



# **COSMOS**

Security Target Lite

# Oberthur Card System - Cosmos

## Security Target Lite

---

© 2006 by Oberthur Card Systems. All rights reserved. The information contained in this publication is accurate to the best of Oberthur Card Systems' knowledge. However, Oberthur Card Systems disclaims any liability resulting from the use of this information and reserves the right to make changes without notice.

Manual reference: 064471 02 UDD AA

# Oberthur Card System - Cosmos

## Security Target Lite

---

### TABLE OF CONTENTS

1	ST INTRODUCTION.....	6
1.1	ST IDENTIFICATION .....	6
1.2	ST OVERVIEW.....	6
1.3	CC CONFORMANCE .....	7
1.4	REFERENCES .....	7
2	TOE DESCRIPTION.....	9
2.1	Introduction.....	9
2.1.1	ID one V3 application.....	10
2.1.2	Javacard platform .....	10
2.1.2.1	Bios .....	10
2.1.2.2	Virtual Machine .....	10
2.1.2.3	APIs.....	11
2.1.2.4	Global Platform.....	11
2.1.2.5	Resident Application.....	11
2.2	TOE Identification.....	11
2.3	TOE overview .....	12
2.4	Description of the application ID One V3 used as a simple signature creation application.....	13
2.4.1	Cryptographic services .....	13
2.4.2	Data structures handled by the application .....	14
2.4.2.1	File system .....	14
2.4.2.2	Security Data Object.....	14
2.4.3	Access conditions .....	15
2.4.4	Security Status .....	15
2.4.5	Secure Messaging.....	15
2.5	TOE intended usage.....	16
2.6	TOE life cycle.....	17
2.7	Description of the TOE environment.....	18
2.7.1	Development environment.....	18
2.7.1.1	Software development (phase 1).....	18
2.7.1.2	Hardware development .....	18
2.7.2	Production environment.....	18
2.7.2.1	IC manufacturing (phase 3) .....	18
2.7.2.2	TOE manufacturing (phase 4 to 6) .....	18
2.7.3	User environment.....	18
2.8	Description of the TOE's scope .....	19
2.8.1	The development phase : phase 1 .....	19
2.8.2	The manufacturing phase : phase 2.....	19
2.8.3	The prepersonalization phase : phase 3 .....	19
2.9	Initialization and personalization of the TOE .....	20
2.9.1.1	Bios : Empty EEPROM .....	21

---

# Oberthur Card System - Cosmos

## Security Target Lite

---

2.9.1.2	Bios : Initialized EEPROM.....	22
2.9.1.3	Resident application : preperso.....	22
2.9.1.4	CM in VOP Personalization.....	22
2.9.1.5	CM in OP Ready.....	22
2.9.1.6	Resident application : use.....	22
2.9.1.7	CM initialized.....	22
2.9.1.8	Javacard packages loaded.....	22
2.9.1.9	Applet selectable.....	22
2.9.1.10	Platform with post issuance terminated.....	22
2.9.1.11	Applet initialized.....	23
2.9.1.12	CM secured.....	23
2.9.1.13	Smart card ready to be delivered.....	23
2.9.1.14	Smart card ready to be used.....	23
2.9.1.15	Smart card locked.....	23
2.9.1.16	Resident Application : locked.....	23
2.9.1.17	Smart card terminated.....	23
3	<b>TOE SECURITY ENVIRONMENT.....</b>	<b>24</b>
3.1	<b>Subjects.....</b>	<b>24</b>
3.2	<b>Assets.....</b>	<b>24</b>
3.3	<b>Assumptions.....</b>	<b>26</b>
3.4	<b>Threats.....</b>	<b>26</b>
3.5	<b>ORGANIZATIONAL SECURITY POLICIES.....</b>	<b>27</b>
4	<b>SECURITY OBJECTIVES.....</b>	<b>27</b>
4.1	<b>Security Objectives for the TOE.....</b>	<b>27</b>
4.2	<b>Security Objectives For The Environment.....</b>	<b>28</b>
5	<b>IT SECURITY REQUIREMENTS.....</b>	<b>29</b>
5.1	<b>TOE IT SECURITY FUNCTIONAL REQUIREMENTS.....</b>	<b>29</b>
5.1.1	<b>FCS: CRYPTOGRAPHIC SUPPORT.....</b>	<b>29</b>
5.1.1.1	FCS_CKM cryptographic key management.....	29
5.1.1.2	FCS_COP Cryptographic operation.....	30
5.1.2	<b>FDP : USER DATA PROTECTION.....</b>	<b>31</b>
5.1.2.1	FDP_ACC Access Control Policy.....	31
5.1.2.2	FDP_ACF access control function.....	32
5.1.2.3	FDP_ETC : Export to outside TSF control.....	38
5.1.2.4	FDP_ITC Import From outside TSF control.....	39
5.1.2.5	FDP_RIP Residual information protection.....	39
5.1.2.6	FDP_SDI Stored data integrity.....	40
5.1.2.7	FDP_UCT Inter-TSF user data confidentiality transfer protection.....	40
5.1.2.8	FDP_UIT Inter-TSF user data integrity transfer protection.....	40
5.1.3	<b>FIA: IDENTIFICATION AND AUTHENTICATION.....</b>	<b>41</b>
5.1.3.1	FIA_AFL Authentication failure.....	41
5.1.3.2	FIA_ATD User attribute definition.....	42
5.1.3.3	FIA_UAU User authentication.....	42
5.1.3.4	FIA_UID User Identification.....	42
5.1.4	<b>FMT: SECURITY MANAGEMENT.....</b>	<b>42</b>
5.1.4.1	FMT_MOF Management of functions in TSF.....	42
5.1.4.2	FMT_MSA Management of security attributes.....	43

---

# Oberthur Card System - Cosmos

## Security Target Lite

---

5.1.4.3	FMT_MTD Management of TSF data.....	45
5.1.4.4	FMT_SMR Security management roles .....	45
<b>5.1.5</b>	<b>FPT: PROTECTION OF THE TSF .....</b>	<b>45</b>
5.1.5.1	FPT_AMT Underlying Abstract machine test.....	45
5.1.5.2	FPT_EMSEC TOE Emanation .....	45
5.1.5.3	FPT_FLS Failure secure .....	45
5.1.5.4	FPT_PHP TSF physical Protection.....	45
5.1.5.5	FPT_TST TSF self test .....	46
<b>5.1.6</b>	<b>FTP: TRUSTED PATH / CHANNEL.....</b>	<b>46</b>
5.1.6.1	FTP_ITC Inter-TSF trusted channel .....	46
5.1.6.2	FTP_TRP Trusted path .....	47
<b>5.2</b>	<b>TOE SECURITY ASSURANCE REQUIREMENTS.....</b>	<b>48</b>
<b>5.2.1</b>	<b>CONFIGURATION MANAGEMENT (ACM).....</b>	<b>48</b>
<b>5.2.2</b>	<b>DELIVERY AND OPERATION (ADO) .....</b>	<b>48</b>
<b>5.2.3</b>	<b>DEVELOPMENT (ADV).....</b>	<b>48</b>
<b>5.2.4</b>	<b>GUIDANCE DOCUMENTS (AGD) .....</b>	<b>48</b>
<b>5.2.5</b>	<b>LIFE CYCLE SUPPORT (ALC).....</b>	<b>48</b>
<b>5.2.6</b>	<b>TESTS (ATE) .....</b>	<b>48</b>
<b>5.2.7</b>	<b>VULNERABILITY ASSESSMENT (AVA) .....</b>	<b>49</b>
<b>5.3</b>	<b>SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT .....</b>	<b>49</b>
<b>5.3.1</b>	<b>Signature key generation (SSCD Type1) .....</b>	<b>49</b>
5.3.1.1	Cryptographic key generation (FCS_CKM.1).....	49
5.3.1.2	Cryptographic key destruction (FCS_CKM.4).....	49
5.3.1.3	Cryptographic operation (FCS_COP.1).....	49
5.3.1.4	Subset access control (FDP_ACC.1).....	50
5.3.1.5	Basic data exchange confidentiality (FDP_UCT.1).....	51
5.3.1.6	Inter-TSF trusted channel (FTP_ITC.1) .....	51
<b>5.3.2</b>	<b>Certification generation application (CGA) .....</b>	<b>51</b>
5.3.2.1	Cryptographic key distribution (FCS_CKM.2) .....	51
5.3.2.2	Cryptographic key access (FCS_CKM.3).....	51
5.3.2.3	Data exchange integrity (FDP_UIT.1).....	51
5.3.2.4	Inter-TSF trusted channel (FTP_ITC.1) .....	51
<b>5.3.3</b>	<b>Signature creation application (SCA) .....</b>	<b>52</b>
5.3.3.1	Cryptographic operation (FCS_COP.1).....	52
5.3.3.2	Data exchange integrity (FDP_UIT.1).....	52
5.3.3.3	Inter-TSF trusted channel (FTP_ITC.1) .....	52
5.3.3.4	Trusted path (FTP_TRP.1).....	52
<b>5.4</b>	<b>SECURITY REQUIREMENTS FOR THE NON - IT ENVIRONMENT .....</b>	<b>53</b>
<b>6</b>	<b>TOE SUMMARY SPECIFICATION.....</b>	<b>53</b>
<b>6.1</b>	<b>security function list .....</b>	<b>53</b>
<b>6.2</b>	<b>Security functions provided by the IC.....</b>	<b>54</b>
<b>6.3</b>	<b>Security functions provided by the TOE.....</b>	<b>54</b>
<b>6.4</b>	<b>Assurance measures .....</b>	<b>54</b>
6.4.1	Assurance measure list.....	55
6.4.2	AM_ACM: Configuration management .....	55


---

# Oberthur Card System - Cosmos

## Security Target Lite

---

6.4.3	AM_ADO: Delivery and Operation.....	55
6.4.4	AM_ADV: Development .....	55
6.4.5	AM_AGD: Guidance documents.....	55
6.4.6	AM_ALC: Life cycle.....	55
6.4.7	AM_ATE: Tests.....	55
6.4.8	AM_AVA: Vulnerability assessment .....	55
7	PP CLAIMS.....	56
8	ACRONYMS.....	56



## **1 ST INTRODUCTION**

### *1.1 ST IDENTIFICATION*

Title: ID One V3 Card Security Target Lite  
064471 01 UDD AA

Reference:

- Microcontroller: Philips Smart MX P5CT072/V0P
- ROM: P5CT072EW1/T0PB6311

Configuration Management label (PVCS): Version «COSMOS V1.1»

Complete identification of the TOE is described in §2.2 **TOE Identification**

This Security Target deals with the evaluation of the application software, as well as the composition with the evaluation of the Integrated Circuit (IC). It claims two SSCD Protection Profiles [PP/TYPE2] and [PP/TYPE3].

This security target refers to the micro-controller MX P5CT072 design V0P security target [STIC] that is compliant to BSI 0002 Protection Profile [BSI-0002] and [IC-AUG] Smartcard Integrated Circuit Platform Augmentations.

### *1.2 ST OVERVIEW*

The TOE is a signature-creation device according to Directive 1999/93/EC [1999/93/EC] of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures .

The context of this ST is the Secure Signature Creation Device following the Protection Profiles ([SSCD1], [SSCD2] and [SSCD3]) developed by CEN/ISSS. These PPs are a translation of the annex concerning the Secure Signature Creation Device of the European directive [1999/93/EC].

The main objectives of this security target are:

- To describe the Target of Evaluation (TOE). This ST focuses on the Secure Signature Creation Device, designed to be embedded in a Smart card integrated circuit. It describes as well the other features the TOE fulfills
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by its environment.
- To describe the security objectives of the TOE and its supporting environment.
- To specify the security requirements which includes the TOE security functional requirements and the TOE security assurance requirements.
- To specify the TOE summary specification, which includes the TOE security functions specifications and the assurance measures.
- To give a rationale to this ST.

The assurance level for this product and its documentation is EAL5 augmented with:

- 
- ALC\_DVS.2 : Sufficiency of security measures
- AVA\_MSU.3: Analysis and testing for insecure states
- AVA\_VLA.4: Highly resistant

The strength level for the TOE security functional requirements is "SOF high" (Strength Of Functions high).

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 1.3 CC CONFORMANCE

This ST is built on [SSCD2] and [SSCD3] and is conformant to these PPs.

This ST is CC V2.2 conformant with Part2 extended due to additional functional components as stated in [SSCD2] and [SSCD3].

### 1.4 REFERENCES

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB-2004-01-001, version 2.2, January 2004
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-2004-01-002, version 2.2, January 2004
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements CCIMB-2004-01-003, version 2.2, January 2004
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCIMB-2004-01-003, version 2.2, January 2004
[CWA]	CEN/ISSS WS/E-Sign Expert Group F - Workshop Agreement CWA14169 Secure Signature-Creation Devices "EAL 4+"
[1999/93/EC]	Directive 1999/93/EC of the European parliament and of the council of the 13 December on a Community framework for electronic signatures
[SSCD1]	Secure Signature-Creation device Protection Profile Type 1 v1.05, EAL4+ BSI -PP-0004-2002 April 2002
[SSCD2]	Secure Signature-Creation device Protection Profile Type 2 v1.04, EAL4+ BSI -PP-0005-2002 April 2002
[SSCD3]	Secure Signature-Creation device Protection Profile Type 3 v1.05, EAL4+ BSI -PP-0006-2002 April 2002
[BSI-0002]	Smartcard IC Platform Protection Profile v 1.0 BSI-PP-0002-2001 Jul 2001
[STIC]	Security Target Lite BSI-DSZ-CC-0348. Evaluation of the Philips P5CT072V0P Secure Smart Card Controller



## Oberthur Card System - Cosmos

### Security Target Lite

[IC-AUG]	Smartcard Integrated Circuit Platform Augmentations Version 1.00, March 8th, 2002
[CryptoCotation]	ID One V3 Applet – Cotation cryptographique – FQR 110 3250 Ed 3
[ID One V3]	ID One V3 Applet – 063253 00 SRS - AA
[GOP ID MX64]	GOP ID MX64 PLATFORM – Mask – 064471 01 SRS AB
[E-SignK]	CWA 14890-1: Part 1 – Basic requirements – Version 1.09 rev2 – 22 December 2003 CWA 14890-2: Part 2 – Additional services – Version 1.01 – 22 December 2003
[JCAPI]	"Java Card 2.2.1 - Application Programming Interfaces", October 21 2003, Sun Microsystems
[JCRE]	"Java Card 2.2.1-JCRE", October 21 2003, Sun Microsystems
[JCVM]	"Java Card 2.2.1-Virtual Machine Specifications", October 21 2003, Sun Microsystems
[GP]	"Global Platform Card Specification", version 2.1.1' March, 2003, Global Platform
[CryptoRules]	"Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard ou renforcé" version 1.02, Novembre 2004

## **2 TOE DESCRIPTION**

This part of the Security Target describes the TOE as an aid to the understanding of its security requirements. It addresses the product type, the intended usage and the main features of the TOE.

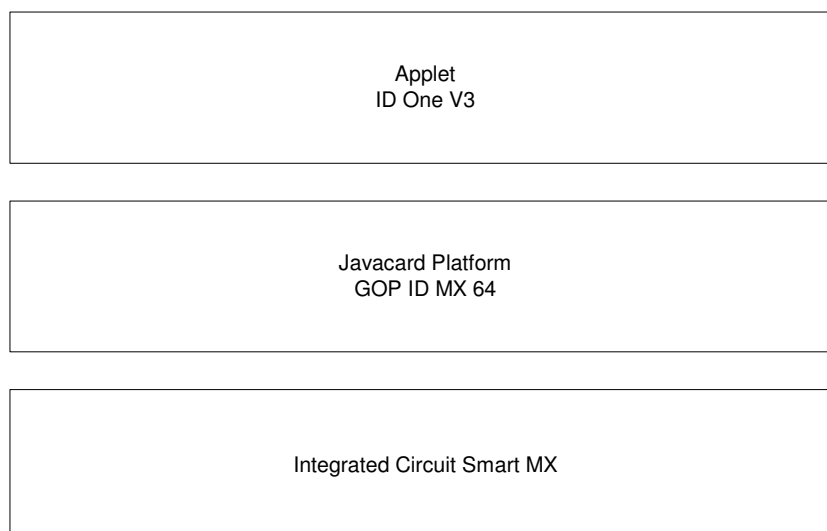
This part includes :

- Introduction
- TOE overview,
- Description of the Application ID One V3
- TOE life-cycle,
- Limits of the TOE
- TOE environment,

### *2.1 Introduction*

The Target of Evaluation (TOE) is the entire Smart card that will be issued  
The smart card consists in the set defined by:

- The underlying Integrated Circuit;
- The javacard platform Operating System called GOP ID MX 64;  
It is a platform based on the Java Card 2.2.1 specifications and on the Global Platform Card specification.
- The applet “ID One V3” used as a SSCD application using the services provided by the javacard platform  
This application offers many cryptographic services including services to create secure signature.



***Figure 1 : Model of the smart card***

The smart card is locked prior to its issuance. No more applications can be loaded on card once the final product is set.

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 2.1.1 ID one V3 application

This application is based on [E-SignK] specification. It is set in a specific configuration so that it only behaves as a simple Signature creation application as required in SSCD Protection Profiles [PP/TYPE2] and [PP/TYPE3], which means

- Generation of SCD and SVD
- Secrecy of the SCD
- Import of the SCD/SVD
- Export of SVD
- Signature Creation
- PIN administration
- Pin Authentication of the Signatory: the RAD used to verify the VAD is held securely.
- External authentication of an administrator
- Implementation of a trusted path to a human interface device

The way the application is set in this configuration is detailed in a specific document.

### 2.1.2 Javacard platform

The javacard platform (second layer of the final product) is based on Java Card technology [JCRE][JCVM][JCAPI] and Global Platform technology [GP]. Its main responsibilities are:

- To provide interface between the Integrated Circuit and the ID One V3 applet
- To provide to ID One V3 applet, basic services to access to memories and all needed cryptographic operations
- To ensure global management of the card (loading, installation and deletion of applets) and monitor the security of the card (data integrity and physical attacks counter-measures).
- The loading mechanism is blocked after the ID One V3 loading. Therefore no loading can be initiated after ID One V3 loading.

The javacard platform contains several entities described hereafter:

#### 2.1.2.1 Bios

The BIOS is an interface between hardware and native components like VM, APIs.

The BIOS implements the following functionalities :

- APDU management (communication protocols : T=0, T=1, USB, TCL),
- Timer management,
- Exceptions management,
- Transaction management,
- EEPROM access,
- Cryptographic modules.

#### 2.1.2.2 Virtual Machine

The Virtual Machine, which is compliant with the JAVACARD 2.2.1 standard [JCVM], interprets the byte code of JAVACARD applets. It handles as well the firewall, ensuring a logical isolation of each applet running on the javacard platform.

The Virtual Machine is activated upon the selection of an applet.

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 2.1.2.3 APIs

The APIs, compliant with the JAVACARD 2.2.1 standard [JCAPI], support key generation, signature and ciphering of messages.

Some proprietary APIS are available as well.

### 2.1.2.4 Global Platform

The Global Platform application consists of the Card Manager, the API GPsysteM, the security domains. It is implemented in Java and its byte-code is stored in ROM.

It is compliant with the standard [GP].

The Global Platform application is activated upon the selection of the Card Manager, by the Card Issuer, the API GPsysteM can be called at any time by the applets.

### 2.1.2.5 Resident Application

It provides a native code application, with a basic main dispatcher, to receive the card commands and dispatch them to the application and module functions to implement the application commands.

It also deals with the Card Manufacturer authentication and logical channels management.

The dispatcher is always activated. Some card commands (for administration) are only available during prepersonalization phase.

## 2.2 TOE Identification

TOE is composed of the following components :

- MicroController: Philips Smart MX P5CT072/V0P
- ROM code of the platform: P5CT072EW1/T0PB6311 – OCS Reference 064471
- Optional Code r1.0 on GOP ID MX64R01 – OCS Reference : 065881
- File System API for JavaCard 2.2 – OCS Reference : 063222
- Security API for JavaCard 2.2 – OCS Reference : 063232
- Secure Messaging for JavaCard 2.2 – OCS Reference : 063242
- Utilities API for JavaCard 2.2 – OCS Reference : 063812
- ID One V3 Applet – OCS Reference : 063253

Platform can be identified by retrieving Card Identification Data (tag **DF52**) : Mask Identification = **E910** - Optional Code Identification : **065881**). For more details, see document [GOP ID MX64], GET DATA command.

JavaCard APIs and applet can be identified by retrieving APIs and applet versions, using GET DATA command :

- File System : **A008**
- Security : **A009**
- Secure Messaging : **A00D**
- Utilities : **A004**
- ID One V3 Applet : **D014**

For more details, see document [ID One V3], §11.12.3 “GET DATA – Administrative data”

All the components of the TOE are maintained under Configuration Management (PVCS), and archived with the label **COSMOS V1.1**.

# Oberthur Card System - Cosmos

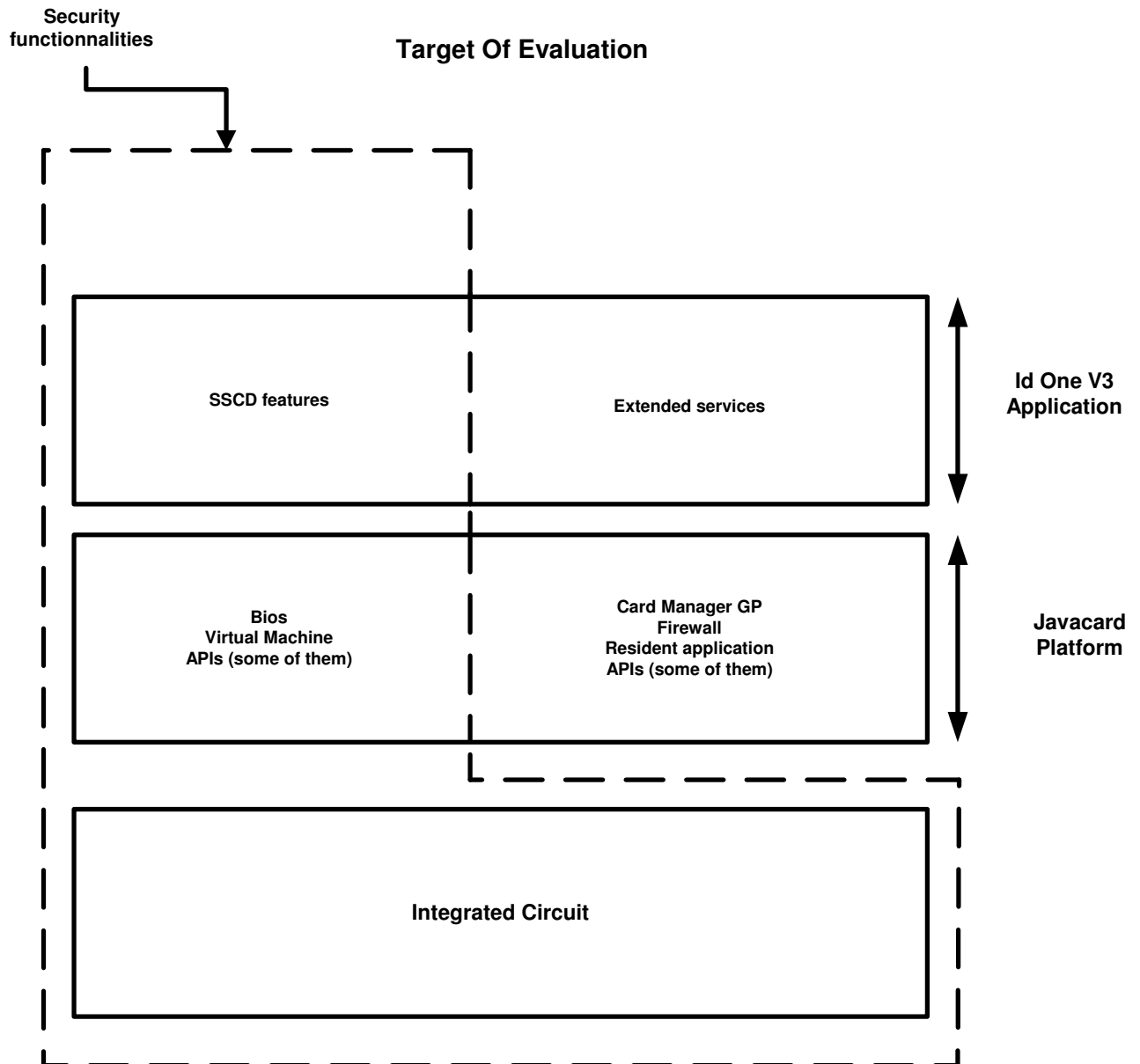
## Security Target Lite

Commercial name of the TOE is :

**IDOne IAS applet (SSCD configuration) loaded on COSMO 64 RSA D v5.4 embedded on a Philips P5CT072V0P MicroControler (COSMOS V1.1)**

### 2.3 TOE overview

The Target of evaluation is made of the whole smart card. For each layer described below, we will consider only features related to the SSCD configuration. The figure below shows the way the features of each layer were singled out.



*Figure 2 : Target Of Evaluation : TSP functions*

The function of the application layer that are related to the SSCD features are the following:

- Generation of SCD and SVD
- Secrecy of the SCD
- Import of the SCD/SVD

# Oberthur Card System - Cosmos

## Security Target Lite

---

- Export of SVD
- Signature Creation
- PIN administration
- Pin Authentication of the Signatory: the RAD used to verify the VAD is held securely.
- External authentication of an administrator
- Implementation of a trusted path to a human interface device

The application of the javacard platform that are related to the SSCD features are the following :

- Bios (some subparts only)
- Virtual Machine (except the firewall)
- APIs the SSCD features use for their implementation (both javacard and proprietary APIs)

The whole functionalities of the Integrated circuit are included in the Target Of Evaluation

The extended services the application contains are the following:

- Symmetric/asymmetric encipherment/decipherment
- C/S authentication
- Computation/Verification of cryptographic checksum
- Signature verification
- Asymmetric external authentication
- Assymmetric device authentication
- PKI handling

Theses functionalities are not available in the configuration in which the application is set and are outside the scope of the TOE.

### *2.4 Description of the application ID One V3 used as a simple signature creation application*

The application ID one V3 used as a simple signature creation application offers only a subset of functionalities that are sufficient to fulfil the requirement of the SSCD type 2 & type 3.

#### **2.4.1 Cryptographic services**

The ID One V3 applet used as a signature creation application is a high security product which provides the following cryptographic services:

- Symmetric secure messaging opening based on [E-SignK] ;
- Secure messaging, based on [E-SignK] ;
- Dynamic management of confidentiality/integrity (Secure Messaging conditions) settings ;
- RSA key pair generation (1024, 1536 and 2048 bits)
- DES based external authentication

# Oberthur Card System - Cosmos

## Security Target Lite

---

- PIN authentication and administration;
- RSA digital signature computation;

### 2.4.2 Data structures handled by the application

Two kinds of data structures are available: files and SDOs (Security Data Object).

#### 2.4.2.1 File system

The file system the application ID One uses is very simple. It is only a master file (MF) that contains several EFs.

The Master File is the root of the file system and is always the initial entry point to the file system. After a reset of the card, the MF is selected.

The Elementary File (EF) is used for data storage –to store certificate for instance. For this reason EFs are also referred to as *data files*. File access is similar to traditional file systems. To access a file (for reading, writing, or any other operation), it has to be selected.

Each file, through the File control Parameters (FCP) contains all the information needed to handle the data it contains:

- The access condition
- The identifier
- The type

The application can administrate the file system (in accordance with the access conditions), i.e.

- Read, write, append, erase the content of the file (EF)
- Block/Terminate an EF

#### 2.4.2.2 Security Data Object

A Security Data Object (SDO) is a container for secret/sensitive data, including SCD, SVD and RAD. All SDOs are stored within DF.

We distinguish several kinds of SDO depending on the typed of secret data they contain:

- SDO for user authentication data (including RAD)
- SDO for symmetric key set
- SDO for RSA private portion (including SCD)
- SDO for RSA public portion (including SVD)

The SDO contains all the information needed to handle the secret data embedded in it:

- The access condition
- The access mode
- The identifier
- The type

The application can administrate these SDOs (in accordance with the access conditions), i.e.

- Use and update the content of the secret data for a given usage
- Generate an asymmetric key pair (RSA)
- Export of SDOs content (except private RSA portion)

The administration of the SDOs includes in particular

- The administration of the SCD and the SVD
- the import of the SCD
- the export of the SVD
- the administration of the RAD

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 2.4.3 Access conditions

An Access Condition can be attached to a file, or to a security data object (SDO). It tells which security status have to be fulfilled in order to allow a specific operation on a specific object.

An access condition on one object may take the following values:

- ALWAYS: operation always allowed
- NEVER: operation never allowed (if so, the access condition is omitted)
- USER AUTHENTICATION : operation granted if the requested user authentication security status is set to true (performed with a PIN) .
- EXTERNAL AUTHENTICATION : operation granted if the requested external authentication security status is set to true
- SECURE MESSAGING : operation granted if the incoming command is protected with the security level expected (confidentiality and/or integrity). This condition can only be fulfilled if a secure channel was opened prior to it.
- LOGICAL COMBINATION AND or OR of the later three ones (USER AUTHENTICATION, EXTERNAL AUTHENTICATION, SECURE MESSAGING)

### 2.4.4 Security Status

A security status is associated to each secret data used to gain an access. Roughly, each authentication scheme grants a right, whatever it is

- a PIN (RAD)
- a Symmetric key set used for external authentication
- three Symmetric key sets used to open secure channels with each entities it might communicate with : SSCD, SCA and CGA.

These security status are very important as they are checked when an access condition is requested to allow an operation (e.g. use of the SVD,...).

At any time, the application keeps track of all the security status it contains.

At reset of the card, all the security status are reset.

When a new authentication with a given secret (PIN, key set) fails, the associated security status is reset, even if it was true.

### 2.4.5 Secure Messaging

The Secure Messaging (SM) is used to protect the communication between the interface device (IFD) and the smart card.

First of all, it ensure a mutual authentication of both parts that have to agree on a common key set for secure exchange (if so).

Two levels of secure messaging are available:

- SM\_SIG: APDU commands with cryptographic checksum (data integrity)
- SM\_SIG\_ENC: APDU commands with enciphered data and cryptographic checksum (data confidentiality and integrity)

It is possible to use one level or the other within the same secure messaging session.

Once a secure messaging is initiated (through a mutual authentication – we say secure channel opening), the incoming command are processed the same way as if they were sent in plain text. The only difference is that it grants the access condition “Secure messaging”.

To fulfill the access condition “Secure Messaging”, the following conditions must be fulfilled:

- the incoming command must be protected at least with the security level requested in the access condition;
- the secure channel opening must have the same type as the one specified in the access condition;
- The secret data used for the secure channel opening must be the one specified in the access condition;



# Oberthur Card System - Cosmos

## Security Target Lite

---

The process that initiates the secure messaging is called “device authentication”. It consists in a mutual authentication of both parts, i.e. ICC and IFD. It generates the session keys used to secure the communications as well. The application ID One V3 used as a simple signature creation application uses a symmetric scheme for the device authentication.

### *2.5 TOE intended usage*

The TOE intended usage is the Creation of Secure Signatures according to [SSCD2] and [SSCD3].

# Oberthur Card System - Cosmos

## Security Target Lite

### 2.6 TOE life cycle

The Smart card life-cycle is decomposed into 7 phases, described hereafter.

This life cycle is related to the different phases the designer/manufacturer/issuer has to go through to get a smart card ready to use. It starts from the design till the end of usage of the card.

It is depicted in the figure below

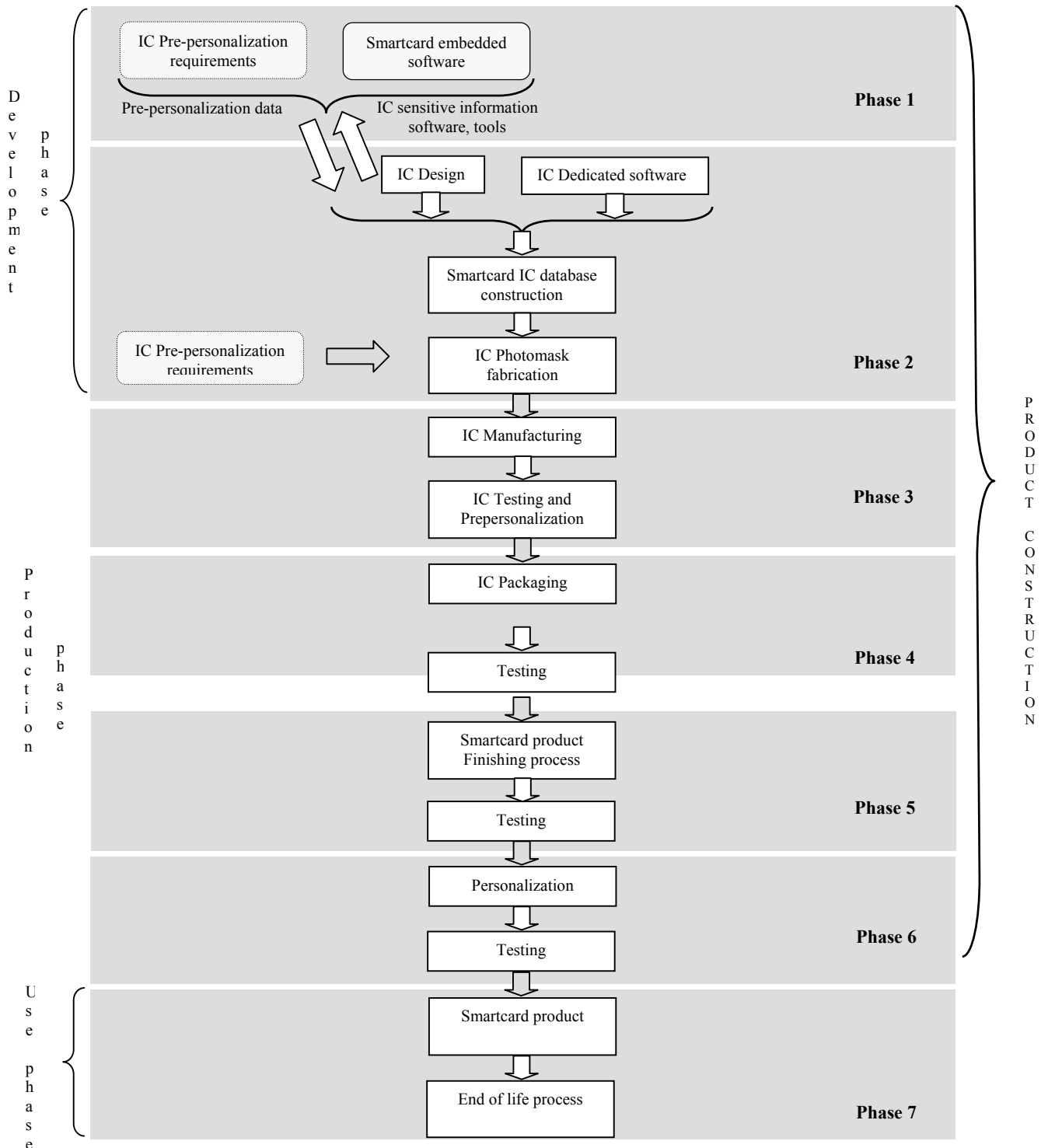


Figure 3 : Smart Card Life cycle

## 2.7 Description of the TOE environment

The TOE environment may be splitted into two different parts:

- The **development environment**, in which the TOE is designed, tested and manufactured. The security requirements that are applied reach the one described in [SSCD2], [SSCD3] and [BSI-0002].
- The **production environment** in which the TOE is tested and manufactured. The security requirements that are applied reach the one described in [SSCD2], [SSCD3] and [BSI-0002].
- The **User environment**, in which the TOE is used as stated in [SSCD2], [SSCD3] and [BSI-0002]. The security requirements that are requested and the assurance levels are met.

### 2.7.1 Development environment

#### 2.7.1.1 Software development (phase 1)

This environment is limited to OBERTHUR CARD SYSTEM Nanterre site.

To ensure security, access to development tools and products elements (PC, emulator, card reader, documentation, source code, etc..) is protected. The protection is based on measures for prevention and detection of unauthorized access. Two levels of protection are applied:

- Access control to OBERTHUR CARD SYSTEM Nanterre offices and sensitive areas.
- Access to development data through the use of a secure computer system to design, implement and test software

#### 2.7.1.2 Hardware development

The environment is limited to PHILIPS site

The IC development environment is described in [STIC]

The IC is certified EAL5+ and the IC certificate reference is BSI-DSZ-CC-0348-2006

### 2.7.2 Production environment

#### 2.7.2.1 IC manufacturing (phase 3)

The IC production environment is described in [STIC]

The IC is certified EAL5+ and the IC certificate reference is BSI-DSZ-CC-0348-2006

#### 2.7.2.2 TOE manufacturing (phase 4 to 6)

All the production sites present adequate security measures that fit the TOE protection during its manufacturing even if they are not in the scope of security assurance requirements for the environment.

More precisely, all the guidance for initialization, pre-personalization and personalization are applied with respect to A.USE\_PROD.

### 2.7.3 User environment

At the end of the phase 6, the card issuer delivers the smart card to the administrator of the SSCD service.

The TOE delivered to the administrator has the following features:

- The TOE can authenticate its administrator using an external authentication performed by a cryptographic mean.

# Oberthur Card System - Cosmos

## Security Target Lite

---

- Terminal can initiate a symmetric mutual authentication and a secure messaging to ensure authenticity of the SSCD, and the integrity and confidentiality of the exchange.
- Terminal can initiate a symmetric mutual authentication and a secure messaging to ensure authenticity of the SCA, and the integrity and confidentiality of the exchange.
- Terminal can initiate a symmetric mutual authentication and a secure messaging to ensure authenticity of the CGA, and the integrity and confidentiality of the exchange.

The TOE contains the following *empty* objects:

- SCD
- SVD
- File (for certificate storage)
- RAD

It is up to the administrator that receives the TOE to initialize and personalize it. Once the TOE is initialized/personalized, the signatory will have to present his PIN (RAD) before being allowed to create signature.

### *2.8 Description of the TOE's scope*

The scope of this present security target is:

- TOE development phase realized in the OBERTHUR CARD SYSTEM environment in phase 1
- TOE manufacturing phase realized in the PHILIPS environment in phase 2 & 3

All other phases are out of the scope of the TOE. (i.e. security assurance requirements for the corresponding environment are out of the scope.

The TOE embedded software, developed and embedded during phases 1 to 3, aims to control and protect the TOE during phases 4 to 7.

As such, this Security Target addresses all the security features put in place in phases 4 to 7 but that are developed in phase 1 while [STIC] addresses the security requirements for phases 2 and 3 for the same objective.

#### **2.8.1 The development phase : phase 1**

This phase is performed at OBERTHUR CARD SYSTEMS' site in NANTERRE (France).

#### **2.8.2 The manufacturing phase : phase 2**

This phase is performed at PHILIPS manufacture. The security of the procedures is described in [STIC] and ensured by the IC certificate reference BSI-DSZ-CC-0348-2006

#### **2.8.3 The prepersonalization phase : phase 3**

This phase is performed at PHILIPS manufacture. It mainly consists in changing the manufacturer's MSK to set the Live MSK.

This phase is performed at PHILIPS manufacture. The security of the procedures is described in [STIC] and ensured by the IC certificate reference BSI-DSZ-CC-0348-2006

### 2.9 Initialization and personalization of the TOE

The behaviour of the TOE is obtained by a relevant electrical personalization made during the phase 6.

The phase 6 is the phase in which the TOE is initialized to be used (in phase 7).

Throughout its initialization, several steps have to be achieved in order to get a smart card “ready to use”.

The Global Platform [GP] defines life cycle state models to control the functionality and security of the following components: Card Manager, Resident application, Card Registry, Key sets, Load Files, and Applet. These life cycle models are presented in this section

Roughly, the global state of the smart card mainly depends on the state of

- the resident application
- the card manager
- the applet

The resident application is the first application available when the smart card is brand new. Its main purpose is to allow the card manager installation. Once the card manager is available, the functionality of resident application is restricted to the APDU dispatch.

The Card Manager is responsible for maintaining the overall security and administration of the card and its contents. Because the Card Manager plays this supervisory role over the entire card, its life cycle can be thought of as the life cycle of the card. The card’s life cycle from a Global Platform perspective only has meaning at the beginning of the Card Manager life cycle.

The Card Manager owns and maintains the card life cycle state information and manages the requested state transitions in response to APDU commands. The end of the Card Manager life cycle is considered to be equivalent to the end of the card’s life cycle.

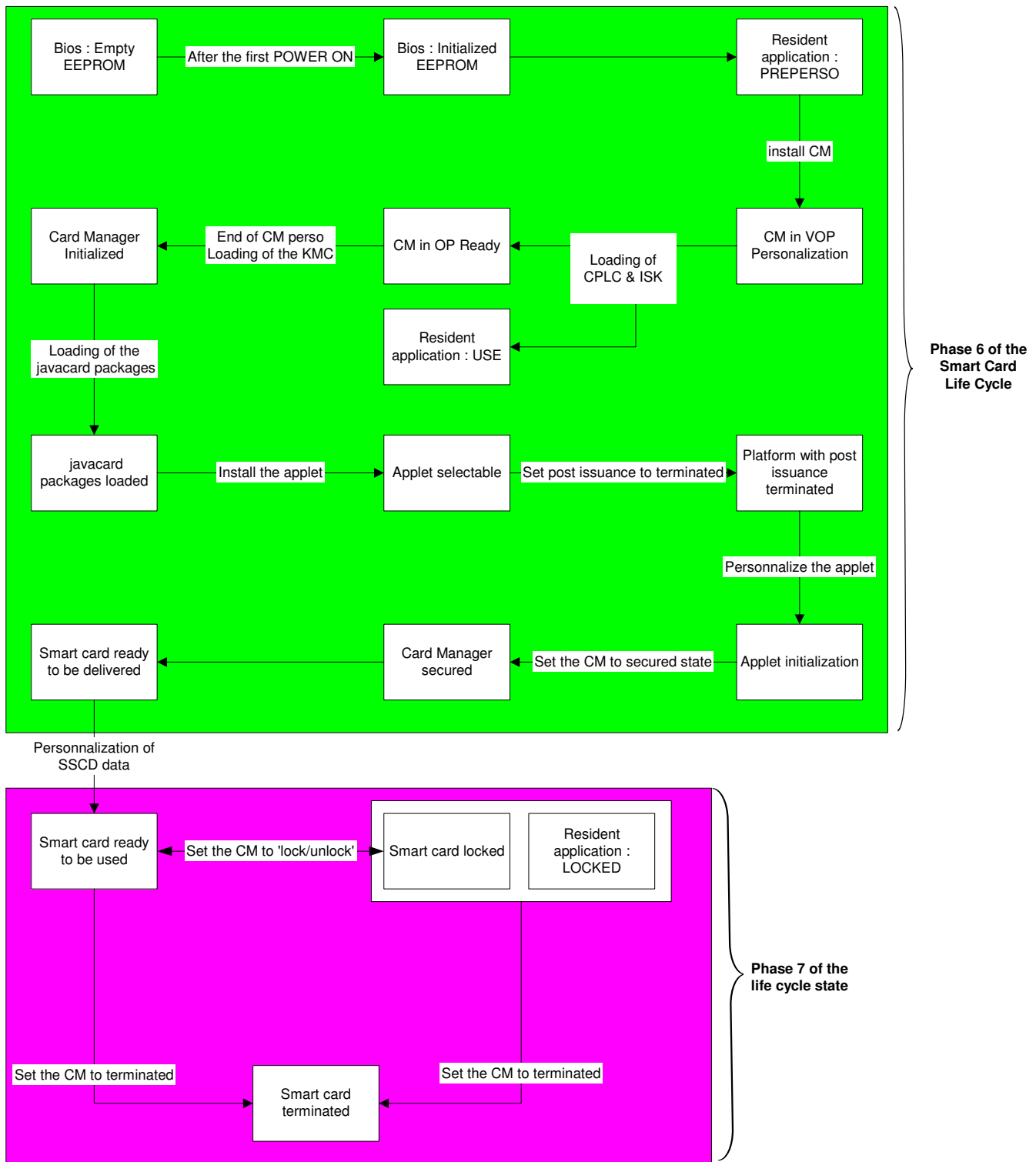
The applet, once its instance is created is in the state “SELECTABLE”. It can be selected to be personalized with its applicative data. Once the personalization is completed, it is switch in the phase “PERSONNALIZED”.

It may be switched to the state “LOCKED” if the card manager is locked, and unlock when the card manager is unlocked.

The smart card life cycle transition is depicted in the figure below:

# Oberthur Card System - Cosmos

## Security Target Lite



*Figure 4 : Smart card life-cycle transition*

### 2.9.1.1 Bios : Empty EEPROM

This is the state of the chip delivered by the IC manufacturer, the EEPROM is empty except the Manufacturer Transport key (MSK).

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 2.9.1.2 Bios : Initialized EEPROM

On the first Power-On, the BIOS initializes its data: the ATR files, the default applet reference, the FAT.

### 2.9.1.3 Resident application : preperso

In prepersonalization state, the set of commands of the resident application (EXTERNAL\_AUTHENTICATE, GET\_CHALLENGE, GET\_DATA, INSTALL, LOAD\_APPLET, LOAD\_STRUCTURE, MANAGE\_CHANNEL) is active. It enables to install the card manager in the next steps

### 2.9.1.4 CM in VOP Personalization

This life state is the initial life state of the Card Manager applet, just after it has been installed.

In this life state, initialization key (ISK) and card and chip CPLC have to be loaded before switching to "OP\_READY" life state.

### 2.9.1.5 CM in OP Ready

In the card life cycle state "OP\_READY", all the basic functionality of the run-time environment is available and the Card Manager is ready to receive, execute and respond to APDU commands.

The card is assumed to have the following functionality in the state "OP\_READY":

- The run-time environment is ready for execution.
- An Initialization key is available within the Card Manager.

### 2.9.1.6 Resident application : use

Once the card manager is in state "OP\_READY", the resident application is switched in the phase use. Its set of commands is shortened (SELECT, MANAGE\_CHANNEL, and GET\_DATA only if no applet is selected).

### 2.9.1.7 CM initialized

The card life cycle state "CM\_INITIALIZED" is an administrative card production state. Most of the personalization of the Card Manager is performed when entering in that state (KMC, CPLC data,..)

### 2.9.1.8 Javacard packages loaded

In this state, the javacard packages needed for the applet instantiation are loaded.

### 2.9.1.9 Applet selectable

In this state the applet can be selected. It is said to be in state "SELECTABLE". The applet is ready to be personalized with its applicative data. In particular, the SCD, the SVD and other keys may be loaded. To ensure the confidentiality and/or integrity of the SCD, of the SVD and other keys, the secure messaging GP may be used during this phase.

### 2.9.1.10 Platform with post issuance terminated

In this state the post issuance features of the platform are locked as the card manager can not load or delete packages anymore, nor instantiating an applet, nor deleting an instance.  
No more applet can be added

# Oberthur Card System - Cosmos

## Security Target Lite

---

No more packages can be loaded  
No instance can be deleted  
No instance can be created

### 2.9.1.11 Applet initialized

In this state, the applet was personalized. It was given all the applicative data structure (Files, SDOs,...) it needed and its state was permanently switched to "PERSONALIZED". During this state, the keys needed to authenticate the administrator as well as the keys needed to open a secure channel are loaded.

### 2.9.1.12 CM secured

The Card life cycle state "CM\_SECURED" is the normal operating life cycle state of the card during issuance. This state is the indicator for Card Manager to enforce the Card Issuer's security policies related to post-issuance card behavior such as applet loading and activation.

- The card is assumed to have the following functionality in the state "CM\_SECURED":
- The Card Manager contains all necessary key sets and security elements for full functionality.
- Card Issuer initiated card content changes can be carried out through the Card Manager.
- Post-issuance personalization of applets belonging to the Card Issuer can be carried out via the Card Manager

### 2.9.1.13 Smart card ready to be delivered

This is the state in which the TOE is when it is delivered to the administrator of the SSCD service. It is ready to store the RAD, the SCD and SVD.

### 2.9.1.14 Smart card ready to be used

Once the administrator loaded the RAD, SCD and SVD, the TOE is ready to be issued to the signatory. The TOE is ready to sign.

### 2.9.1.15 Smart card locked

This state is achieved when the card manager is set to the state "CM\_LOCKED". The state "CM\_LOCKED" is used to tell the Card Manager to temporarily disable the applet on the card except for the Card Manager. This state is created to give the Card Issuer the ability to temporarily disable functionality of the card on detection of security threats (either internal or external to the card). Setting the Card Manager to this state means that the card will no longer work, except via the Card Manager which is controlled by the Card Issuer. When the smart card is locked, the resident applet (application) is switched in state "BLOCKED"

### 2.9.1.16 Resident Application : locked

When the card manager is set in the state "CM\_LOCKED", the resident application is switch to the state "LOCKED". All the commands of the resident application are inactive.

### 2.9.1.17 Smart card terminated

This state is achieved when the card manager is set to the state "CM\_TERMINATED".



# Oberthur Card System - Cosmos

## Security Target Lite

---

The Card Manager is set to the life cycle state "CM\_TERMINATED" to permanently disable all card functionalities including the functionality of the Card Manager itself. This state is created as a mechanism for the Card Issuer to logically 'destroy' the card for such reasons as the detection of a severe security threat or expiration of the card.  
The Card Manager state "CM\_TERMINATED" is irreversible and signals the end of the card's life cycle.

### 3 TOE SECURITY ENVIRONMENT

This section describes the security aspects of the environment in which the TOE is to be used. It describes the assets to be protected, the threats, the organizational security policies and the assumptions.

#### 3.1 Subjects

Subject	Definition
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory.
S.Admin	User who is in charge to perform the TOE initialization, TOE personalisation or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.
S.OFFCARD (Threat agent)	Attacker. A human or a process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a high level potential attack and knows no secret.

#### 3.2 Assets

The assets of the **TOE** are those defined in [SSCD2] and [SSCD3]:

1. **D.SCD**: private key used to perform an electronic signature operation. Confidentiality of the **D.SCD** must be maintained.
2. **D.SVD**: public key linked to the **D.SCD** and used to perform an electronic signature verification. Integrity of the SVD when it is exported must be maintained.
3. **D.DTBS** and **D.DTBS-representation**: set of data, or its representation which is intended to be signed. Their integrity must be maintained.
4. **D.VAD**: PIN code entered by the End User to perform a signature operation. Confidentiality and authenticity of the **D.VAD** as needed by the authentication method employed.
5. **D.RAD**: Reference PIN code used to identify and authenticate the End User. Integrity and confidentiality of **D.RAD** must be maintained.
6. **D.SIGN\_APPLI**: Signature-creation function of the **SSCD** using the **D.SCD**. The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures.
7. **D.SIGNATURE**: Electronic signature. Unforgivably of electronic signatures must be assured.

We detail below the representation of the Asset data in ID One V3:

# Oberthur Card System - Cosmos

## Security Target Lite

Asset data	Attribute	Status
<b>D.SCD</b>		
<b>D.SCD</b> is stored in ID One V3 as a SDO (Security Data Object) of the type RSA private portion	AC_GENKEYPAIR	Access condition for <b>D.SCD / D.SVD</b>
	AC_USE	Access condition for digital signature creation. It must reference the PIN SDO corresponding to the <b>D.RAD</b> .
	AC_CHANGE	Access condition for modifying (import)
<b>D.SVD</b>		
<b>D.SVD</b> is stored in ID One V3 as a SDO (Security Data Object) of the type RSA public portion	AC_READ	Access condition to be satisfied for reading a <b>D.SVD</b>
	AC_GENKEYPAIR	Access condition for <b>D.SCD / D.SVD</b> generation
	AC_CHANGE	Access condition for modifying (import) a new key
PIN (RAD)		
PINs are stored in ID One V3 as a SDO (Security Data Object) of the type user authentication	AC_USE	Access condition to be satisfied for
	AC_CHANGE	Access condition to be satisfied for modifying a PIN value
	AC_INIT	Access condition to be satisfied for initializing a PIN

*Table 1 : ID One V3 Attributes (1)*

The RAD (SCD.AC\_USE) is restricted to be defined as a PIN. Other access conditions (like AC\_GENKEYPAIR for example) are not concerned by this restriction: they are Boolean expressions of PIN, external authentication to be fulfilled and secure messaging level to be satisfied.

To protect the Asset data during communication between the TOE and the terminal, TOE uses Secure Messaging with session keys generated at device authentication. The level of protection of the incoming command (SM\_SIG or SM\_SIG\_ENC) and the keys to use for the device authentication may be specified within the access conditions of the Asset data .

We complete the Asset Data by adding the following keys the TOE manages:

- The keys needed to perform symmetric external authentication
- The keys needed to perform symmetric device authentication

Data	Attribute	status
External and device authentication keys		
	AC_USE	Access condition to be satisfied for using the keys

*Table 2 : ID One V3 Attributes (2)*

# Oberthur Card System - Cosmos

## Security Target Lite

---

The symmetric keys used for external authentication and device authentication can not be modified

### 3.3 Assumptions

#### A.CGA *Trustworthy certification-generation application*

The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.

#### A.SCA *Trustworthy signature-creation application*

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

#### A.SCD\_Generate *Trustworthy SCD/SVD generation*

If a party other than the signatory generates the SCD/SVD-pair of a signatory, then

- (a) this party will use a SSCD for SCD/SVD-generation,
- (b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and
- (c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.
- (d) The generation of the SCD/SVD is invoked by authorised users only
- (e) The SSCD Type1 ensures the authenticity of the SVD it has created and exported

### 3.4 Threats

#### T.Hack\_Phys *Physical attacks through the TOE interfaces*

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.

#### T.SCD\_Divulg *Storing ,copying, and releasing of the signature-creation data*

An attacker can store, copy the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

#### T.SCD\_Derive *Derive the signature-creation data*

An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.

#### T.Sig\_Forgery *Forgery of the electronic signature*

An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

#### T.Sig\_Repud *Repudiation of signatures*

If an attacker can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

#### T.SVD\_Forgery *Forgery of the signature-verification data*

An attacker forges the SVD presented by the TOE. This result in loss of SVD integrity in the certificate of the signatory.

# Oberthur Card System - Cosmos

## Security Target Lite

---

### *T.DTBS\_Forgery Forgery of the DTBS-representation*

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intends to sign.

### *T.SigF\_Misuse Misuse of the signature-creation function of the TOE*

An attacker misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

## 3.5 ORGANIZATIONAL SECURITY POLICIES

### *P.CSP\_QCert Qualified certificate*

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

### *P.QSign Qualified electronic signatures*

The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.

### *P.Sigy\_SSCD TOE as secure signature-creation device*

The TOE stores the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

## 4 SECURITY OBJECTIVES

### 4.1 Security Objectives for the TOE

#### *OT.EMSEC\_Design Provide physical emanations security*

Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

#### *OT.Lifecycle\_Security Lifecycle security*

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-import or re-generation.

#### *OT.SCD\_Secrecy Secrecy of the signature-creation data*

The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.

#### *OT.SCD\_SVD\_Corresp Correspondence between SVD and SCD*

The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.

#### *OT.SVD\_Auth\_TOE TOE ensures authenticity of the SVD*

The TOE provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.

# Oberthur Card System - Cosmos

## Security Target Lite

---

### *OT.Tamper\_ID Tamper detection*

The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.

### *OT.Tamper\_Resistance Tamper resistance*

The TOE prevents or resists physical tampering with specified system devices and components.

### *OT.InitSCD/SVD generation*

The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by authorized users only.

### *OT.SCD\_Unique Uniqueness of the signature-creation data*

The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.

### *OT.SCD\_Transfer Secure transfer of SCD between SSCD*

The TOE shall ensure the confidentiality of the SCD transferred between SSCDs.

### *OT.DTBS\_Integrity\_TOE Verification of the DTBS-representation integrity*

The TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.

### *OT.Sigy\_SigF Signature generation function for the legitimate signatory only*

The TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

### *OT.Sig\_Secure Cryptographic security of the electronic signature*

The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

## 4.2 Security Objectives For The Environment

### *OE.SCD\_SVD\_Corresp Correspondence between SVD and SCD*

The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSCD Type1 shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

### *OE.SCD\_Transfer Secure transfer of SCD between SSCD*

The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

### *OE.SCD\_Unique Uniqueness of the signature-creation data*

The SSCD Type1 shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.

# Oberthur Card System - Cosmos

## Security Target Lite

---

### OE.CGA\_QCert *Generation of qualified certificates*

The CGA generates qualified certificates which include inter alia

- (a) the name of the signatory controlling the TOE,
- (b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,
- (c) the advanced signature of the CSP.

### OE.SVD\_Auth\_CGA *CGA verifies the authenticity of the SVD*

The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

### OE.HI\_VAD *Protection of the VAD*

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

### OE.SCA\_Data\_Intend *Data intended to be signed*

The SCA

- (a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,
- (b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE
- (c) attaches the signature produced by the TOE to the data or provides it separately.

## 5 IT SECURITY REQUIREMENTS

### 5.1 TOE IT SECURITY FUNCTIONAL REQUIREMENTS

#### 5.1.1 FCS: CRYPTOGRAPHIC SUPPORT

##### 5.1.1.1 FCS\_CKM cryptographic key management

FCS\_CKM.1 Cryptographic key generation

##### FCS CKM.1.1 / RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA key generation] and specified cryptographic key sizes [1024 bits or 1536 bits or 2048 bits] that meet the [ANSI X9.31]

##### Application Note:

Even though, a RSA key with a key size of 1024 bits may be used, it is strongly recommended to use at least a key size of 1536 bits as stated in [CryptoRules]

##### FCS CKM.1.1 / DES session keys

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [DES key generation] and specified cryptographic key sizes [128 bits] that meet the [ANSI X9.63]

##### Application Note:

The hashing algorithm used by the TOE to generate the session keys from the Seed is the SHA-1.

# Oberthur Card System - Cosmos

## Security Target Lite

---

FCS\_CKM.4 Cryptographic key destruction

### FCS\_CKM.4.1 / SCD/SVD

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting the buffer containing the key] that meets the following: [ISO 11166].

Application note:

The destruction of D.SCD is mandatory before the SCD/SVD pair is re-generated or re-imported by the TOE.

### FCS\_CKM.4.1 / Symmetric DES keys

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting the buffer containing the key] that meets the following: [ISO 11568].

Application note:

The Symmetric DES key includes the keys used for the device authentication with the symmetric scheme and the External authentication performed with the symmetric keys as well as the secure messaging session keys.

The destruction of the previous External Authentication keys is mandatory when they are updated

## **5.1.1.2 FCS\_COP Cryptographic operation**

FCS\_COP.1 Cryptographic operation

### FCS\_COP.1.1/ CORRESP

The TSF shall perform [SCD/SVD correspondence verification] in accordance with a specified cryptographic algorithm [RSA CRT key computation] and cryptographic key sizes [1024 bits or 1536 bits or 2048 bits] that meet the following: [PKCS #1 V1.5].

Application Note:

Even though, a RSA key with a key size of 1024 bits may be used, it is strongly recommended to use at least a key size of 1536 bits as stated in [CryptoRules]

### FCS\_COP.1.1/ SIGNING

The TSF shall perform [Digital signature-generation] in accordance with a specified cryptographic algorithm [RSA CRT using Private Key] and cryptographic key sizes [1024 bits or 1536 bits or 2048 bits] that meet the following: [PKCS #1 V1.5 Block Type 1].

Application Note:

Even though, a RSA key with a key size of 1024 bits may be used, it is strongly recommended to use at least a key size of 1536 bits as stated in [CryptoRules]

### FCS\_COP.1.1/ Secure Messaging Signature

The TSF shall perform [Secure Messaging Signature] in accordance with a specified cryptographic algorithm [Retail MAC] and cryptographic key sizes [128 bits] that meet the following: [CryptoCotation].

Application Note:

This algorithm is used during secure Messaging: for computation of signature (SM\_SIG) of outgoing APDU commands and verification of signature (SM\_SIG) of incoming APDU commands

# Oberthur Card System - Cosmos

## Security Target Lite

---

### FCS COP.1.1/ Secure Messaging Encryption/Decryption

The TSF shall perform [Secure Messaging Encryption/Decryption] in accordance with a specified cryptographic algorithm [Triple DES CBC encryption/decryption] and cryptographic key sizes [128] that meet the following: [CryptoCotation].

Application Note: This algorithm is used during secure Messaging: for encryption of data (SM\_SIG\_ENC) for outgoing APDU commands and decryption of data (SM\_SIG\_ENC) for incoming APDU commands

### FCS COP.1.1/ External Authentication

The TSF shall perform [External Authentication] in accordance with a specified cryptographic algorithm [using DES] and cryptographic key sizes [128 bits ] that meet the following: [CryptoCotation].

Application Note: This algorithm is used during symmetric external Authentication: to verify the challenge sent by the terminal

### FCS COP.1.1/ Device authentication

The TSF shall perform [Device Authentication] in accordance with a specified cryptographic algorithm [using DES] and cryptographic key sizes [128 bits] that meet the following: [CryptoCotation].

Application Note: This algorithm is used during symmetric device authentication to authenticate both the terminal and the card

### FCS COP.1.1/ Signature verification

The TSF shall perform [Signature verification] in accordance with a specified cryptographic algorithm [RSA CRT using Public Key] and cryptographic key sizes [1024 bits or 1536 bits or 2048 bits] that meet the following: [PKCS #1 V1.5 Block Type 2].

## **5.1.2 FDP : USER DATA PROTECTION**

### **5.1.2.1 FDP\_ACC Access Control Policy**

FDP ACC.1 Subset access control

#### FDP\_ACC.1.1/SVD transfer SFP

The TSF shall enforce the [SVD transfer SFP] on [export of SVD by User].

Application note:

FDP\_ACC.1/SVD Transfer SFP will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

#### FDP\_ACC.1.1/Initialisation SFP

The TSF shall enforce the [Initialisation SFP] on [Generation of SCD/SVD pair by User].

#### FDP\_ACC.1.1/SCD Import SFP

The TSF shall enforce the [SCD Import SFP] on [Import of SCD by User].

#### FDP\_ACC.1.1/ Personalisation SFP

The TSF shall enforce the [Personalisation SFP] on [Creation of PIN RAD by Administrator].



# Oberthur Card System - Cosmos

## Security Target Lite

### FDP\_ACC.1.1/Signature-creation SFP

The TSF shall enforce the [Signature-creation SFP] on

1. [Sending of DTBS representation by SCA]
2. [Signing of DTBS-representation by Signatory].

### 5.1.2.2 FDP\_ACF access control function

FDP\_ACF.1 Security attribute based access control

Correspondence between attributes defined in SSCD Type 2 and Type 3 and ID One V3 attributes:

The security attributes for the subjects, TOE components and related status are:

		SSCD Attribute	ID One V3 Attribute	Explanation
<b>General Attribute</b>				
USER		ROLE	ROLE	Administrator, Signatory
<b>Signature-creation attribute</b>				
operational SCD	Name:	SCD operational	SCD.AC_USE	"SCD operational" corresponds to the access condition SCD.AC_USE. Its status is "Yes" if and only if the access condition is satisfied. "SCD operational" is set to "Yes" if Role = S.Signatory
	Associated to:	SCD	SCD	
	Status:	No, Yes	Not Satisfied (No), Satisfied (Yes)	
sent by an authorised SCA	Name:	sent by an authorised SCA	MAC (protection in integrity of incoming APDU)	"sent by an authorized SCA" is ensured by a device authentication performed prior to the DTBS-representation sending. The device authentication is performed with a key set that only the SCA knows. Once the device authentication is performed, secure messaging is available to protect the communication between the TOE and the SCA (it is broken once a plain text command is sent). Each command is protected at least in integrity. The protection in integrity of the APDU containing the DTBS representation is imposed by SCD.AC_USE : As the SCD must be used for signature just after the DTBS-representation is sent, if its integrity is not verified or missing, SCD.AC_USE can not be fulfilled and no signature will be computed.
	Associated to:	DTBS	DTBS	
	Status:	No, Yes	Not Verified (No), Verified (Yes)	
<b>Initialisation attribute (SSCD Type 2)</b>				
D SCD/SV	Name:	SCD/SVD management	SCD.AC_CHANGE SVD.AC_CHANGE	In ID One V3, there are two ways to import an SCD: - Initialize both SVD and SCD and then define first the SVD and then the SCD
	Associated to:	USER	USER	

# Oberthur Card System - Cosmos

## Security Target Lite

	Status:	Authorised, Not Authorised	Satisfied (Authorised), Not Satisfied (Not Authorised)	<p>object</p> <ul style="list-style-type: none"> <li>- If both SCD and SCD are initialized, update first the SVD and then the SCD object</li> </ul> <p>SVD and SCD definition and update are respectively protected by SVD.AC_CHANGE and SCD.AC_CHANGE</p> <p>The SCD can be updated only once the SVD is fully updated. This operation must be performed within a sequence. Once the sequence is completed, the coherency between SCD and SVD is verified. In any other case, the SCD import will be rejected.</p> <p>SVD.AC_CHANGE, SCD.AC_CHANGE are viewed as attributes of USER since they are used to authenticate the USER.</p>
Secure SCD Import allowed	Name:	Secure SCD Import allowed	protection in confidentiality and integrity of incoming APDU SCD authenticated	<p>“Secure SCD Import allowed” is ensured by a device authentication performed prior to the secure SCD import. The device authentication is performed with a key set that only the SSCD knows.</p> <p>Once the device authentication is performed, secure messaging is available to protect the communication between the TOE and the SSCD (it is broken once a plain text command is sent). Each command is protected at least in integrity.</p>
	Associated to:	SCD	SCD	
	Status:	No, Yes	Not Verified (No), Verified (Yes)	
Initialisation attribute (SSCD Type 3)				
SCD/SVD management	Name:	SCD/SVD management	SCD.AC_GENKEYPAIR SVD.AC_GENKEYPAIR	<p>“SCD/SVD management” corresponds to the access conditions SCD.AC_GENKEYPAIR and SVD.AC_GENKEYPAIR. Key generation is authorized if and only if these access conditions are satisfied.</p> <p>The SCD.AC_GENKEYPAIR and SVD.AC_GENKEYPAIR are viewed as an attribute of USER since it is used to authenticate the USER.</p>
	Associated to:	USER	USER	
	Status:	Authorised, Not Authorised	Satisfied (Authorised), Not Satisfied (Not Authorised)	

**Table 3 : Correspondence between attributes defined in SSCD Type 2 and Type 3 and ID One V3 attributes**

SVD transfer SFP

FDP\_ACF.1.1/ SVD transfer SFP

The TSF shall enforce the [SVD transfer SFP] to objects based on [General attribute]

FDP\_ACF.1.2/ SVD transfer SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

The user with the security attribute "role" set to "Signatory" is allowed to export SVD.

# Oberthur Card System - Cosmos

## Security Target Lite

---

### FDP\_ACF.1.3/ SVD transfer SFP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

Command	Condition to satisfy	Comment
GET DATA	SVD.AC_READ is satisfied	Used to read the SDO containing the SVD

### FDP\_ACF.1.4/ SVD transfer SFP

The TSF shall explicitly deny access of subjects to objects based on the rule: [none]

Application note:

FDP\_ACF.1/SVD Transfer SFP will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

### Initialisation SFP

#### FDP\_ACF.1.1/Initialisation SFP

The TSF shall enforce the [Initialisation SFP] to objects based on [General attribute] and [Initialisation attribute group].

#### FDP\_ACF.1.2/ Initialisation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to generate SCD/SVD pair.

#### FDP\_ACF.1.3/ Initialisation SFP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none]

#### FDP\_ACF.1.4/ Initialisation SFP

The TSF shall explicitly deny access of subjects to objects based on the rule:

The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.

In this requirement, "SCD / SVD management" is defined as follows:

Command	Condition to satisfy	Comment
GENERATE KEY PAIR	SCD.AC_GENKEYPAIR and SVD.AC_GENKEYPAIR are satisfied	Used to generate the SCD/SVD pair

### SCD Import SFP

#### FDP\_ACF.1.1/ SCD Import SFP

The TSF shall enforce the [SCD Import SFP] to objects based on [General attribute] and [Initialisation attribute group].

#### FDP\_ACF.1.2/ SCD Import SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

# Oberthur Card System - Cosmos

## Security Target Lite

The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".

### FDP\_ACF.1.3/ SCD Import SFP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

In this requirement, "SCD / SVD management" is defined as follows:

If the issued Command is:	Condition to satisfy	Comment
PUT DATA	SCD.AC_CHANGE is satisfied SVD must exist and must have been updated	Used to update the SCD

And "Secure SCD Import allowed" is interpreted as follows:

If the issued Command is:	Condition to satisfy	Comment
PUT DATA	SCD.AC_CHANGE is verified SVD must exist and must have been updated	The secure messaging of the incoming APDU must be verified

### FDP\_ACF.1.4/ SCD Import SFP

The TSF shall explicitly deny access of subjects to objects based on the rule:

- a) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".
- b) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".

## Personnalisation SFP

### FDP\_ACF.1.1/ Personnalisation SFP

The TSF shall enforce the [Personalisation SFP] to objects based on Personalisation SFP [General attribute group]

### FDP\_ACF.1.2/ Personalisation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

User with the security attribute "role" set to "Administrator" is allowed to create the PIN

Command	Condition to satisfy	Comment
PUT DATA (initialisation mode)	PIN.AC_INIT is satisfied	The user must verify the access condition PIN.AC_INIT to be authorised to initialize the RAD.

### FDP\_ACF.1.3/ Personalisation SFP

# Oberthur Card System - Cosmos

## Security Target Lite

---

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none]

### FDP\_ACF.1.4/ Personalisation SFP

The TSF shall explicitly deny access of subjects to objects based on the rule: [none]

#### Application Note:

In this requirement, DF is the folder where PIN has to be created.

### PIN SFP

- The "Personalization SFP" controls creation operation on a specific PIN that is the RAD.

### FDP\_ACF.1.1/ PIN SFP

The TSF shall enforce the [PIN SFP] to objects based on

Subjects: Signatory

Objects: PINs

Attributes: see **Table 2**

### FDP\_ACF.1.2/ PIN SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

User with the security attribute "role" set to "Administrator" or set to "Signatory" is allowed to create the PINs.

In the rules below:

- P is a PIN on which the operation acts

Operations	If the issued Command is:	Condition to satisfy
Initialization	PUT DATA (initialization mode)	P.AC_INIT
Update	CHANGE REFERENCE DATA	P.AC_CHANGE
Use	VERIFY PIN	P.AC_USE

### FDP\_ACF.1.3/ PIN SFP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none]

### FDP\_ACF.1.4/ PIN SFP

The TSF shall explicitly deny access of subjects to objects based on the rule: [none]

#### Application Note:

- In this requirement, DF is the folder containing the PIN.

### Signature Creation SFP

### FDP\_ACF.1.1/ Signature-creation SFP

The TSF shall enforce the [Signature-creation SFP] to objects based on [General attribute group] and [Signature-creation attribute group].

### FDP\_ACF.1.2/ Signature-creation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".

# Oberthur Card System - Cosmos

## Security Target Lite

In this requirement, "SCD operational" is interpreted as follows:

Command	Condition to satisfy	Comment
PSO CDS	SCD.AC_USE is satisfied	SCD.AC_USE corresponds to the RAD, and must be a PIN and requires the incoming command to be protected by a signature (MAC)

And "sent by an authorized SCA" is interpreted as follows:

If the issued Command is:	Condition to satisfy	Comment
PSO Hash	Cryptographic checksum (MAC) over the incoming command must be verified SCD.AC_USE must impose At least MAC over the incoming command for signature computation	The Signature (MAC) of the incoming APDU must be verified by the TOE using the secure messaging session key. As the DTBS representation has to be made available just before the signature computation and as the signature computation imposes the incoming command to be protected by a signature (MAC), therefore the command for DTBS representation reception must have a valid signature (MAC) The keys to use for the device authentication may be imposed by SCD.AC_USE This step is used to have a DTBS representation available for the signature computation

### FDP ACF.1.3/ Signature-creation SFP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- Signature creation is only allowed in "Personalised State" life cycle

### FDP ACF.1.4/Signature-creation SFP

The TSF shall explicitly deny access of subjects to objects based on the rule:

- a) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".
- b) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

### External Authentication Keys SFP

#### FDP ACF.1.1/ External Authentication Keys SFP

The TSF shall enforce the [External Authentication Keys SFP] to objects based on

Subjects: Administrator

Objects: External Authentication Keys

Attributes: see **Table 2**

#### FDP ACF.1.2/ External Authentication Keys SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

User with the security attribute "role" set to "Administrator" or set to "Signatory" is allowed to create the symmetric external Authentication Keys.

# Oberthur Card System - Cosmos

## Security Target Lite

---

In the rules below:

- K is an External Authentication Key on which the operation acts

Operations	If the issued Command is:	Condition to satisfy
Use	EXTERNAL AUTHENTICATE	K.AC_USE

### FDP\_ACF.1.3/ External Authentication Keys SFP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none]

### FDP\_ACF.1.4/ External Authentication Keys SFP

The TSF shall explicitly deny access of subjects to objects based on the rule: [none]

### Device authentication Keys SFP

#### FDP\_ACF.1.1/ Device authentication Keys SFP

The TSF shall enforce the [Device authentication Keys SFP] to objects based on Personalization SFP

Subjects: Signatory, Administrator  
 Objects: Device authentication Keys  
 Attributes: see **Table 2**

#### FDP\_ACF.1.2/ Device authentication Keys SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

In the rules below:

- K is a device authentication Keys on which the operation acts

Operations	If the issued Command is:	Condition to satisfy	Comment
Use	MUTUAL AUTHENTICATE	K.AC_USE	Device authentication keys are used to authenticate both parts (ICC & IFD) and to generate session keys to protect incoming and outgoing APDU in confidentiality and/or integrity. The symmetric device authentication keys may be specified in the secure messaging access condition (Identifier of the key, symmetric scheme).

### FDP\_ACF.1.3/ Device authentication keys SFP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none]

### FDP\_ACF.1.4/ Device authentication keys SFP

The TSF shall explicitly deny access of subjects to objects based on the rule: [none]

### **5.1.2.3 FDP\_ETC : Export to outside TSF control**

FDP\_ETC.1: Export of user data without security attributes

# Oberthur Card System - Cosmos

## Security Target Lite

---

### FDP\_ETC.1.1/ SVD transfer

The TSF shall enforce the [SVD transfer SFP] when exporting user data, controlled under the SFP(s), outside of the TSC.

### FDP\_ETC.1.2/ SVD transfer

The TSF shall export the user data without the user data's associated security attributes.

#### Application note:

FDP\_ETC.1/SVD Transfer SFP will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

## **5.1.2.4 FDP\_ITC Import From outside TSF control**

FDP\_ITC.1: Import of user data without security attributes

### FDP\_ITC.1.1/SCD

The TSF shall enforce the [SCD Import SFP] when importing user data, controlled under the SFP, from outside of the TSC.

### FDP\_ITC.1.2/SCD

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

### FDP\_ITC.1.3/SCD

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [SCD shall be sent by an Authorised SSCD].

#### Application note:

A SSCD of Type 1 is authorized to send SCD to a SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorized SSCD of Type 1 is able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FDP\_ITC.1.3/SCD export.

### FDP\_ITC.1.1/DTBS

The TSF shall enforce the [Signature-creation SFP] when importing user data, controlled under the SFP, from outside of the TSC.

### FDP\_ITC.1.2/DTBS

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

### FDP\_ITC.1.3/DTBS

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [DTBS-representation shall be sent by an Authorised SCA].

#### Application note:

A SCA is authorized to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and able to establish a trusted channel to the SSCD as required by FDP\_ITC.1.3/SCA DTBS.

## **5.1.2.5 FDP\_RIP Residual information protection**

FDP\_RIP.1: Subset residual information protection

### FDP\_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [de-allocation of the resource from] the following objects: [SCD, VAD, and RAD].



# Oberthur Card System - Cosmos

## Security Target Lite

---

### 5.1.2.6 FDP\_SDI Stored data integrity

FDP\_SDI2 Stored data integrity monitoring

#### Persistent data

The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data"

- SCD
- RAD
- SVD
- Keys used to authenticate the administrator
- Keys used to perform device authentication

#### FDP\_SDI.2.1/Persistent

The TSF shall monitor user data stored within the TSC for [integrity error] on all objects, based on the following attributes: [integrity checked persistent stored data].

#### FDP\_SDI.2.2/Persistent

Upon detection of a data integrity error, the TSF shall :

- [ 1. prohibit the use of the altered data
2. inform the Signatory about integrity error.]

#### DTBS-representation

The Protection Profiles SSCD TYPE 2 and TYPE3 specify that the DTBS representation temporarily stored by TOE have the user data attribute "integrity checked stored data".

The requirements FDP\_SDI.2.1/DTBS and FDP\_SDI.2.2/DTBS are not application to our TOE since the DTBS (the message to be signed) is not stored by the TOE.

### 5.1.2.7 FDP\_UCT Inter-TSF user data confidentiality transfer protection

FDP\_UCT.1 Basic data exchange confidentiality

#### FDP\_UCT.1.1/ Receiver

The TSF shall enforce the [SCD Import SFP] to be able to [receive] objects in a manner protected from unauthorised disclosure.

Application Note: controlled by the SM condition of SCD.AC\_CHANGE.

### 5.1.2.8 FDP\_UIT Inter-TSF user data integrity transfer protection

FDP\_UIT.1: Data exchange integrity

#### SVD transfer

#### FDP\_UIT.1.1/ SVD transfer

The TSF shall enforce the [SVD transfer SFP] to be able to [transmit] user data in a manner protected from [modification and insertion] errors.

#### FDP\_UIT.1.2/ SVD transfer

The TSF shall be able to determine on receipt of user data, whether [modification and insertion] has occurred.

Application Note: controlled by the SM condition of SVD.AC\_READ

#### Receiver

#### FDP\_UIT.1.1/ TOE DTBS

---

# Oberthur Card System - Cosmos

## Security Target Lite

---

The TSF shall enforce the [Signature-creation SFP] to be able to [receive] user data in a manner protected from [modification, deletion and insertion] errors.

### FDP\_UIT.1.2/ TOE DTBS

The TSF shall be able to determine on receipt of user data, whether [modification, deletion and insertion] has occurred.

Application Note: controlled by the SM condition of SCD.AC\_USE

## 5.1.3 FIA: IDENTIFICATION AND AUTHENTICATION

### 5.1.3.1 FIA\_AFL Authentication failure

FIA\_AFL.1 Authentication failure handling

FIA\_AFL is specific to the RAD. We define as well new requirement "FIA AFL.1.1" applicable for each authentication data:

- RAD
- Symmetric external authentication keys
- Symmetric device authentication keys

. These different authentication data may be used to control access to different operations (examples: RAD.AC\_CHANGE, SCD.AC\_CHANGE, SCD.AC\_GENKEYPAIR,...).

#### FIA AFL.1.1/RAD

The TSF shall detect when [number N] unsuccessful authentication attempts occur related to [consecutive failed authentication attempts].

#### FIA AFL.1.2/RAD

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [block RAD].

Application Note:

The Authentication Try Limit N, defined during personalisation, must verify  $1 \leq N \leq 15$ .

#### FIA AFL.1.1/External authentication keys

The TSF shall detect when [number N] unsuccessful authentication attempts occur related to [consecutive failed authentication attempts].

#### FIA AFL.1.2/External authentication keys

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [block the corresponding external Authentication keys].

Application Note:

The Authentication Try Limit N, defined during personalisation, must verify  $1 \leq N \leq 15$ .

#### FIA AFL.1.1/Device authentication keys

The TSF shall detect when [number N] unsuccessful authentication attempts occur related to [consecutive failed authentication attempts].

#### FIA AFL.1.2/ Device authentication keys

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [block the corresponding symmetric Device authentication Key].

Application Note:

The Authentication Try Limit N, defined during personalisation, must verify  $1 \leq N \leq 15$ .

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 5.1.3.2 FIA\_ATD User attribute definition

FIA ATD.1 User attribute definition

#### FIA ATD.1.1 / S.Signatory

The TSF shall maintain the following list of security attributes belonging to individual users [RAD]

#### FIA ATD.1.1 / S.Admin

The TSF shall maintain the following list of security attributes belonging to individual users [external Authentication keys]

### 5.1.3.3 FIA\_UAU User authentication

FIA UAU.1 Timing of authentication

#### FIA UAU.1.1

The TSF shall allow

- [Identification of the user by means of TSF required by FIA\_UID.1]
- [Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP\_ITC.1/SCD import]
- [Establishing a trusted path between local user and the TOE by means of TSF required by FTP\_TRP.1/TOE]
- [Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP\_ITC.1/DTBS import]

On behalf of the user to be performed before the user is authenticated.

#### FIA UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### Application note:

"Local user" mentioned in component FIA\_UAU.1.1 is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by FTP\_TRP.1/SCA and FTP TRP.1/TOE. It might be either S.Signatory or S.Admin.

### 5.1.3.4 FIA\_UID User Identification

FIA\_UID.1 Timing of identification

#### FIA UID.1.1

The TSF shall allow

- [Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP\_ITC.1/SCD import]
- [Establishing a trusted path between local user and the TOE by means of TSF required by FTP\_TRP.1/TOE]
- [Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP\_ITC.1/DTBS import]

on behalf of the user to be performed before the user is identified.

#### FIA UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

## 5.1.4 FMT: SECURITY MANAGEMENT

### 5.1.4.1 FMT\_MOF Management of functions in TSF

FMT\_MOF.1 Management of security functions behaviour

---

# Oberthur Card System - Cosmos

## Security Target Lite

---

### FMT\_MOF.1.1

The TSF shall restrict the ability to [enable] the [signature-creation function] to [Signatory].

### **5.1.4.2 FMT\_MSA Management of security attributes**

FMT\_MSA.1 Management of security attributes

#### FMT\_MSA.1.1/ Administrator-Initialisation

The TSF shall enforce the [Initialisation SFP] to restrict the ability to [modify] the security attributes [SCD / SVD management] to [Administrator].

Application Note:

In this requirement, "SCD/SVD management" corresponds to SCD.AC\_GENKEYPAIR and SVD.AC\_GENKEYPAIR

#### FMT\_MSA.1.1/ Administrator - Import

The TSF shall enforce the [SCD Import SFP] to restrict the ability to [modify] the security attributes [SCD / SVD management] to [Administrator].

Application Note:

"SCD / SVD management" corresponds to SVD.AC\_CHANGE and SCD.AC\_CHANGE

#### FMT\_MSA.1.1/ Signatory

The TSF shall enforce the [Signature-creation SFP] to restrict the ability to [modify] the security attributes [SCD operational] to [Signatory].

Application Note:

In this requirement, "SCD operational" corresponds to SCD.AC\_USE.

FMT\_MSA.2 Secure security attributes

#### FMT\_MSA.2.1

The TSF shall ensure that only secure values are accepted for security attributes.

FMT\_MSA.3 Static attributes initialisation

#### FMT\_MSA.3.1

The TSF shall enforce the [Initialisation SFP] and [Signature-creation SFP] and [SCD Import SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

Refinement:

The security attribute of the SCD "SCD operational" is set to "no" after generation or import of the SCD. Since in ID One V3, "SCD operational" corresponds to the PIN SCD.AC\_USE (RAD): after generation or import, SCD.AC\_USE is reset (its status is set to "Not Satisfied").

The table below summarizes the recommended values for attributes of sensitive data:

Attribute	Definition	Recommended value
Attributes associated to SCD.		

# Oberthur Card System - Cosmos

## Security Target Lite

AC_GENKEYPAIR	Access condition for SCD/SVD generation	Role = S.Signatory OR S.Admin (the same for the SVD)
AC_USE	Access condition for digital signature creation	Role = S.Signatory SCA authenticated Protection of exchanges
AC_CHANGE	Access condition for modifying (import) a new key	Role = S.Signatory OR S.Admin SSCD is authenticated Protection of exchanges
Attributes associated to SVD.		
AC_GENKEYPAIR	Access condition for SCD/SVD generation	Role = S.Signatory OR S.Admin
AC_READ	Access conditions to be satisfied for reading a SVD	Role = S.Signatory OR S.Admin CGA is authenticated Protection of exchanges
AC_CHANGE	Access condition for modifying (import) a new key	Role = S.Signatory OR S.Admin SSCD is authenticated Protection of exchanges
Attributes associated to PINs		
AC_USE	Access condition to be satisfied for verifying a	Protection of exchanges in both confidentiality
AC_INIT	Access condition to be satisfied for initializing a PIN	Protection of exchanges in both confidentiality and integrity
AC_CHANGE	Access condition to be satisfied for modifying a PIN value	Protection of exchanges in both confidentiality and integrity
External Authentication Keys		
AC_USE	Access condition to be satisfied for using this	Protection of exchanges in both confidentiality
Device authentication Keys		
AC_USE	Access condition to use the key	Free

*Table 4 : Recommended values for Id One V3 attributes*

### FMT\_MSA.3.2

The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 5.1.4.3 FMT\_MTD Management of TSF data

FMT\_MTD.1 Management of TSF data

#### FMT\_MTD.1.1/ Signatory

The TSF shall restrict the ability to [modify] the [RAD] to [Signatory].

Application Note: It is controlled by the access conditions PIN.AC\_CHANGE

### 5.1.4.4 FMT\_SMR Security management roles

FMT\_SMR.1 Security roles

#### FMT\_SMR.1.1

The TSF shall maintain the roles [Administrator] and [Signatory].

#### FMT\_SMR.1.2

The TSF shall be able to associate users with roles.

## 5.1.5 FPT: PROTECTION OF THE TSF

### 5.1.5.1 FPT\_AMT Underlying Abstract machine test

FPT\_AMT.1 Underlying Abstract machine test

#### FPT\_AMT.1.1

The TSF shall run a suite of tests [during initial start-up and periodically during normal operation] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Refinement: In this Security Target (ST), the underlying abstract machine test is the platform.

### 5.1.5.2 FPT\_EMSEC TOE Emanation

FPT\_EMSEC.1.1 TOE Emanation

#### FPT\_EMSEC.1.1

The TOE shall not emit [Side channel emission] in excess of [limits specified by the state-of-the-art attacks on smart card IC] enabling access to [RAD and SCD].

#### FPT\_EMSEC.1.2

The TSF shall ensure [all users] are unable to use the following interface [external contacts emanations] to gain access to [RAD and SCD].

### 5.1.5.3 FPT\_FLS Failure secure

FPT\_FLS.1 Failure with preservation of secure state

#### FPT\_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [power shortage, over voltage, over and under clock frequency, integrity errors, over/under temperature].

### 5.1.5.4 FPT\_PHP TSF physical Protection

FPT\_PHP.1 Passive detection of physical attack

#### FPT\_PHP.1.1

---

# Oberthur Card System - Cosmos

## Security Target Lite

---

The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

### FPT\_PHP.1.2

The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT\_PHP.3 Resistance to physical attack

### FPT\_PHP.3.1

The TSF shall resist [physical manipulation and physical probing] to the [integrated circuit] by responding automatically such that the TSP is not violated

## **5.1.5.5 FPT\_TST TSF self test**

FPT\_TST.1 TSF testing

### FPT\_TST.1.1

The TSF shall run a suite of self-tests [during initial start-up and periodically during normal operation] to demonstrate the correct operation of the TSF.

### FPT\_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

### FPT\_TST.1.3

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

## **5.1.6 FTP: TRUSTED PATH / CHANNEL**

### **5.1.6.1 FTP\_ITC Inter-TSF trusted channel**

FTP ITC.1 Inter-TSF trusted Channel

#### FTP\_ITC.1.1/ SCD import

The TSF shall provide a communication channel between itself and a remote SCD import trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

#### FTP\_ITC.1.2/ SCD import

The TSF shall permit [the remote trusted IT product] to initiate communication via the trusted channel.

#### FTP\_ITC.1.3/ SCD import

The TSF shall initiate communication via the trusted channel for [SCD import]

#### Refinement:

The mentioned remote trusted IT product is a SSCD of type 1.

Application Note: controlled by the SM conditions of SCD.AC\_CHANGE:

If the issued Command is:	AC conditions
PUT DATA (update mode)	SCD.AC_CHANGE

# Oberthur Card System - Cosmos

## Security Target Lite

---

### FTP ITC.1.1/ SVD transfer

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

### FTP ITC.1.2/ SVD transfer

The TSF shall permit [the remote trusted IT product] to initiate communication via the trusted channel.

### FTP ITC.1.3/ SVD transfer

The TSF shall initiate communication via the trusted channel for [SVD transfer]

#### Refinement:

The mentioned remote trusted IT product is a CGA.

#### Application Note:

Key to be used for device authentication may be specified in the of condition SVD.AC\_READ.

#### Application note:

FTP\_ITC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

### FTP ITC.1.1/ DTBS import

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

### FTP ITC.1.2/ DTBS import

The TSF shall permit [the remote trusted IT product] to initiate communication via the trusted channel.

### FTP ITC.1.3 DTBS import

The TSF shall initiate communication via the trusted channel for [signing DTBS-representation]

Refinement: The mentioned remote trusted IT product is a SCA.

Application Note: controlled by the SM conditions of SCD.AC\_USE:

## **5.1.6.2 FTP\_TRP Trusted path**

FTP\_TRP.1 Trusted path

### FTP TRP.1.1/TOE

The TSF shall provide a communication path between itself and [local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

### FTP TRP.1.2/TOE

The TSF shall permit [local users] to initiate communication via the trusted path.

### FTP TRP.1.3/TOE

The TSF shall require the use of the trusted path for [initial user authentication].

Application Note: controlled by the Secure Messaging condition of PIN.AC\_USE.



### 5.2 TOE SECURITY ASSURANCE REQUIREMENTS

The Assurance requirements is EAL5 augmented by components :

- ALC\_DVS.2 : Sufficiency of security measures
- AVA\_MSU.3 Analysis and testing for insecure states
- AVA\_VLA.4 Highly resistant.

#### 5.2.1 CONFIGURATION MANAGEMENT (ACM)

EAL5 augmented claimed level requires the following ACM class components:

- ACM\_AUT.1 Partial CM automation
- ACM\_CAP.4 Generation support and acceptance procedures
- ACM\_SCP.3 Development tools CM coverage

Refer to CC Part 3 for description.

#### 5.2.2 DELIVERY AND OPERATION (ADO)

EAL5 augmented claimed level requires the following ADO class components:

- ADO\_DEL.2 Detection of modification
- ADO\_IGS.1 Installation, generation, and start-up procedures

Refer to CC Part 3 for description.

#### 5.2.3 DEVELOPMENT (ADV)

EAL5 claimed level requires the following ADV class components:

- ADV\_FSP.3 Semiformal functional specification
- ADV\_HLD.3 Semiformal high-level design
- ADV\_IMP.2 Implementation of the TSF
- ADV\_INT.1 Modularity
- ADV\_LLD.1 Descriptive low-level design
- ADV\_RCR.2 Semiformal correspondence demonstration
- ADV\_SPM.3 Formal TOE security policy model

Refer to CC Part 3 for description.

#### 5.2.4 GUIDANCE DOCUMENTS (AGD)

EAL5 augmented claimed level requires the following AGD class components:

- AGD\_ADM.1 Administrator guidance
- AGD\_USR.1 User guidance

Refer to CC Part 3 for description.

#### 5.2.5 LIFE CYCLE SUPPORT (ALC)

EAL5 augmented claimed level requires the following ALC class components:

- ALC\_DVS.2 Sufficiency of security measures
- ALC\_LCD.2 Standardised life-cycle model
- ALC\_TAT.2 Compliance with implementation standards

Refer to CC Part 3 for description.

#### 5.2.6 TESTS (ATE)

EAL5 augmented claimed level requires the following ATE class components:

- ATE\_COV.2 Analysis of coverage
- ATE\_DPT.2 Testing: low-level design
- ATE\_FUN.1 Functional testing
- ATE\_IND.2 Independent testing- sample

# Oberthur Card System - Cosmos

## Security Target Lite

---

Refer to CC Part 3 for description.

### 5.2.7 VULNERABILITY ASSESSMENT (AVA)

EAL5 augmented claimed level requires the following AVA class components:

- AVA\_MSU.3 Analysis and testing of insecure states
- AVA\_SOF.1 Strength of TOE security function evaluation
- AVA\_VLA.4 Highly resistant

Refer to CC Part 3 for description.

## 5.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

This section describes the IT security requirements that are to be met by the IT environment of the TOE. The IT environment of the TOE is composed of the Certification Generation Application (CGA) and the Signature Creation Application (SCA).

These requirements are as stated in [SSCD2] & [SSCD3].

### 5.3.1 Signature key generation (SSCD Type1)

#### 5.3.1.1 Cryptographic key generation (FCS\_CKM.1)

##### FCS\_CKM.1.1 / RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA key generation] and specified cryptographic key sizes [1024 bits or 1536 bits or 2048 bits] that meet the [ANSI X9.31]

##### FCS\_CKM.1.1 / DES session keys

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [DES key generation] and specified cryptographic key sizes [128 bits] that meet the [ANSI X9.63 with SHA-1]

#### 5.3.1.2 Cryptographic key destruction (FCS\_CKM.4)

##### FCS\_CKM.4.1 / SCD/SVD

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting the buffer containing the key] that meets the following: [ISO 11166].

##### Application note:

The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated or re-imported by the TOE.

##### FCS\_CKM.4.1 / Symmetric DES keys

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting the buffer containing the key] that meets the following: [ISO 11568].

##### Application note:

The Symmetric DES key includes the keys used for the device authentication and the External authentication as well as the secure messaging session keys.

#### 5.3.1.3 Cryptographic operation (FCS\_COP.1)

##### FCS\_COP.1.1 / CORRESP

# Oberthur Card System - Cosmos

## Security Target Lite

---

The TSF shall perform [SCD/SVD correspondence verification] in accordance with a specified cryptographic algorithm [RSA CRT key computation] and cryptographic key sizes [1024 bits or 1536 bits or 2048 bits] that meet the following: [PKCS #1 V1.5 Block Type 1].

### FCS COP.1.1/ SIGNING

The TSF shall perform [Digital signature-generation] in accordance with a specified cryptographic algorithm [RSA CRT using Private Key] and cryptographic key sizes [1024 bits or 1536 bits or 2048 bits] that meet the following: [PKCS #1 V1.5 Block Type 1].

#### Application Note:

The biggest RSA key pair that can be imported by ID One V3 is 2048 bits (using the command PUT DATA).

### FCS COP.1.1/ Secure Messaging Signature

The TSF shall perform [Secure Messaging Signature] in accordance with a specified cryptographic algorithm [Retail MAC] and cryptographic key sizes [128 bits] that meet the following: [CryptoCotation].

#### Application Note:

This algorithm is used during secure Messaging: for computation of signature (SM\_SIG) of outgoing APDU commands and verification of signature (SM\_SIG) of incoming APDU commands

### FCS COP.1.1/ Secure Messaging Encryption/Decryption

The TSF shall perform [Secure Messaging Encryption/Decryption] in accordance with a specified cryptographic algorithm [Triple DES CBC encryption/decryption] and cryptographic key sizes [128] that meet the following: [CryptoCotation].

Application Note: This algorithm is used during secure Messaging: for encryption of data (SM\_ENC\_SIG) for outgoing APDU commands and decryption of data (SM\_ENC\_SIG) for incoming APDU commands

### FCS COP.1.1/ External Authentication

The TSF shall perform [External Authentication] in accordance with a specified cryptographic algorithm [using DES] and cryptographic key sizes [128] that meet the following: [CryptoCotation].

Application Note: This algorithm is used during symmetric external Authentication: to verify the challenge sent by the terminal

### FCS COP.1.1/ Device authentication

The TSF shall perform [Device Authentication] in accordance with a specified cryptographic algorithm [using DES] and cryptographic key sizes [128] that meet the following: [CryptoCotation].

Application Note: This algorithm is used during symmetric device authentication to authenticate both the terminal and the card

## **5.3.1.4 Subset access control (FDP\_ACC.1)**

### FDP\_ACC.1.1/SCD Export SFP

The TSF shall enforce the [SCD Export SFP] on [export of SCD by Administrator].

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 5.3.1.5 Basic data exchange confidentiality (FDP\_UCT.1)

#### FDP\_UCT.1.1/ Sender

The TSF shall enforce the [SCD Export SFP] to be able to [transmit] objects in a manner protected from unauthorized disclosure.

### 5.3.1.6 Inter-TSF trusted channel (FTP\_ITC.1)

#### FTP\_ITC.1.1/SCD Export

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

#### FTP\_ITC.1.2/SCD Export

The TSF shall permit [the TSF] to initiate communication via the trusted channel.

#### FTP\_ITC.1.3/ SCD Export

The TSF or the SSCD Type2 shall initiate communication via the trusted channel for [SCD export].

#### Refinement:

The mentioned remote trusted IT product is a SSCD Type2

#### Application note:

If the TOE exports the SVD to a SSCD Type2 and the SSCD Type 2 holds the SVD then the trusted channel between the TOE and the SSCD type 2 will be required .

## 5.3.2 Certification generation application (CGA)

### 5.3.2.1 Cryptographic key distribution (FCS\_CKM.2)

#### FCS\_CKM.2.1/ CGA

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [qualified certificate] that meets the following: [Triple DES 128 bits].

### 5.3.2.2 Cryptographic key access (FCS\_CKM.3)

#### FCS\_CKM.3.1/ CGA

The TSF shall perform [import the SVD] in accordance with a specified cryptographic key access method [import through a secure channel] that meets the following: [ID One V3].

### 5.3.2.3 Data exchange integrity (FDP\_UIT.1)

#### FDP\_UIT.1.1/SVD Import

The TSF shall enforce the [SVD import SFP] to be able to [receive] user data in a manner protected from [modification and insertion] errors.

#### FDP\_UIT.1.2/SVD Import

The TSF shall be able to determine on receipt of user data, whether [modification and insertion] has occurred.

### 5.3.2.4 Inter-TSF trusted channel (FTP\_ITC.1)

#### FTP\_ITC.1.1/SVD Import

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

# Oberthur Card System - Cosmos

## Security Target Lite

---

### FTP\_ITC.1.2/SVD Import

The TSF shall permit [the remote trusted IT product] to initiate communication via the trusted channel.

### FTP\_ITC.1.3/SVD Import

The TSF or the remote trusted IT product shall initiate communication via the trusted channel for import SVD.

## **5.3.3 Signature creation application (SCA)**

### **5.3.3.1 Cryptographic operation (FCS\_COP.1)**

#### FCS\_COP.1.1/SCA Hash

The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm [SHA] and cryptographic key sizes [none] that meet the following: [SHA-1 or partial SHA-1].

#### Application Note:

The hashing algorithm used by the TOE for the signature computation when it performs itself the DTBS hashing is the SHA-1/Partial SHA-1. However, the IT Environment may use any hashing function provided it performs the whole data hashing and that the hashed data sent to the TOE is 20 bytes long. As stated in [CryptoRules], SHA-256 should be use by the IT environment.

### **5.3.3.2 Data exchange integrity (FDP\_UIT.1)**

#### FDP\_UIT.1.1/SCA DTBS

The TSF shall enforce the [Signature-creation SFP] to be able to [transmit] user data in a manner protected from [modification, deletion and insertion] errors.

#### FDP\_UIT.1.2/SCA DTBS

The TSF shall be able to determine on receipt of user data, whether [modification, deletion and insertion] has occurred.

### **5.3.3.3 Inter-TSF trusted channel (FTP\_ITC.1)**

#### FTP\_ITC.1.1/ SCA DTBS

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

#### FTP\_ITC.1.2/ SCA DTBS

The TSF shall permit [local users] to initiate communication via the trusted channel.

#### FTP\_ITC.1.3/SCA DTBS

The TSF or the remote trusted IT product shall initiate communication via the trusted channel for [signing DTBS-representation by means of the SSCD].

### **5.3.3.4 Trusted path (FTP\_TRP.1)**

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

#### FTP\_TRP.1.1/ SCA

The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

#### FTP\_TRP.1.2/ SCA

The TSF shall permit [local users] to initiate communication via the trusted path.

---

# Oberthur Card System - Cosmos

## Security Target Lite

---

### FTP TRP.1.3/ SCA

The TSF shall require the use of the trusted path for [initial user authentication] [SCD import and DTBS representation import and SVD export].

## 5.4 SECURITY REQUIREMENTS FOR THE NON - IT ENVIRONMENT

### R.Administrator\_Guide *Application of Administrator Guidance*

The implementation of the requirements of the Directive, ANNEX II "Requirements for certification service-providers issuing qualified certificates", literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall ensure the ongoing compliance.

### R.Sigy\_Guide *Application of User Guidance*

The SCP implementation of the requirements of the Directive, ANNEX II "Requirements for certification service-providers issuing qualified certificates", literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

### R.Sigy\_Name *Signatory's name in the Qualified Certificate*

The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [1], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (d). The CSP shall verify that this person holds the SSCD, which implements the SCD corresponding to the SVD to be included in the qualified certificate.

## 6 TOE SUMMARY SPECIFICATION

This part covers the IT security functions and specifies how these functions satisfy the TOE security functional requirement

### 6.1 security function list

Identification	Name
SF.RNG	Random number generator
SF.HW_DES	Triple DES coprocessor
SF.HW_AES	AES coprocessor
SF.OPC	Control of operating conditions
SF.PHY	Protection against physical manipulation
SF.LOG	Logical protection
SF.COMP	Protection of mode control
SF.MEM_ACC	Memory access control
SF.SFR_ACC	Special function register access Control
SF.KEYGEN	Key generation management
SF.SIG	Signature creation management
SF.USER_AUTH	User authentication management

# Oberthur Card System - Cosmos

## Security Target Lite

---

SF.PIN	PIN management
SF.KEY	Key management
SF.SM	Secure messaging
SF.TEST	Self tests and actions to take
SF.INTEGRITY	Protection of data integrity
SF.PHYS	Physical protection
SF.ROLLBACK	Safe state management

### 6.2 Security functions provided by the IC

The description of the security functions of the IC is provide in [STIC]

### 6.3 Security functions provided by the TOE

SF.KEYGEN - Key generation management

This security function protects the asymmetric key pair generation

SF.SIG - Signature creation management

This security function protects the signature computation.

SF.USER\_AUTH – User Authentication management

This function ensures the authentication and the protection of S.User, whatever it is S.Signatory or S.Admin.

SF.PIN – PIN Management

This security function manages operations related to PIN (RAD)

SF.KEY – Key Management

This security function manages the keys the TOE handles.

SF.SM – Secure Messaging

This security function ensures the confidentiality and/or integrity of user data exchanged.

SF.TEST - Self tests and actions to take

The TOE performs several self tests. It aims at protecting the TSF.

SF.INTEGRITY – Protection of data Integrity

The TOE ensures integrity of the sensitive data it contains

SF.PHYS - Physical protection: protection against snooping, notification and resistance to physical attack & errors

This security function provides ability for the software to protect the Digital application data D.RAD and D.SCD against snooping.

SF.ROLLBACK – Safe state management : protection against tearing

This security function ensures atomicity of Java objects update in EEPROM

### 6.4 Assurance measures

This chapter defines the list of the assurance measures required for the TOE security assurance requirements

# Oberthur Card System - Cosmos

## Security Target Lite

---

### 6.4.1 Assurance measure list

Measure	Name
AM_ACM	Configuration management
AM_ADO	Delivery and operation
AM_ADV	Development
AM_AGD	Guidance documents
AM_ALC	Life cycle
AM_ATE	Tests
AM_AVA	Vulnerability assessment

*Table 5 : Assurance measures list*

### 6.4.2 AM\_ACM: Configuration management

This assurance measure ensures the configuration management. The CM responsible is in charge to write the CM plan, use the CM system and validate the CM system in order to confirm that ACM\_XXX.Y components are completed

### 6.4.3 AM\_ADO: Delivery and Operation

This assurance measure ensures the delivery and operation. The delivery responsible is in charge to write delivery documentation and validate it in order to confirm that the procedure is applied.

### 6.4.4 AM\_ADV: Development

This assurance measure ensures the development. The development responsible is in charge to design the TOE, write development documentation and validate it in order to confirm that the related security functional requirements are completed by security functions.

### 6.4.5 AM\_AGD: Guidance documents

This assurance measure ensures the guidance documents. The guidance responsible is in charge to write administrator and user guidance. The documentation provides the rules to use and administrate the TOE in a secured manner.

### 6.4.6 AM\_ALC: Life cycle

This assurance measure ensures the life cycle. The life cycle responsible is in charge to confirm that the life cycle process is applied.

### 6.4.7 AM\_ATE: Tests

This assurance measure ensures the tests. The test responsible is in charge to write tests and execute it in order to confirm that the security functions are tested.

### 6.4.8 AM\_AVA: Vulnerability assessment

This assurance measure ensures the vulnerability assessment. The security responsible is in charge to confirm that the security measures are suitable to meet the TOE security objectives conducting a vulnerability analysis.



# Oberthur Card System - Cosmos

## Security Target Lite

---

### 7 PP CLAIMS

The PP [SSCD2] and [SSCD3] are claimed.

The PP "Secure Signature-Creation device Type 2" V1.04 [PP SSCD2] is certified at the German Certification Body under the number BSI-PP-0005-2002T- 03-04-2002

The PP "Secure Signature-Creation device Type 3" V1.05 [PP SSCD3] is certified at the German Certification Body under the number BSI-PP-0006-2002T- 03-04-2002

### 8 ACRONYMS

CC	Common Criteria Version 2.1
CGA	Certification Generation Application
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
HI	Human Interface HW Hardware
I/O	Input/Output
ICC	Integrated Circuit Card
IFD	Interface device
OS	Operating System
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PP	Protection Profile
RAD	Reference authentication Data
SCA	Signature-Creation Application
SCD	Signature-Creation Data
SDO	Signed Data Object
SOF	Strength of Function
SSCD	Secure Signature-Creation Device
SVD	Signature-Verification Data
TOE	Target of Evaluation
VAD	Verification authentication data