ID-One eIDAS v1.0 in SSCD-5 configuration on NXP P60x144 PVA/PVE

Public Security Target

FQR No: 110 7939

FQR Issue: 2

ID-One eIDAS v1.0 in SSCD-5 configuration on NXP P60x144 PVA/PVE

Public Security Target - FQR 110 7939 Issue 2

[redacted]

Table of contents

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

1 SECURITY TARGET INTRODUCTION

1.1 Purpose

The objective of this document is to present the Public Security Target SSCD-5 of the ID-One ePass V3 Full EAC v2 product on NXP components from P60 family.

1.2 Objective of the security target

This security target describes the security needs for ID-One ePass V3 Full EAC v2 product. The product is conforming to PP SSCD-5 and adds requirements for prepersonalization and personalization.

This security target aims to satisfy the requirements of Common Criteria level EAL5 augmented as defined in §0 in defining the security enforcing functions of the Target Of Evaluation and describing the environment in which it operates.
The objectives of this Security Target are:

- To describe the Target of Evaluation (TOE), its life cycle and to position it in the smart card life cycle.
- 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 the operational environment during the platform active phases.
- To describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the product active phases.
- To specify the security requirements which include the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment.
- To describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements.
- To present evidence that this ST is a complete and cohesive set of requirements that the TOE provides on an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements.

1.3 Security Target identification

Title	ID-One eIDAS v1.0 in SSCD-5 configuration on NXP P60x144 PVA/PVE – Public Security Target
Editor	Oberthur Technologies
CC version	3.1 revision 4
EAL	EAL5 augmented with AVA_VAN.5 and ALC_DVS.2
PP	Protection profile for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, version 1.0.1, 2012-11-14 BSI-CC-PP-0072
ST Reference	FQR 110 7847 Issue 2
ITSEF	LETI
Certification Body	ANSSI
Evaluation Scheme	FR

Table 1-1 - General Identification

1.4 TOE technical identification

Product name	ID-One ePass V3 Full EAC v2
Commercial name of TOE	ID-One eIDAS v1.0 in SSCD-5 configuration on P60x144 PVA/PVE
IC type	‘6A15’ (P60D144 VA) ‘6A20’ (P60C144 VA) ‘6E15’ (P60D144 VE) ‘6E20’ (P60C144 VE)
Additional code 1 Mandatory generic Identification	‘082456FF412E4D1EC087005B56A9A2CAC0B6558F4CAAE041D8B5A69345559B562A6F4C8E’
Additional code 2 Optional DBI Identification	‘082844FFE339C30BC6A81162413612FE2698284FA6CD28AA5CF5257A20B83611E58E9BEE’

Table 1-2 - TOE technical identification

Nota bene

- The additional code is encrypted with the LSK key
- An optional additional code (functional) can be loaded. This additional code, relative to the Digitally Blurred Image process (DBI), is part of the product, but not in the scope of the evaluation.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

1.5 IC identification

IC Reference	NXP P60 IC
TOE	NXP P60x144/080 PVA/PVE [R35] EAL6 + ALC_FLR.1 + ASE_TSS.2
Communication protocol	Contact and contactless and dual
Memory	ROM
Chip Manufacturer	NXP Semiconductors

Table 1-3 - Chip Identification

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

2 TOE OVERVIEW

2.1 Product overview

The product **ID-One ePass V3 Full EAC v2** is a multi-applicative native software, embedded in contact and/or contactless smart card integrated circuits of different form factors. During the pre-personalization and personalization phases, the product can be configured to serve different use cases.

The product supports the storage and retrieval of structured information compliant to the Logical Data Structure as specified in [R2]. It also provides standard authentication protocols, namely Basic Access Control [R27], Supplementary Access Control [R33], Extended Access Control ([R28] and [R29]), the Basic Access Protection [R9] and Extended Access Protection [R9]. Additionally, it supplies PIN management [R36] and signature services [R37].

The product is intended to host 4 types of applications: MRTD-IDL, eID, **eSign** and Dauth. Moreover, further configuration may also be done to each type of application to serve use cases other than those behaviourally defined in the referenced normative documents.

This product is embedded on the IC described in § 1.5.

The product is closed. The set of available applications is fully configured at the end of the personalization phase.

The ID-One ePass V3 Full EAC v2 architecture can be viewed as shown in the following picture:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

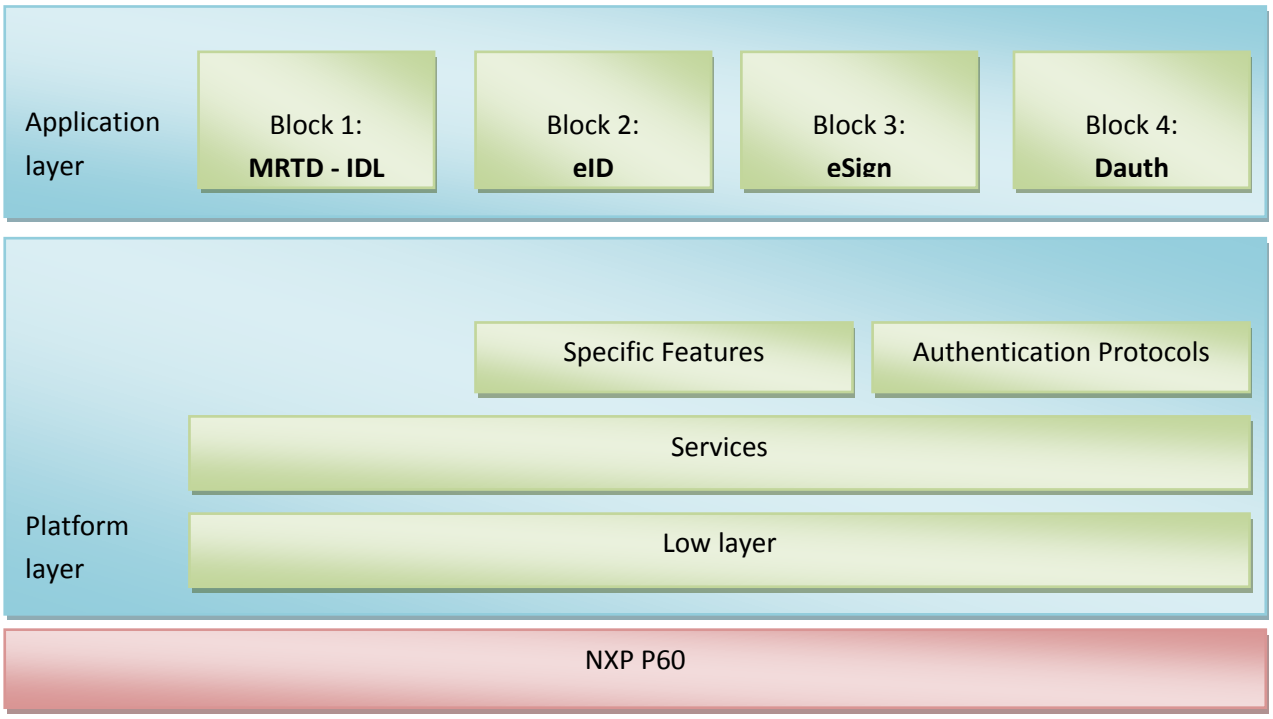

Figure 1 – Product architecture

The TOE is a subset of the product dedicated to the Signature Application. The eSign application contains the following 5 configurations:

eSign Configurations	PP	Targeted EAL
eSign SSCD-2	SSCD 2 CEN/EN 419 211-2 (ex CEN/EN 14169-2) (BSI-CC-PP-0059-2009-MA-01)	EAL5 + DVS.2 + VAN.5
eSign SSCD-3	SSCD 3 CEN/EN 419 211-3 (ex CEN/EN 14169-3) (BSI-CC-PP-0075-2012)	EAL5 + DVS.2 + VAN.5
eSign SSCD-4	SSCD 4 CEN/EN 419 211-4 (ex CEN/EN 14169-4) (BSI-CC-PP-0071-2012)	EAL5 + DVS.2 + VAN.5
eSign SSCD-5	SSCD 5 CEN/EN 419 211-5 (ex CEN/EN 14169-5) (BSI-CC-PP-0072-2012)	EAL5 + DVS.2 + VAN.5
eSign SSCD-6	SSCD 6 CEN/EN 419 211-6 (ex CEN/EN 14169-6)(BSI-CC-PP-0076-2013)	EAL5 + DVS.2 + VAN.5

Table 2-1 - eSign Configurations

The scope of this TOE encompasses configuration SSCD-5 and the features it relies on.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The eSign application is configured during the pre-personalization phase, using the Application Creation Engine. The other secure applications present in the product (MRTD-DL, eID and Dauth) are not in this TOE. They are evaluated separately.

2.2 TOE usages and major security features

The eSign application provides different services that make each card a secure signature creation device as defined in [R23].

The TOE major security features in the operational phase are the functions:

(1) To generate signature creation data (SCD) and the correspondent signature verification data (SVD),
(2) to export the SVD for certification
(3) to, optionally, receive and store certificate info (only if the personalizer creates it)
(4) to switch the TOE from a non-operational state to an operational state, and
(5) if in an operational state, to create digital signatures for data with the following steps (conformant to [R3], [R4], and [R22]; described in Section §5.3) *:*

(a) authenticate the signatory (using the RAD verification) *and determine its intent to sign,*
(b) receive data to be signed or a unique representation thereof (DTBS/R) through a trusted channel with SCA,
(c) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

It also allows the authentication of one (or several) administrator(s) of the TOE who may have special rights to administrate the SCD and SVD (generation), using either symmetric or asymmetric mechanisms or PIN verification.

2.3 TOE type

The TOE (Target of evaluation) is a smartcard based on NXP chip. It is a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature creation process solely by its signatory.

The TOE comprises:

- Circuitry of the chip (the integrated circuit, IC)
- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- IC Embedded Software (operating system)
- eSign application
- Associated guidance documentation

2.4 Required non-TOE hardware/software/firmware

N/A

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3 TOE DESCRIPTION

3.1 TOE scope

The following diagram describes the architecture of the product and highlights (in orange) the components of the product that are part of the TOE.

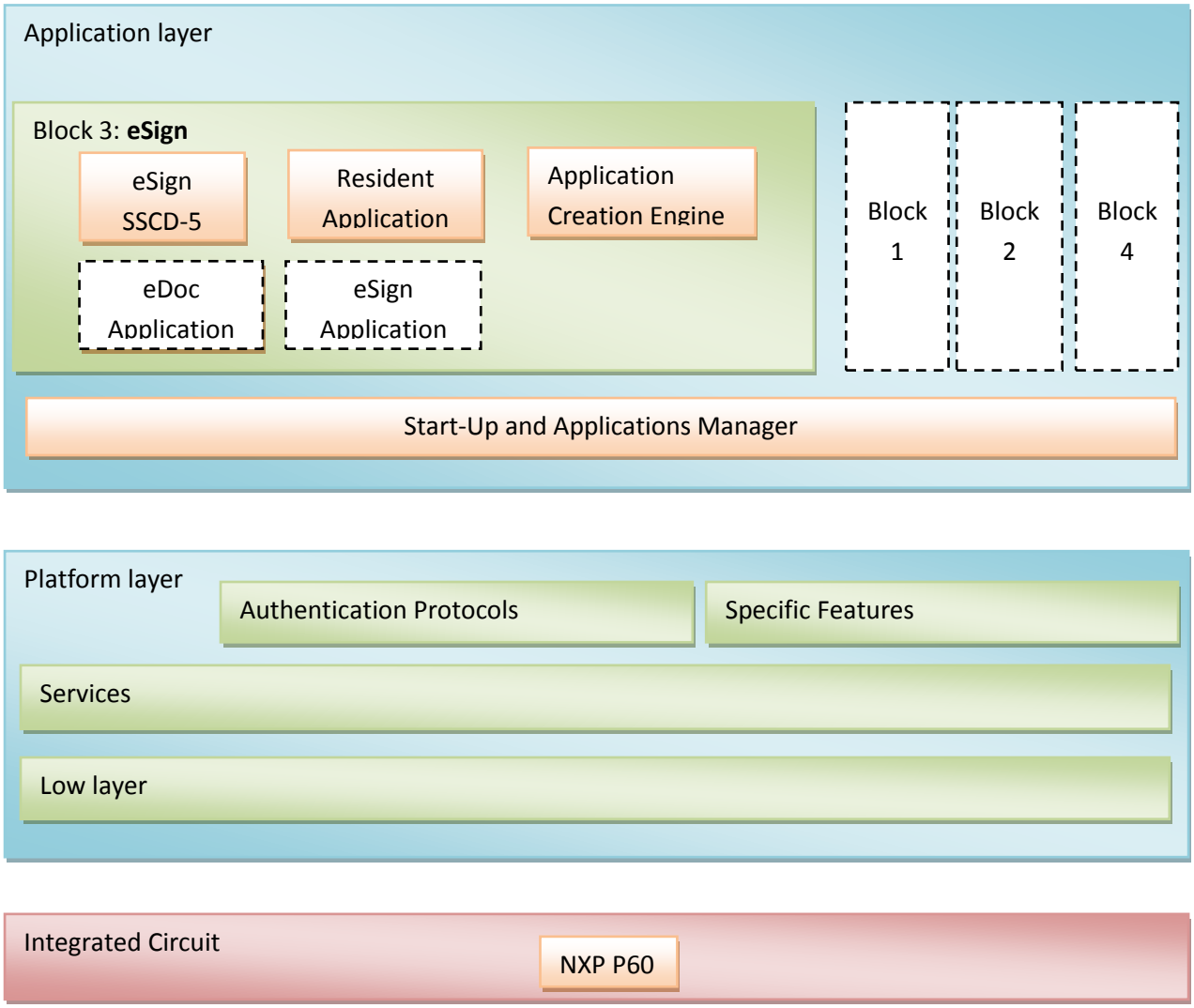

Figure 2 - Product architecture with TOE components

3.2 Block description

This section provides a quick overview of the functionalities of the components of the product. Note that the Resident Application, the eDoc block, the whole Platform Layer and the IC provide functionalities to all the applicative blocks 1 to 4.

3.2.1 Integrated Circuit – NXP P60

The TOE is embedded on NXP chip, as presented in Table 1-3 - Chip Identification. More information on the chips is given in the related certification report [R35] and related Security Target.

3.2.2 Low layer

3.2.2.1 Basic Input and Output System (BIOS)

The BIOS module provides access management (read/write) functionalities to upper-layer application. It also provides exception and communication functionalities.

3.2.2.2 Cryptography (Crypto)

The Cryptography module provides secure cryptographic functionalities to upper-layer applications.

3.2.3 Tools modules

3.2.3.1 File System Management (FSM)

The FSM module manages files and data objects according to ISO 7816-4 and 7816-9.

3.2.3.2 Secure Messaging (SM)

The SM module provides functionalities to encrypt/decrypt data for secure communication in pre-personalization, personalization and operational use phase.

3.2.3.3 Pin Password Management (PPM)

The PPM module provides functionalities for numeric passwords and biometric templates management. The passwords that can be used in connection with the eSign application are a global PIN, PUK, CAN (card access number written on the card where the eSign application is installed on) and the eSign PIN, called “RAD” in this Security Target. The use of the words ‘PIN’ throughout this document refers to a classical PIN as well as to a biometric password.

The RAD management is in the scope of this evaluation. The management of the other PINs and passwords not directly related to the signature application is evaluated separately.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3.2.3.4 Cryptography Key Management (CKM)

The CKM module is responsible for asymmetric cryptography key management and asymmetric cryptography operations.

3.2.3.5 Authentication and Key Management (AKM)

This module supplies:

- Symmetric Key management
- Access Control for 'Change MSK' and 'PUT KEY' APDU
- Authentication and secure messaging to be used by the application integrating this module in Prepersonalization and Personalization phases, based on Global Platform standard

3.2.3.6 Toolbox

The Toolbox module provides different kind of services to other modules.

3.2.4 Applicative modules

3.2.4.1 Terminal Authentication (TA)

The TA module processes the Terminal Authentication (v1 and v2) mechanism. Terminal Authentication v2 is part of the EACv2 procedure.

3.2.4.2 Chip Authentication (CA)

The CA module processes the Chip Authentication (v1 and v2) mechanism. Chip Authentication v2 is part of the EACv2 procedure.

3.2.4.3 Supplemental Access Control (SAC)

The SAC module provides functionalities to process the PACE v2 mechanism.

3.2.4.4 Digitally Blurred Image (DBI)

The Digital Blurred Image module allows the blurring of a JPG file stored in a transparent file during the personalization phase. This functionality is optionally loaded with additional code.

3.2.4.5 Access Conditions Engine (ACE)

The ACE module is in charge of the verification of the Access Conditions of an object (file, key and PIN) when an application tries to access this object.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3.2.5 Operating System

3.2.5.1 Application Creation Engine

The Application Creation Engine is a complete set of commands used to personalize the card and its application(s). It includes:

- Administrative services for card configuration and life cycle management, key storage, pin storage and data storage.
- Storage of the Active Authentication Key (ECC and RSA Keys)
- Storage of multiple Chip Authentication Keys under the ADF (supporting ECC and RSA Keys)
- Storage of Trusted DL Root Keys under the ADF.
- Storage of CVCA Keys under the Master File.
- Storage of CVCA Keys under each ADF.

3.2.6 Application layer

3.2.6.1 Resident Application

The Resident Application is a complete set of commands, which allows the management of the card in the pre-personalization phase.
It supports the execution of an Authentication Procedure. Possible implementations include PACE or PACE with EACv2 (which encompasses Terminal Authentication v2 and Chip Authentication v2).

3.2.6.2 eDoc Application

The eDoc Application is a command dispatcher that is used only when the product is also hosting other applications than eSign. If only the eSign application is present on the card, this application is inactive: the eSign application directly receives all the commands if it has been selected before.

3.2.6.3 eSign Application

The eSign application is a complete set of commands used for eSign application. This includes the management of the RAD and the signature keys, and the signing operation.

3.2.6.4 Authentication Procedure

In the rest of the document, especially in the section SFRs, Authentication Procedure means PACE, EAC, Terminal Authentication, Chip Authentication, Verify PIN or a combination of these.

Note that PACE, EAC, Terminal Authentication and Chip Authentication have already been certified in previous projects. Verify PIN is part of this evaluation (RAD Management).

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

4 TOE LIFE CYCLE

4.1 Life cycle overview

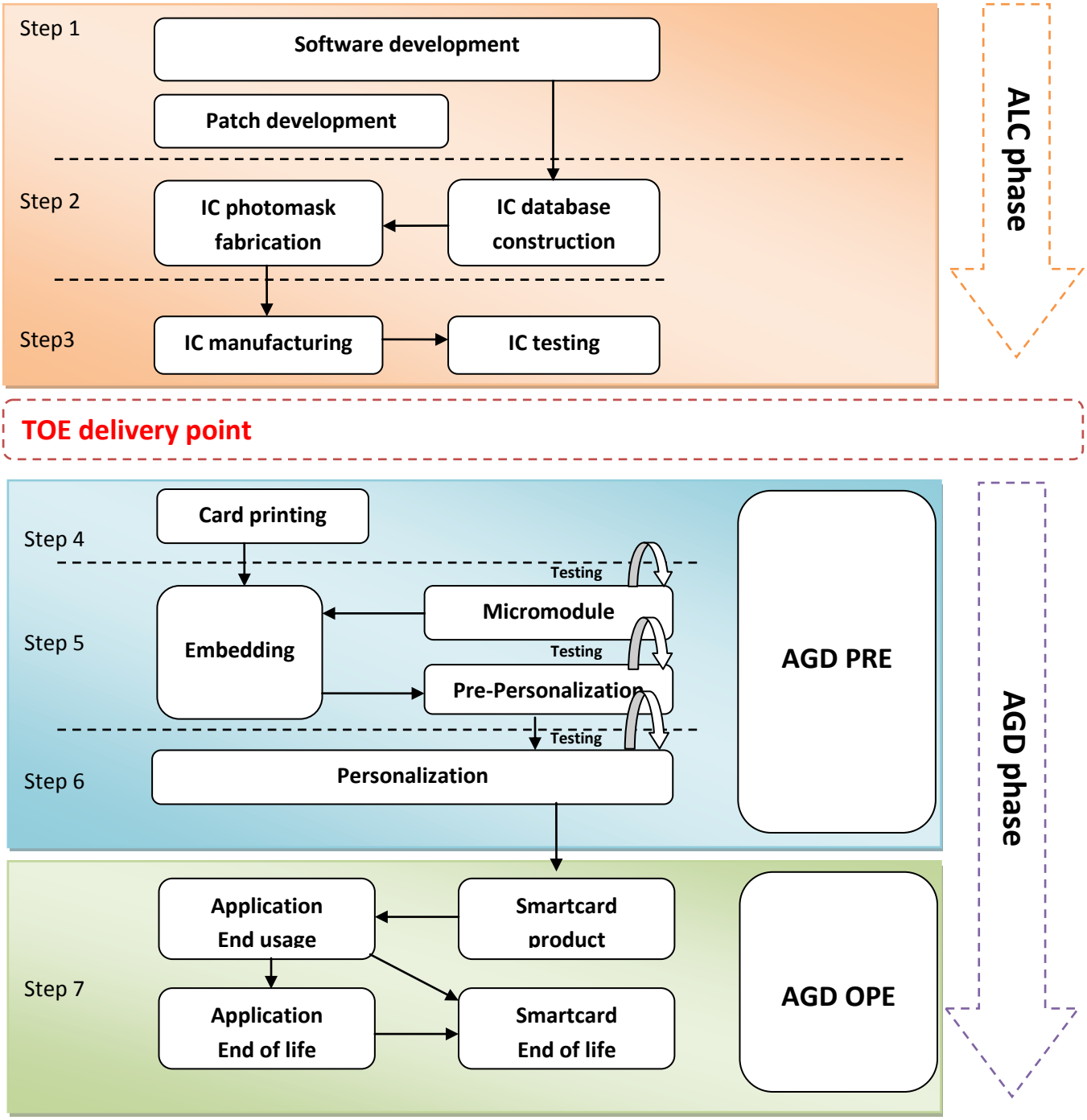

Figure 3 - TOE Lifecycle

The table below presents the roles involved in the development, manufacturing and personalization of the TOE:

Roles	Subject
IC developer	NXP Semiconductors
IC Manufacturer	NXP Semiconductors
TOE developer	Oberthur Technologies
Manufacturer	NXP Semiconductors Oberthur Technologies or another agent
Pre-personalizer	Oberthur Technologies or another agent
Personalization agent	Oberthur Technologies or another agent

Table 4-1 - Roles identification on the life cycle

The table below presents the subjects following TOE life cycle steps in accordance with the standard smart card life cycle [R26] and the Protection Profile life cycle. The table is divided into the phases, the TOE delivery point and the coverage:

Steps	Phase	Subject	Covered by	Sites
Step 1	Development	Oberthur Technologies	ALC R&D Sites	Pessac and Colombes
Step 2	Development	NXP Semiconductors	IC certification	See IC certification document
Step 3	Manufacturing	NXP Semiconductors	IC certification	See IC certification document
TOE delivery point				
Step 4	Manufacturing	eSign Manufacturer (Pre-personalizer)	AGD_PRE	
Step 5	Manufacturing	eSign Manufacturer (Pre-personalizer)	AGD_PRE	
Step 6	Personalization	Personalization agent	AGD_PRE	
Step 7	Operational Use	End user	AGD_OPE	

Table 4-2 - Subjects identification following life cycle steps

4.2 Phase 1 "Development" (Step1 and 2)

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step2) The TOE developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the eSign application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the eSign application and the guidance documentation are securely delivered to the Manufacturer.

4.3 Phase 2 "Manufacturing" (Steps 3 to 5)

(Step3) In a first step, the TOE integrated circuit is produced containing the secure signature creation device's chip Dedicated Software and the parts of the secure signature creation device's chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as secure signature creation device material during the IC manufacturing and the delivery process to the Manufacturer. The IC is securely delivered from the IC manufacture to the Manufacturer. If necessary, the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM). The IC manufacturer adds initialization data in EEPROM and keys (MSK, LSK).

TOE delivery point

(Step4) The Manufacturer combines the IC with hardware for the contact based / contactless interface in the secure signature creation device unless the secure signature creation device consists of the card only.

(Step5) Pre-personalization phase
The Manufacturer

(i) adds the IC Embedded Software or part of it and the additional source code in the non-volatile programmable memories if necessary,
(ii) creates the eSign application, and
(iii) equips the secure signature creation device's chips with pre-personalization Data.

The pre-personalized secure signature creation device together with the IC Identifier is securely delivered from the Manufacturer to the Personalization Agent. The Manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Additional code loading is performed in Pre-personalization phase encrypted with the LSK. It is compliant to ANSSI Note 6 [R61].

The additional code loading process is performed by the Pre-personalizer in the following steps, via the Command LOAD SECURE:

- Additional code generation
- MSK authentication
- LSK derivation
- Memory area definition
- Loading of the additional code
- Secure activation of the additional code

The additional code loading is performed before the creation of the MF file during Pre-personalization.

Identification of the additional code loading is given in Table 1-2 - TOE technical identification .

The additional code is generated by Oberthur Technologies: developed, compiled, ciphered and signed. After generation, it is sent to the eSign manufacturer to load to in the (initial) TOE.

Loading of the additional code

The additional code is loaded to the (initial) TOE by the Pre-personalizer, who shall authenticate itself to the TOE beforehand. Upon reception, the (initial) TOE checks it has been generated by Oberthur Technologies (by verifying the signature) before activating it.

Identification of the TOE

After successful loading and activation of the additional code, the TOE updates its identification data to reflect the presence of the additional code.

Once the additional code(s) is (are) loaded, the following operations should be processed:

- Master File Creation
- Card's Personalization Key Storage under Master File using PUT KEY command (see ISK [R41])
- CPLC Data Storage
- Application Creation (Create eSign ADF)
- eSign's Personalization Key Storage under eSign ADF
- Set the current life phase to Personalization Phase

Keys are loaded encrypted with DEC key and potentially additionally with Secure Messaging.

4.4 Phase 3 "Personalization of the TOE"

(Step 6) Personalization of the Secure Signature Device Creation

The personalization of the SSCD includes:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- Empty PIN container
- Empty key container
- Empty file with EF Identifier 0x0119

Some production steps, e.g. Step 5 (ii) and (iii) in Phase 2, may also take place in the Phase 3.

Keys are loaded encrypted with DEC key and potentially additionally with Secure Messaging.

4.5 Phase 4 “Operational Use”

(Step 7) The TOE is used as a signing document by a user to sign transactions in the « Operational Use » phase.

Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the “Operational Use” (phase 4) have to be considered in the product evaluation process under AGD assurance class.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

5 CONFORMANCE CLAIMS

5.1 Common Criteria conformance

This Security Target (ST) claims conformance to the Common Criteria version 3.1 revision 4 [R58], [R59] and [R60].

The conformance to the CC is claimed as follows:

CC	Conformance Claim
Part 1	Strict conformance
Part 2	Conformance with extensions: - FPT_EMS.1 "TOE Emanation" (defined in [R26]) - FAU_SAS.1 "Audit data storage" (defined in [R26])
Part 3	Conformance with package EAL5 augmented with - AVA_VAN.5 "Advanced methodical vulnerability analysis" - ALC_DVS.2 "Sufficiency of security measures"

Table 5-1 - Conformance Claim

5.2 Protection Profile conformance

The Security Target claims strict conformance to the following Protection Profile written in CC version 3.1 revision 3: Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application. Version 1.0.1, 2012-11-14.

The following tables present the correspondence between the information from the SSCD-5 PP and the information in this security target and when relevant the additions (in red) and the iterations (in blue) of the SFRs of the Protection Profile.

From PP SSCD – 5	In this ST
Assets and objects	
SCD	SCD
SVD	SVD
DTBS and DTBS/R	DTBS and DTBS/R
	RAD
	TOE-ID
	CPLC Data

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Users and subjects acting for users	
S.User	S.User
S.Admin	S.Admin
Signatory (S.Sigy, R.Sigy)	Signatory (S.Sigy, R.Sigy)
Administrator (R.Admin)	Administrator (R.Admin) CSP (Certificate Service Provider); Refinement of Administrator
	Manufacturer
	Pre-personalizer (Refinement of Administrator)
	Personalizer (Refinement of Administrator)
Threat agents	
Attacker	Attacker
Threats	
T.SCD_Divulg	T.SCD_Divulg
T.SCD_Derive	T.SCD_Derive
T.Hack_Phys	T.Hack_Phys
T.SVD_Forgery	T.SVD_Forgery
T.SigF_Misuse	T.SigF_Misuse
T.DTBS_Forgery	T.DTBS_Forgery
T.Sig_Forgery	T.Sig_Forgery
	T.Unauthorized_Load
	T.Bad_Activation
	T.TOE_Identification_Forgery
	T.Pre_Perso
	T.Perso
Organisational Security Policies	
P.CSP_QCert	P.CSP_QCert
P.QSign	P.QSign
P.Sigy_SSCD	P.Sigy_SSCD
P.Sig_Non-Repud	P.Sig_Non-Repud
Assumptions	
A.CGA	A.CGA
A.SCA	A.SCA
Security Objectives for the TOE	
OT.Lifecycle_Security	OT.Lifecycle_Security
OT.SCD/SVD_Gen	OT.SCD/SVD_Gen
OT.SCD_Unique	OT.SCD_Unique

OT.SCD_SVD_Corresp	OT.SCD_SVD_Corresp
OT.SCD_Secrecy	OT.SCD_Secrecy
OT.Sig_Secure	OT.Sig_Secure
OT.Sigy_SigF	OT.Sigy_SigF
OT.DTBS_Integrity_TOE	OT.DTBS_Integrity_TOE
OT.EMSEC_Design	OT.EMSEC_Design
OT.Tamper_ID	OT.Tamper_ID
OT.Tamper_Resistance	OT.Tamper_Resistance
OT.TOE_TC_VAD_Imp	OT.TOE_TC_VAD_Imp
OT.TOE_TC_DTBS_Imp	OT.TOE_TC_DTBS_Imp
	OT.Secure_Load_ACode
	OT.Secure_AC_Activation
	OT.TOE_Identification
	OT.Pre_Perso
	OT.Perso
Security Objectives for Operational Environment	
OE.SVD_Auth	OE.SVD_Auth
OE.CGA_QCert	OE.CGA_QCert
OE.SSCD_Prov_Service	OE.SSCD_Prov_Service
OE.HID_TC_VAD_Exp	OE.HID_VAD
OE.DTBS_Intend	OE.DTBS_Intend
OE.SCA_TC_DTBS_Exp	OE.DTBS_Protect
OE.Signatory	OE.Signatory

Table 5-2 - Conformance with SSCD-5 PP (SPD and Objectives)

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

5.2.1 Correspondences and additions of SFR

SFRs from PP SSCD – 5	SFRs from ST
FCS_CKM.1	FCS_CKM.1/RSA
	FCS_CKM.1/ECDSA
	FCS_CKM.1/MP_Add_code
	FCS_CKM.1/MP
FCS_CKM.4	FCS_CKM.4
FCS_COP.1	FCS_COP.1
	FCS_COP.1/MP_ENC_Add_code
	FCS_COP.1/MP_MAC_Add_code
	FCS_COP.1/MP_ENC_3DES
	FCS_COP.1/MP_ENC_AES
	FCS_COP.1/MP_MAC_3DES
	FCS_COP.1/MP_MAC_AES
	FCS_COP.1/MP_AUTH_3DES
	FCS_COP.1/MP_AUTH_AES
	FCS_COP.1/MP_SHA
FDP_ACC.1/SCD/SVD_Generation	FDP_ACC.1/SCD/SVD_Generation
	FDP_ACC.2/MP
FDP_ACF.1/SCD/SVD_Generation	FDP_ACF.1/SCD/SVD_Generation
	FDP_ACF.1/MP
FDP_ACC.1/SVD_Transfer	FDP_ACC.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	FDP_ACF.1/SVD_Transfer
FDP_ACC.1/Signature_Creation	FDP_ACC.1/Signature_Creation
FDP_ACF.1/Signature creation	FDP_ACF.1/Signature creation
FDP_RIP.1	FDP_RIP.1
FDP_SDI.2/Persistent	FDP_SDI.2/Persistent
FDP_SDI.2/DTBS	FDP_SDI.2/DTBS
	FDP_UCT.1/MP
	FDP_UIT.1/MP
	FDP_UIT.1/MP_Add_code
FIA_UID.1	FIA_UID.1
	FIA_UID.1/MP
FIA_UAU.1	FIA_UAU.1
	FIA_UAU.1/MP
	FIA_UAU.4/MP_3DES
	FIA_UAU.4/MP_AES

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SFRs from PP SSCD – 5	SFRs from ST
	FIA_UAU.5/MP_3DES
	FIA_UAU.5/MP_AES
FIA_AFL.1	FIA_AFL.1
	FIA_AFL.1/MP
FMT_SMR.1	FMT_SMR.1
	FMT_SMR.1/MP_Add_Code
	FMT_SMR.1/MP
FMT_SMF.1	FMT_SMF.1
	FMT_SMF.1/MP
FMT_MOF.1	FMT_MOF.1
FMT_MSA.1/Admin	FMT_MSA.1/Admin
FMT_MSA.1/Signatory	FMT_MSA.1/Signatory
FMT_MSA.2	FMT_MSA.2
FMT_MSA.3	FMT_MSA.3
FMT_MSA.4	FMT_MSA.4
FMT_MTD.1/Admin	FMT_MTD.1/Admin
FMT_MTD.1/Signatory	FMT_MTD.1/Signatory
	FMT_MTD.1/MP_Add_code
	FMT_MTD.1/MP_KEY_READ_Add_code
	FMT_MTD.1/MP
	FMT_MTD.1/MP_INI_ENA
	FMT_MTD.1/MP_INI_DIS
	FMT_MTD.1/MP_KEY_READ
	FMT_MTD.1/MP_KEY_WRITE
FPT_EMS.1	FPT_EMS.1
	FPT_EMS.1/MP_Add_code
	FPT_EMS.1/MP
FPT_FLS.1	FPT_FLS.1
FPT_PHP.1	FPT_PHP.1
FPT_PHP.3	FPT_PHP.3
FPT_TST.1	FPT_TST.1
FDP_UIT.1/DTBS	FDP_UIT.1/DTBS
FTP_ITC.1/DTBS	FTP_ITC.1/DTBS
FTP_ITC.1/VAD	FTP_ITC.1/VAD
	FTP_ITC.1/MP_Add_code
	FTP_ITC.1/MP

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SFRs from PP SSCD – 5	SFRs from ST
	FDP_ITC.1/MP
	FAU_SAS.1/MP
	FAU_STG.2/MP_Add_Code

Table 5-3 - Conformance with SSCD-5 PP (SFR)

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6 SECURITY PROBLEM DEFINITION

6.1 Assets, objects, users and subjects

The assets, objects, users and subjects appearing in the rest of the Security Target are being introduced in this section.

6.1.1 Assets and objects

6.1.1.1 From PP SSCD-5

1. SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.
   SCD key is an asset of "operational use" phase.

2. SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.
   SVD key is an asset of "operational use" phase.

3. DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.
   DTBS and DTBS/R are assets of the "Operational Use" phase.

6.1.1.2 Others

4. TOE ID: Data uniquely identifying the TOE.
   TOE ID is an asset of the "pre-personalization" and "personalization" phases.

5. CPLC data: Card Personalization Life Cycle data
   CPLC is an asset of the "pre-personalization" and "personalization" phases.

6. RAD: Reference Authentication Data

RAD is an asset of the "personalization" and "operational use" phases.

7. Pre-personalization / Personalization keys (including LSK, MSK, DEC, ENC, MAC, keys used for Secure Messaging)

These keys are used for encrypting and charging of additional code and keys during the Pre-personalization and Personalization phases. They count as sensitive data.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.1.2 Users and subjects acting for users

6.1.2.1 From PP SSCD - 5

1. User: End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

2. Administrator: User who is in charge to perform the TOE initialisation, TOE (pre-) personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator. The CSP (Certificate Service Provider) also counts as Administrator.

3. Signatory: User who holds the TOE and uses it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

6.1.2.2 Others

4. Manufacturer: The person that produces the TOE. He will act in the role Manufacturer.

5. Pre-personalizer: This is a refinement of the Administrator and describes the person that is specifically in charge of Pre-personalization.

6. Personalizer: This is a refinement of the Administrator and describes the person that is specifically in charge of Personalization.

6.2 Threats

The threats for the TOE are introduced in this section, beginning with the definition of the threat agents.

6.2.1 Threat agents

6.2.1.1 From PP SSCD - 5

1. Attacker in operational use phase: Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret.

6.2.1.2 Others

2. Attacker in pre-personalization or personalisation phases: human or process acting on their behalf located outside the TOE. The goal of the attacker is to read or modify the TOE pre-personalisation and personalization data that he does not have the right to read or modify (sensitive data), or to forge the additional code. The attacker has got a high attack potential.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.2.2 Threats from PP SSCD - 5

6.2.2.1 T.SCD_Divulg Storing, copying and releasing of the signature creation data

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

6.2.2.2 T.SCD_Derive Derive the signature creation data

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

6.2.2.3 T.Hack_Phys Physical attacks through the TOE interfaces

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

6.2.2.4 T.SVD_Forgery Forgery of the signature verification data

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

6.2.2.5 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.

6.2.2.6 T.DTBS_Forgery Forgery of the DTBS/R

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

6.2.2.7 T.Sig_Forgery Forgery of the electronic signature

An attacker forges a signed data object, maybe using an electronic signature, which has been 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 created 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.

6.2.3 Threats for Loading of Additional Code

6.2.3.1 T.Unauthorized_Load

Adverse action: An attacker tries to load an additional code that is not intended to be assembled with the initial TOE, i.e. the evidence of authenticity or integrity is not correct.

Threat agent: having high attack potential, knowing the MSK, LSK and derivation data, being in possession of a legitimate eSign card

Asset: RAD

6.2.3.2 T.Bad_Activation

Adverse action: An attacker tries to perturbate the additional code activation such that the final TOE is different than the expected one (initial TOE or perturbated TOE).

Threat agent: having high attack potential, knowing the MSK, LSK and derivation data, being in possession of a legitimate eSign card, being in possession of an additional code that is authorized to be loaded

Asset: RAD

6.2.3.3 T.TOE_Identification_Forgery

Adverse action: An attacker tries to perturb the TOE identification and in particular the additional code identification.

Threat agent: having high attack potential, being in possession of a legitimate eSign card.

Asset: TOE ID

Application Note: This threat is not applicable in phase 7, as the TOE identification is not possible in phase 7.

6.2.4 Threats for pre-personalization and personalization

6.2.4.1 T.Pre_Perso

Adverse action: An attacker tries to read or modify TOE assets available in pre-personalization phase that he does not have the right to read or modify (sensitive data).

Threat agent: having high attack potential, being in possession of a legitimate eSign card.

Assets: CPLC data, TOE-ID.

6.2.4.2 T.Perso

Adverse action: An attacker tries to read or modify TOE assets available in personalization phase that he does not have the right to read or modify (sensitive data).

Threat agent: having high attack potential, being in possession of a legitimate eSign card.

Assets: CPLC data, TOE-ID, RAD.

6.3 Organizational security policies

6.3.1 Organizational Security Policies from the PP SSCD – 5

6.3.1.1 P.CSP_QCert Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the directive, article 2, clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least 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 as SSCD is evident with signatures through the certificate or other publicly available information.

6.3.1.2 P.QSign Qualified electronic signatures

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the directive, article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the directive Annex I)[1]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

6.3.1.3 P.Sigy_SSCD TOE as secure signature creation device

The TOE meets the requirements for an SSCD laid down in Annex III of the directive [1]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

6.3.1.4 P.Sig_Non-Repud Non-repudiation of signatures

The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

[1] *It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.4 Assumptions

6.4.1 Assumptions from the PP SSCD – 5

6.4.1.1 A.CGA Trustworthy certificate generation application

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

6.4.1.2 A.SCA Trustworthy signature creation application

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

7 SECURITY OBJECTIVES

7.1 Security Objectives for the TOE

7.1.1 Security Objectives from PP SSCD - 5

7.1.1.1 Relation to core ST SSCD KG

This ST includes all security objectives for the TOE as defined in the core ST SSCD KG [R7]: OT.Lifecycle_Security, OT.SCD/SVD_Gen, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance.

This ST additionally describes the objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp.

7.1.1.2 *OT.Lifecycle_Security* Lifecycle security

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

The TOE only contains one set of SCD at a time.

7.1.1.3 OT.SCD/SVD_ Gen Authorized SCD/SVD generation

The TOE shall provide security features to ensure that authorized users only may invoke the generation of the SCD and the SVD.

7.1.1.4 OT.SCD_Unique Uniqueness of the signature creation data

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

7.1.1.5 OT.SCD_SVD_Corresp Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

7.1.1.6 OT.SCD_Secrecy Secrecy of the signature creation data

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

7.1.1.7 OT.Sig_Secure Cryptographic security of the electronic signature

The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

7.1.1.8 OT.Sigy_SigF Signature creation function for the legitimate signatory only

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

7.1.1.9 OT.DTBS_Integrity_TOE DTBS/R integrity inside the TOE

The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

7.1.1.10 OT.EMSEC_Design Provide physical emanations security

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

7.1.1.11 OT.Tamper_ID Tamper detection

The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches.

7.1.1.12 OT.Tamper_Resistance Tamper resistance

The TOE shall prevent or resist physical tampering with specified system devices and components.

7.1.1.13 OT.TOE_TC_DTBS_Imp Trusted channel of TOE for DTBS import

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS.

Application note: This security objective for the TOE is partly covering OE.DTBS_Protect from the core ST. While OE.DTBS_Protect in the core ST requires only the operational environment to protect DTBS, this ST requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this ST re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

7.1.1.14 *OT.TOE_TC_VAD_Imp* Trusted channel of TOE for VAD export

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentictation method employed.

Application note: This security objective for the TOE is partly covering OE.HID_VAD from the core ST. While OE.HID_VAD in the core ST requires only the operational environment to protect VAD, this ST requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

7.1.2 Security Objectives for the Loading of Additional Code

7.1.2.1 OT.Secure_Load_ACode

The Loader of the Initial TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE.

During the Load Phase of an Additional Code, the TOE shall remain secure.

7.1.2.2 OT.Secure_AC_Activation

Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation. If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE), the Initial TOE shall remain in its initial state or fail secure.

7.1.2.3 OT.TOE_Identification

The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user must be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE. TOE must support the terminal to verify the authenticity.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

7.1.3 Security Objectives for pre-personalization and personalization

7.1.3.1 OT.Pre_Perso

The TOE must protect the stored data from unauthorized disclosure or modification. Sensitive data cannot be read nor modified by anyone else than the pre-personalizer. The TOE shall protect sensitive data against unauthorized disclosure or modification by logical or physical means. To perform any operation on sensitive data, the pre-personalizer shall be authenticated. He may use secure messaging to exchange data with the TOE. The loading of the keys is always executed encrypted with the DEC key, and optionally with additional SM.

The code is always loaded during the pre-personalization phase encrypted with the LSK key.

7.1.3.2 OT.Perso

The TOE must protect the stored data from unauthorized disclosure or modification. Sensitive data cannot be read or modified by anyone else than the personalizer. The TOE shall protect sensitive data against unauthorized disclosure or modification by logical or physical means. To perform any operation on sensitive data, the personalizer shall be authenticated. He may use secure messaging to exchange data with the TOE. The loading of the keys is always executed encrypted with the DEC key, and optionally with additional SM.

7.2 Security objectives for the operational environment

7.2.1 Security objectives from PP SSCD-5

7.2.1.1 Relation to core ST SSCD-2 KG (key generation)

This ST includes the following security objectives for the operational environment as defined in the core ST SSCD KG [R7]: OE.SVD_Auth, OE.CGA_Qcert, OE.SSCD_Prov_Service, OE.DTBS_Intend, and OE.Signatory.

This PP substitutes OE.HI_VAD from the core PP by OE.HID_TC_VAD_Exp and OE.DTBS_Protect from the core PP by OE.SCA_TC_DTBS_Exp as follows.

7.2.1.2 OE.SVD_Auth Authenticity of the SVD

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

7.2.1.3 OE.CGA_QCert Generation of qualified certificates

The CGA shall generate a qualified certificate that includes (amongst others)

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

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

7.2.1.4 OE.SSCD_Prov_Service Authentic SSCD provided by SSCD-provisioning service

The SSCD-provisioning service shall initialize and personalize for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

7.2.1.5 OE.HID_TC_VAD_Exp Trusted channel of HID for VAD export

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

Application note: This security objective for the TOE is partly covering OE.HID_VAD from the core ST. While OE.HID_VAD in the core ST requires only the operational environment to protect VAD, this ST requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

7.2.1.6 OE.DTBS_Intend SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that

- generates the DTBS/R 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,
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- attaches the signature produced by the TOE to the data or provides it separately.

7.2.1.7 OE.SCA_TC_DTBS_Exp Trusted channel of SCA for DTBS export

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Application note: This security objective for the TOE is partly covering OE.DTBS_Protect from the core ST. While OE.DTBS_Protect in the core ST requires only the operational environment to protect DTBS, this ST requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this ST re-assigns partly the DTBS protection from the operational environment as described by

OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

7.2.1.8 OE.Signatory Security obligation of the signatory

The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

8 EXTENDED COMPONENTS DEFINITION

8.1 Definition of the Family FPT_EMS

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMS is taken from the *Protection Profile Secure Signature Creation Device* [5].

FPT_EMS TOE Emanation

Family behavior: This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS TOE Emanation	1

FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emitting intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emitting interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if **FAU_GEN** (*Security audit data generation*) is included in a PP or ST using FPT_EMS.1.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FPT_EMS.1 *TOE Emanation*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

The TOE shall not emit [*assignment: types of emissions*] in excess of [*assignment: specified limits*] enabling access to [assignment*: list of types of TSF data*] and [assignment*: list of types of user data*].

FPT_EMS.1.2

The TSF shall ensure [assignment*: type of users*] are unable to use the following interface [assignment*: type of connection*] to gain access to [assignment*: list of types of TSF data*] and [assignment*: list of types of user data*].

8.2 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behavior: This family defines functional requirements for the storage of the audit data

Component leveling:

FAU_SAS Audit data	1

FAU_SAS.1	Requires the TOE to provide the possibility to store audit data
Management: FAU_SAS.1	There are no management activities foreseen
Audit: FAU_SAS.1	There are no actions defined to be auditable

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FAU_SAS.1 Audit storage

Hierarchical to: No other components
Dependencies: No Dependencies

FAU_SAS.1.1	The TSF shall provide [assignment: *list of subjects*] with the capability to store [assignment: *list of audit information*] in the [assignment: *type of persistent memory*]

9 SECURITY REQUIREMENTS

9.1 Security functional requirements from PP SSCD – 5

Underlined parts correspond to instantiations, where the ones referenced by a footnote are the instantiations of this Security Target and the ones without instantiations of the Protection Profile. Bold parts correspond to editorial refinements.

9.1.1 Cryptographic support (FCS)

FCS_CKM.1/RSA **Cryptographic key generation**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/RSA The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm RSA key generation and specified cryptographic key sizes RSA 1024 to 4096 bits in steps of 256 bits[2] that meet the following:

- FIPS 186.3

FCS_CKM.1/ECDSA **Cryptographic key generation**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

[2] *[assignment*: cryptographic key sizes*]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_CKM.1.1/ECDSA The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm ECDSA key generation and specified cryptographic key sizes 192 up to 521 bits where the field length of a given elliptic curve is used to determine the maximum length of signature's input, where the field length L is computed as follows:

L = [log256 N] = (N size in bits) / 8 = N size in bytes

Where N is the elliptic curve's order.[3] These are keys that meet the following:

- ECDSA – Elliptic Curve Digital Signature Scheme (TR 3111),
- FIPS 186-4.

9.1.1.1 *FCS_CKM.4* Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroisation[4] that meets the following: none[5].

9.1.1.2 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

[3] *[assignment*: cryptographic key sizes*]*
[4] *[assignment*: cryptographic key destruction method*]*
[5] [assignment*: list of standards*].

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_COP.1.1 The TSF shall perform digital signature creation[6] in accordance with a specified cryptographic algorithm

- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- Signature based on RSA and elliptic curve signature scheme:
  - RSA PKCS#v1.5
  - RSA PSS
- Without the following combinations:
  - ESIGN_RSA_PKCS#v1.5_1024_SHA384
  - ESIGN_RSA_PKCS#v1.5_1024_SHA512
  - ESIGN_RSA_PKCS#v1.5_1280_SHA512
  - ESIGN_RSA_PKCS#v1.5_1536_SHA512
- Signature based on Elliptic curves signature schemes:
  - ECDSA plain
  - ECDSA BER-TLV

and cryptographic key sizes RSA 1024 to 4096 bits in steps of 256 bits and EC 192 up to 521 bits that meet the following:

- RSA Digital Signature Schemes with Appendix (RSA labs)
  - PKCS version 1.5 RSASSA-PKCSv1_5
  - PKCS version 2.1 Probabilistic Signature Scheme RSASSA-PSS
- ECDSA – Elliptic Curve Digital Signature Scheme (TR 3111)
  - Plain format
  - X9.62 format[7].

9.1.2 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin R.Sigy
	SCD/SVD Management	Authorized Not authorized
SCD	SCD Operational	No Yes
	SCD Identifier	Arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

[6] *[assignment :* list of cryptographic operations*]*
[7] *[assignment:* list of standards*]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.1.2.1 FDP_ACC.1/SCD/SVD_Generation Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SCD/SVD_Generation The TSF shall enforce the SCD/SVD Generation SFP[8] on

(1) subjects: S.User,

(2) objects: SCD, SVD,

(3) operations: generation of SCD/SVD pair.

9.1.2.2 FDP_ACF.1/SCD/SVD_Generation Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/SCD/SVD_Generation The TSF shall enforce the SCD/SVD Generation SFP to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management".

FDP_ACF.1.2/ SCD/SVD_Generation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

S.User with the security attribute "SCD/SVD Management" set to "authorized" is allowed to generate SCD/SVD pair.

FDP_ACF.1.3/ SCD/SVD_Generation The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

[8] *[assignment :* access control SFP*]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FDP_ACF.1.4/ SCD/SVD_Generation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD/SVD management" set to "not authorized" is not allowed to generate SCD/SVD pair.

9.1.2.3 FDP_ACC.1/SVD_Transfer Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP on (1) subjects: S.User, (2) objects: SVD (3) operations: export.

9.1.2.4 FDP_ACF.1/SVD_Transfer Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP to objects based on the following: (1) the S.User is associated with the security attribute Role, (2) the SVD.
FDP_ACF.1.2/ SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin is allowed to export SVD.
FDP_ACF.1.3/ SVD_Transfer	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FDP_ACF.1.4/ SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

Application note: The CSP (Certificate Service Provider) is a refinement of R.Admin and the one responsible for fulfilling the SFR.

9.1.2.5 *FDP_ACC.1/Signature_Creation* Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature_Creation	The TSF shall enforce the Signature Creation SFP on (1) subjects: S.User, (2) objects: DTBS/R, SCD, (3) operations: signature creation.

9.1.2.6 *FDP_ACF.1/Signature creation* Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signature_Creation	The TSF shall enforce the Signature Creation SFP to objects based on the following: (1) the user S.User is associated with the security attribute "Role" and (2) the SCD with the security attribute "SCD Operational".
FDP_ACF.1.2/ Signature_Creation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes".

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FDP_ACF.1.3/ Signature_Creation	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Signature_Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no".

9.1.2.7 *FDP_RIP.1* Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

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.

9.1.2.8 *FDP_SDI.2/Persistent* Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/ Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked 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 S.Sigy about integrity error.

Application note: The following data persistently stored by the TOE has the user data attribute "integrity checked persistent stored data":

1. SCD
2. SVD

9.1.2.9 *FDP_SDI.2/DTBS* Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Dependencies: No dependencies.

FDP_SDI.2.1/DTBS The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored DTBS.

FDP_SDI.2.2/DTBS Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

(2) inform the S.Sigy about integrity error.

Application note: The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data".

9.1.3 Identification and authentication (FIA)

9.1.3.1 *FIA_UID.1* Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1) Self-test according to FPT_TST.1
2) Read EF.CardAccess
3) Execute Authentication Procedure (see 3.2.6.4)
4) Select File
5) Verification of the RAD[9]

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.

[9] [assignment: *list of additional TSF-mediated actions*]

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.1.3.2 *FIA_UAU.1* Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow

1) Self-test according to FPT_TST.1,
2) Identification of the user by means of TSF required by FIA_UID.1
3) Establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD[10]

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.

9.1.3.3 *FIA_AFL.1* Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when the allowed number fixed by the Personalizer for[11] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL .1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall block the RAD.

[10] *[assignment:* list of additional TSF-mediated actions*]*

[11] *[selection:* [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.1.4 Security Management (FMT)

9.1.4.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles R.Admin and R.Sigy.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

9.1.4.2 *FMT_SMF.1* Security management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- Creation and modification of RAD,
- Management of data related to the Authentication Procedure (see 3.2.6.4)
- Enabling the signature creation function,
- Modification of the security attribute SCD/SVD management, SCD operational,
- Change the default value of the security attribute SCD Identifier.

9.1.4.3 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to enable the functions signature creation function to R.Sigy.

9.1.4.4 FMT_MSA.1/Admin Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/ Admin	The TSF shall enforce the SCD/SVD Generation SFP to restrict the ability to modify[12] the security attributes SCD/SVD management to R.Admin.

9.1.4.5 *FMT_MSA.1/Signatory* Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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 R.Sigy.

9.1.4.6 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

[12] *[assignment*: other operations*]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational.

9.1.4.7 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP a and Signature Creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

9.1.4.8 FMT_MSA.4 Security attribute value inheritance

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

- If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated, the security attribute “SCD operational” of the SCD shall be set to “no” as a single operation.
- If S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD operational” of the SCD shall be set to “yes” as a single operation.

9.1.4.9 FMT_MTD.1/Admin Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FMT_MTD.1.1/Admin	The TSF shall restrict the ability to create the RAD to R.Admin.

9.1.4.10 *FMT_MTD.1/Signatory* Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Signatory	The TSF shall restrict the ability to modify[13] the RAD to R.Sigy.

9.1.5 Protection of the TSF (FPT)

9.1.5.1 FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1	The TOE shall not emit power variations, timing variations during command execution in excess of unuseful information[14] enabling access to RAD and SCD.
FPT.EMS.1.2	The TSF shall ensure unauthorized users[15] are unable to use the following interface IC contacts[16] to gain access to RAD and SCD.

[13] *[assignment*: other operations*]*
[14] *[assignment*: specified limits*]*
[15] *[assignment*: type of users*]*
[16] *[assignment*: type of connection*]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.1.5.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- self-test according to FPT_TST fails
- Exposure to out-of-range operating conditions that could lead to malfunction[17].

9.1.5.3 FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 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.

9.1.5.4 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[18] to the TSF[19] by responding automatically such that the SFRs are always enforced.

[17] [assignment: *list of other types of failures in the TSF*]

[18] *[assignment:* physical tampering scenarios*]*

[19] *[assignment:* list of TSF devices/elements*]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.1.5.5 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self-tests

- At reset
- Before any cryptographic operation
- When accessing a Data Group or any EF
- Prior to any use of TSF data
- Before execution of any command[20]

to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of TSF.

9.1.5.6 *FDP_UIT.1/DTBS* Data exchange integrity

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control , or
FDP_IFC.1 Subset information flow control]
[FTP_ITC Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1/DTBS The TSF shall enforce the Signature Creation SFP to receive user data in a manner protected from modification and insertion errors.

FDP_UIT.1.2/DTBS The TSF shall be able to determine on receipt of user data, whether modification and insertion has occurred.

[20] *[selection:* during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-test should occur]*]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.1.5.7 FTP_ITC.1/VAD Inter-TSF trusted channel – TC Human Interface Device

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/VAD	The TSF shall provide a communication channel between itself and another trusted IT product **HID** 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/VAD	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/VAD	The TSF **or the HID** shall initiate communication via the trusted channel for (1) User authentication according to FIA_UAU.1[21].

9.1.5.8 FTP_ITC.1/DTBS Inter-TSF trusted channel – Signature Creation Application

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/DTBS	The TSF shall provide a communication channel between itself and another trusted IT product **SCA** 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	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

[21] [assignment: *list of other functions for which a trusted channel is required*]

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FTP_ITC.1.3/DTBS	The TSF **or the SCA** shall initiate communication via the trusted channel for (1) Signature creation[22].

9.2 Security Functional Requirements for Manufacturing, Personalization and Loading of Additional Code

This chapter covers the Manufacturing and Personalisation SFR. It also includes additional SFRs for the compliance with the Loading of Additional Code.

9.2.1 SFRs for additional code

9.2.1.1 FAU_STG.2/MP_Add_code Guarantees of audit data availability

FAU_STG.2.1/MP_Add_Code	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.2.2/MP_Add_code	The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.
FAU_STG.2.3/MP_Add_code	The TSF shall ensure that Additional code identification stored audit records will be maintained when the following conditions occur: failure and attack.

Application Note: Additional code is loaded with its integrity information. This integrity information is verified by the TOE after the loading and before the writing of the identification information by calculating the signature and comparing it to the expected value. The signature is protected in integrity through the TOE lifecycle: At each power on, the card verifies the integrity of this signature.

9.2.1.2 FCS_CKM.1/MP_Add_code Cryptographic key generation

FCS_CKM.1.1/MP_Add_code	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Calculation of LSK_LOAD, from initial LSK and derivation data entered - AES 128 ECB[23] and specified cryptographic key sizes 128 bits[24] that meet the following: none[25]:

[22] [assignment: *list of other functions for which a trusted channel is required*]

[23] *[cryptographic key generation algorithm]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.1.3 *FCS_COP.1/MP_ENC_Add_code* Cryptographic operation

FCS_COP.1.1/MP_ENC_Add_code	The TSF shall perform Decryption of the additional code (ciphered with LSK_LOAD) and signature verification[26] in accordance with a specified cryptographic algorithm AES[27] and cryptographic key sizes 128 bits[28] that meet the following: [R51][29].

9.2.1.4 *FCS_COP.1/MP_MAC_Add_code* Cryptographic operation

FCS_COP.1.1/MP_MAC_Add_code	The TSF shall perform Secure Messaging with AES[30] in accordance with a specified cryptographic algorithm AES CMAC[31] and cryptographic key sizes 128 bits[32] that meet the following: [R51][33].

9.2.1.5 *FDP_UIT.1/MP_Add_code* Data exchange integrity

FDP_UIT.1.1/MP_Add_code	The TSF shall enforce the Pre-personalization access control SFP to receive user data in a manner protected from modification errors.
FDP_UIT.1.2/MP_Add_code	**[Editorially Refined]** The TSF shall be able to determine on receipt of user data, whether modification of some of the pieces of the application sent by the TOE developer has occurred.

Application Note: Modification errors should be understood as modification, substitution, unrecoverable ordering change of data and any other integrity error that may cause the additional code to be installed on the card to be different from the one sent by the TOE Developer. This SFR controls integrity of data import in phase 5, including the additional code but not only.

---

[24] *[key length]*
[25] *[standard]*
[26] *[cryptographic operation]*
[27] *[cryptographic algorithm]*
[28] *[cryptographic key sizes]*
[29] *[standard]*
[30] *[cryptographic operation]*
[31] *[cryptographic algorithm]*
[32] *[cryptographic key sizes]*
[33] *[standard]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.1.6 *FMT_MTD.1/MP_Add_code* Management of TSF data

FMT_MTD.1.1/MP_Add_code	The TSF shall restrict the ability to activate[34] the additional code[35] to TOE developer[36].

Application note: The Activation of the additional code modifies the TOE. This additional code is ciphered with the LSK_LOAD (LSK and Derivation Data) and activated after the authentication of the TOE developer.

9.2.1.7 *FMT_MTD.1/MP_KEY_READ_Add_code* Management of TSF data

FMT_MTD.1.1/MP_KEY_READ_Add_code	The TSF shall restrict the ability to read the LSK[37] to none[38]:

9.2.1.8 *FMT_SMR.1/MP_Add_Code* Security roles

FMT_SMR.1.1/MP_Add_code	The TSF shall maintain the roles TOE developer.
FMT_SMR.1.2/MP_Add_code	The TSF shall be able to associate users with roles.

9.2.1.9 *FPT_EMS.1/MP_Add_code* TOE Emanation

FPT_EMS.1.1/MP_Add_code	The TOE shall not emit power variations, timing variations during command execution in excess of non-useful information enabling access to LSK.
FPT_EMS.1.2/MP_Add_code	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to LSK.

[34] *[selection]*
[35] *[list of TSF data]*
[36] *[authorized identified roles]*
[37] *[data]*
[38] *[authorized identified roles]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.1.10 *FTP_ITC.1/MP_Add_code* Inter-TSF trusted channel

FTP_ITC.1.1/MP_Add_code	The TSF shall provide a communication channel between itself and another 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/MP_Add_code	**[Editorially Refined]** The TSF shall permit the TOE Developer and Pre-personalizer to initiate communication via the trusted channel.
FTP_ITC.1.3/MP_Add_code	The TSF shall initiate communication via the trusted channel for Additional code loading.

9.2.2 Manufacturing and Personalization

9.2.2.1 *FCS_CKM.1/MP* Cryptographic key generation

FCS_CKM.1.1/MP	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm MSK derivation from initial MSK loaded in phase 1 using SHA 256[39] and specified cryptographic key sizes 256 bits[40] that meet the following: none[41].

9.2.2.2 *FCS_COP.1/MP_ENC_3DES* Cryptographic operation

FCS_COP.1.1/MP_ENC_3DES	The TSF shall perform Secure Messaging – encryption and decryption[42] in accordance with a specified cryptographic algorithm 3DES in CBC mode[43] and cryptographic key sizes 112 bits[44] that meet the following: [R48][45]

[39] [cryptographic key generation algorithm]

[40] *[key length]*
[41] *[standard]*
[42] *[cryptographic operation]*
[43] *[cryptographic operation]*
[44] *[cryptographic key sizes]*
[45] *[standard]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.2.3 *FCS_COP.1/MP_ENC_AES* Cryptographic operation

FCS_COP.1.1/MP_ENC_AES	The TSF shall perform Secure Messaging – encryption and decryption[46] in accordance with a specified cryptographic algorithm AES in CBC mode[47] and cryptographic key sizes 128, 192 abd 256 bits[48] that meet the following: [R51][49]

9.2.2.4 *FCS_COP.1/MP_MAC_3DES* Cryptographic operation

FCS_COP.1.1/MP_MAC_3DES	The TSF shall perform Secure Messaging MAC[50] in accordance with a specified cryptographic algorithm 3DES MAC[51] and cryptographic key sizes 112 bits[52] that meet the following: [R15][53]

9.2.2.5 *FCS_COP.1/MP_MAC_AES* Cryptographic operation

FCS_COP.1.1/MP_MAC_AES	The TSF shall perform Secure Messaging MAC[54] in accordance with a specified cryptographic algorithm AES[55] and cryptographic key sizes 128, 192 abd 256 bits[56] that meet the following: [R51][57]

9.2.2.6 *FCS_COP.1/MP_AUTH_3DES* Cryptographic operation

FCS_COP.1.1/MP_AUTH_3DES	The TSF shall perform Card Manufacturer Authentication[58] in accordance with a specified cryptographic algorithm 3DES[59] and cryptographic key sizes 112 bits[60] that meet the following: [R48][61]

[46] *[cryptographic operation]*
[47] *[cryptographic operation]*
[48] *[cryptographic key sizes]*
[49] *[standard]*
[50] *[cryptographic operation]*
[51] *[cryptographic operation]*
[52] *[cryptographic key sizes]*
[53] *[standard]*
[54] *[cryptographic operation]*
[55] *[cryptographic operation]*
[56] *[cryptographic key sizes]*
[57] *[standard]*
[58] *[cryptographic operation]*
[59] *[cryptographic operation]*
[60] *[cryptographic key sizes]*
[61] *[standard]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.2.7 FCS_COP.1/MP_AUTH_AES **Cryptographic operation**

FCS_COP.1.1/MP_AUTH_AES	The TSF shall perform Card Manufacturer Authentication[62] in accordance with a specified cryptographic algorithm AES[63] and cryptographic key sizes 128, 192 and 256 bits[64] that meet the following: [R51][65]

9.2.2.8 FCS_COP.1/MP_SHA **Cryptographic operation**

FCS_COP.1.1/MP_SHA	The TSF shall perform Hashing[66] in accordance with a specified cryptographic algorithm SHA256[67] and cryptographic key sizes none[68] that meet the following: [R43][69]

9.2.2.9 FDP_ACC.2/MP **Complete access control**

FDP_ACC.2.1/MP	The TSF shall enforce the Pre-personalization Access Control on all subjects and all objects and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2/MP	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: This SFR enforces access control over all the operation performed in phase 5, including additional code loading but not only.

[62] *[cryptographic operation]*
[63] *[cryptographic operation]*
[64] *[cryptographic key sizes]*
[65] *[standard]*
[66] *[cryptographic operation]*
[67] *[cryptographic operation]*
[68] *[cryptographic key sizes]*
[69] *[standard]*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.2.10 *FDP_ACF.1/MP* Security attribute based access control

FDP_ACF.1.1/MP	The TSF shall enforce the Pre-personalization Access Control to objects based on the following Pre-personalizer Authentication (AS_AUTH_MSK_STATUS).
FDP_ACF.1.2/MP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: AS_AUTH_MSK_STATUS=TRUE (EXTERNAL AUTHENTICATE).
FDP_ACF.1.3/MP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/MP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

Application Note: This SFR enforces access control over all the operation in phase 5, including additional code loading but not only.

9.2.2.11 *FDP_ITC.1/MP* Import of user data without security attributes

FDP_ITC.1.1/MP	The TSF shall enforce the Pre-personalization access control when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2/MP	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3/MP	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none.

Application Note: This SFR controls import of data in phase 5, including the additional code but not only. This SFR ensures also the MSK diversification, which is performed once, at first command, without any security requirements preliminary to this action.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.2.12 *FDP_UCT.1/MP* Basic data exchange confidentiality

FDP_UCT.1.1/MP	The TSF shall enforce the Pre-personalization access control to receive user data in a manner protected from unauthorized disclosure.

Application note: For the Additional code loading access control, the LSK_LOAD is used to cipher the data transmitted. This SFR controls confidentiality of data import in phase 5, including the additional code but not only.

9.2.2.13 *FDP_UIT.1/MP* Data exchange integrity

FDP_UIT.1.1/MP	The TSF shall enforce the Pre-personalization Access Control SFP to receive user data in a manner protected from modification errors
FDP_UIT.1.2/MP	**[Editorially refined]** The TSF shall be able to determine on receipt of user data, whether modification of some pieces of the application sent by the Pre-personalizer has occurred

9.2.2.14 FIA_AFL.1/MP Authentication failure handling

FIA_AFL.1.1/MP	The TSF shall detect when 3 unsuccessful authentication attempts occur related to authentication of Pre-personalizer and Personalizer
FIA_AFL.1.2/MP	When the defined number of unsuccessful authentication attempts has been met, the TSF shall slow-down authentication operation of, the Pre-Personalizer and the Personalizer.

9.2.2.15 *FIA_UAU.1/MP* Timing of authentication

FIA_UAU.1.1/MP	The TSF shall allow GET DATA, SELECT FILE on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/MP	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.2.16 *FIA_UID.1/MP*	**Timing of identification**
FIA_UID.1.1/MP	The TSF shall allow GET DATA, SELECT FILE on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/MP	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
9.2.2.17 *FIA_UAU.4/MP_3DES*	**Single-use authentication mechanisms**
FIA_UAU.4.1/MP_3DES	The TSF shall prevent reuse of authentication data related to Authentication Mechanisms based on 3DES.
9.2.2.18 *FIA_UAU.4/MP_AES*	**Single-use authentication mechanisms**
FIA_UAU.4.1/MP_AES	The TSF shall prevent reuse of authentication data related to Authentication Mechanisms based on AES.
9.2.2.19 FIA_UAU.5/MP_3DES	**Multiple authentication mechanisms**
FIA_UAU.5.1/MP_3DES	The TSF shall provide Symmetric Authentication Mechanism based on 3DES to support user authentication.
FIA_UAU.5.2/MP_3DES	The TSF shall authenticate any user's claimed identity according to the: The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with the Personalization Agent Key.
9.2.2.20 FIA_UAU.5/MP_AES	**Multiple authentication mechanisms**
FIA_UAU.5.1/MP_AES	The TSF shall provide Symmetric Authentication Mechanism based on AES to support user authentication.
FIA_UAU.5.2/MP_AES	The TSF shall authenticate any user's claimed identity according to the: The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with the Personalization Agent Key.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.2.21 *FMT_MTD.1/MP* Management of TSF data

FMT_MTD.1.1/MP	The TSF shall restrict the ability to switch the TOE lifecycle from phase 5 to phase 6 to the Pre-personalizer.

9.2.2.22 *FTP_ITC.1/MP* Inter-TSF trusted channel

FTP_ITC.1.1/MP	The TSF shall provide a communication channel between itself and another 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/MP	**[Editorially Refined]** The TSF shall permit the Pre-personalizer to initiate communication via the trusted channel.
FTP_ITC.1.3/MP	The TSF shall initiate communication via the trusted channel for: • Personalization Agent key storage • Lifecycle transition from Pre-personalization to Personalization phase

9.2.2.23 *FMT_MTD.1/MP_INI_ENA* Management of TSF data

FMT_MTD.1.1/MP_INI_ENA	The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Pre-personalizer.

9.2.2.24 *FMT_MTD.1/MP_INI_DIS* Management of TSF data

FMT_MTD.1.1/MP_INI_DIS	The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Pre-personalizer.

9.2.2.25 *FMT_MTD.1/MP_KEY_READ* Management of TSF data

FMT_MTD.1.1/MP_KEY_READ	The TSF shall restrict the ability to read the MSK and Personalization Agent keys to none.

9.2.2.26 *FMT_MTD.1/MP_KEY_WRITE* Management of TSF data

FMT_MTD.1.1/MP_KEY_WRITE	The TSF shall restrict the ability to write the MSK to IC manufacturer (created by the developer) and Personalization Agent keys to none.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

9.2.2.27 FAU_SAS.1/MP Audit storage

FAU_SAS.1.1/MP — The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.

9.2.2.28 *FMT_SMF.1/MP* Specification of Management Functions

FMT_SMF.1.1/MP — The TSF shall be capable of performing the following management functions:

- Initialization
- Pre-personalization
- Personalization

9.2.2.29 *FMT_SMR.1/MP* Security Roles

FMT_SMR.1.1/MP — The TSF shall maintain the roles Manufacturer.

FMT_SMR.1.2/MP — The TSF shall be able to associate users with roles.

9.2.2.30 FPT_EMS.1/MP TOE Emanation

FPT_EMS.1.1/MP — The TOE shall not emit power variations, timing variations during command execution in excess of non-useful information enabling access to

1. Pre-personalizer Key
2. Personalization Agent Key
3. MSK

FPT_EMS.1.2/MP — The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to

1. Pre-personalizer Key
2. Personalization Agent Key
3. MSK

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

10 TOE SUMMARY SPECIFICATION

10.1 TOE Summary Specification

Pre-personalization

This security functionality ensures that the TOE, when delivered to the Pre-personalization Agent, provides an authentication mechanism for data exchange. This authentication is based on Triple DES or AES symmetric authentication mechanism. The pre-personalization function allows to

- Pre-initialize the product with CPLC data, additional code identification,
- Load and activate additional code if needed,
- Load data in clear text or with secure messaging,
- Load encrypted keys directly or through secure messaging,
- Create the eSign application,
- Load personalization authentication keys.

This functionality is conformant with [R61]. The prepersonalizer can use Secure Messaging described in the functionality Secure Messaging to protect integrity and/or confidentiality of the communication.

Personalization

This security functionality ensures that the TOE, when delivered to the Personalization Agent, provides authentication for data exchange. This authentication is based on a Triple DES or AES authentication mechanism.

This personalization function allows to

- Load data in clear text or with secure messaging,
- Load encrypted keys directly or through secure messaging,
- Create the eSign application (if not performed during pre-personalization).

The personalizer can use Secure Messaging described in the functionality Secure Messaging to protect integrity and/or confidentiality of the communication.

Secure Messaging

This security functionality ensures the confidentiality, authenticity and integrity of the communication between the TOE and the interface device. In the operational phase, after a successful Authentication Procedure (see 3.2.6.4), a secure channel is established.

This security functionality also provides a Secure Messaging (SCP02 and SCP03) for the pre-personalization and personalization phases. The protocols can be configured to protect the exchanges integrity and/or confidentiality.

If an error occurs in the secure messaging layer, the session keys are destroyed.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Access Control in reading

This function controls access to read functions and enforces the security policy for data retrieval. Prior to any data retrieval, it authenticates the actor attempting to access the data, and checks that the access conditions as well as the life cycle state are fulfilled. It ensures that at any time, the following keys are never readable:

- Personalization Agent keys
- MSK and LSK
- Chip Authentication keys,
- The signature keys

It controls access to the CPLC data as well:

- It ensures the CPLC data can be read during the personalization phase
- It ensures it cannot be readable without authentication at the end of the personalization step

If the SCD is deleted, no data related to it can be accessed anymore.

In operational use phase, the three functionalities of the eSign application can only be accessed with the corresponding authorization. These functionalities are RAD management, Signature Key management and Signature creation. The access control to these three functions is assured by executing the Authentication Procedure (see 3.2.6.4) proving the possession of the necessary rights.

Access Control in writing

This function controls access to write functions (in EEPROM) and enforces the security policy for data writing. Prior to any data update, it authenticates the actor, and checks that the access conditions as well as the life cycle state are fulfilled. It also ensures that the CPLC data (data uniquely identifying the chip) can not be written anymore once the TOE is personalized and that it is not possible to load or modify an additional code. It ensures that the DTBS cannot be altered.

If the RAD is blocked, the function insures that no writing of any data is possible anymore in operational use phase.

In operational phase, the three functionalities of the eSign application can only be accessed with the corresponding authorization. These functionalities are RAD management, Signature Key management and Signature creation. The access control to these three functions is assured by executing the Authentication Procedure (see 3.2.6.4) proving the possession of the necessary rights.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Signature Creation

This functionality provides the following functions:

- Sign Data (PERFORM SECURITY OPERATION Command) with RSA or Elliptic Curve keys such that the SCD cannot be reverse-engineered from a known signature and the integrity of the DTBS is assured.

For a signature to be created, the Signature Creation functionality assures that

- the user has successfully authenticated with the rights required for R.Sigy,
- the SCD is operational,
- the integrity of the card data and the DTBS has been confirmed.

This security functionality manages the signature computation respecting the rights corresponding with [R5].

Signature Key Management

This functionality provides the following functions:

- Generate Key (GENERATE ASYMMETRIC KEY PAIR Command) only by an authorized user.
- Terminate Key (TERMINATE Command)

It ensures the correspondence and uniqueness of SVD and SCD.

It controls access to the Signature keys SVD/SCD, depending on the roles (User, Admin).

RAD Management

The modification and creation rights of the RAD depending on the roles (Sigy, Admin) are enforced by this function.

This functionality provides the following functions:

- Set PIN (CHANGE REFERENCE DATA Command)
- Verify PIN (VERIFY PIN Command)
- Change PIN (CHANGE REFERENCE DATA Command)
- Unblock PIN (RESET RETRY COUNTER Command)
- Terminate PIN (TERMINATE Command)
- Activate PIN (ACTIVATE PIN Command)
- Deactivate PIN (DEACTIVATE PIN Command)

It is used to verify the will of the Signatory to sign data.

Physical protection

This security functionality protects the TOE against physical attacks so that the integrity and confidentiality of TOE data is ensured, including the SCD, the DTBS, the RAD, the CPLC and the TOE ID. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Secure state management

This security functionality ensures that the TOE gets back to a secure state when

- an integrity error is detected during self-testing (including detection of corrupted data or physical tampering),
- a tearing occurs (during a copy of data in EEPROM).

This security functionality ensures that if such a case occurs, the TOE is either switched to the state "kill card" or becomes mute. This includes assuring the atomic activation of additional code.

Self-tests

The TOE performs self-tests to verify the integrity of the TSF data:

- Before the TSF data usage
- The additional code integrity is checked at each POWER ON of the card
- The integrity of keys and sensitive data is ensured (including the DTBS and the TOE ID)

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

11 RATIONALES

11.1 Security objectives and Security Problem Definition

11.2 Security objectives rationale

11.2.1 Security objectives backtracking

The columns and lines with green background are the elements added to the PP SSCD-5.

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.Secure_Load_ACode	OT.Secure_AC_Activation	OT.TOE_Identification	OT.Pre_Perso	OT.Perso	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_TC_VAD_Exp	OE.DTBS_Intend	OE.SCA_TC_DTBS_Exp	OE.Signatory
T.SCD_Divulg					X																				
T.SCD_Derive		X				X																			
T.Hack_Phys					X				X	X	X														
T.SVD_Forgery				X																X					
T.SigF_Misuse	X						X	X				X	X									X	X	X	X
T.DTBS_Forgery								X					X										X	X	
T.Sig_Forgery			X			X													X						
T.Unauthorized_Load														X											
T.Bad_Activation															X										
T.TOE_Identification_Forgery																X									
T.Pre_Perso																	X								

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.Secure_Load_ACode	OT.Secure_AC_Activation	OT.TOE_Identification	OT.Pre_Perso	OT.Perso	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_TC_VAD_Exp	OE.DTBS_Intend	OE.SCA_TC_DTBS_Exp	OE.Signatory
T.Perso																		X							
P.CSP_QCert	X			X															X						
P.QSign						X	X												X				X		
P.Sigy_SSCD	X	X	X		X	X	X	X	X		X										X				
P.Sig_Non-Repud	X		X	X	X	X	X	X	X	X	X	X	X						X	X	X	X	X	X	X
A.CGA																			X	X					
A.SCA																							X		

Table 11-1 - Mapping of security problem definition to security objectives

11.2.2 Security objectives sufficiency

The rationales are available in the complete ST.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

11.3 Security requirements and security objectives

11.3.1 Rationale tables of Security Objectives and SFRs

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.Secure_Load_ACode	OT.Secure_AC_Activation	OT.TOE_Identification	OT.Pre_Perso	OT.Perso
FCS_CKM.1/RSA	X		X	X	X													
FCS_CKM.1/ECDSA	X		X	X	X													
FCS_CKM.4	X				X									X				
FCS_COP.1	X					X												
FDP_ACC.1/SCD/SVD_Generation	X	X																
FDP_ACC.1/SVD_Transfer	X																	
FDP_ACC.1/Signature_Creation	X						X											
FDP_ACF.1/SCD/SVD_Generation	X	X																
FDP_ACF.1/SVD_Transfer	X																	
FDP_ACF.1/Signature_Creation	X						X											
FDP_RIP.1					X		X											
FDP_SDI.2/Persistent				X	X	X											X	X
FDP_SDI.2/DTBS							X	X										
FDP_UIT.1/DTBS													X					
FIA_AFL.1							X											
FIA_UAU.1		X					X											
FIA_UID.1		X					X										X	X
FMT_MOF.1	X						X											
FMT_MSA.1/Admin	X	X																
FMT_MSA.1/Signatory	X						X											
FMT_MSA.2	X	X					X											
FMT_MSA.3	X	X					X											
FMT_MSA.4	X	X					X											
FMT_MTD.1/Admin	X						X											
FMT_MTD.1/Signatory	X						X											

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.Secure_Load_ACode	OT.Secure_AC_Activation	OT.TOE_Identification	OT.Pre_Perso	OT.Perso
FMT_SMR.1	X						X										X	X
FMT_SMF.1	X						X										X	X
FPT_EMS.1					X				X								X	X
FPT_FLS.1					X													
FPT_PHP.1										X							X	X
FPT_PHP.3					X						X						X	X
FPT_TST.1	X				X	X										X		
FTP_ITC.1/VAD												X						
FTP_ITC.1/DTBS													X					
FAU_STG.2/MP_Add_code														X	X	X		
FCS_CKM.1/MP_Add_code														X				
FCS_COP.1/MP_ENC_Add_code														X				
FCS_COP.1/MP_MAC_Add_code														X				
FDP_UIT.1/MP_Add_code														X			X	X
FMT_MTD.1/MP_Add_code															X			
FMT_MTD.1/MP_KEY_READ_Add_code														X			X	X
FMT_SMR.1/MP_Add_code														X				
FPT_EMS.1/MP_Add_code									X					X			X	
FTP_ITC.1/MP_Add_code														X			X	
FCS_CKM.1/MP														X				
FCS_COP.1/MP_ENC_3DES														X			X	X
FCS_COP.1/MP_ENC_AES														X			X	X
FCS_COP.1/MP_MAC_3DES														X			X	X

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.Secure_Load_ACode	OT.Secure_AC_Activation	OT.TOE_Identification	OT.Pre_Perso	OT.Perso
FCS_COP.1/MP_MAC_AES														X			X	X
FCS_COP.1/MP_AUTH_3DES														X			X	X
FCS_COP.1/MP_AUTH_AES														X			X	X
FCS_COP.1/MP_SHA														X			X	X
FDP_ACC.2/MP														X			X	
FDP_ACF.1/MP														X			X	
FDP_ITC.1/MP														X			X	
FDP_UCT.1/MP														X			X	
FDP_UIT.1/MP																	X	
FIA_AFL.1/MP														X			X	
FIA_UAU.1/MP														X				
FIA_UID.1/MP														X				
FIA_UAU.4/MP_3DES														X			X	X
FIA_UAU.4/MP_AES														X			X	X
FIA_UAU.5/MP_3DES	X																	X
FIA_UAU.5/MP_AES	X																	X
FMT_MTD.1/MP														X			X	
FTP_ITC.1/MP																	X	X
FMT_MTD.1/MP_INI_ENA	X																X	
FMT_MTD.1/MP_INI_DIS	X																X	
FMT_MTD.1/MP_KEY_READ	X																	X
FMT_MTD.1/MP_KEY_WRITE	X																	X
FAU_SAS.1/MP																X		
FMT_SMF.1/MP	X																X	X
FMT_SMR.1/MP	X																X	X
FPT_EMS.1/MP	X								X								X	X

Table 11-2 - SFR vs Objectives

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

11.3.2 Rationale of Security Objectives and SFRs

The rationales are available in the complete ST.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

12 REFERENCES

Specifications

[R1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[R2] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization

[R3] BSI TR-03110 V2.10 Part 1 eMRTDs with BAC/PACE

[R4] BSI TR-03110 V2.10 Part 2 Extented Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)

[R22] BSI TR-03110 V2.10 Part 3 Common Specifications

[R23] BSI TR-03117 V1.0 eCard with contactless interface as a secure signature creation device

Oberthur Specifications

[R15] SRS Auth and Key Management – 079711 00 AC – Oberthur Technologies

Protection Profiles

[R7] Protection Profile written in CC version 3.1 revision 3: Protection profiles for secure signature creation device – Part 2: Device with key generation. Version 2.0.1, 2012-01-23.

[R9] Information Technology - Personal Identification — ISO Compliant Driving Licence — Part 3: Access control, authentication and integrity validation, ISO/IEC 18013-3:2009

[R26] Smartcard IC Platform Protection Profile v 1.0 - BSI-PP-0035 15/06/2007

[R27] Machine readable travel documents with “ICAO Application”, Basic Access control – BSI- PP-0055 v1.10 25th march 2009

[R28] Machine readable travel documents with “ICAO Application”, Extended Access control – BSI-PP-0056 v1.10 25th march 2009

[R29] Machine readable travel documents with “ICAO Application”, Extended Access Control with PACE (EAC PP) – BSI-PP-0056 V2 – 2012

[R33] Technical Report, Supplemental Access Control for Machine Readable Travel Documents – version v1.01

Chips References

[R35] Certification report - BSI-DSZ-CC-0978- 2016 - NXP Secure Smart Card Controller P60x144/080 VA/VE (Y/B) with IC dedicated software FW5.0

Standards

[R36] ISO/IEC 7816-4:2013 – Organization, security and commands for interchange

[R37] ISO/IEC 7816-8:2004 – Commands for security operations

[R41] ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function

[R43] Federal Information Processing Standards Publication 180-2 Secure Hash Standard (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[R48] FIPS 46-3 Data Encryption Standard (DES)

[R51] FIPS 197 – Advance Encryption Standard (AES)

CC

[R58] Common Criteria for Information Technology security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, version 3.1 Revision 4 Final, September 2012

[R59] Common Criteria for Information Technology security Evaluation Part 2: Security Functional Components, CCMB-2012-09-002, version 3.1 Revision 4 Final, September 2012

[R60] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Components, CCMB-2012-09-003, version 3.1 Revision 4 Final, September 2012

[R61] ANSSI-CC note 6 – v0.91

13 ACRONYMS

CA	Chip Authentication
CC	Common Criteria
CPLC	Card Personalization Life Cycle
DGA	Certificate Generation Application
DES	Digital Encryption Standard
DTBS/R	Data to be signed or its unique representation
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
HID	Human Interface Device
IC	Integrated Circuit
LSK	Load Secret Key (Key for Loading of Additional Code)
MRTD	Machine Readable Travel Document
MSK	Manufacturer Secret Key
PP	Protection Profile
RAD	Reference Authentication Data. Could be a PIN or a Biometric password
SCA	Signature Creation Application
SCD	Signature Creation Data
SDO	Signed Data Object
SHA	Secure Hashing Algorithm
SFP	Security Function Policy
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature verification data
TA	Terminal Authentication
TOE	Target Of Evaluation
TSF	TOE Security Functionality
VAD	Verification Authentication Data. Could be a PIN or a Biometric password

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

14 LIST OF TABLES AND FIGURES

Figures

Tables

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534