JAVACARD 32K

Common Criteria / ISO 15408

Security Target – Public version

EAL4+

JAVACARD 32K EAL4+ Security Target

CONTENT

List of figures

List of tables

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

Title: JAVACARD 32K CRISTAL EAL4+ Security Target

Ref: MRD06SBG023034 rev 1.1

Origin: SCHLUMBERGER SEMA

TOE reference: M256LCAC2

Commercial names:

CYBERFLEX JavaCard 32K

ICITIZEN JavaCard 32K

The TOE is composed with:

Component	Version number	Supplier
Micro-controller SLE66CX322P	GC/A23	Infineon
RMS library	0.7	Infineon
ACE library	0.44	Infineon
ROM MASK	SB80 (Infineon)	Schlumberger
SOFT MASK	SM01_V3.0.0	Schlumberger
GEOS	SC_V3.0.0	Schlumberger
Cristal Applet	AC_V1.0.0	Schlumberger

TOE function type and options: Secure signature generation card.

This ST claims three Protection Profiles [PP/TYPE2].and [PP/TYPE3] for the application; [PP/BSI-0002] for the IC.

The IC is evaluated under the German scheme for Common Criteria. The certification body is the Bundesamt für Sicherheit in der Informationstechnik (BSI).

This Security Target deals with the evaluation of the application software, as well as the composition with the evaluation of the IC. This evaluation is done under the French scheme for Common Criteria. The certification body is the Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI).

1.2 ST OVERVIEW

Context

The explosive development of electronic transaction, such as "e commerce" and the worldwide range of the electronic transactions and contacts emphasise the necessity for security. The European Council has voted a directive [European_DIR], concerning digital signature, and the CEN/ISSS has translated the annex concerning the Secure Signature Creation Device into three Protection Profiles [PP/TYPE1], [PP/TYPE2] and [PP/TYPE3].

The European governments are issuing laws giving electronic signature directive.

The product to be evaluated complies with the requirements of the European directive translated into the claimed PP [PP/TYPE2] and [PP/TYPE3].

The main objectives of this security target are:

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

The assurance level for this product and its documentation is EAL4 augmented with:

ADV_IMP.2: Implementation of the TSF,

ALC_DVS.2: Sufficiency of security measures.

AVA_MSU.3: Analysis of insecure states,

AVA_VLA.4: Highly resistant,

AVA_MSU.3 and AVA_VLA.4 are required in [PP/TYPE2] and [PP/TYPE3].

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 are required in [PP/BSI-0002].

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

1.3 CC CONFORMANCE

The compliance is assumed with CC version V2.1 (ISO 15408) (see reference in 1.4.1).

This ST is built on [PP/TYPE2], [PP/TYPE3] and [PP/BSI-0002] and is conformant to these PP.

This ST is CC V2.1 conformant with Part2 extended due to additional functional components as stated in [PP/TYPE2] and [PP/TYPE3].

This ST is CC V2.1 conformant with Part3 augmented as stated in [PP/TYPE2], [PP/TYPE3], [PP/BSI-0002].

1.4 REFERENCES

1.4.1 EXTERNAL REFERENCES [ER]

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB - 99-031, version 2.1, August 1999 (conform to ISO 15408)
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-99-032, version 2.1, August 1999 (conform to ISO 15408)
[CC-3]	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIMB-99-033, version 2.1, August 1999 (conform to ISO 5408)
[CEM]	Common Methodology for Information Technology Security Evaluation CEM-99/045, version 1.0, August 1999.
[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 for Secure Electronic Signatures
[European_DIR]	Directive 1999/93/EC of the European parliament and of the council of the 13 December on a Community framework for electronic signatures
[PP/TYPE1]	Secure Signature-Creation device Protection Profile Type 1 v1.05, EAL4+ BSI –PP-0004-2002 April 2002
[PP/TYPE2]	Secure Signature-Creation device Protection Profile Type 2 v1.05, EAL4+ BSI –PP-0005-2002 April 2002
[PP/TYPE3]	Secure Signature-Creation device Protection Profile Type 3 v1.05, EAL4+ BSI –PP-0006-2002 April 2002
[PP/BSI-0002]	Smartcard IC Platform Protection Profile v 1.0 BSI-PP-0002-2001 July 2001
[ST/Infineon]	Security Target of SLET66CX322P Integrated Circuit
[WS/E-Sign]	CEN/ISSS Workshop on Electronic Signatures CEN/ISSS WS/E-Sign N 1XX, Berlin/2001-02-27
[VOP]	Open Platform – Card Specification version 2.0.1 dated 7 April 00

1.4.2 ACRONYMS

CC Common Criteria Version 2.1

CGA Certification Generation Application

DTBS Data to be Signed

EAL Evaluation Assurance Level

GEOS Generic OS

HI Human Interface

HW Hardware

I/O Input/Output

OS Operating System

PDA Personal Digital Assistant

PIN Personal Identification Number

PP Protection Profile

SCA Signature-Creation Application

SCD Signature-Creation Data

SDO Signed Data Object

SOF Strength of Function

SSCD Secure Signature-Creation Device

SVD Signature-Verification Data

TOE Target of Evaluation

2 TOE DESCRIPTION

This part of the ST describes the TOE as an aid to the understanding of its security requirements.

It addresses the product type, the smart card product life cycle, the TOE environment along the smart card life cycle and the general IT features of the TOE.

2.1 PRODUCT TYPE

2.1.1 SCOPE OF THE TOE

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

- The underlying Integrated Circuit and its libraries;
- The Generic Operating System (GEOS), corresponding to the generic system software and the Java Virtual Machive (JVM);
- The SSCD Application.

The Figure below gives a description of the TOE and its boundaries. The grey parts are the limits of the TOE.

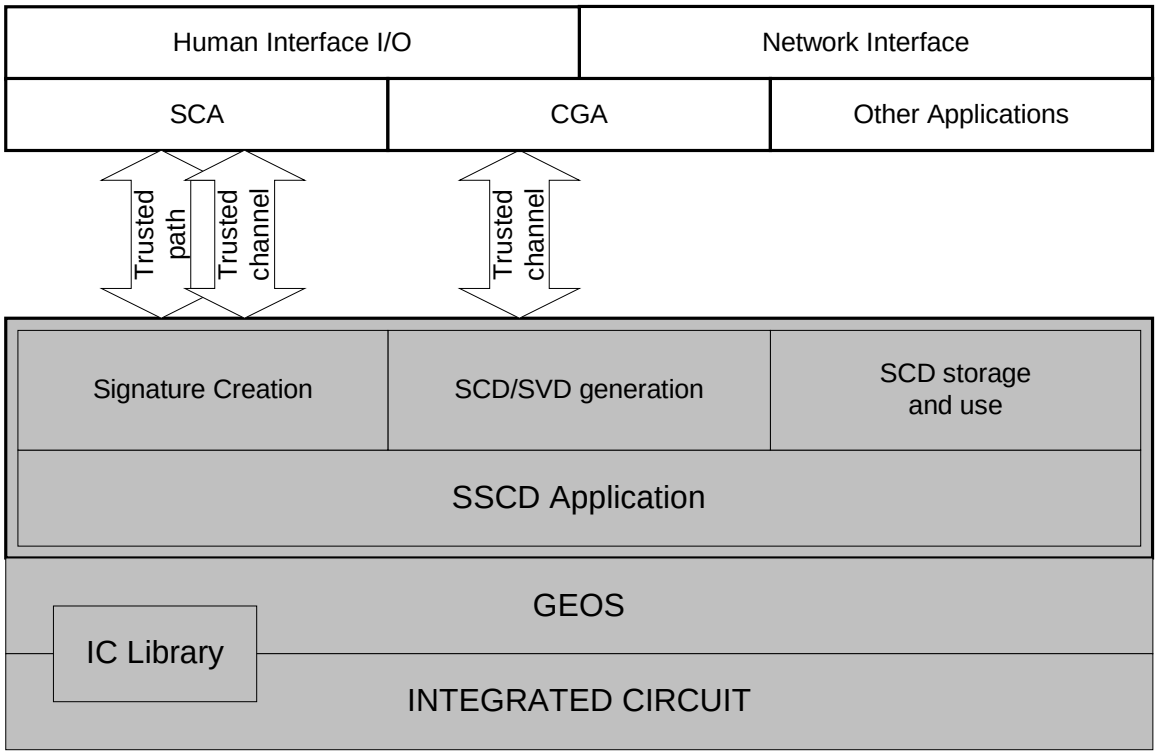

Figure 1 Secure Signature Creation Device (card) and its boundaries

The TOE is the embedded software (ES), the Integrated Circuit (IC) and the plastic card. The ES comprises GEOS and the SSCD Applet. It includes the associated embedded data of the smart card working on the micro-controller unit in accordance with the functional specifications.

Other smart card product elements, (such as holograms, magnetic stripes, security printing,…) are outside the scope of this Security Target.

2.1.2 TOE DESCRIPTION

Terminology

This document uses the terminology of [PP/TYPE2] and [PP/TYPE3].

The SSCD Application uses public key encryption. The Signature Creation Data (SCD) is the private key and the Signature Verification Data (SVD) is the public key.

The Reference Authentication Data (RAD) is the PIN stored in the card and the Verification Authentication Data (VAD) is the PIN provided by the user.

SSCD Application

It provides the following functions necessary for devices involved in secure electronic signatures:

(1) Generate the (SCD) and the correspondent (SVD), or Load the SCD,

(2) Create qualified electronic signatures:

(a) after allowing for the Data To Be Signed (DTBS) to be displayed correctly by an appropriate environment,

(b) using appropriate hash functions agreed according to [CWA-ALGO] suitable for qualified electronic signatures,

(c) after appropriate authentication of the signatory by the TOE itself,

(d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed according to [CWA-ALGO].

The TOE ensures the secrecy of the SCD.

To prevent the unauthorised usage of the SSCD the TOE provides user authentication and access control. The TOE implements IT measures to support a trusted path to a trusted human interface device. Therefore, the TOE holds the RAD that is used to verify the VAD provided by the user.

The TOE is initialised by importing a SCD or by generating a pair of SCD and SVD.

Only the legitimate signatory can use the SCD in the signature-creation process, during the validity of this SCD/SVD pair.

The TOE stores the SCD and may export the SVD. The SVD corresponding to the signatory's SCD is included in the certificate of the signatory by the certificate-service-provider (CSP).

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.

The SCA presents the DTBS to the signatory and prepares the DTBS-representation that the signatory wishes to sign for performing the cryptographic function of the signature. The TOE returns the secure electronic signature.

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

The Figure below shows the type3 and type 2 TOE operations as defined in [CWA].

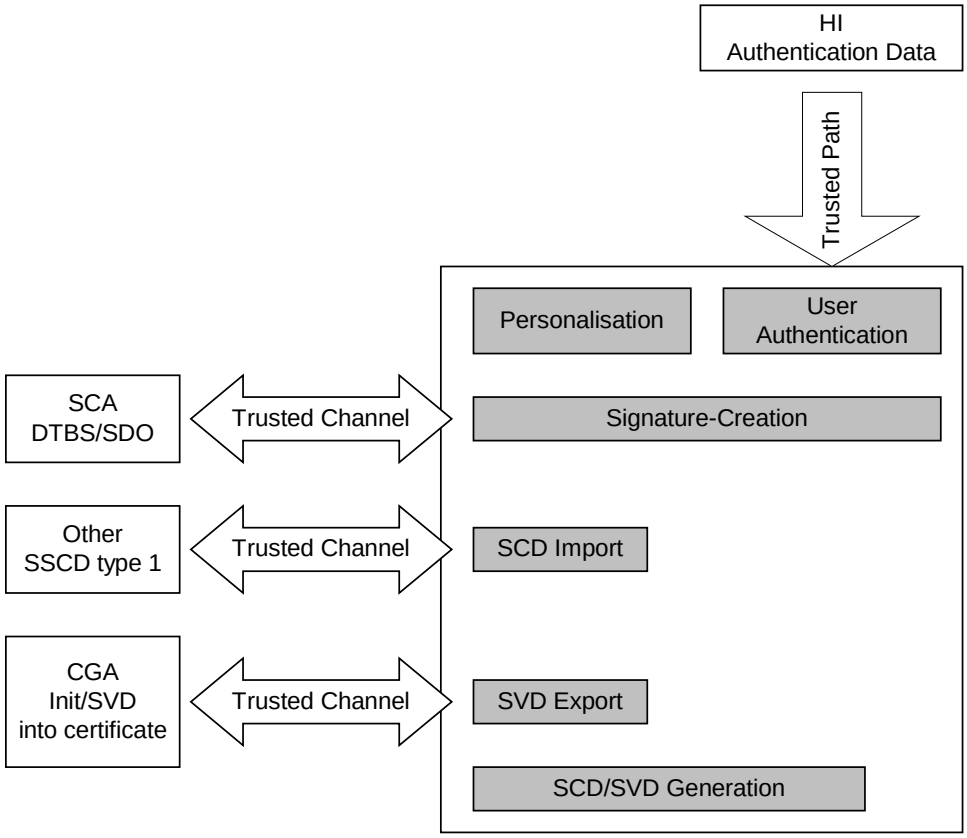

Figure 2 Type 2 and Type 3 SSCD operations

2.2 SMART CARD PRODUCTS LIFE-CYCLE

The Smart card product life cycle, as defined in [PP/BSI-0002], is split up into 7 phases where the following authorities are involved:

Phase 1	Smart card software development	**The smart card embedded software developer** is in charge of the smart card embedded software development and the specification of IC pre-personalisation requirements.
Phase 2	IC Development	**The IC designer** designs the integrated circuit, develops IC firmware if applicable, provides information, software or tools to the smart card software developer, and receives the software from the developer, through **trusted delivery and verification procedures**. From the IC design, IC firmware and smart card embedded software, he constructs the smart card IC database, necessary for the IC photomask fabrication.
Phase 3	IC manufacturing and testing	**The IC manufacturer** is responsible for producing the IC through three main steps: IC manufacturing, testing, and IC pre-personalisation.
Phase 4	IC packaging and testing	**The IC packaging manufacturer** is responsible for the IC packaging and testing.
Phase 5	Smart card product finishing process	**The smart card product manufacturer** is responsible for the smart card product finishing process and testing, and the smart card pre-personalisation
Phase 6	Smart card personalisation	**The Personaliser** is responsible for the smart card personalisation and final tests.
Phase 7	Smart card end-usage	**The smart card issuer** is responsible for the smart card product delivery to **the smart card end-user**, and for the end of life process.

The Secure Signature Creation Device life as described in [PP/TYPE2], [PP/TYPE3] and the standard smart cards life cycle can be matched as shown in Figure 3 SSCD Life Cycle.

OS design and **application design** correspond to life phase 1 “Smart card software development”.

Hardware design corresponds to life phase 2 “IC development”.

Hardware fabrication OS and Application implementation correspond to life phase 3 “IC manufacturing and testing”, phase 4 “IC packaging and testing”, phase 5 “Smart card product finishing process”.

Loading of general application data and **SCD import (type 2)** corresponds to life phase 6 “Smart card personalisation”.

SCD/SVD generation and Signature creation (type 3) correspond to life phase 7 “Smart card usage”.

SSCD destruction corresponds to the end of life phase 7.

The global security requirements of the TOE mandate to consider, during the development phase, the threats to security occurring in the other phases. This is why this ST addresses the functions used in phases 6 and 7 but developed during phases 1 to 5.

The limits of the evaluation process correspond to phases 1 to 5 including the TOE under development delivery from the party responsible of each phase to the parties responsible of the following phases.

These different phases may be performed at different sites. This implies that procedures on the delivery process of the TOE must exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from phase 1 to 5 to subsequent phases, including:

Intermediate delivery of the TOE or the TOE under construction within a phase,

Delivery of the TOE or the TOE under construction from one phase to the next.

These procedures must be compliant with the security assurance requirements developed in section 5.2.

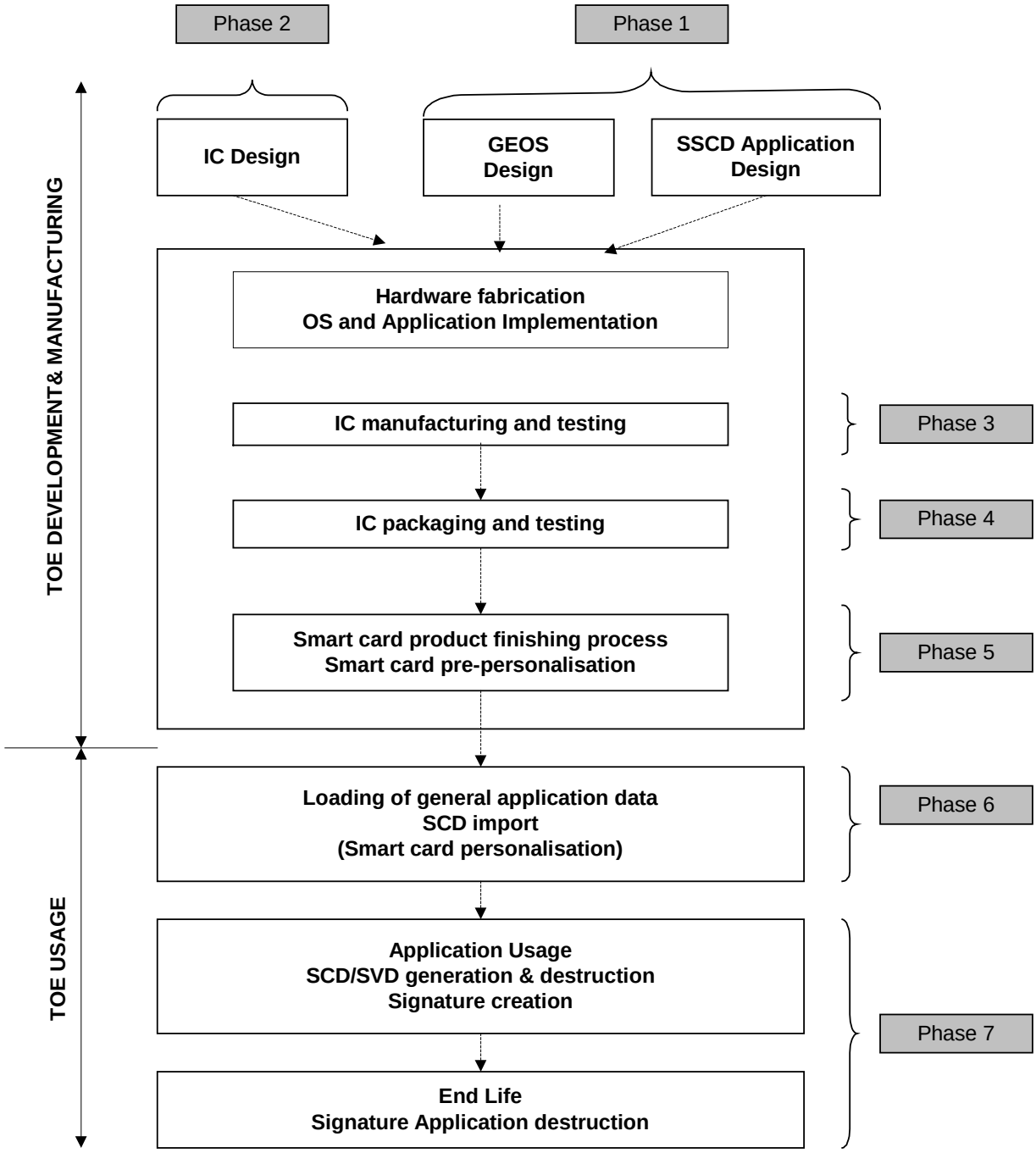

Figure 3 SSCD Life Cycle

2.3 TOE ENVIRONMENT

Considering the TOE, four types of environment are defined:

- Development and fabrication environment (phase 1 to 4),
- Initialisation environment corresponding to smart card pre-personalisation (phase 5) the loading of TOE application data and the import of the SCD (phase 6),
- User environment, during which the card generates the signatures on behalf of the end user. The

card also destructs and generates SCD/SVD pairs (phase 7),

- End of life environment, during which the TOE is made inapt for the signature creation (end of the phase 7).

2.3.1 TOE DEVELOPMENT & PRODUCTION ENVIRONMENT

The TOE described in this ST is developed in different places as indicated below:

IC design	Infineon München
Secure OS Design	Schlumberger Montrouge
SSCD Application design	Schlumberger Montrouge
IC manufacturing and Testing	Infineon München
IC packaging and testing	Schlumberger Orleans

In order to ensure security, the environment in which the development takes place must be made secure with access control tracing entries. Furthermore, it is important that all authorised personnel feels involved and fully understands the importance and the rigid implementation of the defined security procedures.

The development begins with the TOE specification. All parties in contact with sensitive information are required to abide by Non-disclosure Agreement.

Design and development of the ES then follows. The engineers use a secure computer system (preventing unauthorised access) to make the conception, design, implementation and test performances.

Storage of sensitive documents, databases on tapes, diskettes, and printed circuit layout information are in appropriately locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

Testing, programming and deliveries of the TOE then take place. When these are done offsite, they must be transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.

During the electronic transfer of sensitive data, procedures must be established to ensure that the data arrive, only at the destination and is not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies). It must also be ensured that transfer is done without modification or alteration.

During fabrication, phases 3, and 4, all the persons involved in storage and transportation operations should fully understand the importance of the defined security procedures.

Moreover, the environment in which these operations take place must be secured.

The TOE Initialisation is performed in [Infineon München phase 3 ; Orleans phase 4 & 5].

In the initialisation environment of the TOE, smart card pre-personalisation takes place (phase 5).

During smart card pre-personalisation the application data structure is created. At the end of this phase, the loader of executable files is blocked.

Initialisation requires a secure environment, which guarantees the integrity and confidentiality of operations.

2.3.2 USAGE ENVIRONMENT

In the usage environment, the personalisation takes place (phase 6). Additional data may be loaded and the SCD may be imported. Then the TOE is issued to the end User.

Once delivered to the end user (phase 7), the TOE can generate the SCD/SVD key pair. The TOE then exports the public part of the key to the Certification Authority for certification.

The TOE is owned by the end user who cannot impose strict security rules. It is the responsibility of the TOE and of the signature protocols to ensure that the signature security requirements are met.

2.3.3 END OF LIFE ENVIRONMENT.

End of life must be considered for several reasons:

The SCD can be compromised

The TOE can be stolen

The TOE physical support can come to the end of its useful life

In all these cases, it must be ensured that the TOE cannot be used any more for signature creation.

2.3.4 THE ACTORS AND ROLES

For the secure signature application, two roles have been identified, the Administrator and the Signatory.

The Administrator acts during the personalisation phase (TOE life cycle phase 6). He creates the Signatory's PIN and optionally imports the first SCD into the TOE.

The Signatory that owns the TOE is the End-User in the usage phase (phase 7). He can sign, destroy the SCD and generate a new SCD/SVD pair.

At the first usage of the TOE, the Signatory must change his PIN code before he is allowed to sign.
A new PIN is also required each time a new SCD/SVD pair is generated.

2.4 TOE INTENDED USAGE

The TOE intended usage is the Creation of Secure Signatures.

3 TOE SECURITY ENVIRONMENT

This section describes the security aspects of the environment in which the TOE is to be used.

It describes the assets to be protected, the threats, the organisational security policies and the assumptions.

3.1 ASSETS

The assets of the TOE are those defined in [PP/TYPE2], [PP/TYPE3] and [PP/BSI-0002].

The present Security Target deals with the assets of [PP/TYPE2] and [PP/TYPE3]. The assets of [PP/BSI-0002] are studied in [ST/Infineon].

Asset name	Data type	Description
D.SCD	USER DATA	SCD: private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).
D.SVD	USER DATA	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).
D.DTBS	USER DATA	DTBS and DTBS-representation: set of data, or its representation which is intended to be signed (Their integrity must be maintained).
D.VAD	TSF DATA	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 are required)
D.RAD	TSF DATA	RAD: Reference PIN code used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)
D.SSCD	TSF executable 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)
D.SIG	USER DATA	Electronic signature: (Unforgeability of electronic signatures must be assured).

3.2 ASSUMPTIONS

3.2.1 ASSUMPTIONS FROM THE PP

The Assumptions of the TOE are those defined in [PP/TYPE2], [PP/TYPE3] and [PP/BSI-0002].

The present Security Target deals with the Assumptions of [PP/TYPE2] and [PP/TYPE3]. The Assumptions of [PP/BSI-0002] are studied in [ST/Infineon].

Assumption name	Description
A.CGA	*Trustworthy certification-generation application* The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.
A.SCA	*Trustworthy signature-creation application* The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.
A.SCD_Generate	*Trustworthy SCD/SVD generation* If a party other than the signatory generates the SCD/SVD-pair of a signatory, then (a) this party will use a SSCD for SCD/SVD-generation, (b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and (c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory. (d) The generation of the SCD/SVD is invoked by authorised users only (e) The SSCD Type1 ensures the authenticity of the SVD it has created an exported

3.2.2 ADDITIONAL ASSUMPTION

Assumption name	Description
A.KEY_Secrecy	*Secrecy of the keys* The IT Environment SCA and CGA shall protect the confidentiality of the keys used for the secure communications with the TOE.

3.3 THREATS

The TOE as defined in chapter 2 is required to counter the threats described hereafter.

A threat agent wishes to abuse the assets either by functional attacks or by environmental manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.

The threats of the TOE are those defined in [PP/TYPE2], [PP/TYPE3] and [PP/BSI-0002].

The present Security Target deals with the threats of [PP/TYPE2] and [PP/TYPE3]. The threats of [PP/BSI-0002] are studied in [ST/Infineon].

Threat name	Description
T.Hack_Phys	*Physical attacks through the TOE interfaces* An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.
T.SCD_Divulg	*Storing ,copying, and releasing of the signature-creation data* An attacker can store, copy, the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.
T.SCD_Derive	*Derive the signature-creation data* An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.
T.Sig_Forgery	*Forgery of the electronic signature* An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.
T.Sig_Repud	*Repudiation of Signatures* If an attacker can successfully threaten any of the assets, then the non-repudiation of the electronic signature is compromised. This results in the signatory being 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 signature-verification data* An attacker forges the SVD presented by the TOE to the CGA. This result in loss of SVD integrity in the certificate of the signatory.
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 intended to sign.
T.SigF_Misuse	*Misuse of the signature creation function of the TOE*

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

3.4 ORGANIZATIONAL SECURITY POLICIES

The Secure Signature Creation Device usage is for advanced electronic signature. So it is mandatory to follow the organisational security policy proposed by [PP/TYPE2] and [PP/TYPE3].

OSP name.	Description
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 implements the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

4 SECURITY OBJECTIVES

The security objectives in this Security Target are those named and described in [PP/TYPE2] and [PP/TYPE3].

They cover the following aspects:

- The security objectives for the TOE,
- The security objectives for the environment.

The security objectives stated in [PP/BSI-0002] can be found in [ST/Infineon].

4.1 SECURITY OBJECTIVES FOR THE TOE

Security Objectives	Description
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 initialization, personalization and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-generation.
OT.SCD_Secrecy	*Secrecy of 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 by 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 the 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.
OT.SCD_Transfer	*Secure transfer of SCD between SSCD* The TOE shall ensure the confidentiality of the SCD transferred between SSCDs.
OT.Init	*SCD/SVD generation* The TOE provides security features to ensure that the generation of the

Security Objectives	Description
	SCD and the SVD is invoked by authorized users only.
OT.SCD_Unique	*Uniqueness of the signature-creation data* The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means the probability of equal SCDs is negligibly low.
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 by others. The TOE shall resist attacks with high attack potential.
OT.Sig_Secure	*Cryptographic security of the electronic signature* The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

This section describes the security objectives for the environment.

The IT environment of the TOE is composed of the Certification Generation Application (CGA) and the Signature Creation Application (SCA).

Security Objectives	Description
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 prove the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.
OE.SCD_Transfer	*Secure transfer of SCD between SSCD* The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type1. 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 (a) the name of the signatory controlling the TOE, (b) the SVD matching the SCD implemented in the TOE under sole control of the signatory, (c) the advanced signature of the CSP.
OE.SVD_AUTH_CGA	*CGA verifies the authenticity of the SVD* The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.
OE.HI_VAD	*Protection of the VAD* If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.
OE.SCA_Data_Intend	*Data intended to be signed*

	The SCA (a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE, (b) sends the DTBS-representation to the TOE and enables verification of the integrity of DTBS-representation by the TOE, (c) attaches the signature produced by the TOE to the data or provides it separately .
OE.KEY_Secrecy	*Secrecy of the keys* The IT Environment SCA and CGA shall protect the confidentiality of the keys used for the secure communications with the TOE.

5 IT SECURITY REQUIREMENTS

5.1 TOE IT SECURITY FUNCTIONAL REQUIREMENTS

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP/TYPE2] and [PP/TYPE3].

[PP/Infineon] deals with the security functional requirements of [PP/BSI-0002].

5.1.1 FCS: CRYPTOGRAPHIC SUPPORT

5.1.1.1 FCS_CKM cryptographic key management

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1 / RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[RSA key generation]** and specified cryptographic key sizes **[1024 bits]** that meet the **[No standard]**
FCS_CKM.1 / TDES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Triple DES key generation]** and specified cryptographic key sizes **[112 bits]** that meet the **[[VOP] Session keys]**

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[physical irreversible destruction of the stored key value]** that meets the following: **[no standard]**.

Application note (refined):
The cryptographic key SCD will be destroyed on demand of the Signatory. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

5.1.1.2 FCS_COP Cryptographic operation

FCS_COP.1 Cryptographic operation

FCS_COP.1.1/ CORRESP	The TSF shall perform **[SCD / SVD correspondence proof]** in accordance with a specified cryptographic algorithm **[RSA key computation]** and cryptographic key sizes [**1024 bits]** that meet the following**: [no standard]**.

Application note:
When the SVD is requested, it is computed using the SCD and the public exponent.

FCS_COP.1.1/ SIGNING	The TSF shall perform **[Digital signature-generation]** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[1024 bits]** that meet the following**: [PKCS #1]**.

FCS_COP.1.1/ HASH	The TSF shall perform **[DTBS Hashing]** in accordance with a specified cryptographic algorithm **[Hashing]** and cryptographic key sizes **[not applicable]** that meet the following**: [SHA-1]**.
FCS_COP.1.1/ MAC	The TSF shall perform **[MAC computation]** in accordance with a specified cryptographic algorithm **[TDES-CBC]** and cryptographic key sizes **[112 bits]** that meet the following**: [FIPS 46-3]**.

5.1.2 FDP : USER DATA PROTECTION

5.1.2.1 FDP_ACC Access Control policy

FDP_ACC.1 Subset access control

FDP_ACC.1.1/ Initialisation SFP	The TSF shall enforce the **[Initialisation SFP]** on **[Generation of SCD by User]**.
FDP_ACC.1.1/ SVD transfer SFP	The TSF shall enforce the **[SVD transfer SFP]** on **[export of SVD by User]**.
FDP_ACC.1.1/ SCD Import SFP	The TSF shall enforce the **[SCD Import SFP]** on **[Import of SCD by User]**.
FDP_ACC.1.1/ Personalisation SFP	The TSF shall enforce the **[Personalisation SFP]** on **[Creation of RAD by Administrator]**.
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]**.

5.1.2.2 FDP_ACF access control function

FDP_ACF.1 Security attribute based access control

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

Groups of security attributes [User, subject or object the attribute is associated with]	**Attributes**	**Attributes status**
General Attribute Group		
[USER]	Role	Administrator, Signatory
Initialisation attribute group		
[USER]	SCD/SVD management	Authorised / not Authorised
[SCD]	Secure SCD Import allowed	No/Yes
Signature-creation attribute group		
[SCD]	SCD operational	No/Yes
[DTBS]	Sent by an authorised SCA	No/Yes

Refinement :

The rules for specific functions that implement access control SFP defined in FDP_ACC.1 are the following:

Initialisation SFP

FDP_ACF.1.1/ Initialisation SFP	The TSF shall enforce the **[Initialisation SFP]** to objects based on **[General attribute group]** and **[Initialisation attribute group]**.
FDP_ACF.1.2/ Initialisation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Signatory" and with the security attribute "SCD / SVD management" set to " authorised" is allowed to generate SCD/SVD pair.
FDP_ACF.1.3/ Initialisation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**
FDP_ACF.1.4/ Initialisation SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.

SVD transfer SFP

FDP_ACF.1.1/ SVD transfer SFP	The TSF shall enforce the **[SVD transfer SFP]** to objects based on **[General attribute group]**
FDP_ACF.1.2/ SVD transfer SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Signatory" is allowed to export SVD.
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 rule: **[none]**.

SCD Import SFP

FDP_ACF.1.1/ SCD Import SFP	The TSF shall enforce the **[SCD Import SFP]** to objects based on **[General attribute group] 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: The user with the security attribute "role" set to "Administrator" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".
FDP_ACF.1.3/ SCD Import SFP	The TSF shall explicitly Authorise access of subjects to objects based on the following additional rules **[none]**.
FDP_ACF.1.4/ SCD Import SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: (a) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes". (b) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".

Personalisation SFP

FDP_ACF.1.1/ Personalisation SFP	The TSF shall enforce the **[Personalisation SFP]** to objects based on **[General attribute group]**
FDP_ACF.1.2/ Personalisation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute "role" set to "Administrator" is allowed to create the 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 rule: **[none]**.

Signature Creation SFP

FDP_ACF.1.1/ Signature-creation SFP	The TSF shall enforce the **[Signature-creation SFP]** to objects based on **[General attribute group]** and **[Signature-creation attribute group].**
FDP_ACF.1.2/ Signature-creation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".
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 rule: (a) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes". (b) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

5.1.2.3 FDP_ETC :Export to outside TSF control

FDP_ETC.1: 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 TSC.
FDP_ETC.1.2/ SVD transfer	The TSF shall export the user data without the user data's associated security attributes.

5.1.2.4 FDP_ITC Import From outside TSF control

FDP_ITC.1: Import of user data without security attributes

FDP_ITC.1.1/SCD	The TSF shall enforce the **[SCD Import SFP]** when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2/SCD	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3/SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[SCD shall be sent by an Authorised SSCD]**.

FDP_ITC.1.1/DTBS	The TSF shall enforce the **[Signature-creation SFP]** when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2/DTBS	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3/DTBS	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[DTBS-representation shall be sent by an Authorised SCA]**.

5.1.2.5 FDP_RIP Residual information protection

FDP_RIP.1: Subset residual information protection

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

5.1.2.6 FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1

Persistent data

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

1. SCD
2. RAD
3. SVD (if persistently stored by TOE)

FDP_SDI.2.1/ Persistent	The TSF shall monitor user data stored within the TSC for **[integrity error]** on all objects, based on the following attributes: **[integrity checked persistent stored data]**.
FDP_SDI.2.2/ Persistent	Upon detection of a data integrity error, the TSF shall : **[1. prohibit the use of the altered data** **2. inform the Signatory about integrity error.]**

DTBS-representation

The DTBS representation temporarily stored by TOE have the user data attribute “integrity checked stored data”

FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored within the TSC 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 : **[1. prohibit the use of the altered data** **2. inform the Signatory about integrity error.]**

5.1.2.7 FDP_UCT Inter-TSF user data confidentiality transfer protection

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT1.1/Receiver	The TSF shall enforce the [**SCD Import SFP, Personalization SFP and Change RAD SFP**] to be able to [**receive**] objects in a manner protected from unauthorised disclosure.
FDP_UCT1.1/ SVD Transfer	The TSF shall enforce the [**SVD Transfer SFP**] to be able to [**transmit**] objects in a manner protected from unauthorised disclosure.

5.1.2.8 FDP_UIT Inter-TSF user data integrity transfer protection

FDP_UIT.1: Data exchange integrity

SVD transfer

FDP_UIT.1.1/ SVD transfer	The TSF shall enforce the **[SVD transfer SFP]** to be able to **[transmit]** user data in a manner protected from **[modification and insertion]** errors.
FDP_UIT.1.2/ SVD transfer	The TSF shall be able to determine on receipt of user data, whether **[modification and insertion]** has occurred.

Receiver

FDP_UIT.1.1/ Receiver	The TSF shall enforce the **[SCD Import SFP, Personalization SFP, Change RAD SFP and Signature-creation SFP]** to be able to **[receive]** user data in a manner protected from **[modification, deletion and insertion]** errors.
FDP_UIT.1.2/ Receiver	The TSF shall be able to determine on receipt of user data, whether **[modification, deletion and insertion]** has occurred.

Refinement: The mentioned user data is the DTBS-representation.

5.1.3 FIA: IDENTIFICATION AND AUTHENTICATION

5.1.3.1 FIA_AFL Authentication failure

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1	The TSF shall detect when **[*3*]** unsuccessful authentication attempts occur related to **[consecutive failed authentication attempts]**.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[block RAD]**

Refinement:

When the RAD is blocked, any attempt of authentication fails.

5.1.3.2 FIA_ATD User attribute definition

FIA_ATD.1User attribute definition

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

5.1.3.3 FIA_UAU User authentication

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow **1 [Identification of the user by means of TSF required by FIA_UID.1]** **2 [Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import]** **3 [Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE]** **4 [Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

“Local user” mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

Note: The TSF shall allow no Signature generation related action to be performed before user is authenticated. That means that other actions, not specifically related to the Signature creation, may be performed before user is authenticated.

5.1.3.4 FIA_UID User Identification

FIA_UID.1Timing of identification

FIA_UID.1.1	The TSF shall allow **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]** **2 [Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE]** **3 [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.

Note: The TSF shall allow no Signature generation related action to be performed before user is identified. That means that other actions, not specifically related to the Signature creation, may be performed before user is identified.

5.1.4 FMT: SECURITY MANAGEMENT

5.1.4.1 FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behaviour

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

5.1.4.2 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1/ Administrator	The TSF shall enforce the **[Initialisation SFP]** and **[SCD Import SFP]** to restrict the ability to **[modify]** the security attributes **[SCD / SVD management and secure SCD import allowed]** to **[Administrator]**.
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

Initialisation SFP

FMT_MSA.3.1/ Initialisation SFP	The TSF shall enforce the **[Initialisation SFP]** and **[Signature-creation SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

Refinement

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

FMT_MSA.3.2/ Initialisation SFP	The TSF shall allow the **[Administrator]** to specify alternative initial values to override the default values when an object or information is created.

SCD Import SFP

FMT_MSA.3.1/ SCD Import SFP	The TSF shall enforce the **[SCD Import SFP]** and **[Signature-creation SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

Refinement

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

FMT_MSA.3.2/ SCD Import SFP	The TSF shall allow the **[Administrator]** to specify alternative initial values to override the default values when an object or information is created.

5.1.4.3 FMT_MTD Management of TSF data

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1/ Signatory	The TSF shall restrict the ability to **[modify] [no other operation]** the **[RAD]** to **[Signatory]**.

Note: RAD being the PIN code, RAD and VAD are the same data.

5.1.4.4 FMT_SMR Security management roles

FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles **[Administrator]** and **[Signatory]**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

5.1.5 FPT: PROTECTION OF THE TSF

5.1.5.1 FPT_AMT Underlying Abstract machine test

FPT_AMT.1 Underlying Abstract machine test

FPT_AMT.1.1	The TSF shall run a suite of tests **[*during initial start-up*]** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Refinement:

In this document, the underlying abstract machine test is the IC and its library.

5.1.5.2 FPT_EMSEC TOE Emanation

FPT_EMSEC.1.1 TOE Emanation

FPT_EMSEC.1.1	The TOE shall not emit **[Side channel current]** in excess of **[State of the art limits]** enabling access to [**RAD and SCD**].

Notes:

This SFR is an extension to [CC-2].

State of the art limits are the limits currently expected for IC meeting EAL4+ level of security.

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

5.1.5.3 FPT_FLS Failure secure

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur **:[power shortage, over voltage, over and under clock frequency, integrity problems].**

5.1.5.4 FPT_PHP TSF physical Protection

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.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1	The TSF shall resist **[clock frequency, voltage tampering and penetration of protection layer]** to the **[integrated circuit]** by responding automatically such that the TSP is not violated

5.1.5.5 FPT_TST TSF self test

FPT_TST.1 TSF testing

FPT_TST.1.1	The TSF shall run a suite of self-tests **[during initial start-up or when calling a sensitive module]** to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.6 FTP: TRUSTED PATH / CHANNEL

5.1.6.1 FTP_ITC Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted Channel

FTP_ITC.1.1 SCD import	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 SCD import	The TSF shall permit **[the remote trusted IT product]** to initiate communication via the trusted channel.
FTP_ITC.1.3 SCD import	The TSF shall initiate communication via the trusted channel for **[SCD import]** Refinement: The mentioned remote trusted IT product is a SSCD of type 1.
FTP_ITC.1.1 SVD transfer	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 SVD transfer	The TSF shall permit [***the remote trusted IT product***] to initiate communication via the trusted channel.
FTP_ITC.1.3 SVD transfer	The TSF shall initiate communication via the trusted channel for **[SVD transfer]** Refinement: The mentioned remote trusted IT product is a CGA.
FTP_ITC.1.1 DTBS import	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 DTBS import	The TSF shall permit **[the remote trusted IT product]** to initiate communication via the trusted channel.
FTP_ITC.1.3 DTBS import	The TSF shall initiate communication via the trusted channel for **[signing DTBS-representation]** Refinement: The mentioned remote trusted IT product is a SCA.

5.1.6.2 FTP_TRP Trusted path

FTP_TRP.1 Trusted path

FTP_TRP.1.1	The TSF shall provide a communication path between itself and **[local]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2	The TSF shall permit **[*local users*]** to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for **[initial user authentication][no other service].**

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

The Assurance requirements is EAL 4 augmented by components :

ADV_IMP.2 : Implementation of the TSF,

ALC_DVS.2 : Sufficiency of security measures,

AVA_MSU.3 : Analysis of insecure states,

AVA_VLA.4 : Highly resistant.

5.2.1 CONFIGURATION MANAGEMENT (ACM)

EAL4 augmented claimed level requires the following ACM class components:

ACM_AUT.1 Partial CM automation

ACM_CAP.4 Generation support and acceptance procedures

ACM_SCP.2 Problem tracking CM coverage

Refer to CC Part 3 for description.

5.2.2 DELIVERY AND OPERATION (ADO)

EAL4 augmented claimed level requires the following ADO class components:

ADO_DEL.2 Detection of modification

ADO_IGS.1 Installation, generation, and start-up procedures

Refer to CC Part 3 for description.

5.2.3 DEVELOPMENT (ADV)

EAL4 augmented claimed level requires the following ADV class components:

ADV_FSP. 2 Fully defined external interfaces

ADV_HLD. 2 Security enforcing high level design

ADV_IMP.2 Implementation of the TSF

ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ADV_SPM.1 Informal TOE security policy model

Refer to CC Part 3 for description.

5.2.4 GUIDANCE DOCUMENTS (AGD)

EAL4 augmented claimed level requires the following AGD class components:

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Refer to CC Part 3 for description.

5.2.5 LIFE CYCLE SUPPORT (ALC)

EAL4 augmented claimed level requires the following ALC class components:

ALC_DVS.2 Sufficiency of security measures

ALC_LCD.1 Developer defined life-cycle model

ALC_TAT.1 Well-defined development tools

Refer to CC Part 3 for description.

5.2.6 TESTS (ATE)

EAL4 augmented claimed level requires the following ATE class components:

ATE_COV.2 Analysis of coverage

ATE_DPT.1 Testing high level design

ATE_FUN.1 Functional testing

ATE_IND.2 Independent testing- sample

Refer to CC Part 3 for description.

5.2.7 VULNERABILITY ASSESSMENT (AVA)

EAL4 augmented claimed level requires the following AVA class components:

AVA_MSU.3 Analysis and testing of insecure states

AVA_SOF.1 Strength of TOE security function evaluation

AVA_VLA.4 Highly resistant

Refer to CC Part 3 for description.

5.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

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

These requirements are as stated in [PP/TYPE2] & [PP/TYPE3].

5.3.1 CERTIFICATION GENERATION APPLICATION SECURITY REQUIREMENTS :

FCS_CKM.2: Cryptographic key distribution

FCS_CKM.2.1/ CGA	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method qualified certificate that meets the following: [**Triple DES 112 bits**].

FCS_CKM.3: Cryptographic key access

FCS_CKM.3.1/ CGA	The TSF shall perform import of the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following: [**no standard**].

FDP_UIT.1: Data exchange integrity

FDP_UIT.1.1/ SVD import	The TSF shall enforce the SVD transfer SFP to be able to receive user data in a manner protected from modification and insertion errors.
FDP_UIT.1.2/ SVD import	The TSF shall be able to determine on receipt of user data, whether modification and insertion has occurred.

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1/ SVD import	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SVD import	The TSF shall permit [the TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3/ SVD import	The TSF shall initiate communication via the trusted channel for SVD import .

5.3.2 SIGNATURE CREATION APPLICATION SECURITY REQUIREMENTS

FCS_COP.1: Cryptographic operations

FCS_COP.1.1/ SCA Hash	The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm [SHA_1] and cryptographic key sizes none that meet the following: [FIPS PUB 108-1 , length=160 bits]

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1/ SCA DTBS	The TSF shall enforce the Signature-creation SFP to be able to transmit user data in a manner protected from modification, deletion and insertion errors.
FDP_UIT.1.2/ SCA DTBS	The TSF shall be able to determine on receipt of user data, whether modification, deletion and insertion has occurred.

FTP_ITC.1 Inter TSF trusted channel

FTP_ITC.1.1/ SCA DTBS	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SCA DTBS	The TSF shall permit the TSF to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCA DTBS	The TSF shall initiate communication via the trusted channel for signing DTBS-representation by means of the SSCD.

FTP_TRP.1 Trusted path

FTP_TRP.1.1/ SCA	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ SCA	The TSF shall permit **[the TSF]** to initiate communication via the trusted path.
FTP_TRP.1.3/ SCA	The TSF shall require the use of the trusted path for **[initial user authentication]**.

5.4 SECURITY REQUIREMENTS FOR THE NON-IT ENVIRONMENT

R.Administrator_Guide *Application of Administrator Guidance*

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

R.Sigy_Guide *Application of User Guidance*

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

R.Sigy_Name *Signatory’s name in the Qualified Certificate*

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

6 TOE SUMMARY SPECIFICATION

6.1 STATEMENT OF TOE SECURITY FUNCTIONS

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

This ST deals with the application security functions that reply to the SFR defined previously.

The security functions that reply to the SFR of the IC are described in [ST/Infineon].

This document shows how the SF of this ST relies on the SF of [ST/Infineon].

6.1.1 BASIC SECURITY FUNCTIONS

SF.TEST - Self test

When starting a work session, the TSF tests the RAM, the IC and its environment. When required, the TSF tests the integrity of EEPROM and random number generator.

Upon detection of an anomaly, the TSF ends the working session.

SF.EXCEPTION - Error Messages and exceptions

The TOE reports the errors on Message format, Integrity, range of environment conditions, Life cycle status.

Upon detection of a fault that could lead to a potential security violation, the card enters a secure Fail State. In this state, the card is mute.

SF.ERASE - Destruction of data

The TOE erases its working memory when starting a working session and before allocation/deallocation of sensitive data.

The TOE destroys the cryptographic keys.

SF.INTEGRITY - Data Integrity

The TOE checks the integrity of the cryptographic keys, the authentication data, the DTBS-representation.

If an integrity error is found, an error flag is issued, the corresponding data is made unavailable and the corresponding operation is aborted.

SF.HIDE - Data and operation hiding

TOE shall hide sensitive data transfers and operations from outside observations.

SF.CARD_MGR - Card manager

This function controls the execution of the card internal process corresponding to management command messages sent by the user to the card. The messages that it handles are defined as specified in ISO 7816.

This SF analyses the format of the command and the consistency of the instruction code and the P1/P2/P3 parameters

This SF checks that the command sequence is respected and that the command is allowed in the current TOE life phase.

This SF executes the command.

6.1.2 CRYPTOGRAPHIC RELATED FUNCTIONS

SF.KEY_GEN - Key generation

The TOE generates the key pair for Secure Signature: RSA 1024 bits

When required, The TOE generates the SVD, using the SCD and the public exponent.

The TOE generates the Session keys, triple DES with 2 keys, according to the VOP standard.

The strength of this function is SOF_High.

SF.SIG - Signature creation

The TOE signs a hash of data imported from outside or resident in the card, using an RSA 1024 bit private key and conforming to PKCS#1.

The signature function has an access condition based upon previous authentication of user.

The strength of this function is SOF_High.

SF.HASH - Message hashing

The TOE generates a hashing of both internal data and data imported from outside, using SHA_1. The TOE can complete the hashing process on importation of data and of intermediate hash result.

The strength of this function is SOF_High.

SF.MAC - MAC generation and verification

This SF generates and verifies a MAC, using Triple DES with 2 keys.

The strength of this function is SOF_High.

SF.TRUSTED - Trusted Path

This function establishes a secure channel.

It checks the candidate authenticity with a mutual authentication using a cryptogram based on MAC. A ratification counter limits the number of authentication attempts.

This function encrypts, and decrypts messages transmitted via the secure channel.

TOE deciphers keys imported from outside the TOE.

Encipher & decipher operations use triple TDES with 2 keys.

The strength of this function is SOF_High.

SF.PIN - PIN management

This SF controls all the operations relative to the PIN management, including the Cardholder (signatory) authentication i.e. PIN creation, PIN verification, Cardholder authentication and PIN modification.

The strength of this function is SOF_High.

6.1.3 SECURITY MANAGEMENT FUNCTIONS

SF.ACC - Access Authorisation

The function checks that the access conditions are met before allowing the following operations:

- Generation of SCD and creation of RAD by Administrator;
- Modification of RAD, Transfer of SVD and Signature of DTBS by Signatory,

SF.PHASE - Life Phase Control

This SF ensures the management of the TOE life cycle as defined in paragraph 2.2. The TOE checks the integrity of the life cycle status, determines the current state and phase, changes to the requested state and changes to the next phase if required. The change of phase is irreversible.

6.1.4 IDENTIFICATION AND AUTHENTICATION FUNCTIONS

SF.ATTRI - User attribute definition

This SF maintains the following list of security attributes:

Attributes	values
Role	Administrator/signatory
SCD/SVD management	Authorized /Not Authorized
SCD Secure Import allowed	Yes/No
SCD Operational	Yes/No
DTBS Sent by an Authorised SCA	Yes/No

Table 1- User attributes

6.1.5 PHYSICAL MONITORING

SF.DRIVER - Chip driver

This SF ensures the management of the chip security features. It starts the state analysis, records and audits events, performs shield actions according to violation severity and controls random clock generation.

SF.ROLLBACK - Safe fail state recovery

This SF ensures that the TOE returns to its previous secure state when one of the following events occurs: Power shortage, overvoltage, Out of range clock frequency and integrity error.

7 PP CLAIMS

The PP [PP/TYPE2], [PP/TYPE3] and [PP/BSI-0002] are claimed.

END OF SECURITY TARGET