and D+. The power supply and ground connections are shared between the 7816-3 and USB interfaces.



5.2 Physical Port: USB connector

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

5.2.1 Interface Electrical Specifications



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

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

D- and D+ connections are physically different and distinct from the connections used to transfer signal in contact plate interface used or in contactless interface.

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

5.2.2 Transmission protocol and speed

The APDU-TPDU transmission protocol is similar to the one defined for ISO/IEC 7816-3 T=1 (half duplex block oriented transmission protocols).

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

5.3 Physical Port: Contactless Mode

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

5.3.1 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.

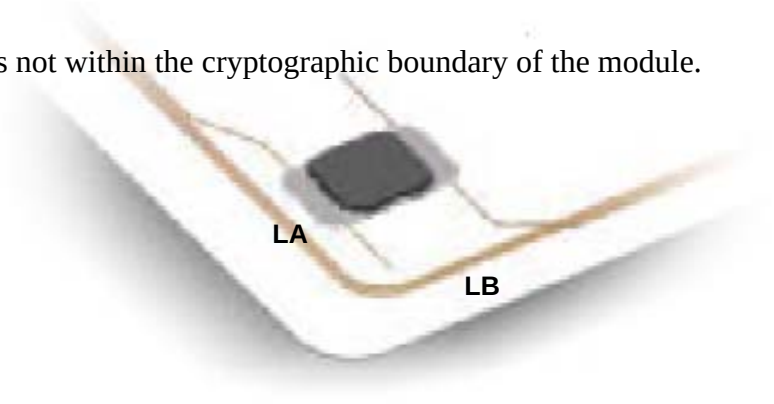


Figure 8: Example of connection of the cryptographic module to the antenna for a contactless mode.

5.3.2 Interface Electrical Specifications

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

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

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

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

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

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

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

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

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 standard.

5.3.3 Condition of use

5.3.3.1 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

5.3.3.2 Frequency

The module nominal frequency for contactless communication is 13.56 MHz

5.3.3.3 Speed

The supported bit rates of the Oberthur ID-One Cosmo 64 v5.4 D are:

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

5.3.3.4 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.

5.4 Logical Interface Description

Once communication is established between the reader and the platform, the platform functions as a "slave" processor to implement and respond to the reader commands. The platform adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible. The I/O ports[5] of the platform (either physical in contact mode or virtual in the case of RF transmission) provide the following logical interfaces:

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

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

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

5.4.1 APDU Commands

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

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

5.4.2 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 & Services

6.1 Roles

The module defines two distinct roles that are supported by the internal cryptographic system: the Card Security Controller (CSC) and the Applet Provider (AP).

6.1.1 Cryptographic Officer Role

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

6.1.2 User Roles

- ***Applet Provider (AP) Role*** – The Applet Provider is the applet developer that uses the Java API, available on the module. The developer is regarded as an internal user to the platform. The cryptographic services provided by the module are delivered through the use of well-documented APIs. An applet can have a dedicated security domain instance (Applet Provider Security Domain), or may rely on the Card Manager Security Domain.

6.1.3 Identity based Authentication

- ***Identification***. The operator identifies him/herself by selecting the application and a key set associated with the application. The application of the Cryptographic Officer is the Card manager. The application of the applet providers is their own applet. The selection of the application is done by a SELECT command. The selection of the key set is done through the INITIALIZE UPDATE command. (The same command that will be used to start the authentication that follows the identification.)

- ***Authentication***. The operator authenticates him/herself using a mutual authentication comprising two commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATION. During this mutual authentication, the operator has to encrypt a message sent by the card, proving knowledge of the TDES key set that was referenced during the identification.

Each INITIALIZE UPDATE must be immediately followed by a successful EXTERNAL AUTHENTICATE command. Otherwise, the event is recorded in the card Audit Log and the next Initialize Update performed on the same key set will be exponentially slowed down to discourage attacks. This provides a strong protection against brute force attacks as no more than a few consecutive unsuccessful authentication attempts are possible within one minute.

The authentication remains valid until the next Identification phase (SELECT command) or until an unsuccessful authentication or a card reset (power-off) has been initiated.

Please refer to section 16.2 “Strength of Authentication Mechanisms” for information on the strength of authentication.

6.1.4 Logical Channels

The module provides a full support for Logical Secure Channels as defined by GP2.1.1. Secure channel protocol is used to establish a secure communication channel between the module and an external entity during an Application Session.

Logical Channels facilitate the possibility of more than one of the above external entities to communicate concurrently with multiple applications on the card, each within its own logical secure environment.

6.2 Services

6.2.1 Cryptographic Officer Services

Several services are made available to an authenticated Cryptographic Officer 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 remains in FIPS mode, this command shall not be used to load non FIPS approved executable code.
- ***DELETE:*** this APDU is used by the CSC role to delete an application from the cryptographic module. Load File (package) or an applet (applet instance).
- ***PUT TDES KEY:*** this APDU is used to add or replace security domain key sets (TDES). Keys are loaded protected by the double encryption of the global Platform Secure Channel and a KCV is included in the transmission to ensure integrity of the key loading operation.
- ***PUT PUBLIC KEY***: this APDU is used to load RSA public keys such as the Token Verification Key or the DAP Verification Key. These keys are used for Delegated Management and DAP verification as specified by Global Platform.
- ***STORE DATA:*** This command is used by the CSC to clear the audit log and load Data Objects at the platform level.
- ***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 FIPS Mode and that only FIPS approved applications are instantiated.

- ***INITIALIZE UPDATE***: this APDU is used by the CSC to exchange with the crypto module data needed to establish the session keys and initiate a GP Secure Channel with a given Security Domain in the crypto module.

- ***EXTERNAL AUTHENTICATE***: this APDU is used by the CSC to authenticate to the crypto module and to finalize the establishment of the GP Secure Channel by providing the level of security required for all subsequent commands within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.

- ***DELEGATE MANAGEMENT***: Delegated Management gives a CSC the possibility of empowering another CSC the ability to initiate approved and pre-authorized Card Content changes (loading, installation, extradition or deletion) on his behalf.

- ***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 Secure Messaging in the context of a Secure Channel; its level of security must so match the security level of the current Secure Channel.
- **All Services under "No Role"**

6.2.2 User Services

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

- ***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.
- **STORE DATA**: This command is used to load Data Objects in the selected application.
- ***SET STATUS***: This APDU is used to temporary lock an application, and unlock it later on. It can also be used to terminate the application.
- ***GET STATUS:*** this APDU is used to get the life cycle state of an application.
- ***INITIALIZE UPDATE***: this APDU is used 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 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.

- ***DAP VERIFICATION**:* DAP verification allows an Application Provider (User) to own a Security Domain which can be requested to check application code integrity and authenticity before the application code is loaded by the Crypto-Officer or any entity other than the Application Provider itself. More details on how DAP verification works can be found in the product manual.
- **All Services under "No Role"**

6.2.3 No Role

The following services are available without authentication

- ***MANAGE CHANNEL**:* This 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.
- ***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 other 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.

6.2.4 Relationship between Roles, Services and CSP Access

Roles/Services	CSC	AP	No Role	CSP[6] involved		CSP Access type
				From CSC	From AP	
INSTALL	X			CSK		Execute
LOAD	X			CSK		Execute
DELETE	X			CSK		Execute
PUT TDES KEY	X	X		CSK, CDK	ASK, ADK	Execute, Write
PUT PUBLIC KEY	X			CSK, $\mathbf{K}_{TOKEN,}$ $\mathbf{K}_{DAP}$		Execute, Write
STORE DATA	X	X		CSK	ASK	Execute
SET STATUS	X	X		CSK	ASK	Execute
GET STATUS	X	X		CSK	ASK	Execute
INITIALIZE UPDATE	X	X				
EXTERNAL AUTHENTICATE	X	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	X	X			
GET DATA			X			
SELECT	X	X	X			

[6] See Section 7for further CSP pointer details.

7 Cryptographic Key Management

The cryptographic module handles various keys and a PIN

- Global PIN
- Card Manager and Security Domain Keys

7.1 Global PIN

The Global PIN (Personal Identification Number) supported by the ID-One Cosmo 64 v5.4 D can be a sequence from 6 to 254 digits, or a passphrase of 127 characters max (any characters that could be coded in hexa on one byte). It may be used through a standard GP 2.1.1 API to authenticate the future Cardholder to the module with a probability of false authentication of less than 1/1,000,000. By successfully entering a PIN sequence, a cardholder 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 lock 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 Cryptographic Keys

The ID-One Cosmo 64 v5.4 in FIPS mode (i.e. in Card Manager OP-Secured) includes the following keys that conform to Global Platform Specifications v2.1:

7.2.1 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.

7.2.2 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. $\mathbf{K}_{RECEIPT}$**:** Key Receipt: Triple DES Key (16 bytes) used to compute a receipt on Delegated Management Commands. See Delegated Management in section 8.1.2. 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.

7.2.3 User/Applet Provider 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. $\mathbf{K}_{DAP}$: 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 section 8.1.3 on DAP verification). This key may or may not be loaded into the module. It is an added feature and is not intended to satisfy any of the FIPS 140-2 requirements for applet loading. This key is present only in Security

Domain with DAP Verification. More information on how this key is used can be found in section 8.1.3 DAP Verification.

7.2.4 Keys Exchange

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

The values of the root secrets used to retrieve a module unique CDK, (with optionally $\mathbf{K}_{\text{RECEIPT}}$) and ADK are securely exchanged between Oberthur production HSM and respectively the Cryptographic Officer HSM and the User/applet provider HSM using a well defined and highly secure key ceremony described in a separate document.

The values of the RSA public Keys $\mathbf{K}_{\text{TOKEN}}$ and $\mathbf{K}_{\text{DAP}}$, are provided respectively by the Cryptographic Officer and the User/applet provider 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 sessions keys.

7.2.5 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 PUT3KEY 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/Applet provider 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 PUT3KEY 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.

7.2.6 EEPROM encryption Key

A higher level of protection against attack is provided through the encryption with TDES_CBC of the EEPROM content. This is done in an automated and transparent way by the module operating system

using a special Triple DES key called LSK. LSK is a 16 byte TDES key. The LSK is entered during wafer manufacturing by the silicon vendor and is not updatable, and not zeroizable.

8 Card Cryptographic Functions

The purpose of the cryptographic module is to provide a FIPS approved platform 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 64 v5.4 D to provide cryptographic services. (see section 4.7 FIPS Approved Security Functions)

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 or a Security Domain.

- **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 TDESMAC to authenticate the originator and to the verification the integrity of the message.

  TDES is also used to sign receipts from Delegated Management.

- **RSA (1024 up to 2048 bit keys)[7]:** RSA functions are provided as services to Card Manager (see Delegated Management below) and to Security domain (see section 8.1.3 DAP Verification below)

8.1.1 Random Number Generators

The cryptographic module offers the services of a FIPS 140-2 approved DRNG (Deterministic Random Number Generator). The random generation algorithm has been certified 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.

[7] In this FIPS configuration, without an application (applet) loaded, the only available service which utilizes the RSA algorithm is one that uses an RSA public key for DAP verification (see section 10.2.3, DAP VERIFICATION). As a result, the use of RSA for encryption, decryption, key wrapping and unwrapping, is not available in this module.

8.1.2 Delegated Management

The design of the Oberthur ID-One Cosmo 64 v5.4 D 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 Application Providers the ability to initiate approved and pre-authorized Card Content changes (loading, installation, extradition[8] 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 Application Provider more flexibility in managing its Application.

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 $\mathbf{K}_{TOKEN}$, 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 64 v5.4 D 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 $\mathbf{K}_{TOKEN}$ 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 $\mathbf{K}_{RECEIPT}$ 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

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

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 $\mathbf{K}_{\text{RECEIPT}}$, 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.

8.1.3 DAP Verification

If the Application 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 Cardholder 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 Application 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 $\mathbf{K}_{\text{DAP}}$ 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 $\mathbf{K}_{\text{DAP}}$ 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[9] – Encryption and decryption in CBC mode
  - SHA1 Hashing
  - SHA 256 Hashing
  - RSA signature generation and signature verification
  - RSA Key wrapping and unwrapping
  - Deterministic Random Number Generator (DRNG)
- Critical Function Tests
  - CRC-16 KAT
  - RAM functional test
  - Sensor bit test
  - Audit log scan
  - Resident applet life cycle

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

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

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

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

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.

Random Number Generators: Continuous testing is performed on every output of the Random Number Generators. Checks on the non-deterministic (Hardware) component are made on 16 bits and

[9] AES is available only in firmware version E910-065972

checks on deterministic part (FIPS approved) are made on 160 bits. Description of the implementation of this test is provided in a separate document.

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

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

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

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

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 platform 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 a separate document.

11 Physical Security

The Oberthur ID-One Cosmo 64 D v5.4 D is a single chip cryptographic module. It is designed to meet FIPS 140-2 Level 3 requirements for physical security.

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

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

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

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

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

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

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

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

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

During the manufacturing process, any applet executable load file can be loaded into the ID-One Cosmo 64 D v5.4 D Java Card platform, but those files remain dead code until activated through an instantiation process, and only trusted (FIPS validated) applets can be instantiated.

After completion of the manufacturing process (including pre-issuance), when the chip has reached its normal Operating Life Cycle State (Card Manager in Secured State), 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 therefore not applicable.

14 Security Rules

14.1 Approved mode of Operation

The ID-One Cosmo 64 D v5.4 D 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 64 v5.4 D 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 FIPS mode 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. The Cryptographic Officer can then at any time check that only FIPS approved executable load files have been instantiated.

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 User Identification and Authentication

The operator who wishes to authenticate into the User/Applet Provider role must first identify him/herself by providing both an application identifier 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. This is the same process as the Crypto-Officer authentication (Initialize Update & External Authenticate commands) but it uses the TDES keys of the Applet Provider Security Domains.

14.2.2 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. This is the same process as the User authentication (Initialize Update & External Authenticate commands).

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 64 v5.4 D platform, the applet is always loaded by the Issuer (Cryptographic Officer). The optional mechanism designated as “DAP” in GP 2.1.1 enables the applet provider to check, independently of the Issuer (Cryptographic Officer), that his applet has been correctly loaded. This check is done by verifying an 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. See section 17 Applicable Documents.

For the ID-One Cosmo 64 v5.4 D 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 64 v5.4 D destroys cryptographic keys by reloading another key-set with the same version number for Crypto-Officer Keys and User/Application Provider Keys, using the **PUT TDES KEY** or **PUT PUBLIC KEY** command.

User/Application Provider 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 section 9.2 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.

16 Security Policy Check List Tables

16.1 Roles and required Identification and Authentication

Role	Type of Authentication	Authentication Data
Crypto-Officer	TDES Authentication	TDES Keys (Crypto-Officer Security Domain)
User/Applet Provider	TDES Authentication	TDES Keys (User/Applet Provider Security Domain)

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

16.3 Services Authorized for Roles

Role	Authorized Services
Crypto-Officer	All Crypto-Officer Services are listed in section 6.2.
User/Applet Provider	All User/Applet Provider Services are listed in section 6.2.

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

17 Applicable Documents

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

- "Numbering system and registration procedure for application identifiers" ISO/IEC 7816-5 (1994), ISO/IEC 7816-5 AMD1 (1996)
- “Information technology – Security techniques – Digital signature scheme giving message recovery - Part 2: Mechanism using a hash function.” ISO/IEC 9796-2 (1997)
- “Information technology – Security techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher” ISO/IEC 9797-1 (1999)
- Contactless integrated circuit(s) cards – Proximity cards — Part 2: Part 2: Radio frequency power and signal interface, ISO/IEC 14443-2 (2001)
- Contactless integrated circuit(s) cards – Proximity cards — Part 3: Initialization and anti-collision, ISO/IEC 14443-3 (2001)
- Contactless integrated circuit(s) cards – Proximity cards — Part 4: Part 4: Transmission protocol, ISO/IEC 14443-4 (2001)
- "Integrated Circuit Card Specifications for Payment Systems" – EMV 2000
    - Part 1: Electromechanical Characteristics, Logical Interface, and Transmission Protocols (version 3.0)
    - Part 2: Data Elements and Commands (version 3.0)
    - Part 3: Application Selection (version 3.0)
    - Part 4: Security Aspects (Version 3.0)
- "API File System Library" Ref: 055731 00 SRS revision-issue 1-AA, Oberthur Card Systems
- "API Utils File System" Ref: 055901 00 SRS revision-issue 1-AA, Oberthur Card Systems
- "Java Card 2.2 Biometry API proposal" Javadoc version (4-4-02) on JCF web site
- "Format des templates biométriques" FQR 110 1767 Ed 1, Oberthur Card Systems

18 Definitions and Acronyms

18.1 Definitions

18.1.1 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, CVM (Card Holder Verification Method) management, and multiple selections (through logical channels).

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. If the card supports Supplementary Logical Channels, the Issuer Security Domain shall also have the multiple selection privilege.

18.1.2 Security Domains

Security Domains allow a number of distinct identities to be established on the ID-One Cosmo 64 v5.4 D 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.

18.1.3 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:

1. 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.
2. 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.

18.2 Acronyms

- AES Advanced Encryption Standard
- AID Application Identifier
- AP Application Provider
- APDU Application Protocol Data Unit
- API Application Programming Interface
- ATR Answer To Reset (contact mode)
- ATS Answer to Select (contactless mode)
- API Application Programming Interface
- CBC Cipher Block Chaining
- CRC Cyclic Redundancy Check
- 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
- ICAO International Civil Aviation Organization
- ISO International Standard Organization
- JC Java Card ™
- JCRE Java Card ™ Runtime Environment

- MAC Message Authentication Code
- NDRNG Non Deterministic Random Number Generator
- OP Open Platform
- PIN Personal Identification Number
- PKCS Public Key Cryptographic Standards
- RAM Random Access Memory
- ROM Read only Memory
- RSA Public key cryptographic algorithm invented by Rivest, Shamir and Adleman
- SHA Secure Hash Algorithm
- SPA Simple Power Analysis
- TDES Triple DES
- TLV Tag Length Value
- WHQL Microsoft Windows Hardware Quality Lab