Oberthur Technologies

ID ONE CIE ON

ID ONE COSMO V7.0-A STANDARD AND BASIC CONFIGURATIONS

PUBLIC SECURITY TARGET

ISSUE: 1

Verification and approval

Function	Name	Visa
Security certification project manager / Author	CAPEL Clément	Approbation de FQR 110 5041 ED1 par CAPEL Clément le 19-4-2010.oft

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Issue Date	Author	Status	Purpose
1 - 16/04/10	C.CAPEL	Final	Creation of the document

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Table of contents

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

List of figures

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

List of tables

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

1 Security Target introduction

1.1 Security Target identification

General identification:

Title:	**ID One CIE Card Security Target**
Editor:	Oberthur Technologies
CC version:	3.1 revision 3
EAL:	EAL4 + ALC_DVS.2 + AVA_VAN.5
PPs:	SSCD Type 2 [SSCD2] and Type 3 [SSCD3]

Applet technical identification:

Name:	**ID One CIE Java Aplet**
version:	1.01.1

Platform technical identification:

Name:	**ID One Cosmo V7.0-a,** Standard and Basic configuration
Certificate:	DCSSI-2009/46
Chips:	AT90SC28872RCU rev G & E, AT90SC28848RCU rev G & E

Important

In the following, platform, ID One Cosmo v7.0 or Cosmo v7.0 will refer to this specific platform.

1.2 Overview of the TOE

The current document aims at defining the functions and assurance security requirements which apply to ID One ClassIC smart card. This device is composed of an open JavaCard platform embedded on an Integrated Circuit (IC) and a loaded application providing signature services to the end user; this document is therefore a composite Security Target (ST). In the following, the smart card will be called “Target Of Evaluation” or TOE.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d’auteur.

The TOE is a signature-creation device according to Directive 1999/93/EC [1999/93/EC] of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures.
The context of this ST is the Secure Signature Creation Device following the Protection Profiles ([SSCD1], [SSCD2] and [SSCD3]) developed by CEN/ISSS. These PPs are a translation of the annex concerning the Secure Signature Creation Device of the European directive [1999/93/EC].

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

2 TOE DESCRIPTION

This part of the ST describes the TOE as an aid to the understanding of its security requirements and addresses the product type, the intended usage and the general features of the TOE.

2.1 PRODUCT TYPE

The Target of Evaluation (TOE) is the Secure Signature Creation Device (SSCD) defined by:

- an underlying Integrated Circuit (IC);
- an ID One Cosmo V7.0 JavaCard platform including Global Platform support,
- The SSCD Applet.

The Figure below gives a description of the TOE and its boundaries.

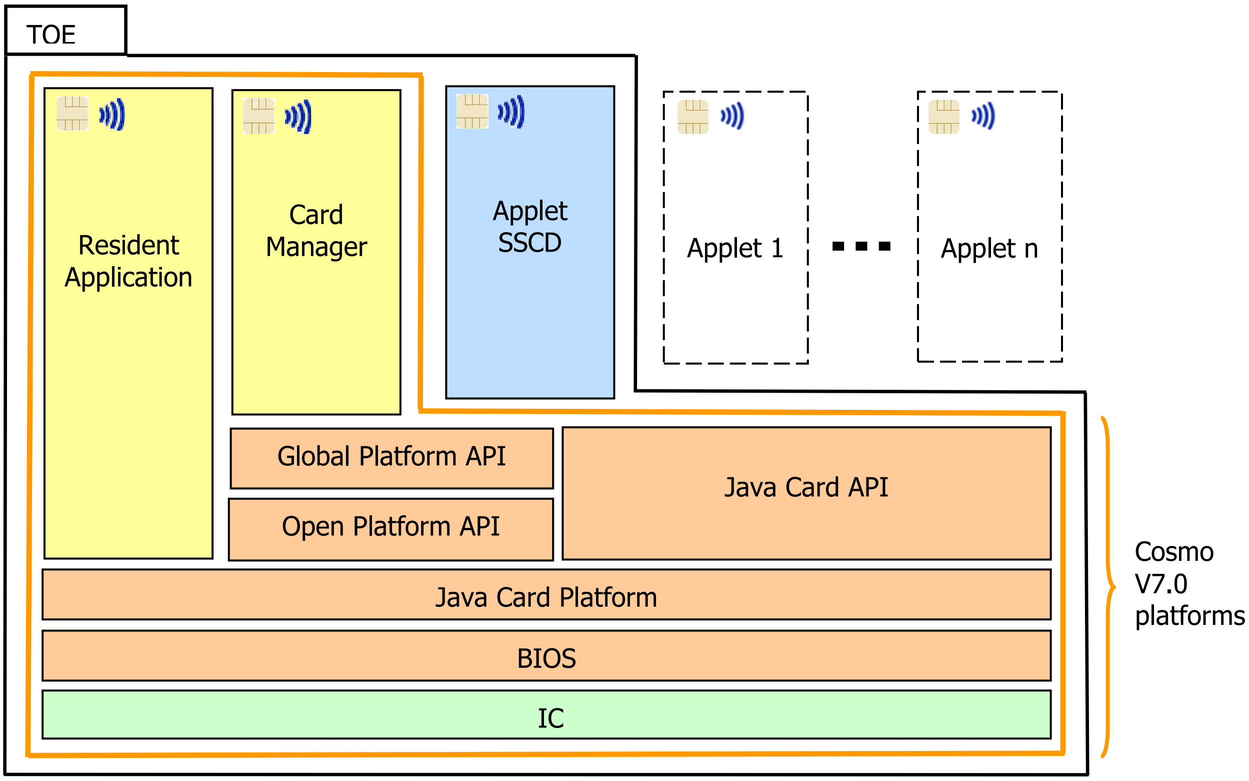

Figure 1 Smartcard architecture overview

2.2 TOE DESCRIPTION

2.2.1 Platform functions

The Operating is System based on Java Card technology [JCRE][JCVM][JCAPI] and Global Platform technology [GP]. His main responsibilities are:

- providing interface between the Integrated Circuit and the applet,

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

- providing to the applet, basic services to access to memories and all needed cryptographic operations,
- ensuring global management of the card (loading, installation and deletion of applets) and monitor the security of the card (data integrity and physical attacks counter-measures).

For details see [COSMO-ST] §3.1 and §3.2.

2.2.2 SSCD functions

The TOE implements a SSCD of type 2 and type 3, and all functions concerning the SSCD to create electronic signatures in a secure way:

- Generation of SCD and SVD – The TOE ensures the secrecy of the SCD,
- Import of the SCD,
- Export of SVD,
- Signature Creation,
- Pin Authentication of the Signatory: the TOE holds the RAD that is used to verify the VAD provided by the user,
- Implementation of a trusted path to a human interface device.

The TOE destroys the SCD if it is no longer used for signature generation. In usage phase, the TOE allows the creation of a new SCD/SVD pair. The previous SCD must be destroyed before the creation of a new SCD/SVD pair.

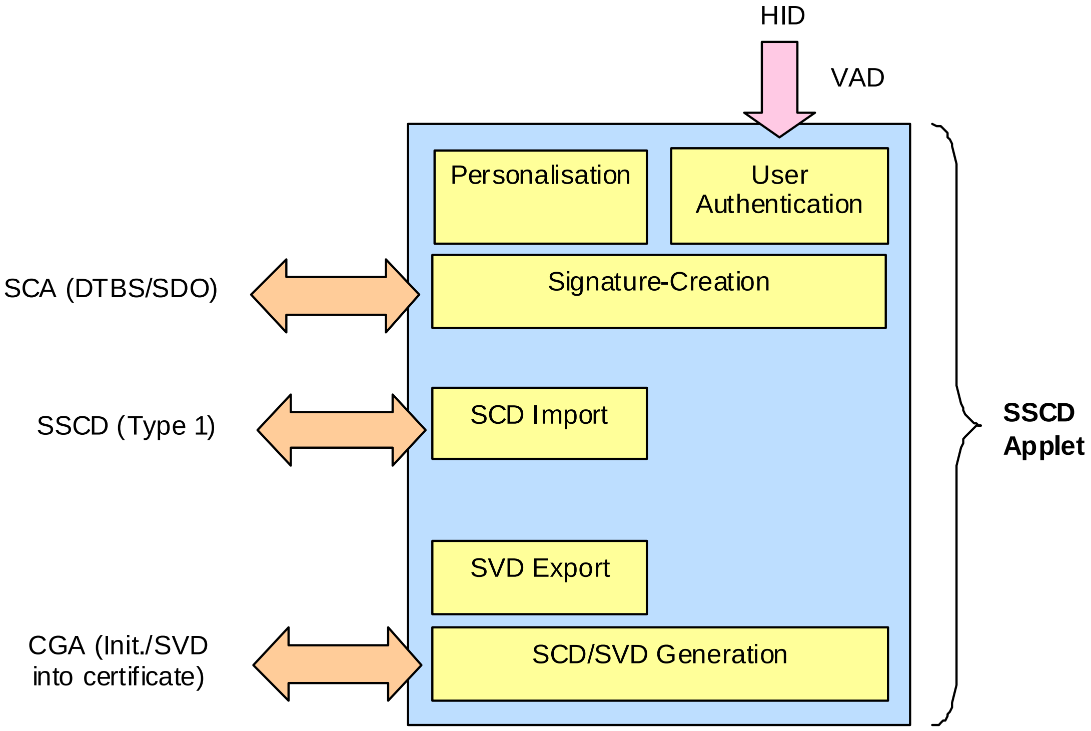

Figure 2 SSCD security features overview

To that purpose the following services are provided by the application:

- A highly secure and configurable framework to store sensitive and user data, based on ISO7816-4 and ISO7816-9,
- secure messaging, based on ISO 7816-4,

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

- dynamic management of access control rules ;
- dynamic management of confidentiality/integrity (Secure Messaging conditions) settings,
- onboard RSA key pair generation (up to 2048 bits), compliant with ISO 7816-8,
- Triple DES based authentication, encryption and decryption, compliant with ISO 7816-4 and ISO 7816-8,
- RSA digital signature, compliant with ISO7816-8,
- PIN management.

For more information about SSCD see [SSCD2] and [SSCD3].

Note: card services are available using contact or contactless interfaces.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

2.3 TOE product life cycle

2.3.1 Card life cycle

The Smart card product life cycle is split up into 7 phases[1] where evaluation scope goes from phase 1 to phase 5.

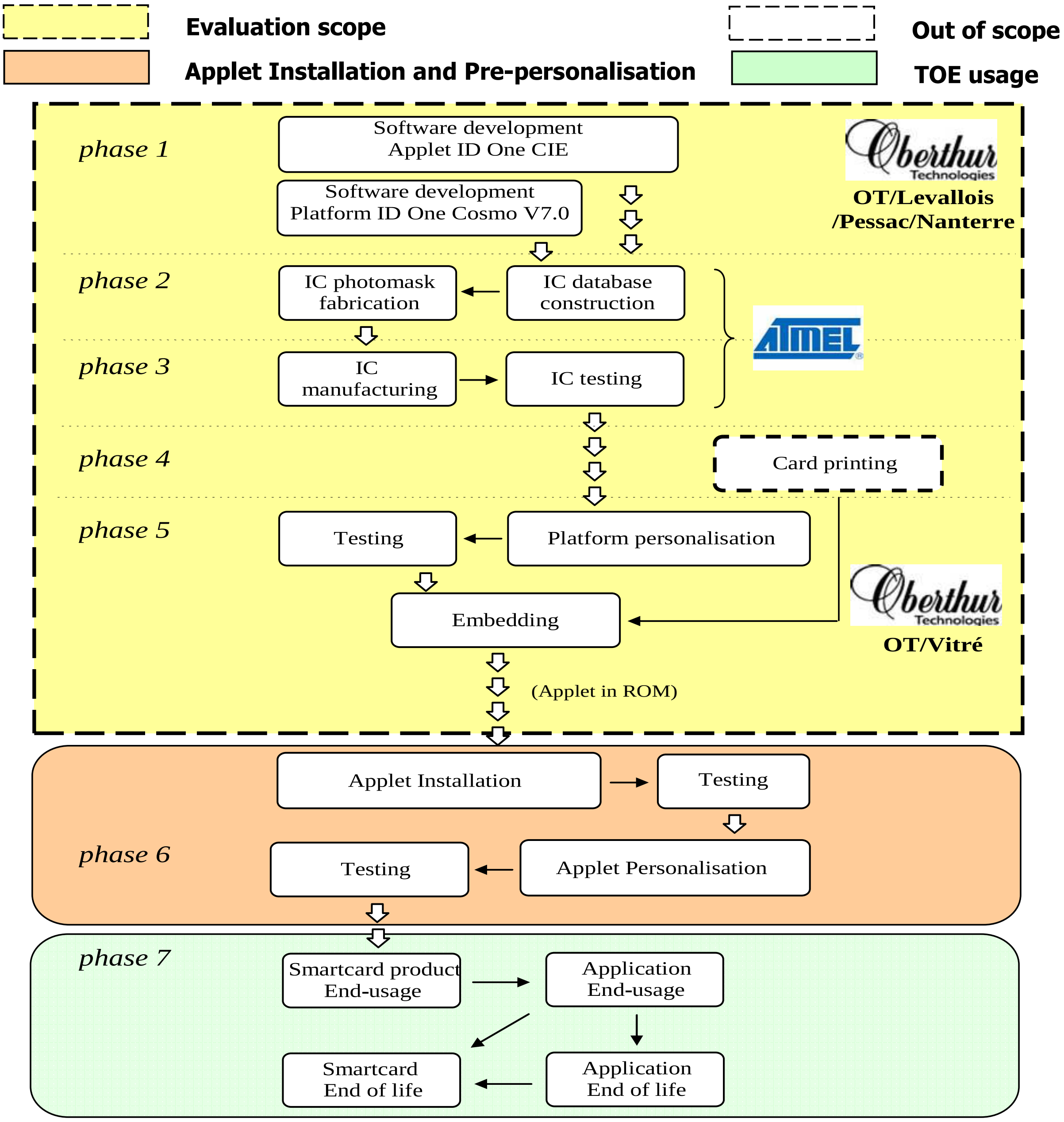

figure 3 Smartcard product life-cycle for the TOE

[1] For details regarding phases see [COSMO-ST] §3.5.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

2.3.2 Application life cycle

The application is a Java Card applet loaded in phase 5 on the platform or masked in phase 2 and instantiated in phase 6. The lifecycle follows the standard defined in [COSMO-ST] §3.5 which is depicted by the following figure:

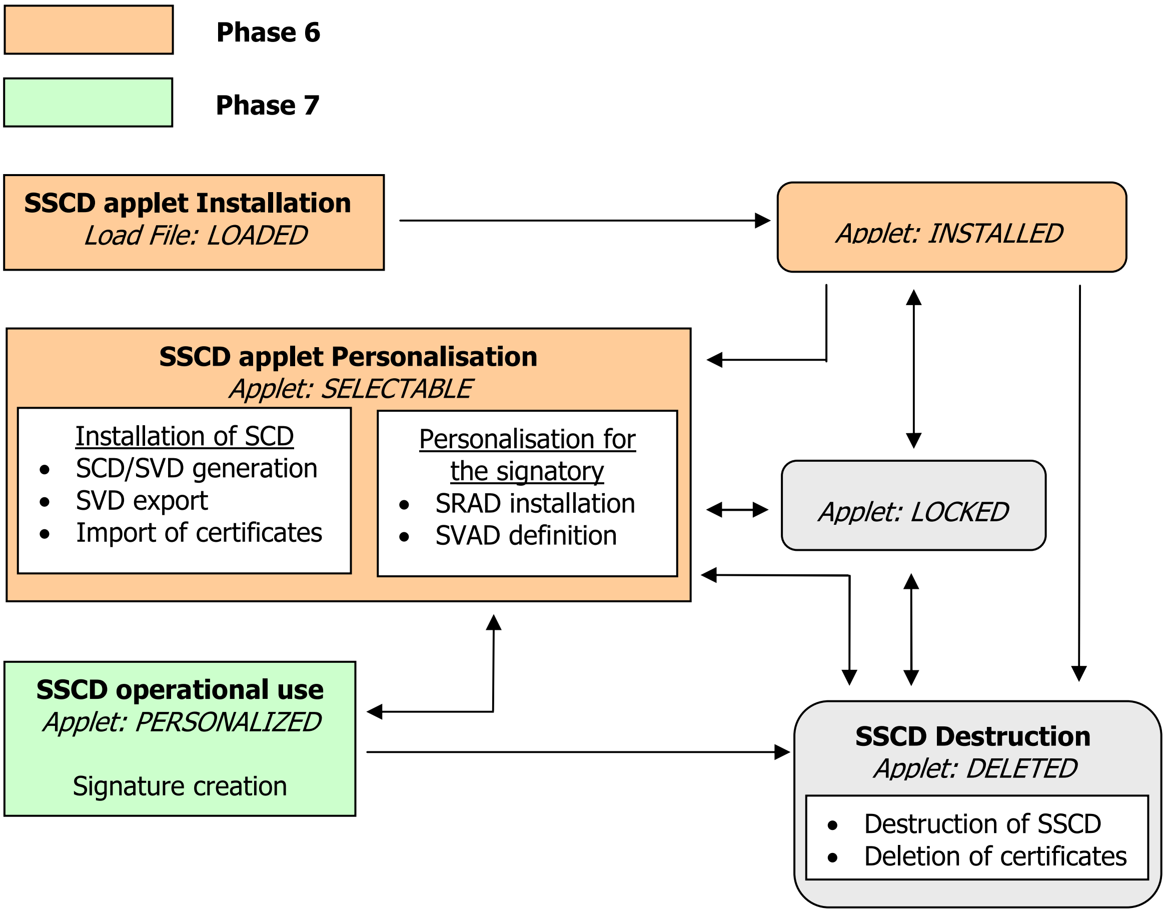

Figure 4 SSCD applet lifecycle

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

3 Conformance claims

3.1 Common Criteria conformance

This Security Target (ST) is CC Part 2 extended[2] [CC-2] and CC Part 3 conformant [CC-3] and written according to the Common Criteria version 3.1 Part 1 [CC-1].

3.2 Package conformance

This ST is conformant to the EAL4 package as defined in [CC-3].

Application Note:
The EAL4 have been augmented with the following requirement to fulfil[3] the requirements of [SSCD2] and [SSCD3]:

Requirement	Name	Type
ALC_DVS.2	Advanced methodical vulnerability analysis	Higher hierarchical component
AVA_VAN.5	Advanced methodical vulnerability analysis	Higher hierarchical component

3.3 Protection Profile conformance

The Security Target is conformant[4] to the following PPs:

- Machine Secure Signature-Creation device Protection Profile Type 2 v1.04 [SSCD2]
- Secure Signature-Creation device Protection Profile Type 3 v1.05 [SSCD3]

Remark:

Since this [SSCD2] and [SSCD3] are not yet available in CC 3.1, requirements have been translated from CC2.x to CC3.1 revision 3.

[2] See section 6.
[3] According to the current draft of the PP SSCD in CC3.1, the assurance level is translated to EAL4 augmented with AVA_VAN.5.
[4] Due to evolutions of the Common Criteria this conformity is considered as demonstrable.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

4 Security problem definition

4.1 Assets

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

SCD

private key used to perform an electronic signature operation. Confidentiality of the SCD must be maintained.

SVD

public key linked to the SCD and used to perform an electronic signature verification. Integrity of the SVD when it is exported must be maintained.

DTBS and DTBS-representation

Set of data, or its representation which is intended to be signed. Their integrity must be maintained.

VAD

PIN code entered by the End User to perform a signature operation. Confidentiality and authenticity of the VAD as needed by the authentication method employed.

RAD

Reference Pass Phrase code used to identify and authenticate the End User. Integrity and confidentiality of RAD must be maintained. The specification references also RAD as a PIN even it is an alphanumeric code.

Signature-creation function of the SSCD using the SCD

The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures.

Electronic signature

Unforgeabilty of electronic signatures must be assured.

External Authentication keys

Keys used in the processing of External Authentication which aims at authentifying the user communicating with the TOE as a substitute to VAD/RAD.

Secure Messaging keys

Keys used to open a secure channel between the TOE and another trusted device by using secure messaging features.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

PINs

All PINs except RAD used by the TOE to control access to sensitive data.

Application Note

In particular a PIN is dedicated to the administrator in order to perform administration operations. Actually, this PIN can be associated to every sensitive assets leading to a PIN verification prior to the operation execution.

4.2 Users / Subjects

S.User

End user of the TOE which can be identified as S.Admin or S.SignatoryEnd user of the TOE which can be identified as S.Admin or S.Signatory

S.Admin

User who is in charge to perform the TOE initialisation, TOE personalisation and other administrative functions:

- SCD import as SSCD Type1,
- SCD/SVD generation and SVD export as CGA,
- Secure Messaging and External Authentication keys import,
- PIN updating and unblocking.

S.Signatory

User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

S.Offcard (Threat agent)

Attacker.

A human or a process acting on his behalf being located outside the TOE. The main goal of the S.Offcard attacker is to access Application sensitive information. The attacker has a high level potential attack and knows no secret.

4.3 Threats

T.Hack_Phys

Physical attacks through the TOE interfaces

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

T.SCD_Divulg

Storing, copying, and releasing of the signature-creation data

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

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

T.SCD_Derive

Derive the signature-creation data

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

T.Sig_Repud

Repudiation of signatures

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

T.SVD_Forgery

Forgery of the signature-verification data

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

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.

T.DTBS_Forgery

Forgery of the DTBS-representation

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

T.Sig_Forgery

Forgery of the electronic signature

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

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

4.4 Organisational Security Policies

P.CSP_QCert

Qualified certificate

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

P.QSign

Qualified electronic signatures

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

P.Sigy_SSCD

TOE as secure signature-creation device

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

4.5 Assumptions

A.CGA

Trustworthy certification-generation application

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

A.SCA

Trustworthy signature-creation application

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

A.SCD_Generate

Trustworthy SCD/SVD generation

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

- o this party will use a SSCD for SCD/SVD-generation,
- o confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and,
- o the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory,

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

- The generation of the SCD/SVD is invoked by authorised users only,
- The SSCD Type1 ensures the authenticity of the SVD it has created an exported.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

5 Security Objectives

5.1 Security Objectives for the TOE

OT.EMSEC_Design

Provide physical emanations security

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

OT.Lifecycle_Security

Lifecycle security

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

OT.SCD_Secrecy

Secrecy of the signature-creation data

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

OT.SCD_SVD_Corresp

Correspondence between SVD and SCD

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

OT.SVD_Auth_TOE

TOE ensures authenticity of the SVD

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

OT.Tamper_ID

Tamper detection

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

OT.Tamper_Resistance

Tamper resistance

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

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

OT.Init

SCD/SVD generation

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

OT.SCD_Unique

Uniqueness of the signature-creation data

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

OT.SCD_Transfer

Secure transfer of SCD between SSCD

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

OT.DTBS_Integrity_TOE

Verification of the DTBS-representation integrity

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

OT.Sigy_SigF

Signature generation function for the legitimate signatory only

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

OT.Sig_Secure

Cryptographic security of the electronic signature

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

5.2 Security objectives for the Operational Environment

OE.SCD_SVD_Corresp

Correspondence between SVD and SCD

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

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

OE.SCD_Transfer

Secure transfer of SCD between SSCD

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

OE.SCD_Unique

Uniqueness of the signature-creation data

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

OE.CGA_QCert

Generation of qualified certificates

The CGA generates qualified certificates which include inter alia

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

OE.SVD_Auth_CGA

CGA CGA verifies the authenticity of the SVD

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

OE.HI_VAD

Protection of the VAD

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

OE.SCA_Data_Intend

Data intended to be signed

The SCA

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

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

5.3 Security Objectives Rationale

5.3.1 Threats

T.Hack_Phys See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

T.SCD_Divulg See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

T.SCD_Derive See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

T.Sig_Repud See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

T.SVD_Forgery See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

T.SigF_Misuse See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

T.DTBS_Forgery See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

T.Sig_Forgery See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

5.3.2 Organisational Security Policies

P.CSP_QCert See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

P.QSign See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

P.Sigy_SSCD See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

5.3.3 Assumptions

A.CGA See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

A.SCA See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

A.SCD_Generate See [SSCD2] and [SSCD3] §6.2 for a detailed rationale.

5.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Hack_Phys	OT.EMSEC_Design, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance	Section 2.3.1
T.SCD_Divulg	OT.SCD_Transfer, OT.SCD_Secrecy, OE.SCD_Transfer	Section 2.3.1

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Threats	Security Objectives	Rationale
T.SCD_Derive	OT.Sig_Secure, OT.SCD_Unique, OE.SCD_Unique	Section 2.3.1
T.Sig_Repud	OT.EMSEC_Design, OT.Lifecycle_Security, OT.SCD_Secrecy, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, OT.Tamper_ID, OT.Tamper_Resistance, OT.SCD_Unique, OT.SCD_Transfer, OT.DTBS_Integrity_TOE, OT.Sigy_SigF, OT.Sig_Secure, OE.SCD_SVD_Corresp, OE.SCD_Transfer, OE.CGA_QCert, OE.SVD_Auth_CGA, OE.SCA_Data_Intend	Section 2.3.1
T.SVD_Forgery	OT.SVD_Auth_TOE, OE.SVD_Auth_CGA	Section 2.3.1
T.SigF_Misuse	OT.DTBS_Integrity_TOE, OT.Sigy_SigF, OE.HI_VAD, OE.SCA_Data_Intend	Section 2.3.1
T.DTBS_Forgery	OT.DTBS_Integrity_TOE, OE.SCA_Data_Intend	Section 2.3.1
T.Sig_Forgery	OT.EMSEC_Design, OT.Lifecycle_Security, OT.SCD_Transfer, OT.SCD_Secrecy, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, OT.Tamper_ID, OT.Tamper_Resistance, OT.Sig_Secure, OE.SCD_SVD_Corresp, OE.SCD_Transfer, OE.CGA_QCert, OE.SVD_Auth_CGA, OE.SCA_Data_Intend	Section 2.3.1

Tableau 1 Threats and Security Objectives - Coverage

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Security Objectives	Threats
OT.EMSEC_Design	T.Hack_Phys, T.Sig_Repud, T.Sig_Forgery
OT.Lifecycle_Security	T.Sig_Repud, T.Sig_Forgery
OT.SCD_Secrecy	T.Hack_Phys, T.SCD_Divulg, T.Sig_Repud, T.Sig_Forgery
OT.SCD_SVD_Corresp	T.Sig_Repud, T.Sig_Forgery
OT.SVD_Auth_TOE	T.Sig_Repud, T.SVD_Forgery, T.Sig_Forgery
OT.Tamper_ID	T.Hack_Phys, T.Sig_Repud, T.Sig_Forgery
OT.Tamper_Resistance	T.Hack_Phys, T.Sig_Repud, T.Sig_Forgery
OT.Init	
OT.SCD_Unique	T.SCD_Derive, T.Sig_Repud
OT.SCD_Transfer	T.SCD_Divulg, T.Sig_Repud, T.Sig_Forgery
OT.DTBS_Integrity_TOE	T.Sig_Repud, T.SigF_Misuse, T.DTBS_Forgery
OT.Sigy_SigF	T.Sig_Repud, T.SigF_Misuse
OT.Sig_Secure	T.SCD_Derive, T.Sig_Repud, T.Sig_Forgery
OE.SCD_SVD_Corresp	T.Sig_Repud, T.Sig_Forgery
OE.SCD_Transfer	T.SCD_Divulg, T.Sig_Repud, T.Sig_Forgery
OE.SCD_Unique	T.SCD_Derive
OE.CGA_QCert	T.Sig_Repud, T.Sig_Forgery
OE.SVD_Auth_CGA	T.Sig_Repud, T.SVD_Forgery, T.Sig_Forgery
OE.HI_VAD	T.SigF_Misuse
OE.SCA_Data_Intend	T.Sig_Repud, T.SigF_Misuse, T.DTBS_Forgery, T.Sig_Forgery

Tableau 2 Security Objectives and Threats - Coverage

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Organisational Security Policies	Security Objectives	Rationale
P.CSP_QCert	OT.SCD_SVD_Corresp, OE.SCD_SVD_Corresp, OE.CGA_QCert	Section 2.3.2
P.QSign	OT.Sigy_SigF, OT.Sig_Secure, OE.CGA_QCert, OE.SCA_Data_Intend	Section 2.3.2
P.Sigy_SSCD	OT.Sigy_SigF, OT.Init, OT.SCD_Unique, OE.SCD_Unique	Section 2.3.2

Tableau 3 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.EMSEC_Design	
OT.Lifecycle_Security	
OT.SCD_Secrecy	
OT.SCD_SVD_Corresp	P.CSP_QCert
OT.SVD_Auth_TOE	
OT.Tamper_ID	
OT.Tamper_Resistance	
OT.Init	P.Sigy_SSCD
OT.SCD_Unique	P.Sigy_SSCD
OT.SCD_Transfer	
OT.DTBS_Integrity_TOE	
OT.Sigy_SigF	P.QSign, P.Sigy_SSCD
OT.Sig_Secure	P.QSign
OE.SCD_SVD_Corresp	P.CSP_QCert
OE.SCD_Transfer	
OE.SCD_Unique	P.Sigy_SSCD
OE.CGA_QCert	P.CSP_QCert, P.QSign
OE.SVD_Auth_CGA	
OE.HI_VAD	
OE.SCA_Data_Intend	P.QSign

Tableau 4 Security Objectives and OSPs - Coverage

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Assumptions	Security objectives for the Operational Environment	Rationale
A.CGA	OE.CGA_QCert, OE.SVD_Auth_CGA	Section 2.3.3
A.SCA	OE.SCA_Data_Intend	Section 2.3.3
A.SCD_Generate	OE.SCD_SVD_Corresp, OE.SCD_Transfer, OE.SCD_Unique	Section 2.3.3

Tableau 5 Assumptions and Security Objectives for the Operational Environment - Coverage

Security objectives for the Operational Environment	Assumptions
OE.SCD_SVD_Corresp	A.SCD_Generate
OE.SCD_Transfer	A.SCD_Generate
OE.SCD_Unique	A.SCD_Generate
OE.CGA_QCert	A.CGA
OE.SVD_Auth_CGA	A.CGA
OE.HI_VAD	
OE.SCA_Data_Intend	A.SCA

Tableau 6 Security Objectives for the Operational Environment and Assumptions - Coverage

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

6 Extended requirements

6.1 Extended component FPT_EMSEC.1

6.1.1 Description

See [SSCD2] and [SCCD3] section 6.6.1 for more information.

6.1.2 Definition

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.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_EMSEC.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].

Dependencies: No dependencies.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

7 Security Functional Requirements

7.1 Security Functional Requirements

For a detail description of security attributes see [SSCD2] §5.1.2.2.

7.1.1 SSCD Protection Profile

FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA SFM and CRT** and specified cryptographic key sizes **1024, 1280, 1536, 1792 or 2048 bits** that meet the following: **ANSI X9.31**.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 [Editorially Refined] The TSF shall destroy cryptographic keys *in case of regeneration of a new SCD or in case of re-importation of the SCD* in accordance with a specified cryptographic key destruction method **overwriting of the buffer containing the key** that meets the following: **no specific standard**.

Application note:

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated or re-imported by the TOE. The re-import and re-generation are the unique way to ask for the destruction of SCD.

FCS_COP.1/Corresp Cryptographic operation

FCS_COP.1.1/Corresp The TSF shall perform **SCD/SVD correspondence verification** in accordance with a specified cryptographic algorithm **RSA key computation** and cryptographic key sizes **1024, 1280, 1536, 1792 or 2048 bits** that meet the following: **PKCS#1**.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FCS_COP.1/Signing Cryptographic operation

FCS_COP.1.1/Signing The TSF shall perform **Digital signature-generation** in accordance with a specified cryptographic algorithm **RSA using Private Key** and cryptographic key sizes **1024, 1280, 1536, 1792 or 2048 bits** that meet the following: **PKCS#1 V1.5 Block Type 1**.

Application note:

The biggest RSA private key which can be imported by this applet is 2048 bits (using the command PUT DATA).

FDP_ACC.1/Initialisation SFP Subset access control

FDP_ACC.1.1/Initialisation SFP The TSF shall enforce the **Initialisation SFP** on **Generation of SCD/SVD pair by User**.

FDP_ACC.1/SVD Transfer SFP Subset access control

FDP_ACC.1.1/SVD Transfer SFP The TSF shall enforce the **SVD transfer SFP** on **export of SVD by User**.

Application note:

FDP_ACC.1/SVD Transfer SFP is only relevant if the TOE imports the SVD from a SSCD Type1. In this case, the SVD will be exported to the CGA for certification.

FDP_ACC.1/Personalisation SFP Subset access control

FDP_ACC.1.1/Personalisation SFP The TSF shall enforce the **Personalisation SFP** on **Creation of PIN RAD by Administrator**.

FDP_ACC.1/SCD Import SFP Subset access control

FDP_ACC.1.1/SCD Import SFP The TSF shall enforce the **SCD Import SFP** on **Import of SCD by User**.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FDP_ACC.1/Signature-creation SFP Subset access control

FDP_ACC.1.1/Signature-creation SFP The TSF shall enforce the **Signature-creation SFP** on

- **Sending of DTBS representation by SCA,**
- **Signing of DTBS representation by Signatory**.

FDP_ACF.1/Initialisation SFP Security attribute based access control

FDP_ACF.1.1/Initialisation SFP The TSF shall enforce the **Initialisation SFP** to objects based on the following: **General attribute and Initialisation attribute**.

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

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

FDP_ACF.1.3/Initialisation SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/Initialisation SFP The TSF shall explicitly deny access of subjects to objects based on the **The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair**.

FDP_ACF.1/SVD Transfer SFP Security attribute based access control

FDP_ACF.1.1/SVD Transfer SFP The TSF shall enforce the **SVD transfer SFP** to objects based on the following: **General attributes**.

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

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

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FDP_ACF.1.3/SVD Transfer SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SVD Transfer SFP The TSF shall explicitly deny access of subjects to objects based on the **none**.

Application note:

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

FDP_ACF.1/Personalisation SFP Security attribute based access control

FDP_ACF.1.1/Personalisation SFP The TSF shall enforce the **Personalisation SFP** to objects based on the following: **General attribute**.

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

- o **User with the security attribute "role" set to "Administrator" is allowed to create the RAD**.

FDP_ACF.1.3/Personalisation SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/Personalisation SFP The TSF shall explicitly deny access of subjects to objects based on the **none**.

Application note:

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

FDP_ACF.1/SCD Import SFP Security attribute based access control

FDP_ACF.1.1/SCD Import SFP The TSF shall enforce the **SCD Import SFP** to objects based on the following: **General attribute and Initialisation attribute group**.

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

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

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FDP_ACF.1.3/SCD Import SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SCD Import SFP The TSF shall explicitly deny access of subjects to objects based on the

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

FDP_ACF.1/Signature-creation SFP Security attribute based access control

FDP_ACF.1.1/Signature-creation SFP The TSF shall enforce the **Signature-creation SFP** to objects based on the following: **General attributes and Signature-creation attributes**.

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

- **User with the security attribute “role” set to “Signatory” is allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”**.

FDP_ACF.1.3/Signature-creation SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

FDP_ACF.1.4/Signature-creation SFP The TSF shall explicitly deny access of subjects to objects based on the

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

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FDP_ETC.1/SVD Transfer Export of user data without security attributes

FDP_ETC.1.1/SVD Transfer The TSF shall enforce the **SVD transfer SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/SVD Transfer The TSF shall export the user data without the user data's associated security attributes

Application note:

This instance is only relevant if the SVD is held by the TOE and exported to the CGA for certification.

FDP_ITC.1/SCD Import of user data without security attributes

FDP_ITC.1.1/SCD The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/SCD The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/SCD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **the SCD shall be sent by an Authorised SSCD**.

Application note:

If it is has been designated to generate an SCD for a SSCD Type2, A SSCD Type1 is authorised to export SCD to this specific SSCD Type2.

Authorised SSCDs Type1 are able to establish a trusted channel with SSCDs Type2 for SCD transfer.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FDP_ITC.1/DTBS Import of user data without security attributes

FDP_ITC.1.1/DTBS The TSF shall enforce the **Signature-creation SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/DTBS The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/DTBS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **the DTBS-representation shall be sent by an Authorised SCA**.

Application note:

A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and is able to establish a trusted channel to the SSCD.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **SCD, VAD and RAD**.

FDP_SDI.2/DTBS Stored data integrity monitoring and action

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 data"**.

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

- **prohibit the use of the altered data,**
- **inform the Signatory about integrity error**.

Refinement:

In the specific case of the TOE, the DTBS-representation is not stored on the TOE. Therefore this instance related to a "DTBS-representation temporarily stored by the TOE" is not applicable.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FDP_SDI.2/Persistent Stored data integrity monitoring and action

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 persistent stored data"**.

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

- **prohibit the use of the altered data,**
- **inform the Signatory about integrity error**.

Application note:

The following data persistently stored by the TOE have the user data attribute "integrity checked persistent stored data": SCD, RAD and SVD (if persistently stored by the TOE).

FDP_UCT.1/Receiver Basic data exchange confidentiality

FDP_UCT.1.1/Receiver The TSF shall enforce the **SCD Import SFP** to be able to **receive** user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/SVD Transfer Data exchange integrity

FDP_UIT.1.1/SVD Transfer The TSF shall enforce the **SVD transfer SFP** to be able to **transmit** user data in a manner protected from **modification and insertion** errors.

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

FDP_UIT.1/TOE DTBS Data exchange integrity

FDP_UIT.1.1/TOE DTBS The TSF shall enforce the **Signature-creation SFP** to be able to **receive** user data in a manner protected from **modification, deletion and insertion** errors.

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

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **n** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

FIA_AFL.1.2 [Editorially Refined] When the defined number of unsuccessful authentication attempts has been **met or surpassed**, the TSF shall **block RAD**.

Application note:

The Authentication Try Limit **n** is defined during personalisation and must verify 1 <= **n** <= 3.

This instance is specific to RAD so a new requirement "FIA AFL.1.1/General" is defined, applicable for all authentication data (External Authentication keys, Secure Messaging Key for Signature/Verification). These different authentication data may be used to control access to different operations such as file update or key generation.

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **RAD**.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow**:**

- **identifying the user by means of TSF required by FIA_UID.1,**
- **establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import,**
- **establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import,**
- **establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE,**

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

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

"Local user" mentioned in this instance is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by FTP_TRP.1/TOE.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow**:**

- **establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE,**
- **establishing a trusted channel between the TOE and a SSCD type1 by means of TSF required by FTP_ITC.1/SCD import,**
- **establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import,**

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

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **enable** the functions **signature-creation function** to **Signatory**.

FMT_MSA.1/Administrator-Import Management of security attributes

FMT_MSA.1.1/Administrator-Import The TSF shall enforce the **SCD Import SFP** to restrict the ability to **modify** the security attributes **SCD/SVD management** to **the Administrator**.

FMT_MSA.1/Administrator-Initialisation Management of security attributes

FMT_MSA.1.1/Administrator-Initialisation The TSF shall enforce the **Initialisation SFP** to restrict the ability to **modify** the security attributes **SCD/SVD management** to **the Administrator**.

FMT_MSA.1/Signatory Management of security attributes

FMT_MSA.1.1/Signatory The TSF shall enforce the **Signature-creation SFP** to restrict the ability to **modify** the security attributes **SCD operational** to **Signatory**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for **security attributes**.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Initialisation SFP, Signature-creation SFP, SCD Import SFP, External Authentication Keys SFP and Secure Messaging Keys 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 **Administrator or Signatory** to specify alternative initial values to override the default values when an object or information is created.

Application note:

The security attribute of the SCD "SCD operational" is set to "no" after generation or import of the SCD.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **modify** the **RAD** to **Signatory**.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **Administrator and Signatory**.

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

FMT_SMF.1 Specification of Management Functions

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

- **Creation and modification of RAD,**
- **Enabling the signature-creation function,**
- **Modification of the security attribute SCD/SVD management and SCD operational,**
- **Modification of the security attributes related to External Authentication keys and Secure Messaging keys**.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FPT_TEE.1 Testing of external entities

FPT_TEE.1.1 The TSF shall run a suite of tests **during initial start-up** to check the fulfillment of **the security assumptions made about the underlying platform**.

FPT_TEE.1.2 If the test fails, the TSF shall **respond automatically such that the TSP is not violated**.

Application note:

This requirement is the translation of FPT_AMT.1 in CC3.1.

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit **side channel emission** in excess of **limits specified by the state-of-the-art attacks on smart card IC** enabling access to **RAD** and **SCD**.

FPT_EMSEC.1.2 The TSF shall ensure **all users** are unable to use the following interface **external contacts emanations** to gain access to **RAD** and **SCD**.

FPT_FLS.1 Failure with preservation of secure state

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

- **power shortage,**
- **over voltage,**
- **over and under clock frequency, integrity errors**.

FPT_PHP.1 Passive detection of physical attack

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.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **physical manipulation and physical probing** to the **integrated circuit** by responding automatically such that the SFRs are always enforced.

Application note:

This requirement is connected to the FPT_PHP.3 requirements of the platform. It detects physical attacks and reacts to these attacks by resetting the card or raising an exception. In these two cases, IC notifies the attack to the software.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **the TSF**.

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

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

FTP_ITC.1/SCD Import Inter-TSF trusted channel

FTP_ITC.1.1/SCD Import 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/SCD Import The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SCD Import The TSF shall initiate communication via the trusted channel for **SCD import**.

Refinement:

The mentioned trusted IT product is a SSCD Type1.

FTP_ITC.1/SVD Transfer Inter-TSF trusted channel

FTP_ITC.1.1/SVD Transfer The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SVD Transfer The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD Transfer The TSF shall initiate communication via the trusted channel for **SVD export**.

Refinement:

The CGA can also initiate the communication.

The mentioned trusted IT product is a CGA.

Application note:

In this security target, SVD is exported but never imported. Thus only "FTP_ITC.1.1/ SVD transfer"" from [SSCD3] is applicable. In [SSCD2], "FTP_ITC.1.1/ SVD transfer" concerns import and export of SVD. The part concerning the SVD export has exactly the same text than the requirement included in this Security Target.

FTP_ITC.1/DTBS Import Inter-TSF trusted channel

FTP_ITC.1.1/DTBS Import 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/DTBS Import The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/DTBS Import The TSF shall initiate communication via the trusted channel for **signing DTBS-representation**.

Refinement:

The mentioned trusted IT product is a SCA.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FTP_TRP.1/TOE Trusted path

FTP_TRP.1.1/TOE The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification and disclosure**.

FTP_TRP.1.2/TOE The TSF shall permit **local users** to initiate communication via the trusted path.

FTP_TRP.1.3/TOE The TSF shall require the use of the trusted path for **initial user authentication**.

7.1.2 Added Requirements

FCS_CKM.4/External Authentication Keys Cryptographic key destruction

FCS_CKM.4.1/External Authentication Keys The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting of the buffer containing the key** that meets the following: **no specific standard**.

Refinement:

Keys are External Authentication Keys in this instance.

Application note:

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

FCS_CKM.4/Secure Messaging Keys Cryptographic key destruction

FCS_CKM.4.1/Secure Messaging Keys The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the buffer containing the key** that meets the following: **no specific standard**.

Refinement:

Keys are Secure Messaging Keys in this instance.

Application note:

The destruction of the previous Secure Messaging keys is mandatory when they are updated.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FCS_COP.1/3DES External Authentication Cryptographic operation

FCS_COP.1.1/3DES External Authentication The TSF shall perform **3DES External Authentication** in accordance with a specified cryptographic algorithm **MAC Algorithm 3** and cryptographic key sizes **128 and 192 bits** that meet the following: **FIPS PUB 46-3 and CNS**.

Application note:

This algorithm is used during External Authentication to verify the challenge sent by the terminal.

FCS_COP.1/RSA External Authentication Cryptographic operation

FCS_COP.1.1/RSA External Authentication The TSF shall perform **RSA External Authentication** in accordance with a specified cryptographic algorithm **RSA using Public Key** and cryptographic key sizes **1024, 1280, 1536, 1792 or 2048 bits** that meet the following: **RSA External Authentication**.

Application note:

This algorithm is used during RSA External Authentication to verify the challenge sent by the terminal. The biggest RSA public key which can be imported by the applet is 2048 bits (using the command PUT DATA).

FCS_COP.1/Secure Messaging Signature Cryptographic operation

FCS_COP.1.1/Secure Messaging Signature The TSF shall perform **Secure Messaging Signature** in accordance with a specified cryptographic algorithm **MAC Algorithm 3** and cryptographic key sizes **128 and 192 bits** that meet the following: **FIPS PUB 46-3 and CNS**.

Application note:

This algorithm is used during Secure Messaging: for computation of signature (SIG OUT) of outgoing APDU commands and verification of signature (SIG IN) of received APDU commands.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FCS_COP.1/Secure Messaging Encryption/Decryption Cryptographic operation

FCS_COP.1.1/Secure Messaging Encryption/Decryption The TSF shall perform **Secure Messaging Encryption/Decryption** in accordance with a specified cryptographic algorithm **3DES CBC** and cryptographic key sizes **128 and 192 bits** that meet the following: **FIPS PUB 46-3** and **CNS**.

Application note:

This algorithm is used during Secure Messaging for encryption of data (ENC OUT) for outgoing APDU commands and decryption of data (ENC IN) for received APDU commands.

FDP_ACC.1/External Authentication Keys SFP Subset access control

FDP_ACC.1.1/External Authentication Keys SFP The TSF shall enforce the **Authentication Keys SFP** on **creation, update and unblocking of External Authentication Keys by Administrator and Signatory**.

FDP_ACC.1/Secure Messaging keys SFP Subset access control

FDP_ACC.1.1/Secure Messaging keys SFP The TSF shall enforce the **Secure Messaging keys SFP** on **creation, update and unblocking of Secure Messaging Keys by Administrator**.

FDP_ACC.1/PIN SFP Subset access control

FDP_ACC.1.1/PIN SFP The TSF shall enforce the **PIN SFP** on

- **creation of PINs (different from RAD) by Administrator and Signatory,**
- **update and unblocking of PINs (including RAD) by Administrator and Signatory**.

Application note:

RAD creation is already covered by Personalisation SFP.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FDP_ACF.1/External Authentication Keys SFP Security attribute based access control

FDP_ACF.1.1/External Authentication Keys SFP The TSF shall enforce the **External Authentication Keys SFP** to objects based on the following: **general attributes**.

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

- **A user with the security attribute "role" set to "Administrator" or set to "Signatory" is allowed to create, update or unblock External Authentication Keys**.

FDP_ACF.1.3/External Authentication Keys SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/External Authentication Keys SFP The TSF shall explicitly deny access of subjects to objects based on the **none**.

FDP_ACF.1/Secure Messaging Keys SFP Security attribute based access control

FDP_ACF.1.1/Secure Messaging Keys SFP The TSF shall enforce the **Secure Messaging Keys SFP** to objects based on the following: **general attributes**.

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

- **A user with the security attribute "role" set to "Administrator" is allowed to create, update or unblock Secure Messaging Keys**.

FDP_ACF.1.3/Secure Messaging Keys SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/Secure Messaging Keys SFP The TSF shall explicitly deny access of subjects to objects based on the **none**.

FDP_ACF.1/PIN SFP Security attribute based access control

FDP_ACF.1.1/PIN SFP The TSF shall enforce the **PIN SFP** to objects based on the following: **general attributes**.

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

- **A user with the security attribute "role" set to "Administrator" or set to "Signatory" is allowed to update**, **unblock and create PINs**,

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FDP_ACF.1.3/PIN SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/PIN SFP The TSF shall explicitly deny access of subjects to objects based on the **none**.

Application note:

The "Personalisation SFP" controls creation operation on a specific PIN that is the RAD. The "PIN FSP" concerns:

- all PINs (except RAD) of the application and all their related operations (creation, update, unblock)

FDP_ITC.1/External Authentication Keys Import of user data without security attributes

FDP_ITC.1.1/External Authentication Keys The TSF shall enforce the **External Authentication keys SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/External Authentication Keys The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/External Authentication Keys The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

FDP_ITC.1/Secure Messaging Keys Import of user data without security attributes

FDP_ITC.1.1/Secure Messaging Keys The TSF shall enforce the **Secure Messaging keys Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/Secure Messaging Keys The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/Secure Messaging Keys The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

FIA_AFL.1/General Authentication failure handling

FIA_AFL.1.1/General The TSF shall detect when **n** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

FIA_AFL.1.2/General [Editorially Refined] When the defined number of unsuccessful authentication attempts has been **met or surpassed**, the TSF shall **block the corresponding authentication data External Authentication keys or Secure Messaging Key for Signature/Verification**.

Application note:

The Authentication Try Limit **n** is defined during personalisation and must verify 1 <= **n** <= 3.

FMT_MSA.1/External Authentication Keys Management of security attributes

FMT_MSA.1.1/External Authentication Keys The TSF shall enforce the **External Authentication Keys SFP** to restrict the ability to **modify** the security attributes **related to External Authentication Keys** to **Administrator**.

Application note:

This requirement deals with Secure Messaging Keys used for operations on the SCD and the RAD.

FMT_MSA.1/Secure Messaging Keys Management of security attributes

FMT_MSA.1.1/Secure Messaging Keys The TSF shall enforce the **Secure Messaging Keys SFP** to restrict the ability to **modify** the security attributes **related to Secure Messaging Keys** to **Administrator**.

7.2 Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with AVA_VAN.5.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

7.3 Security Requirements Rationale

7.3.1 Objectives

7.3.1.1 Security Objectives for the TOE

OT.EMSEC_Design See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

OT.Lifecycle_Security See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

Note: FPT_TEE.1 is the translation of FPT_AMT.1 in CC3.1. The same rationale applies.

OT.SCD_Secrecy See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

Note: FPT_TEE.1 is the translation of FPT_AMT.1 in CC3.1. The same rationale applies.

OT.SCD_SVD_Corresp See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

OT.SVD_Auth_TOE See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

This objective is also covered by SFRs that precise the mechanisms used to establish a secure channel (based on secure messaging) as required in FTP_ITC.1/SVD Transfer. Correct management and protection of the secure messaging keys avoid that an attacker may indirectly compromise the SVD authenticity:

- FCS_COP.1/Secure Messaging Signature, and FCS_COP.1/Secure Messaging Encryption/Decryption, provide cryptographic means for encryption and MAC signature for secure messaging,
- FCS_CKM.4/Secure Messaging Keys, provides secure destruction of the secure messaging keys,
- FDP_ACC.1.1/Secure Messaging keys SFP, and FDP_ACF.1.1/Secure Messaging keys SFP, ensure access control on all operations on secure messaging keys,
- FDP_ITC.1/Secure Messaging Keys, protects secure messaging during their import in the TOE,
- FMT_MSA.1.1/Secure Messaging Keys, provides the attributes of the secure messaging keys,
- FMT_SMF.1 provides required attributes management functions.

OT.Tamper_ID See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

OT.Tamper_Resistance See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

OT.Init See [SSCD2] and [SSCD3] §6.3 for a detailed rationale for requirements of the SSCD PP.

This objective is also covered by the following SFRs in this Security Target:

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

- FCS_COP.1/3DES External Authentication, and FCS_COP.1/RSA External Authentication, provide cryptographic operations for verifying challenge for authentication,
- FIA_AFL.1/General, limits the successive wrong authentications to prevent attacks by exhaustive search of authentication data. This requirement applies for authentication keys and PINs,
- FMT_MSA.1.1/External Authentication Keys, provides the attributes of the authentication data,
- FDP_ACC.1.1/External Authentication Keys SFP, FDP_ACC.1.1/PIN SFP, FDP_ACF.1.1/External Authentication Keys SFP, FDP_ACF.1.1/PIN SFP, contribute to provide proper authentication by ensuring access control on authentication data,
- FDP_ITC.1/External Authentication Keys, participates to provide proper authentication by protecting authentication keys (used for AC_GENKEYPAIR) during their import,
- FCS_CKM.4/External Authentication Keys, provides secure destruction of the external authentication keys,
- FMT_SMF.1 provides required attributes management functions.

Indeed, SCD/SVD generation requires an access control which is a combination of authentication data (authentication keys and PINs). Management and protection of authentication data of avoids that an attacker may indirectly gain information on the SCD.

OT.SCD_Unique See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

OT.SCD_Transfer See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

This objective is also covered by the following SFRs in this Security Target:

- SFRs that precise the mechanisms used to establish a secure channel (based on secure messaging) as required in FDP_ITC.1/SCD Import. Correct management and protection of the secure messaging keys avoid that an attacker may indirectly gain information on the SCD;
  - FCS_COP.1/Secure Messaging Signature, and FCS_COP.1/Secure Messaging Encryption/Decryption, provide cryptographic means for decryption and MAC verification for secure messaging.
  - FCS_CKM.4/Secure Messaging Keys, provides secure destruction of the secure messaging keys.
  - FDP_ACC.1.1/Secure Messaging keys SFP and FDP_ACF.1.1/Secure Messaging keys SFP, ensure access control on all operations on secure messaging keys,
  - FDP_ITC.1/Secure Messaging Keys, protects secure messaging during their import in the TOE,
  - FIA_AFL.1/General limits the number of the successive wrong authentications to prevent attacks on the secure messaging signature/verification key by exhaustive search,
  - FMT_MSA.1.1/Secure Messaging Keys, provides the attributes of the secure messaging keys,

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

- SFRs clarifying the authentication mechanisms used for ensuring access control on SCD. These mechanisms are required to satisfy the access conditions controlling the SCD import. These access conditions are expressed as a combination of authentication data (authentication keys and PINs). Proper management and protection of these authentication data avoid that an attacker may indirectly gain information on the SCD;
  - FCS_COP.1/3DES External Authentication, and FCS_COP.1/RSA External Authentication, provide cryptographic operations for verifying challenge for authentication,
  - FIA_AFL.1/General, limits the successive wrong authentications to prevent attacks by exhaustive search of authentication data. This requirement apply for authentication keys and PINs,
  - FMT_MSA.1.1/External Authentication Keys, provides the attributes of the authentication data,
  - FDP_ACC.1.1/External Authentication Keys SFP, FDP_ACC.1.1/PIN SFP, FDP_ACF.1.1/External Authentication Keys SFP, and FDP_ACF.1.1/PIN SFP, contribute to provide proper authentication by ensuring access control on authentication data. For example, this requirement ensures that only authenticated user can unblock authenticated data controlling the SCD import,
  - FDP_ITC.1/External Authentication Keys, participates to provide proper authentication by protecting authentication keys (used for SCD import) during their import,
  - FCS_CKM.4/External Authentication Keys provides secure destruction of the external authentication keys,
- FMT_SMF.1 provides required attributes management functions.

OT.DTBS_Integrity_TOE See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

This objective is also covered by SFRs that precise the mechanisms used to establish a secure channel (based on secure messaging) as required in FTP_ITC.1/DTBS Import. Correct management and protection of the secure messaging keys avoid that an attacker may indirectly compromise the SVD authenticity:

- FCS_COP.1/Secure Messaging Signature, and FCS_COP.1/Secure Messaging Encryption/Decryption, provide cryptographic means for decryption and MAC verification for secure messaging,
- FCS_CKM.4/Secure Messaging Keys, provides secure destruction of the secure messaging keys,
- FDP_ACC.1.1/Secure Messaging keys SFP, and FDP_ACF.1.1/Secure Messaging keys SFP, ensure access control on all operations on secure messaging keys,
- FDP_ITC.1/ Secure Messaging Keys, protects secure messaging during their import in the TOE,
- FMT_MSA.1.1/Secure Messaging Keys, provides the attributes of the secure messaging keys.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

OT.Sigy_SigF See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

This objective is also covered by the following SFR in this Security Target:

- FMT_SMF.1 provides required attributes management functions.

OT.Sig_Secure See [SSCD2] and [SSCD3] §6.3 for a detailed rationale.

Note: FPT_TEE.1 is the translation of FPT_AMT.1 in CC3.1. The same rationale applies.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

7.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.EMSEC_Design	FPT_EMSEC.1	Section 4.3.1
OT.Lifecycle_Security	FCS_CKM.4, FPT_TST.1, FPT_TEE.1	Section 4.3.1
OT.SCD_Secrecy	FCS_CKM.1/RSA, FCS_CKM.4, FDP_ACC.1/Initialisation SFP, FDP_ACF.1/Initialisation SFP, FDP_RIP.1, FDP_SDI.2/Persistent, FMT_MOF.1, FMT_MSA.1/Administrator-Import, FMT_MSA.3, FMT_SMR.1, FPT_FLS.1, FTP_ITC.1/SCD Import, FMT_MSA.1/Administrator-Initialisation, FPT_TEE.1	Section 4.3.1
OT.SCD_SVD_Corresp	FCS_CKM.1/RSA, FCS_COP.1/Corresp, FDP_SDI.2/Persistent	Section 4.3.1
OT.SVD_Auth_TOE	FDP_ACC.1/SVD Transfer SFP, FDP_ACF.1/SVD Transfer SFP, FDP_ETC.1/SVD Transfer, FDP_UIT.1/SVD Transfer, FTP_ITC.1/SVD Transfer, FCS_CKM.4/Secure Messaging Keys, FCS_COP.1/Secure Messaging Signature, FCS_COP.1/Secure Messaging Encryption/Decryption, FDP_ACC.1/Secure Messaging keys SFP, FDP_ACF.1/Secure Messaging Keys SFP, FDP_ITC.1/Secure Messaging Keys, FMT_MSA.1/Secure Messaging Keys, FMT_SMF.1	Section 4.3.1
OT.Tamper_ID	FPT_PHP.1	Section 4.3.1
OT.Tamper_Resistance	FPT_PHP.3	Section 4.3.1
OT.Init	FDP_ACC.1/Initialisation SFP, FDP_ACF.1/Initialisation SFP, FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FMT_MSA.3, FCS_CKM.4/External Authentication Keys, FCS_COP.1/3DES External Authentication, FCS_COP.1/RSA External Authentication, FDP_ACC.1/External Authentication Keys SFP, FDP_ACC.1/PIN SFP, FDP_ACF.1/External Authentication Keys SFP, FDP_ACF.1/PIN SFP, FDP_ITC.1/External Authentication Keys, FIA_AFL.1/General, FMT_MSA.1/External Authentication Keys, FMT_MSA.1/Administrator-Initialisation, FMT_SMF.1	Section 4.3.1
OT.SCD_Unique	FCS_CKM.1/RSA	Section 4.3.1

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Security Objectives	Security Functional Requirements	Rationale
OT.SCD_Transfer	FDP_ACF.1/SCD Import SFP, FDP_ITC.1/SCD, FDP_UCT.1/Receiver, FMT_MSA.2, FMT_MSA.3, FMT_SMR.1, FCS_CKM.4/External Authentication Keys, FCS_CKM.4/Secure Messaging Keys, FCS_COP.1/3DES External Authentication, FCS_COP.1/RSA External Authentication, FCS_COP.1/Secure Messaging Signature, FCS_COP.1/Secure Messaging Encryption/Decryption, FDP_ACC.1/External Authentication Keys SFP, FDP_ACC.1/Secure Messaging keys SFP, FDP_ACC.1/PIN SFP, FDP_ACF.1/External Authentication Keys SFP, FDP_ACF.1/Secure Messaging Keys SFP, FDP_ACF.1/PIN SFP, FDP_ITC.1/External Authentication Keys, FDP_ITC.1/Secure Messaging Keys, FIA_AFL.1/General, FMT_MSA.1/External Authentication Keys, FMT_MSA.1/Secure Messaging Keys, FDP_ACC.1/SCD Import SFP, FCS_CKM.4, FMT_SMF.1	Section 4.3.1
OT.DTBS_Integrity_TOE	FDP_ACC.1/Signature-creation SFP, FDP_ACF.1/Signature-creation SFP, FDP_ITC.1/DTBS, FDP_SDI.2/DTBS, FDP_UIT.1/TOE DTBS, FTP_ITC.1/DTBS Import, FCS_CKM.4/Secure Messaging Keys, FCS_COP.1/Secure Messaging Signature, FCS_COP.1/Secure Messaging Encryption/Decryption, FDP_ACC.1/Secure Messaging keys SFP, FDP_ACF.1/Secure Messaging Keys SFP, FDP_ITC.1/Secure Messaging Keys, FMT_MSA.1/Secure Messaging Keys	Section 4.3.1
OT.Sigy_SigF	FDP_ACC.1/Personalisation SFP, FDP_ACC.1/Signature-creation SFP, FDP_ACF.1/Personalisation SFP, FDP_ACF.1/Signature-creation SFP, FDP_RIP.1, FDP_SDI.2/Persistent, FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1, FTP_TRP.1/TOE, FMT_SMF.1	Section 4.3.1
OT.Sig_Secure	FCS_COP.1/Signing, FDP_SDI.2/Persistent, FPT_TST.1, FPT_TEE.1	Section 4.3.1

Tableau 7 Security Objectives and SFRs - Coverage

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Security Functional Requirements	Security Objectives
FCS_CKM.1/RSA	OT.SCD_Secrecy, OT.SCD_SVD_Corresp, OT.SCD_Unique
FCS_CKM.4	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.SCD_Transfer
FCS_COP.1/Corresp	OT.SCD_SVD_Corresp
FCS_COP.1/Signing	OT.Sig_Secure
FDP_ACC.1/Initialisation SFP	OT.SCD_Secrecy, OT.Init
FDP_ACC.1/SVD Transfer SFP	OT.SVD_Auth_TOE
FDP_ACC.1/Personalisation SFP	OT.Sigy_SigF
FDP_ACC.1/SCD Import SFP	OT.SCD_Transfer
FDP_ACC.1/Signature-creation SFP	OT.DTBS_Integrity_TOE, OT.Sigy_SigF
FDP_ACF.1/Initialisation SFP	OT.SCD_Secrecy, OT.Init
FDP_ACF.1/SVD Transfer SFP	OT.SVD_Auth_TOE
FDP_ACF.1/Personalisation SFP	OT.Sigy_SigF
FDP_ACF.1/SCD Import SFP	OT.SCD_Transfer
FDP_ACF.1/Signature-creation SFP	OT.DTBS_Integrity_TOE, OT.Sigy_SigF
FDP_ETC.1/SVD Transfer	OT.SVD_Auth_TOE
FDP_ITC.1/SCD	OT.SCD_Transfer
FDP_ITC.1/DTBS	OT.DTBS_Integrity_TOE
FDP_RIP.1	OT.SCD_Secrecy, OT.Sigy_SigF
FDP_SDI.2/DTBS	OT.DTBS_Integrity_TOE
FDP_SDI.2/Persistent	OT.SCD_Secrecy, OT.SCD_SVD_Corresp, OT.Sigy_SigF, OT.Sig_Secure
FDP_UCT.1/Receiver	OT.SCD_Transfer
FDP_UIT.1/SVD Transfer	OT.SVD_Auth_TOE
FDP_UIT.1/TOE DTBS	OT.DTBS_Integrity_TOE
FIA_AFL.1	OT.Init, OT.Sigy_SigF
FIA_ATD.1	OT.Init, OT.Sigy_SigF
FIA_UAU.1	OT.Init, OT.Sigy_SigF
FIA_UID.1	OT.Init, OT.Sigy_SigF

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Security Functional Requirements	Security Objectives
FMT_MOF.1	OT.SCD_Secrecy, OT.Sigy_SigF
FMT_MSA.1/Administrator-Import	OT.SCD_Secrecy
FMT_MSA.1/Administrator-Initialisation	OT.SCD_Secrecy, OT.Init
FMT_MSA.1/Signatory	OT.Sigy_SigF
FMT_MSA.2	OT.SCD_Transfer, OT.Sigy_SigF
FMT_MSA.3	OT.SCD_Secrecy, OT.Init, OT.SCD_Transfer, OT.Sigy_SigF
FMT_MTD.1	OT.Sigy_SigF
FMT_SMR.1	OT.SCD_Secrecy, OT.SCD_Transfer, OT.Sigy_SigF
FMT_SMF.1	OT.Sigy_SigF, OT.Init, OT.SVD_Auth_TOE, OT.SCD_Transfer
FPT_TEE.1	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure
FPT_EMSEC.1	OT.EMSEC_Design
FPT_FLS.1	OT.SCD_Secrecy
FPT_PHP.1	OT.Tamper_ID
FPT_PHP.3	OT.Tamper_Resistance
FPT_TST.1	OT.Lifecycle_Security, OT.Sig_Secure
FTP_ITC.1/SCD Import	OT.SCD_Secrecy
FTP_ITC.1/SVD Transfer	OT.SVD_Auth_TOE
FTP_ITC.1/DTBS Import	OT.DTBS_Integrity_TOE
FTP_TRP.1/TOE	OT.Sigy_SigF
FCS_CKM.4/External Authentication Keys	OT.Init, OT.SCD_Transfer
FCS_CKM.4/Secure Messaging Keys	OT.SVD_Auth_TOE, OT.SCD_Transfer, OT.DTBS_Integrity_TOE
FCS_COP.1/3DES External Authentication	OT.Init, OT.SCD_Transfer
FCS_COP.1/RSA External Authentication	OT.Init, OT.SCD_Transfer

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Security Functional Requirements	Security Objectives
FCS_COP.1/Secure Messaging Signature	OT.SVD_Auth_TOE, OT.SCD_Transfer, OT.DTBS_Integrity_TOE
FCS_COP.1/Secure Messaging Encryption/Decryption	OT.SVD_Auth_TOE, OT.SCD_Transfer, OT.DTBS_Integrity_TOE
FDP_ACC.1/External Authentication Keys SFP	OT.Init, OT.SCD_Transfer
FDP_ACC.1/Secure Messaging keys SFP	OT.SVD_Auth_TOE, OT.SCD_Transfer, OT.DTBS_Integrity_TOE
FDP_ACC.1/PIN SFP	OT.Init, OT.SCD_Transfer
FDP_ACF.1/External Authentication Keys SFP	OT.Init, OT.SCD_Transfer
FDP_ACF.1/Secure Messaging Keys SFP	OT.SVD_Auth_TOE, OT.SCD_Transfer, OT.DTBS_Integrity_TOE
FDP_ACF.1/PIN SFP	OT.Init, OT.SCD_Transfer
FDP_ITC.1/External Authentication Keys	OT.Init, OT.SCD_Transfer
FDP_ITC.1/Secure Messaging Keys	OT.SVD_Auth_TOE, OT.SCD_Transfer, OT.DTBS_Integrity_TOE
FIA_AFL.1/General	OT.Init, OT.SCD_Transfer
FMT_MSA.1/External Authentication Keys	OT.Init, OT.SCD_Transfer
FMT_MSA.1/Secure Messaging Keys	OT.SVD_Auth_TOE, OT.SCD_Transfer, OT.DTBS_Integrity_TOE

Tableau 8 SFRs and Security Objectives

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

7.3.3 *Dependencies*

7.3.3.1 SFRs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1/RSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/Signing
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/RSA, FDP_ITC.1/SCD
FCS_COP.1/Corresp	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA, FCS_CKM.4, FDP_ITC.1/DTBS
FCS_COP.1/Signing	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA, FCS_CKM.4, FDP_ITC.1/SCD
FDP_ACC.1/Initialisation SFP	(FDP_ACF.1)	FDP_ACF.1/Initialisation SFP
FDP_ACC.1/SVD Transfer SFP	(FDP_ACF.1)	FDP_ACF.1/SVD Transfer SFP
FDP_ACC.1/Personalisation SFP	(FDP_ACF.1)	FDP_ACF.1/Personalisation SFP
FDP_ACC.1/SCD Import SFP	(FDP_ACF.1)	FDP_ACF.1/SCD Import SFP
FDP_ACC.1/Signature-creation SFP	(FDP_ACF.1)	FDP_ACF.1/Signature-creation SFP
FDP_ACF.1/Initialisation SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/Initialisation SFP, FMT_MSA.3
FDP_ACF.1/SVD Transfer SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SVD Transfer SFP, FMT_MSA.3
FDP_ACF.1/Personalisation SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/Personalisation SFP, FMT_MSA.3
FDP_ACF.1/SCD Import SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD Import SFP, FMT_MSA.3
FDP_ACF.1/Signature-creation SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/Signature-creation SFP, FMT_MSA.3
FDP_ETC.1/SVD Transfer	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/SVD Transfer SFP

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ITC.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD Import SFP, FMT_MSA.3
FDP_ITC.1/DTBS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/Signature-creation SFP, FMT_MSA.3
FDP_RIP.1	No dependencies	
FDP_SDI.2/DTBS	No dependencies	
FDP_SDI.2/Persistent	No dependencies	
FDP_UCT.1/Receiver	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/SCD Import SFP, FTP_ITC.1/SCD Import
FDP_UIT.1/SVD Transfer	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/SVD Transfer SFP, FTP_ITC.1/SVD Transfer
FDP_UIT.1/TOE DTBS	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/Signature-creation SFP, FTP_ITC.1/DTBS Import
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.1
FIA_ATD.1	No dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_UID.1	No dependencies	
FMT_MOF.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Administrator-Import	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SCD Import SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Administrator-Initialisation	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/Initialisation SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/Signature-creation SFP, FMT_SMR.1, FMT_SMF.1

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.1/Personalisation SFP, FMT_MSA.1/Administrator-Import, FMT_MSA.1/Administrator-Initialisation, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/Administrator-Import, FMT_MSA.1/Administrator-Initialisation, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MTD.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_SMF.1	No dependencies	
FPT_TEE.1	No dependencies	
FPT_EMSEC.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_PHP.1	No dependencies	
FPT_PHP.3	No dependencies	
FPT_TST.1	No dependencies	
FTP_ITC.1/SCD Import	No dependencies	
FTP_ITC.1/SVD Transfer	No dependencies	
FTP_ITC.1/DTBS Import	No dependencies	
FTP_TRP.1/TOE	No dependencies	
FCS_CKM.4/External Authentication Keys	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1/External Authentication Keys
FCS_CKM.4/Secure Messaging Keys	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1/Secure Messaging Keys
FCS_COP.1/3DES External Authentication	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/External Authentication Keys, FDP_ITC.1/External Authentication Keys
FCS_COP.1/RSA External Authentication	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/External Authentication Keys, FDP_ITC.1/External Authentication Keys

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Requirements	CC Dependencies	Satisfied Dependencies
FCS_COP.1/Secure Messaging Signature	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/Secure Messaging Keys, FDP_ITC.1/Secure Messaging Keys
FCS_COP.1/Secure Messaging Encryption/Decryption	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/Secure Messaging Keys, FDP_ITC.1/Secure Messaging Keys
FDP_ACC.1/External Authentication Keys SFP	(FDP_ACF.1)	FDP_ACF.1/External Authentication Keys SFP
FDP_ACC.1/Secure Messaging keys SFP	(FDP_ACF.1)	FDP_ACF.1/Secure Messaging Keys SFP
FDP_ACC.1/PIN SFP	(FDP_ACF.1)	FDP_ACF.1/PIN SFP
FDP_ACF.1/External Authentication Keys SFP	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/External Authentication Keys SFP
FDP_ACF.1/Secure Messaging Keys SFP	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/Secure Messaging keys SFP
FDP_ACF.1/PIN SFP	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/PIN SFP
FDP_ITC.1/External Authentication Keys	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/External Authentication Keys SFP
FDP_ITC.1/Secure Messaging Keys	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/Secure Messaging keys SFP
FIA_AFL.1/General	(FIA_UAU.1)	FIA_UAU.1
FMT_MSA.1/External Authentication Keys	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_ACC.1/External Authentication Keys SFP, FMT_SMF.1
FMT_MSA.1/Secure Messaging Keys	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_ACC.1/Secure Messaging keys SFP, FMT_SMF.1

Tableau 9 SFRs dependencies

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

7.3.3.2 SARs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_LCD.1, ALC_DVS.2
ALC_CMS.4	No dependencies	
ALC_DEL.1	No dependencies	
ALC_DVS.2	No dependencies	
ALC_LCD.1	No dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies	
ASE_INT.1	No dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.2	(ADV_ARC.1) and (ADV_TDS.3) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.2) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1

Tableau 10 SARs dependencies

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

7.3.4 Rationale for the Security Assurance Requirements

EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this protection profile is just such a product.

7.3.5 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. This assurance component is a higher hierarchical component to EAL4 (only ALC_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.

ALC_DVS.2 has no dependencies.

7.3.6 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

Advanced methodical vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication. AVA_VAN.5 has dependencies with ADV_ARC.1 "Security architecture description", ADV_FSP.2 "Security-enforcing functional specification", ADV_IMP.1 "Implementation representation of the TSF", ADV_TDS.3 "Basic modular design", AGD_PRE.1 "Preparative procedures" and AGD_OPE.1 "Operational user Guidance".

All these dependencies are satisfied by EAL4.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d’auteur.

8 TOE Summary Specification

8.1 TOE Summary Specification

SF.Keygen

The TOE generates the RSA key pair SCD/SVD of size 1024 bits or 1280 bits or 1536 bits or 1792 bits and 2048 bits. The private key (SCD) is used for signature creation. The generation algorithm ensures that the keys SCD and SVD form a correct pair of RSA keys. The SCD is destroyed before the TOE generates a new pair SCD/SVD. Moreover temporary buffers used during generation are erased to avoid disclosure of information on previous or current SCD.

The key generation function has an access condition based upon previous authentication of user: SF.KEYGEN check that SCD.AC_GENKEYPAIR is satisfied to allow the key generation. This function is available in Smart card Personalisation phase (SELECTABLE state) and Smart card end-usage phase (PERSONALIZED state) for Signatory and Administrator.

SF.SIG

The TOE signs with an RSA private key, a data (DTBS) imported from outside. The signature function has an access condition based upon previous authentication of user. This access condition is defined during personalisation by the Administrator; it corresponds to the PIN RAD. The cryptographic operation must be resistant to attack based on external observation. To ensure the SCD confidentiality, the TOE erases temporary buffers after signature creation. This function is available only for the signatory at the Smart card end-usage phase (PERSONALIZED state).

SF.USER_AUTH

This function ensures the user authentication. In order to avoid the systematic search of the authentication data, the TOE limits the number of successive authentication failures. When the limit is exceeded the User Authentication function is blocked. Several authentication mechanisms are available:

- PIN comparison: the function checks that the referenced PIN and the transmitted PIN have the same length and the same value. The same algorithm is applicable for all PINs verifications including RAD. The RAD is mandatory to authenticate the Signatory.
- External Authentication using Challenge/response protocol with 3DES keys (128 or 192 bits) and MAC retail algorithm (MAC3)
- External Authentication using Challenge/response protocol with Public RSA keys (1024 bits or 1280 bits or 1536 bits or 1792 bits and 2048 bits) If the check is successful, then the TOE has authenticated the user. The function erases all temporary buffers used during the authentication.

The Pin comparison and Challenge verification must be resistant to attack based on external observation.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

This function is available in Smart card Personalisation phase (SELECTABLE state) and Smart card end-usage phase (PERSONALIZED state) for Signatory and Administrator.

SF.PIN

This function manages operations related to PIN. It enforces access control on PIN related operations, based on access condition and secure messaging conditions. These operations are:? Creation of PIN? RAD creation is performed by the administrator? Modification of a PIN value (a PIN update is also possible when unblocking the PIN)? Unblock a PIN Security attributes related to PINs are defined during the creation and the update operations.

The creation of the RAD is available only in Smart card Personalisation phase (SELECTABLE state) and is restricted to the Administrator. Other operations are available in Smart card Personalisation phase (SELECTABLE state) and Smart card end-usage phase (PERSONALIZED state) for Signatory and Administrator.

SF.KEY

This function manages operations related to keys. It enforces access control on key related operations, based on access condition and secure messaging conditions. These operations are:

- Key creation
- Key update: the previous value of the SCD is destroyed to allow a key re-import
- Key unblock (when applicable: for authentication keys and secure messaging for MAC3 verification) It covers several functionalities:
- Export of SVD
- Import of SCD (import covers the creation and update operations)
- Authentication and Secure Messaging keys: creation, update and unblock.

Security attributes related to keys are defined during the creation and the update operations.

This function is available in Smart card Personalisation phase (SELECTABLE state) and Smart card end-usage phase (PERSONALIZED state) for Signatory and Administrator.

SF.SM

The TOE provides security services related to information exchanged between the TOE and external users. It ensures:

- the integrity and/or confidentiality of received sensitive data
- and the integrity and/or confidentiality of transmitted sensitive data The function is based on secure messaging algorithm for Signature and Encryption based on ISO7816-4:
- For the received APDU: the MAC is verified using 3DES MAC3 algorithm (retail MAC) and the data is decrypted using 3DES CBC algorithm
- For the transmitted APDU: the MAC is computed using 3DES MAC3 algorithm (retail MAC) and the data is encrypted using 3DES CBC algorithm

Secure messaging ensures protection of data during the following operations:

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

  - o Protection on Confidentiality: SCD import, Pin verification
  - o Protection on Integrity: SCD import, Pin verification, SVD export, DTBS presentation

This function is available in Smart card Personalisation phase (SELECTABLE state) and Smart card end-usage phase (PERSONALIZED state).

SF.TEST

During startup sequence, if any of the following events occurs, the card mutes itself:

  - o Blocked random generator
  - o Incorrect operation of the cryptographic module This function is automatically executed at the startup of the smart card.

SF.INTEGRITY

The TOE checks the integrity of the cryptographic key SCD and the RAD (PIN). It is based on checksum computation and verification.

SF.PHYS

This function provides ability for the software to react to physical attacks notified by the IC: In case of abnormal processing or environmental conditions or in case of integrity errors, the TOE generates either an informative or self-blocking action. This SF ensures also that the TOE returns to its previous secure state.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

8.2 SFRs / TSS

Security Functional Requirements	TOE Summary Specification
FCS_CKM.1/RSA	SF.Keygen
FCS_CKM.4	SF.Keygen, SF.KEY
FCS_COP.1/Corresp	SF.Keygen
FCS_COP.1/Signing	SF.SIG
FDP_ACC.1/Initialisation SFP	SF.Keygen
FDP_ACC.1/SVD Transfer SFP	SF.KEY
FDP_ACC.1/Personalisation SFP	SF.PIN
FDP_ACC.1/SCD Import SFP	SF.KEY, SF.SM
FDP_ACC.1/Signature-creation SFP	SF.SIG, SF.SM
FDP_ACF.1/Initialisation SFP	SF.Keygen
FDP_ACF.1/SVD Transfer SFP	SF.KEY
FDP_ACF.1/Personalisation SFP	SF.PIN
FDP_ACF.1/SCD Import SFP	SF.KEY, SF.SM
FDP_ACF.1/Signature-creation SFP	SF.SIG, SF.SM
FDP_ETC.1/SVD Transfer	SF.KEY
FDP_ITC.1/SCD	SF.KEY, SF.SM
FDP_ITC.1/DTBS	SF.SIG, SF.SM
FDP_RIP.1	SF.Keygen, SF.SIG, SF.USER_AUTH
FDP_SDI.2/DTBS	
FDP_SDI.2/Persistent	SF.INTEGRITY
FDP_UCT.1/Receiver	SF.KEY, SF.SM
FDP_UIT.1/SVD Transfer	SF.KEY, SF.SM
FDP_UIT.1/TOE DTBS	SF.SIG, SF.SM
FIA_AFL.1	SF.USER_AUTH
FIA_ATD.1	SF.USER_AUTH
FIA_UAU.1	SF.SIG, SF.SM
FIA_UID.1	SF.SIG, SF.SM
FMT_MOF.1	SF.SIG
FMT_MSA.1/Administrator-Import	SF.KEY
FMT_MSA.1/Administrator-Initialisation	SF.KEY

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Security Functional Requirements	TOE Summary Specification
FMT_MSA.1/Signatory	SF.KEY
FMT_MSA.2	SF.KEY
FMT_MSA.3	SF.KEY
FMT_MTD.1	SF.USER_AUTH, SF.PIN
FMT_SMR.1	SF.USER_AUTH
FMT_SMF.1	
FPT_TEE.1	
FPT_EMSEC.1	SF.SIG, SF.USER_AUTH
FPT_FLS.1	SF.PHYS
FPT_PHP.1	SF.PHYS
FPT_PHP.3	SF.PHYS
FPT_TST.1	SF.TEST
FTP_ITC.1/SCD Import	SF.KEY, SF.SM
FTP_ITC.1/SVD Transfer	SF.KEY, SF.SM
FTP_ITC.1/DTBS Import	SF.SIG, SF.SM
FTP_TRP.1/TOE	SF.USER_AUTH, SF.SM
FCS_CKM.4/External Authentication Keys	SF.KEY
FCS_CKM.4/Secure Messaging Keys	SF.KEY
FCS_COP.1/3DES External Authentication	SF.USER_AUTH
FCS_COP.1/RSA External Authentication	SF.USER_AUTH
FCS_COP.1/Secure Messaging Signature	SF.SM
FCS_COP.1/Secure Messaging Encryption/Decryption	SF.SM
FDP_ACC.1/External Authentication Keys SFP	SF.KEY
FDP_ACC.1/Secure Messaging keys SFP	SF.KEY
FDP_ACC.1/PIN SFP	SF.PIN
FDP_ACF.1/External Authentication Keys SFP	SF.KEY
FDP_ACF.1/Secure Messaging Keys SFP	SF.KEY
FDP_ACF.1/PIN SFP	SF.PIN
FDP_ITC.1/External Authentication Keys	SF.KEY
FDP_ITC.1/Secure Messaging Keys	SF.KEY
FIA_AFL.1/General	SF.USER_AUTH

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Security Functional Requirements	TOE Summary Specification
FMT_MSA.1/External Authentication Keys	SF.KEY
FMT_MSA.1/Secure Messaging Keys	SF.KEY

Tableau 11 SFRs and TSS - Coverage

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

TOE Summary Specification	Security Functional Requirements
SF.Keygen	FCS_CKM.1/RSA, FCS_CKM.4, FCS_COP.1/Corresp, FDP_ACC.1/Initialisation SFP, FDP_ACF.1/Initialisation SFP, FDP_RIP.1
SF.SIG	FCS_COP.1/Signing, FDP_ACC.1/Signature-creation SFP, FDP_ACF.1/Signature-creation SFP, FDP_ITC.1/DTBS, FDP_RIP.1, FDP_UIT.1/TOE DTBS, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FPT_EMSEC.1, FTP_ITC.1/DTBS Import
SF.USER_AUTH	FDP_RIP.1, FIA_AFL.1, FIA_ATD.1, FMT_MTD.1, FMT_SMR.1, FPT_EMSEC.1, FTP_TRP.1/TOE, FCS_COP.1/3DES External Authentication, FCS_COP.1/RSA External Authentication, FIA_AFL.1/General
SF.PIN	FDP_ACC.1/Personalisation SFP, FDP_ACF.1/Personalisation SFP, FMT_MTD.1, FDP_ACC.1/PIN SFP, FDP_ACF.1/PIN SFP
SF.KEY	FCS_CKM.4, FDP_ACC.1/SVD Transfer SFP, FDP_ACC.1/SCD Import SFP, FDP_ACF.1/SVD Transfer SFP, FDP_ACF.1/SCD Import SFP, FDP_ETC.1/SVD Transfer, FDP_ITC.1/SCD, FDP_UCT.1/Receiver, FDP_UIT.1/SVD Transfer, FMT_MSA.1/Administrator-Import, FMT_MSA.1/Administrator-Initialisation, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FTP_ITC.1/SCD Import, FTP_ITC.1/SVD Transfer, FCS_CKM.4/External Authentication Keys, FCS_CKM.4/Secure Messaging Keys, FDP_ACC.1/External Authentication Keys SFP, FDP_ACC.1/Secure Messaging keys SFP, FDP_ACF.1/External Authentication Keys SFP, FDP_ACF.1/Secure Messaging Keys SFP, FDP_ITC.1/External Authentication Keys, FDP_ITC.1/Secure Messaging Keys, FMT_MSA.1/External Authentication Keys, FMT_MSA.1/Secure Messaging Keys
SF.SM	FDP_ACC.1/SCD Import SFP, FDP_ACC.1/Signature-creation SFP, FDP_ACF.1/SCD Import SFP, FDP_ACF.1/Signature-creation SFP, FDP_ITC.1/SCD, FDP_ITC.1/DTBS, FDP_UCT.1/Receiver, FDP_UIT.1/SVD Transfer, FDP_UIT.1/TOE DTBS, FIA_UAU.1, FIA_UID.1, FTP_ITC.1/SCD Import, FTP_ITC.1/SVD Transfer, FTP_ITC.1/DTBS Import, FTP_TRP.1/TOE, FCS_COP.1/Secure Messaging Signature, FCS_COP.1/Secure Messaging Encryption/Decryption
SF.TEST	FPT_TST.1
SF.INTEGRITY	FDP_SDI.2/Persistent
SF.PHYS	FPT_FLS.1, FPT_PHP.1, FPT_PHP.3

Tableau 12 TSS and SFRs - Coverage

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

9 PP tailoring

9.1 PP refinements

Those refinements (i.e. tailoring) are performed in order to ensure conformance with CC3.1r3:

- Some parts of the documents have been removed especially those related to SOF and IT Environment requirements,
- FPT_AMT.1 does not exist any more in CC3.1r3 and have therefore been removed. Nevertheless, it can be translated using the new requirement FPT_TEE.1 which requires the TSF to test platform security features for correct work of the dependent TSF,
- In FPT_PHP.3, CC3.1r3 has rewritten “The TSP is not violated” by “SFRs are always enforced”. These two sentences are actually equivalent. The SFR has therefore been rewritten to fulfil CC3.1r3,
- FMT_MSA.1, FMT_MOF.1 and FMT_MTD.1 now require dependency with FMT_SMF.1 (see §9.2). These dependencies have been added,
- FMT_SMR.1 now requires dependency with FIA_UID.1. This dependency has been added,

9.2 PP additions

Due to addition in CC3.1r3 of several dependencies with the requirement FMT_SMF.1, this one has been added to the Security Target. It summarizes the management functions, the TSF has to perform. By its purpose, this requirement does not interfere with other SFRs present in the ST.
The additional functionalities are External Authentication, Secure Messaging and extra PINs management. They imply some addition to the standard PP.

The following assets have been added to the standard PP:

- External Authentication keys,
- Secure Messaging keys,
- PINs.

The following SFRs have been added to the standard PP:

- FCS_CKM.4/External Authentication Keys Cryptographic key destruction
- FCS_CKM.4/Secure Messaging Keys Cryptographic key destruction
- FCS_COP.1/3DES External Authentication Cryptographic operation
- FCS_COP.1/RSA External Authentication Cryptographic operation
- FCS_COP.1/Secure Messaging Signature Cryptographic operation
- FCS_COP.1/Secure Messaging Encryption/Decryption Cryptographic operation
- FDP_ACC.1/External Authentication Keys SFP Subset access control
- FDP_ACC.1/Secure Messaging keys SFP Subset access control
- FDP_ACC.1/PIN SFP Subset access control
- FDP_ACF.1/External Authentication Keys SFP Security attribute based access control
- FDP_ACF.1/Secure Messaging Keys SFP Security attribute based access control
- FDP_ACF.1/PIN SFP Security attribute based access control
- FDP_ITC.1/External Authentication Keys Import of user data without security attributes
- FDP_ITC.1/Secure Messaging Keys Import of user data without security attributes
- FIA_AFL.1/General Authentication failure handling
- FMT_MSA.1/External Authentication Keys Management of security attributes

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d’auteur.

10 Conformity and composition

10.1 PP SSCD claim rationale

All elements specified in [SSCD2] and [SSCD3] have been transferred in this Security target word by word. Tailoring required by the move to CC3.1r3 has been specified section 9.1.

10.2 PPs composition

This ST claims both [SSC2] and [SSCD3], therefore elements of these two PPs have been merged. An SSCD Type 3 includes the SCD/SVD generation an the difference of an SSCD Type 2 which externalizes this step to an SSCD Type 1. Therefore an SSCD Type 2 is a subset of an SSCD Type 3 and those are mutually consistent from a security point of view as stated in the introduction of the two PPs.

Additions have been performed on the PPs but target only assets and requirements. Since SPD and objectives remains the same and SFRs are just a translation of objectives in another formalism, these additions are not contradictory to base PPs. Security consistency is therefore preserved.

10.3 Not applicable requirements

FDP_SDI.2/DTBS is not applicable to the TOE because the DTBS is not stored on-card and as a consequence its integrity during storage cannot be an objective of the TOE. This situation is described in the application note of [SSCD2] and [SSCD3].

Requirements related to SVD import are not applicable to the TOE since the card does not allow the import of the SVD. The corresponding requirements FDP_ACC.1/SVD transfer SFP, FDP_ACF.1/SVD transfer SFP and FDP_UIT.1/ SVD transfer are limited to SVD export. The TOE holds SVD only when a pair SCD/SVD is generated On-Card. This situation is described in the application note of [SSCD2] and [SSCD3].

Nevertheless, these requirements are still present in the Security Target to comply with Protection Profiles.

10.4 Statement of compatibility with the platform

10.4.1 Compatibility of assumptions

All threats stated in the platform security target applied to the current composite ST.

Since platform objectives are consistent (see 10.4.4 and 10.4.5) with the current composite ST objectives and all assumptions are covered by at least one objective for the environment, platform assumptions are also consistent with the SPD of the current composite ST.

The security compatibility of assumptions is therefore ensured.

10.4.2 Compatibility of OSP

All threats stated in the platform security target applied to the current composite ST.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d’auteur.

Since platform objectives are consistent (see 10.4.4 and 10.4.5) with the current composite ST objectives and all OSPs are covered by at least one objective, platform OSPs are also consistent with the SPD of the current composite ST.

The security compatibility of OSP is therefore ensured.

10.4.3 Compatibility of threats

All threats stated in the platform security target applied to the current composite ST.

Since platform objectives are consistent (see 10.4.4 and 10.4.5) with the current composite ST objectives and all threats are countered by at least one objective, platform threats are also consistent with the SPD of the current composite ST.

The security compatibility of threats is therefore ensured.

10.4.4 Compatibility of objectives for the environment

All objectives for the environment stated in the platform security target applied to the current composite ST.

Objectives added in the current ST deal with specific external entities (SSCD Type1, CGA, SCA) which communicate with the TOE in the case of an SSCD. This does not interfere with the platform security environment.

Platform objective OE.NATIVE deals with native code. That is not relevant in this case since the application is a Java applet.

Platform objective OE.APPLET which is explicitly applicable to the current TOE is fulfilled since the application does not include native methods.

Platform objective OE.VERIFICATION applied to current composite ST. This is not contradictory to objectives of the current ST which are related to the specific usage of an SSCD and do not deal with the applet lifecycle.

The security compatibility of objectives for the environment is therefore ensured.

10.4.5 Compatibility of objectives for the TOE

All objectives for TOE stated in the platform security target applied to the current composite ST.

Except OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance, the objectives for the TOE target the security behavior of the SSCD and do not address the lower layer (i.e. the platform) which works independently. The providing of secure services by the platform is not contradictory with any objective of the TOE since by definition a service can or cannot be used depending on the request of the application.

OT.Tamper_ID and O.ALARM of the platform are compatible since both require to provide detection of security violation.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

OT.EMSEC_Design and OT.Tamper_Resistance are also compatible with O.SCP.IC which enforces protection against tampering and probing.

The security compatibility of objectives for the TOE is therefore ensured.

10.4.6 Compatibility of SFRs

All SFRs stated in the platform security target applied to the current composite ST.

Since platform objectives for the TOE are consistent (see 10.4.5) with the current composite ST objectives for the TOE and SFRs are a translation of objective for the TOE in the CC formalism, platform SFRs are also consistent with the SFRs of the current composite ST.

The security compatibility of SFRs is therefore ensured.

10.4.7 Compatibility of SARs

Since the platform is EAL5 augmented with ADV_IMP.2, ALC_DVS.2 and AVA_VAN.5 and the current ST requires a subset of these SARs (i.e. EAL4 augmented with AVA_VAN.5) compatibility is straight forward.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

10.4.8 Mapping between SFRs and enforcing entity

Requirements	Enforcing entity
FCS_CKM.1/RSA	Platform
FCS_CKM.4	Applet/Platform
FCS_COP.1/Corresp	Applet
FCS_COP.1/Signing	Applet
FDP_ACC.1/Initialisation SFP	Applet
FDP_ACC.1/SVD Transfer SFP	Applet
FDP_ACC.1/Personalisation SFP	Applet
FDP_ACC.1/SCD Import SFP	Applet
FDP_ACC.1/Signature-creation SFP	Applet
FDP_ACF.1/Initialisation SFP	Applet
FDP_ACF.1/SVD Transfer SFP	Applet
FDP_ACF.1/Personalisation SFP	Applet
FDP_ACF.1/SCD Import SFP	Applet
FDP_ACF.1/Signature-creation SFP	Applet
FDP_ETC.1/SVD Transfer	Applet
FDP_ITC.1/SCD	Applet
FDP_ITC.1/DTBS	Applet
FDP_RIP.1	Platform
FDP_SDI.2/DTBS	n/a
FDP_SDI.2/Persistent	Platform
FDP_UCT.1/Receiver	Applet
FDP_UIT.1/SVD Transfer	Applet
FDP_UIT.1/TOE DTBS	Applet
FIA_AFL.1	Applet
FIA_ATD.1	Applet
FIA_UAU.1	Applet

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Requirements	Enforcing entity
FIA_UID.1	Applet
FMT_MOF.1	Applet
FMT_MSA.1/Administrator-Import	Applet
FMT_MSA.1/Administrator-Initialisation	Applet
FMT_MSA.1/Signatory	Applet
FMT_MSA.2	Applet
FMT_MSA.3	Applet
FMT_MTD.1	Applet
FMT_SMR.1	Applet
FMT_SMF.1	Applet
FPT_TEE.1	Applet
FPT_EMSEC.1	Platform
FPT_FLS.1	Platform
FPT_PHP.1	Platform
FPT_PHP.3	Platform
FPT_TST.1	Applet
FTP_ITC.1/SCD Import	Applet
FTP_ITC.1/SVD Transfer	Applet
FTP_ITC.1/DTBS Import	Applet
FTP_TRP.1/TOE	Applet
FCS_CKM.4/External Authentication Keys	Platform
FCS_CKM.4/Secure Messaging Keys	Platform
FCS_COP.1/3DES External Authentication	Applet/Platform
FCS_COP.1/RSA External Authentication	Applet/Platform
FCS_COP.1/Secure Messaging Signature	Applet/Platform
FCS_COP.1/Secure Messaging Encryption/Decryption	Applet/Platform

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Requirements	Enforcing entity
FDP_ACC.1/External Authentication Keys SFP	Applet
FDP_ACC.1/Secure Messaging keys SFP	Applet
FDP_ACC.1/PIN SFP	Applet
FDP_ACF.1/External Authentication Keys SFP	Applet
FDP_ACF.1/Secure Messaging Keys SFP	Applet
FDP_ACF.1/PIN SFP	Applet
FDP_ITC.1/External Authentication Keys	Applet
FDP_ITC.1/Secure Messaging Keys	Applet
FIA_AFL.1/General	Applet
FMT_MSA.1/External Authentication Keys	Applet
FMT_MSA.1/Secure Messaging Keys	Applet

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

11 References

[1999/93/EC] Directive 1999/93/EC of the European parliament and of the council of the 13December on a Community framework for electronic signatures

[BSI-0002] Smartcard IC Platform Protection Profile v 1.0 BSI-PP-0002-2001 Jul 2001

[CC-1] Common Criteria for Information Technology security Evaluation Part 1: Introduction and general model, CCMB-2009-07-001, version 3.1 Revision 3, July 2009

[CC-2] Common Criteria for Information Technology security Evaluation Part 2: Security Functional Components, CCMB-2009-07-002, version 3.1 Revision 3, July 2009

[CC-3] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Components, CCMB-2009-07-003, version 3.1 Revision 3, July 2009

[CEM] Common Criteria for Information Technology security Evaluation: Evaluation Methodology, CCMB-2009-07-004, version 3.1 Revision 3, July 2009

[CNS] CNS – Carta Nazionale dei Servici – Functional Specification –1.1.2

[COSMO-ST] ID-ONE COSMO V7.0 - CLIO SECURITY TARGET Lite For AT90SC28872RCU / AT90SC28848RCU, FQR 110 4777 Ed 1 - Oberthur Technologies

[CWA] CEN/ISSS WS/E-Sign Expert Group F - Workshop Agreement CWA14169 Secure Signature Creation Devices "EAL 4+"

[CWA-ALGO] CEN/ISSS WS/E-Sign Expert Group F - Algorithms and Parameters forSecure Electronic Signatures

[GP] "Global Platform Card Specification", version 2.1.1' March, 2003, Global Platform

[JCAPI] "Java Card 2.2.1 - Application Programming Interfaces", October 21 2003, Sun Microsystems

[JCRE] "Java Card 2.2.1-JCRE", October 21 2003, Sun Microsystems

[JCVM] "Java Card 2.2.1-Virtual Machine Specifications", October 21 2003, Sun Microsystems

[SSCD1] Secure Signature-Creation device Protection Profile Type 1 v1.05, EAL4+ BSI –PP 0004-2002 April 2002

[SSCD2] Secure Signature-Creation device Protection Profile Type 2 v1.04, EAL4+ BSI -PP-0005-2002 April 2002

[SSCD3] Secure Signature-Creation device Protection Profile Type 3 v1.05, EAL4+ BSI -PP-0006-2002 April 2002

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

Index

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.

All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Tous droits de Oberthur Technologies réservés. Reproduction intégrale ou partielle interdite sans autorisation écrite du titulaire des droits d'auteur.