ID-One Cosmo V7-n Lite

Smart Card Cryptographic Module

FIPS 140-2 Security Policy

Public Version

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

Change Record

Revision	*Date*	*Author*	*Description of Change*
1	Dec. 3, 2009	C. GOYET	First Public version
2	Jan. 28, 2010	C. GOYET	Update FW version to include latest service packs
3	July 20, 2010	C. GOYET	Update FW version to include latest service packs

Table 1 - Document Version History

CONTENTS

TABLES

FIGURES

1 Introduction

1.1 Scope

This document defines the Security Policy for the Oberthur ID-One Cosmo V7-n Lite cryptographic module. The module is validated to FIPS 140-2 Level 3.

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

The ID-One Cosmo V7-n Lite is part of the Oberthur family of cryptographic modules called ID-One Cosmo V7. Modules within this family share the same functionalities except that the “Lite” version does not support the AES algorithm, nor does it support contactless communication.

In the remainder of this document, the name “ID-One Cosmo V7” is used to refer to specification that are generic to the family and therefore applicable to the “Lite” version subject to this validation.

1.2 Module Overview

The module is a single chip Smart Card micro-controller containing an operating system that loads and runs applications written in Java™ programming language.

The main purpose of the module is to provide a secure Smart Card chip Javacard™ platform with data storage and enhanced cryptographic processing capabilities specifically designed to fit the needs of government and enterprise personnel identification applications. Such applications would have to be loaded into the module to provide the business functionality, and the module has been designed to enable a re-validation to be performed in a short time and with the minimum possible risk whenever a FIPS 140-2 validated application is to be loaded into the module. However the validation described in this security policy is limited in scope to the cryptographic module with no loaded applications. The loading of an application voids the FIPS 140-2 validation of the module unless a new validation has been achieved with an extended scope that encompasses the loaded application.

The module operating system 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 management of programmable platforms. Multiple applications loaded into the module can be securely separated by a firewall.

High and low level services, inclusive of communications, memories management (both persistent and volatile), cryptographic algorithms and physical security are addressed.

Java Card Services can be accessed by a loaded application using the Java Card™ Application Programming Interface (API).

Global Platform Services are provided to an external operator through Security Domains and to a loaded application using the Global Platform API.

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).

On-board cryptographic services with:

- Secure Hash Algorithm (SHA up to 512) for message digest; (message integrity)
- Elliptic-Curve Digital Signature Algorithm (ECDSA) with NIST Recommended Elliptic Curves over Prime Field GF(p) up to P-521 for digital signatures (non repudiation).
- Elliptic-Curve Diffie-Hellman for key agreement (simplified key management);

Additional cryptographic features 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 FIPS 186-2 Random Number Generators.

Card Holder Verification (CHV) services include a built-in on card fingerprint matching engine (Match-On-Card) using ISO/IEC 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.

The Communication services support ISO/IEC 7816-3 extended length fields, allowing up to 32,767 bytes of data in each direction (In/Out) to be transmitted within a single APDU, as opposed to a maximum of 256 bytes with previous modules. Large files such as Photo ID or X509 certificates can now be read in a single APDU without requiring chaining.

The module operates under multiple classes of voltages (Class A = 5V and Class B = 3V) making it the perfect cryptographic module for a new range of application using lower voltage portable readers.

In addition to the security requirements from FIPS 140-2, the module has been independently tested to meet the requirements often asked in Common Criteria Certifications but not addressed by this FIPS 140-2 validation, such as:

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

1.3 Module Identification

The ID-One Cosmo V7-n Lite cryptographic module is available in multiple memory sizes.

The following commercial products are available with the version “Lite” described in this validation:

Product Name	Amount of Persistent Memory (EEPROM) available to customers	Contactless Interface
ID-One Cosmo V7 Basic No AES	30k-> 50k	No

Table 2 – Commercial product names

Please note that the above commercial products can be initialized during manufacturing with alternative modes of operation that are not necessarily compliant with FIPS 140-2 but may offer better performances. When required, the FIPS mode of operation MUST be specified at the time of purchasing.

Information whether the module has been initialized in FIPS 140-2 mode of operation during manufacturing can be retrieved at any time using the GET DATA command.

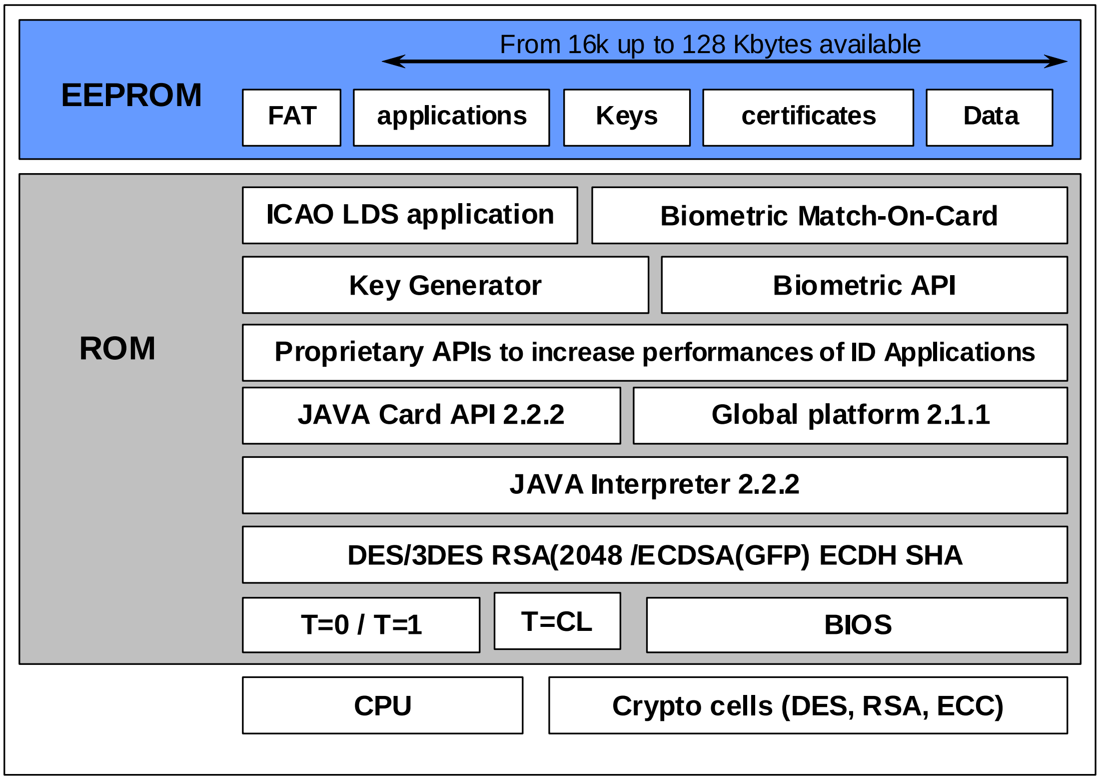

Figure 1: Logical Block Diagram of the Oberthur ID-One Cosmo V7-n Lite module

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2, with Physical Security being validated against level 4 requirements.

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 3 - Module Security Level Specification

3 Cryptographic Module Specification

3.1 Overview

The ID-One Cosmo V7-n Lite is a single chip implementation of a cryptographic module.

The module comprises the following elements:

1. Secure Micro-Controller Integrated Circuit (Hardware)
2. Embedded Operating System (Firmware).
3. Common Open Platform Card Manager (Global Platform)
4. Applets (Applications) that are to be installed onto the module (outside the scope of this validation).

The micro controller Integrated Circuit provides hardware resources like ROM, RAM, EEPROM, Main CPU and Cryptographic Co-Processors.

The Embedded Operating Systems provides the Basic Input/Output System (BIOS), the Javacard Virtual Machine version 2.2.2 with its Runtime Environment and Application Programming interface (API), Oberthur Additional cryptographic API, Biometric API, and fingerprint Match-On-Card.

The Common Open Platform Card Manager (COP) provides external interfaces as well as internal API to allow for the mutual authentication of identities using strong cryptography with “off card application” or terminals that they might be connected to, and to secure subsequent communications.

A special instance of the Common Open Platform Card Manager is called the Issuer Security Domain. The Issuer Security Domain (ISD) is the on card representative of the Card Issuer. It allows the Card Issuer to manage the applications on the card as well as the card life cycle.

Other instances of the COP provide Supplementary Security Domains allowing application providers to separate their key spaces from the Card Administrator.

The COP fully complies with the following specifications:

- Global Platform
  - Global Platform 2.1.1 Card Implementation Requirements –March 2003
  - Global Platform Card Specification - Version 2.1.1 – Mars, 2003
  - Global Platform Card Specification Amendment A – February,2004
- Visa
  - Visa Open Platform Card Implementation Requirements Configuration 3 – Multiple Security Domains with DAP Capability October 2001
  - Visa Global Platform 2.1.1 Card Implementation Requirements May 2003

In the scope of this document, there are no applets instantiated other than the Security Domain(s). (Issuer Security Domain and potentially Supplementary Security Domains)

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

3.2 Cryptographic Module Boundary

The cryptographic module boundary is the edge of the die.

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

The cryptographic module boundary separates the chip from the card and contact plate

3.3 Module Hardware

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

- For ID-One Cosmo Basic no AES, the module HW P/N is C6

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

3.4 Module Firmware

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

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

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

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

3.5 Service Packs

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

The ID-One Cosmo V7-n Lite cryptographic module has been validated with the following Optional Codes:

Firmware version	Optional Codes	Note
FC10	069778	Generic r8 (for PIV ECC)
FC10	071964	BIO r4 (Generic r8 + MOC 3.21 for PIV BIO)

Table 4: Optional Codes included in this validation

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

3.6 Locks Configurations

The module includes several locks that can be set by Oberthur during the manufacturing phase to configure the module in a specific electrical configuration and meet customer requirements or export control regulations.

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.

3.7 Electrical Profile

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

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

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

3.8 FIPS Mode of Operation

Please make sure you specify at the time of ordering that you want the product to operate in FIPS 140-2 Approved mode as it may not be the default configuration from all Oberthur factories. Modules that are not configured in FIPS 140-2 Approved mode of operation during manufacturing offer better performances for short transactions such as physical access control as time consuming cryptographic Known Answer Test (KAT) are no longer performed systematically during the power-up initialization sequence but only prior to the first use of the algorithm (which may not always happen if not all algorithms are used during each session). The KAT can also be completely disabled during manufacturing for configuration where speed is more important than security, but the resulting module will not be in FIPS 140-2 Approved mode of operation.

Once set during manufacturing, the FIPS mode of operation cannot be changed. 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 140-2 Approved mode are listed as such in the BAP document associated with your delivery.

Once set in FIPS mode during manufacturing, the module only provides a FIPS Approved mode of operation, comprising all the services described in section 5 below.

The module will enter a FIPS Approved mode following a successful power up initialization.

It is possible at anytime during the life of the module to know if the module is in FIPS mode of operation by checking the value of the FIPS mode lock that can be read from the Card Identification Data Object under the sub-element with tag ‘05’ (FIPS Mode). If set to ‘01’, the module is in FIPS mode of operation. In addition Modules in FIPS mode have the Issuer Security Domain (ISD) in OP-SECURED state.

3.9 Cryptographic Algorithms

The purpose of the cryptographic module is to provide a FIPS approved Javacard Chip Platform for applications that may in turn provide cryptographic services to end-user applications. A variety of algorithms are used in the module to provide cryptographic services. Some of these cryptographic services are made available only to applications via internal APIs. Since the module described in this security policy does not include any instantiated applications, some security services may not be available to any operator of the module. There are however listed in this section to inform applet developers of all cryptographic services built into the module. Please contact Oberthur for further information on these cryptographic services.

3.9.1 FIPS Approved Algorithms

The following table lists the cryptographic algorithms that have been validated on the ID One Cosmo V7-n Lite module.

Algorithm	Modes	Key Size	Bits of Security	CAVP Cert. #
TDES	ECB and CBC in both Encryption and Decryption	**128 bits**	**80**	**698**
	ECB and CBC in both Encryption and Decryption	**192 bits**	**112**	
TDES- MAC	MAC Mode	**128 bits**	**80**	**698, vendor affirmed**
	MAC Mode	**192 bits**	**112**	
SHA-1	Byte-oriented messages	**N/A**	**80**	**833**
SHA-224			**112**	
SHA-256			**128**	
SHA-384			**192**	
SHA-512			**256**	
DRNG	FIPS 186-2[1]			**480**
RSA	GenKey (ANSI X9.31)	**Modulus sizes: 1024 to 2048 in 64 bit increments**	**80 to 112**	**403**
	SigGenPKCS1.5 with SHA-1, SHA-256, SHA-384 and SHA-512			
	SIgGenPSS with SHA-1, SHA-256, SHA-384 and SHA-512			
	SigVerPKCS1.5 with SHA-1, SHA-256, SHA-384 and SHA-512			
	SigVerPSS with SHA-1, SHA-256, SHA-384 and SHA-512			
ECDSA	Key Pair Generation	**Curves: P-192, P-224, P-256, P-384, P-521**	**80 112 128 192 256**	**94**
	SigGen with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512			
	SigVer with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512			

Table 5: FIPS Approved Algorithms implemented in Current Module

Note that SHA-224, SHA-256, SHA-384, SHA 512, RSA Signature Generation, RSA key generation, and all ECDSA functionalities are only available through APIs to be called by loaded applications. They are not used by the current module.

3.9.2 Cryptographic Padding

The ID One Cosmo V7 module has a native implementation of the following padding schemes to be used with the above cryptographic algorithms:

- **ISO/IEC 9796**; Digital signature schemes giving message recovery.

[1] FIPS PUB 186-2 "Digital Signature Standard", appendix 3.1 "Random Number Generation for the DSA", section 3.4 "Constructing the function G from the DES" updated with Change Notice 1 for General Purpose Random Number Generation.

- **ISO/IEC 9797**, Message Authentication Codes (MACs).
- **PKCS#1 v2.1** signature and encryption schemes using RSA.
- **OAEP** (Optimal Asymmetric Encryption Padding) for encryption.
- **PSS** (Probabilistic Signature Scheme) for signature.

These padding schemes are available from the module via internal APIs.

3.9.3 Random Number Generators

The cryptographic module offers the services of a FIPS 140-2 approved DRNG (Deterministic Random Number Generator). See Table 5

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.

3.9.4 Other Elliptic Curves

Other Elliptic Curves using GF(P) with "f" from 160 to 521 are available to loaded applets through internal APIs.

3.9.5 Elliptic Curve Diffie-Hellman

Elliptic curve secret value derivation primitive, Diffie-Hellman version, with or without cofactor multiplication, as per IEEE P1363 are available to loaded applets through internal APIs.

3.9.6 Key Establishment

Key agreements services based on Diffie Helman and Diffie Helman Elliptic Curves are available to loaded applets through internal APIs.

Key transport is performed by TDES. TDES key establishment provides 80 bits of encryption strength.

3.9.7 Other RSA keys

The The ID One Cosmo V7-n Lite module makes available to loaded applets through internal API additional RSA key sizes that are not allowed by NIST. These have a modulus size of 512/576/640/704/768/832/896/960 bits.

It is the responsibility of the developer of the FIPS validated applet to ensure that these key sizes are not used in FIPS validated modules.

3.9.8 Global PIN

The module supports the Global Platform PIN available to loaded application through the Global Platform API. It is not used by the cryptographic module is the configuration described in this security policy as no applet is loaded to exercise this functionality.

3.9.9 Biometric Fingerprint On Card Verification

The module supports fingerprint match on card functionality through API. It is not used by the cryptographic module in the configuration described in this security policy as no applet is loaded to exercise this functionality.

4 Ports and Interfaces

The ID-One Cosmo V7-n Lite supports only operations in Contact mode.

Contact communication is achieved through a physical connection to a smart card contact plate according to ISO 7816 standard.

4.1 Physical Interfaces

The cryptographic module follows the standard ISO/IEC 7816 part 2 and 3 for physical and logical interfaces:

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

Table 6: Physical Interface for contact mode

Transmission parameters

The module supports two transmission half duplex oriented ISO protocols: T=0 and T=1.

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

The module also supports the PPS to negotiate communication speed with the reader (Interface Device). Data communication speed on the I/O line is defined by the Values of the clock rate conversion integer “F” and the baud rate adjustment integer “D” agreed upon between the reader and the module during the power on sequence. The values supported by the module are as follows (see ISO 7816-3:2006):

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

Table 7: Transmission parameters for contact mode

4.2 Logical Interface

The module functions as a slave processor to process and respond to the reader commands. The I/O port of the module provides the following logical interfaces:

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

Table 8: Module Ports and Interfaces

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

5 Roles & Services

5.1 Roles

Cryptographic Officer Roles	
Card Administrator (CA)	This role is responsible for managing the security configuration of the module. The CA authenticates to the module through a Global Platform (GP) mutual authentication protocol with the Issuer Security Domain (ISD). A successful authentication demonstrates the knowledge of the ISD Global Platform Keyset and establishes a GP Secure Channel Session to execute services allowed to the CA in a secure manner. (See Global Platform Specifications for more details)
User Roles	
Application Provider (AP)	This role is responsible for managing the security configuration of a loaded application. The AP authenticates to the module through a Global Platform (GP) mutual authentication protocol with the Application Security Domain (ASD). A successful authentication demonstrates the knowledge of the ASD Global Platform Keyset and establishes a GP Secure Channel Session to execute services allowed to the AP in a secure manner. (See Global Platform Specifications for more details)
No Roles	
Public Operator (PO)	This role is available to any operators without authentication. It can only access non security relevant services provided by the module.
Maintenance Roles	
None	The module does not support any maintenance role.

Table 9: Roles and required Identification and Authentication

5.1.1 Concurrent Operators

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

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

However only one communication session can be open per authenticated role.

5.2 Role Identification

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

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

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

Within each application, a unique ID and version number are associated with each cryptographic keys to uniquely identify the off-card identity performing the authentication.

See Global Platform Specifications for more details.

5.3 Role Authentication

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

This authentication mechanism has the following properties:

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

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

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

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

5.3.1 Card Administrator and Application Provider Authentication

The Card Administrator and Application Provider authenticate by opening a Global Platform Secure Channel Session with respectively the Issuer Security Domain and the Application Security Domain. This Secure Channel Session establishment involves three APDU commands as follows:

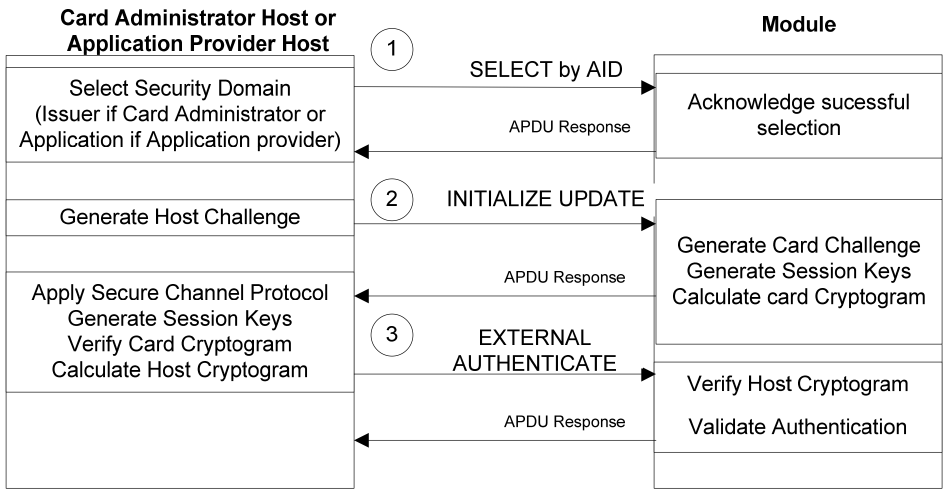

Figure 2: Logical Block Diagram of the Oberthur ID-One Cosmo V7 module

5.4 Services

5.4.1 Card Administrator Services

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

Authentication	
INITIALIZE UPDATE	This command is used by the CA to initiate a Global Platform Secure Channel Session, setting the key set version and index.
EXTERNAL AUTHENTICATE	This command is used by the CA to open a Global Platform Secure Channel Session with the Issuer Security Domain, in order to communicate in a secure and confidential way.
Card Content Management	
INSTALL	This command is used by the CA to add an application to the module.
LOAD	This command is used by the CA to load the byte-code of a new application (executable load file). For the module to remain FIPS validated, this command shall not be used to load non FIPS approved executable code.
DELETE	This command is used by the CA to delete a uniquely identifiable object. The object may be an Application, a load file, or a key set.
PUT KEY	This command is used by the CA to add or replace ISD keys. Keys are loaded protected by the double encryption of the global Platform Secure Channel and a KCV is included in the transmission to ensure integrity of the key loading operation. This command is also used by the CA to load RSA public keys such as the Token Verification Key or the DAP Verification Key. These keys are used for Delegated Management and DAP verification as specified by Global Platform.
STORE DATA	This command is used by the CA to transfer data to the module. It is also used to clear the audit log.

SET STATUS	This command is used by the CA to temporary lock an application, and to unlock it later on. It can also be used to terminate the crypto module.
GET STATUS	This command is used by the CA to retrieve identification and life cycle status information for all applications, executable load files, and security domains present in the module. It can also be used by the CA to verify that the module is still in the FIPS validated configuration and that only FIPS approved applications are available.
DELEGATE MANAGEMENT	Delegated Management gives the CA the possibility of empowering an AP the ability to initiate approved and pre-authorized Card Content changes (loading, installation, extradition or deletion) on his behalf.
Public Commands	
SELECT	This command is used for selecting an application (Card Manager, Security Domain or Applet Instance) on a specific logical channel. A successful selection logs out the role currently active on the same logical channel, if any.
MANAGE CHANNEL	This command allows opening or closing a logical channel in the card. Up to 4 logical channels may be open at a time.
GET DATA	The GET DATA command is used to retrieve public data from the selected application. No CSP can be read using this service.

Table 10: Card Administrator Services

5.4.2 Application Provider Services

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

Authentication	
INITIALIZE UPDATE	This command is used by the AP to initiate a Global Platform Secure Channel Session, setting the key set version and index.
EXTERNAL AUTHENTICATE	This command is used by the AP to open a Global Platform Secure Channel Session with the Application Security Domain, in order to communicate in a secure and confidential way.
Card Content Management	
DAP VERIFICATION	DAP verification allows the module to check the CA signature on an application code being loaded and abort the loading if the signature is not verified. Such verification can be made mandatory or optional. The optional DAP functionality is allowed in the Approved mode.
DELETE	This command is used by the CA to delete a uniquely identifiable object. The object may be an Application, a load file, or a key set.
PUT KEY	This command is used by the CA to add or replace ISD keys. Keys are loaded protected by the 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 by the CA to transfer data to the module.

SET STATUS	This command is used by the CA to temporary lock one of its application, and to unlock it later on.
GET STATUS	This command is used by the CA to retrieve identification and life cycle status information for all applications, executable load files, and security domains present in the module.
Public Commands	
SELECT	This command is used for selecting an application (Card Manager, Security Domain or Applet Instance) on a specific logical channel. A successful selection logs out the role currently active on the same logical channel, if any.
MANAGE CHANNEL	This command allows opening or closing a logical channel in the card. Up to 4 logical channels may be open at a time.
GET DATA	The GET DATA command is used to retrieve public data from the selected application. No CSP can be read using this service.

Table 11: Application Provider Services

5.4.3 Public User Services

The following table lists the services that the module make available to without authentication (unauthenticated service).

Public Commands	
SELECT	This command is used for selecting an application on a specific logical channel. A successful selection logs out the role currently active on the same logical channel, if any.
MANAGE CHANNEL	This command allows opening or closing a logical channel in the card. Up to 4 logical channels may be open at a time.
GET DATA	The GET DATA command is used to retrieve public data from the selected application. No CSP can be read using this service.

Table 12: Public User Services

5.4.4 Delegated Management

The design of the module from Oberthur takes into account the possibility that the the Card Administrator (Card Issuer) 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 Administrator the possibility of empowering Application Providers the ability to initiate approved and pre-authorized Card Content changes (loading, installation, extradition[2] or deletion). This approval, which is central to the concept of Delegated Management, ensures that only Card Content changes that the Card Administrator 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.

[2] 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 the Card Administrator 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 Card Administrator token signature private RSA key, must be present in the Issuer Security Domain.

When the Application Provider wants to perform the pre-authorized function, it appends to the function's data transmitted through a secure channel with its Application Security Domain (ASD) the associated token. The ASD will then decrypt and verify the secure channel communication using its ASK. The function and its associated Token are then automatically transmitted to the Issuer Security Domain for token verification using the Card Administrator $\mathbf{K}_{TOKEN}$ Public RSA key. If the signature is verified, the function is authorized to complete. Otherwise, it is aborted and cleared from memory.

The Card Issuer's security policy may require the generation of Receipts for Delegated Management operations. A Receipt is a cryptographic value (TDES MAC on the receipt data) generated by the Issuer Security Domain $\mathbf{K}_{RECEIPT}$ 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 Data generated by the Issuer Security Domain. The Issuer Security Domain also keeps track of a Confirmation Counter value that is incremented when generating each Receipt.

See Global Platform Specification fur further details on Delegated Management.

5.4.5 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 Administrator and require a check of application code integrity and authenticity by the module before the application code is loaded. 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 Card Administrator or by an Application Provider with Delegated Management. The DAP Verification privilege for a 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. Loading of external code is optional. If non-validated firmware is loaded, the module is no longer FIPS validated.

The way it works is as follows: The Applet Provider or Controlling Authority first computes a SHA-1 message digest of the application that is to be subsequently loaded into the module. it then uses his DAP RSA private key (matching the public key $\mathbf{K}_{DAP}$ in the 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 Security Domain with DAP verification uses its DAP public key $\mathbf{K}_{DAP}$ to check the DAP signature. The application code can be loaded into the module only if the verification succeeds.

See Global Platform Specification fur further details on DAP verification.

5.4.6 Relationship between Roles, Services and CSP Access

Roles/Services	Card Administrator (CA)	Application Provider (AP)	Public Operator	CSP involved		CSP Access type
				From CA	From AP	
INSTALL	X			CSK		Execute
LOAD	X			CSK		Execute
DELETE	X	X		CSK		Execute
PUT KEY	X	X		CSK, CDK, **K**$_{TOKEN}$, **K**$_{DAP}$	ASK, ADK	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, **K**$_{TOKEN}$, **K**$_{RECEIPT}$		Execute
DAP VERIFICATION		X		**K**$_{DAP}$		Execute
SELECT			X			
MANAGE CHANNEL			X			
GET DATA			X			

Table 13: Relationship between Roles, Services and CSP Access

6 Critical Security Parameters and Public Keys

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

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

6.1 Card Administrator Keys in Issuer Security Domain

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

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

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

2. **CSK**: Card Administrator Session Keyset: Set of two transient Keys (called CSK_{ENC} and CSK_{MAC}) of 16 bytes each generated by diversification of the CDK as per Global Platform specifications [6] CSK_{ENC} is used for Secure Channel

Encryption, and CSK_{MAC} is used for Secure Channel MAC verification and to authenticate the operator. CSK keys are used with the same algorithm (Triple DES 128) as the CDK from which they derived.

3. **K_{TOKEN}**: Key Token (Public Key): Public RSA Key (1024 bits) used to verify the tokens included in Delegated Management commands that embed the signature of these commands as per Global Platform [6]. 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 128 Key used to compute a receipt on Delegated Management Commands as per Global Platform specifications [6]. This key may or may not be loaded into the module. It is an added feature and is not intended to satisfy any of the FIPS 140-2 requirements for applet loading.

6.2 Application Provider Keys in Application Security Domains

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

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

   The loading of ADK keys set is done with a PUT KEY command and is protected by a Global Platform Secure Messaging using another ADK.
2. **ASK**: Applet Provider Session Keyset: Set of two transient Keys (called ASK_{ENC} and ASK_{MAC}) of 16 bytes each generated by diversification of the ADK as per Global Platform specifications [6]. ASK_{ENC} is used for Secure Channel Authentication and optionally Encryption, and ASK_{MAC} is used for Secure Channel MAC verification and to authenticate the operator. ASK keys are used with the same algorithm (Triple DES 128) as the ADK from which they derived.
3. **K_{DAP}**: Key DAP (Public Key): Public part of the Card Administrator RSA DAP Key (1024 bits) used verify the signature of a executable load file being loaded by the Application Provider. This key may or may not be loaded into the module. It is an added feature and is not intended to satisfy any of the FIPS 140-2 requirements for applet loading. This key is present only in Security Domain with DAP Verification. See Global Platform Specification for more information on the use of DAP.

6.3 Other CSP

6.3.1 DRNG Seed

The seed used by the DRNG is a 20 byte value generated by the Hardware NDRNG.

To get the best possible entropy, only 40 bytes are retrieved from the DRNG before it is re-seeded from the Hardware NDRNG.

7 Self Tests

7.1 Power on Self Tests

Each time the module is powered by a reader, 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:

- System tests
- EEPROM code integrity check
- Cryptographic algorithm tests (KAT)
    - Random Generator
    - CRC Algorithms
    - SHA hashing algorithms (SHA-1, SHA 224, SHA 256, SHA 386, SHA 512)
    - TDES – Encryption and Decryption
    - RSA – Signature and Verification
    - Elliptic Curves ECDSA – Signature and verification

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 returns an error status before entering an error state in which further commands are not processed.

7.2 Conditional Self-Tests

7.2.1 Key Pair-Wise Consistency Tests

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

Elliptic Curve Key generation: In the current implementation, the pair-wise consistency check on newly generated ECC keys is under the responsibility of the application (applet) calling on the ECC Key generation API.

7.2.2 Continuous Random Number Generator test

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

7.2.3 CSP Integrity Test

Each time a Critical Security Parameter is used, its integrity is checked.

7.2.4 Software Load Test

Application loading follows the Global Platform specifications. At a minimum, a MAC of the executable load file is verified each time an applet is loaded onto the cryptographic module.

8 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

8.1 Authentication Security Rules

The module implements identical authentication mechanisms for each of its roles. Each authentication mechanism includes verification of the knowledge of a secret shared between the module and the external operator, and for each restricted service, verification that the authentication security status is granted.

Each of these secrets is referenced with a unique identifier that is used by the external operator to identify them:

- For the Card administrator (CA), the secret is the CDK (see 6.1) and the identifier is a combination of the ISD AID (Application Identifier) and the key set ID within the ISD.
- For the Application Provider (AP), the secret is the ADK (see 6.2) and the identifier is a combination of the ASD AID (Application Identifier) and the key set ID within the ASD.

8.2 Application Life Cycle Security Rules

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

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

For the module to run in a validated FIPS 140-2 Level 3 mode of operation, all applets must be validated to the same level prior being loaded into the module. It is the responsibility of the Cryptographic Officer to insure that applets loaded post-validation have been FIPS 140-2 Level 3 validated.

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

8.3 Access Control Security Rules

CDK and ADK Keys must be loaded through a secure channel session ensuring their integrity and confidentiality.

8.4 Key Management Security Policy

8.4.1 Cryptographic keys

The module uses the following CSPs and public keys:

Key Name (CSP/Public Key)	Type	Length	Strength
CDK_{DES}	TDES	128-bits	80-bits
ADK_{DES}			
CSK_{DES}	TDES Session Keys	128-bits	80-bits
ASK_{DES}			
K_{DAP}	RSA Public Key	1024 bit	80-bits
K_{TOKEN}	RSA Public Key	1024 bit	80-bits
$\mathbf{K}_{RECEIPT}$	TDES	128-bits	80-bits

Table 14: CSP/Public Key used

In addition, the module supports a large range of FIPS-Approved or FIPS-Allowed symmetric and asymmetric keys available to loaded applets through Java API:

Key Name	Type	Length	Strength
TDES Keys	TDES ECB and CBC	192-bits	112-bits
RSA Keys	RSA Signature & Verification» Key Wrapping & Unwrapping	1024 to 2048 bits	80 to112 bits
ECC Keys	P-192, P-224, P-256, P-384, P-521	192, 224, 256, 384, 521	80 112 128 192 256

Table 15: CSP available only to loaded applets

8.4.2 Cryptographic key generation

- TDES Session key generation using FIPS186-2 approved DRNG for secure channel opening.
- RSA key pair generations (up to 2048 bit key length) fully compliant with ANSI X9.31 and using a FIPS140-2 approved DRNG. Both standard RSA key and RSA Chinese Remainder Keys can be generated.
- ECC key pair generations (on GF(P) curves with “f” up to 521)

8.4.3 Cryptographic key entry

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

The secure channel session used must be such that the cryptographic strength of the encryption key is at least equal to the cryptographic strength of the key being loaded.

Keys can never be output by the module.

8.4.4 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.

8.4.5 Cryptographic Key Zeroization

Cryptographic keys stored in non volatile memory (CDK and ADK) can be zeroized by reloading another value using the **PUT KEY** command.

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

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

9 Physical Security

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

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

Key features include:

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

10 Mitigation of Other Attacks

10.1 Power Analysis (SPA/DPA)

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

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

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

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

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

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

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

10.2 Timing Analysis

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

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

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

10.3 Fault Induction

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

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

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

10.4 Flash Gun

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

10.5 ElectroMagnetic Attacks

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

10.6 Card Tearing

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

11 Security Policy Check List Tables

11.1 Roles and required Identification and Authentication

Role	Type of Authentication	Authentication Data
Card Administrator	TDES Authentication using GP secure channel mutual authentication protocol	Issuer Security Domain Key Set (CDK)
Application Provider	TDES Authentication using GP secure channel mutual authentication protocol	Application Security Domain Key Set (ADK)

Table 16: Roles and required Identification and Authentication

11.2 Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism	Strength of Successful Random Attempt in 1 Minute
TDES Authentication	2^{80}	$8/2^{80}$

Table 17: Strength of Authentication Mechanisms

11.3 Services Authorized for Roles

Role	Authorized Services
Card Administrator	Card Administrator Services are listed in section 5.4.1.
Application Provider	Application Provider Services are listed in section 5.4.2.

Table 18: Services Authorized for Roles

11.4 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
Card Tearing	Counter Measures against card tearing	N/A

Table 19: Mitigation of other attacks

12 References

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

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

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

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

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

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

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

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

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

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

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

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

[12] JavaCard 2.2.2 Virtual Machine Specification, March 2006

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

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

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

13 Definitions and Acronyms

13.1 Acronyms

Acronym	**Definition**
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)
BAP	Batch Approval Process (First article validation from Production line)
CBC	Cipher Block Chaining
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DES	Data Encryption Standard
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
ECC	Elliptic Curve Cryptography
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
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
PPS	Protocol Parameters Selection
RAM	Random Access Memory
ROM	Read only Memory
RSA	Public key cryptographic algorithm invented by Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
TDES	Triple DES