CEN

WORKSHOP

AGREEMENT

CWA 14169

March 2004

ICS 35.160; 35.040; 35.100.05

Supersedes CWA 14169:2002

English version

Secure signature-creation devices “EAL 4+”

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

© 2004 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No.:CWA 14169:2004 E

Contents

Foreword

Successful implementation of European Directive 1999/93/EC on a Community framework for electronic signatures [Dir.1999/93/EC] requires standards for services, processes, systems and products related to electronic signatures as well as guidance for conformity assessment of such services, processes, systems and products.

In 1999 the European ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players, to create the European Electronic Signature Standardisation Initiative (EESSI).

Within this framework the Comité Européen de Normalisation / Information Society Standardisation System (CEN/ISSS) and the European Telecommunications Standards Institute / Electronic Signatures and Infrastructures (ETSI/ESI) were entrusted with the execution of a work programme to develop generally recognized standards to support the implementation of [Dir.1999/93/EC] and development of a European electronic signature infrastructure.

The CEN/ISSS Workshop on electronic signatures (WS/E-SIGN) resulted in a set of deliverables, CEN Workshop Agreements (CWA), which contributed towards those generally recognized standards. The present document is one such CWA.

This version of this CWA was published 2004-03.
A list of the individuals and organizations which supported the technical consensus represented by this CEN Workshop Agreement is available to purchasers from the CEN Central Secretariat.

Introduction

This document defines security requirements for SECURE SIGNATURE-CREATION DEVICES (SSCD) in accordance with the Annex III of the “DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures” (EU Directive).

The aim of the effort to standardise the security requirements for SSCDs is to ensure their conformity with the EU Directive and their mutual interoperability. Such requirements need to be as technology neutral as possible. Following this approach the presented CWA tries to cover as many different SSCD implementations as possible according to the current technology status. The CWA shall be updated regularly as technology develops to allow for future developments to be considered.

Although different SSCD implementations may vary to some extent, this approach is structured to cover the functionality around the signature-creation data (SCD, private key) as depicted in **Figure 1**.

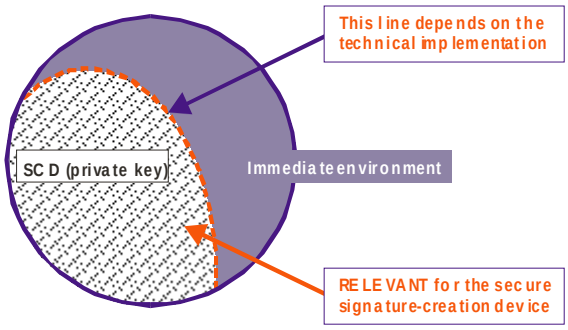


Figure 1: SSCD and its immediate environment

The presented CWA defines three Protection Profiles (PP) according to the Common Criteria (CC [cc211-cc213]) for a SSCD containing SCD and relating to signature-verification data (SVD) in the corresponding certificate.

To cope with the requirements defined in Annex III of the EU Directive, security requirements have to be specified and fulfilled also for elements which represent components or mechanisms within the immediate environment of the SSCD. Such components or mechanisms shall be clearly identified during the evaluation process.

The document formulates general security requirements and assumptions. However, detailing such requirements is left to the particular implementation and its environment. An implementation of a SSCD is considered valid if it complies with the requirements of this PP. Evaluation of conformity will be carried out as necessary to demonstrate the compliance. This procedure shall enable maximum flexibility for industry in developing SSCDs which meet the security requirements laid down in Annex III of the EU Directive.

1 Scope

This document specifies the security requirements for a SSCD which is the TOE. It is formulated as three Protection Profiles (PPs) following the rules and formats of the Common Criteria [cc211]. SSCDs are mandatory for implementing signatures fulfilling the requirements of Article 5.1 of the EU Directive. Therefore, the use of such devices should be made evident. Visible signs making compliance evident are useful and contribute to confidence in products but are not covered by this document.

Application of devices conforming to this standard shall require appropriate and adequately secure environment as set out in the requirements of the PPs. The PPs are an integral part of this document and included as normative Annexes A, B and C. The Protection Profiles themselves have been evaluated according to Common Criteria and certified by BSI, Germany. The Protection Profiles have been registered as follows:

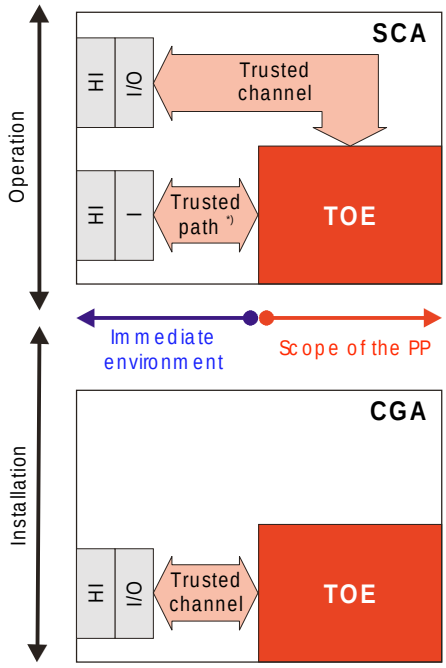
Protection Profile - Secure Signature-Creation Device Type 1, Version 1.05	EAL 4+ BSI-PP-0004-2002 03.04.2002
Protection Profile - Secure Signature-Creation Device Type 2, Version 1.04	EAL 4+ BSI-PP-0005-2002 03.04.2002
Protection Profile - Secure Signature-Creation Device Type 3, Version 1.05	EAL 4+ BSI-PP-0006-2002 03.04.2002

After the evaluation and certification of the Protection Profiles, a number of small errors have been found, which are described in chapter 5 of the CWA. These errors do not have any substantial significance for the Protection Profiles, but should be taken into account by anyone writing a Security Target based on the Protection Profiles.

This document is applicable to determining conformance of SSCDs with the regulations set out in laws of the member states specifying security requirements of SSCDs. The document is also applicable to SSCDs consisting of more than one component. This is, for example, the case when the SCD are created within one component (e.g. a key generation device) and transferred to another component (e.g., a smart card). In such scenarios the key generation device also “implements” the SCD according to the definition from the EU Directive and thus forms part of the SSCD.

The document is also applicable to signature-creation devices at a certification-service-provider (CSP) when creating signatures for certification services (e.g., signing certificates, timestamping, signing directories and revocations).

The scope of the PP (i.e., the TOE) is illustrated in Figure 2. The TOE is represented by the SSCD including SCD/SVD generation, SCD storage, and signature-creation functionality. Although it is possible that the TOE includes additional functionality, such as the signature-creation application (SCA) or the certification generation application (CGA), the PP assumes the SCA to be part of the immediate environment of the TOE.



*) The trusted path will be required if the HI is not provided by the TOE itself (e. g., it is provided by a SCA outside the SSCD).

Figure 2: Scope of the PP

Following the principles of the EU Directive on electronic signatures the PPs contained in this document are as technology neutral as possible and thus covers a wide area of possible devices to be used as SSCDs fulfilling the requirements laid down in Annex III of the EU Directive. A separate document [CWA 14355] gives guidelines for the implementation of SSCDs on different platforms.

The SSCD security requirements also include a minimum set of requirements to be fulfilled by the signature algorithms and their parameters allowed for use with SSCDs. A separate document [ALGO] defines an initial set of algorithms and corresponding parameters to be included in a list of approved methods for producing or verifying Electronic Signatures in Secure Signature-Creating Devices (SSCD).

2 References

2.1 Normative References

[Dir.1999/93/EC] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures.

[cc211] International Organization for Standardization, ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model, 1999.

[cc212] International Organization for Standardization, ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements, 1999.

[cc213] International Organization for Standardization, ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements, 1999.

2.2 Informative References

[ALGO] ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures V1.1.1 (2003-03).

[CWA 14355] CEN CWA 14355: Guidelines for the Implementation of Secure Signature-Creation Devices.

3 Definitions and abbreviations

3.1 Definitions

All relevant definitions are given in Annexes A, B and C (Protection Profiles).

3.2 Abbreviations

CC	Common Criteria Version 2.1
CGA	Certification Generation Application
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
HI	Human Interface
HW	Hardware
I/O	Input/Output
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

4 Security requirements of secure signature-creation devices

4.1 Signature-creation

The present document assumes a well defined signature-creation process to take place. The signature-creation process is specified in a separate CWA. The present document defines three possible SSCD implementations, referred to as 'SSCD types', as illustrated in **Figure 3**.

The left part of **Figure 3** shows two SSCD components: A SSCD of Type 1 representing the SCD/SVD generation component, and a SSCD of Type 2 representing the SCD storage and signature-creation component. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel.

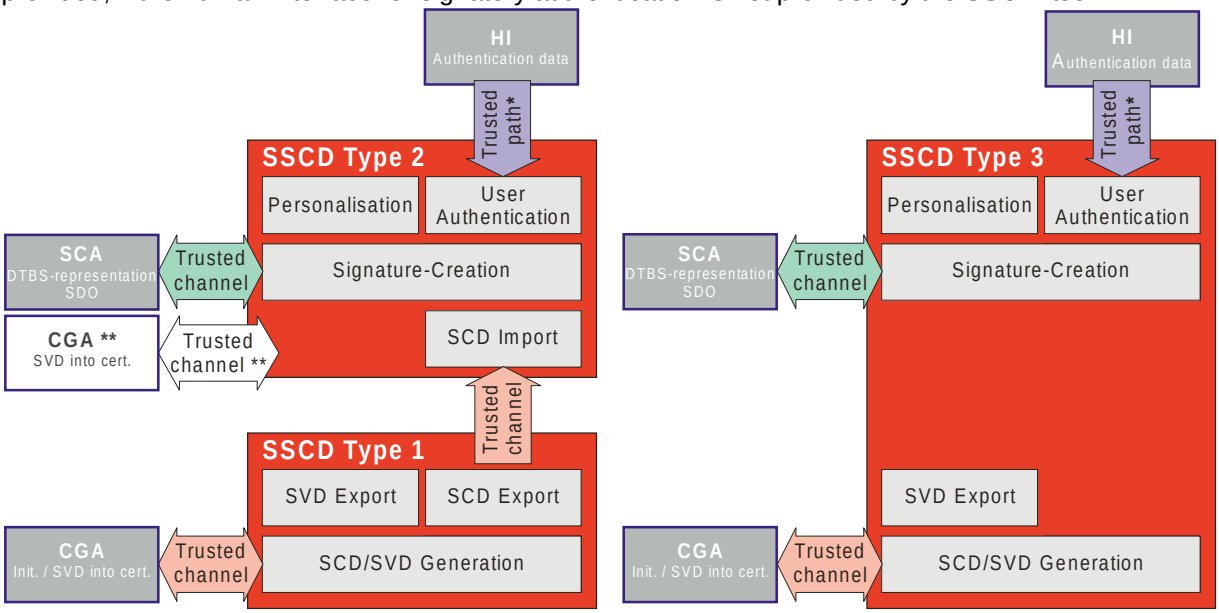
The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be transferred by the SCA to the SSCD only over a trusted channel. The same shall apply to the signed data object (SDO) returned from a SSCD Type 2 to the SCA.

SSCD Type 2 is a personalized component which means that it can be used by one specific user only (e.g., a smart card). This user must therefore first be authenticated in that he sends his authentication data (e.g., a PIN) to the SSCD Type 2. If the human interface (HI) for such signatory authentication is not provided by the SSCD, a trusted path (e.g., a encrypted channel) between the SSCD and the SCA implementing to HI is to be provided. If the SSCD Type 2 holds the SVD and exports the SVD to a CGA for certification, a trusted channel is to be provided.

SSCD Type 1 is not a personalized component in the sense that it may be used by a specific user only, but the SCD/SVD generation and export shall be initiated by authorized persons only (e.g., system administrator).

The right part of **Figure 3** shows a SSCD consisting of one part, SSCD Type 3 (e.g., a personal digital assistant PDA). SSCD Type 3 is analogous to a combination of Type 1 and Type 2, but no exporting of the SCD is provided.

The SVD shall be exported by a SSCD Type 1 or a SSCD Type 3 to the CGA over a trusted channel. The CGA initiates SCD/SVD generation ("Init.") and the SSCD exports the SVD for generation of the corresponding certificate ("SVD into cert."). As for the type 2 component, a trusted path to the SCA is provided, if the human interface for signatory authentication is not provided by the SSCD itself.



* The trusted path for user authentication will be required if the HI is not provided by the TOE itself (e. g., it is provided by a SCA outside the SSCD)

** The trusted channel between the SSCD Type 2 and the CGA is required for cases where the SSCD type 2 holds the SVD and export of the SVD to the CGA for certification is provided.

Figure 3: SSCD types and modes of operation

Figure 4 shows the PP scope from the structural perspective. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the SCD/SVD generation, SCD storage and use, and signature-creation functionality. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE. They shall communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively.

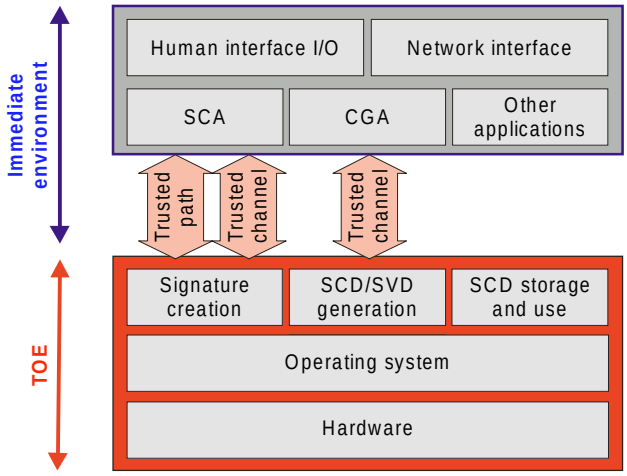


Figure 4: Scope of the PP, structural view

The TOE life cycle is shown in Figure 5. Basically, it consists of a development phase and the operational phase. This document refers to the operational phase which starts with personalisation including SCD/SVD generation and SCD import if necessary. This phase represents installation, generation, and start-up in the CC terminology [cc212]. The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., SCD storage and SCD use). The life cycle ends with the destruction of the SSCD.

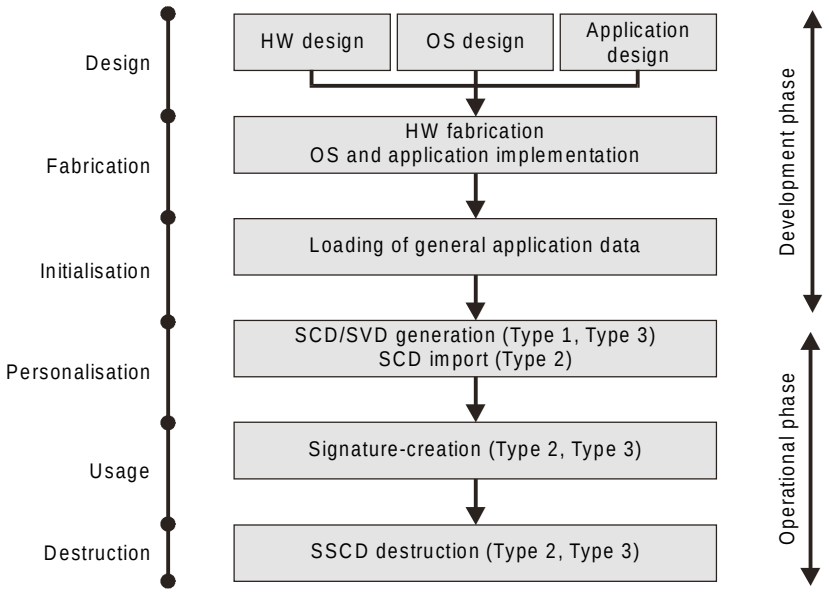


Figure 5. SSCD life cycle

4.2 Protection profile for secure signature-creation devices

The Protection Profiles are given as Annexes A, B and C to this document because they must follow a well-defined format. The Common Criteria [cc211] provides a well defined format for PPs which has been followed in structuring Annexes A, B and C.

The PPs are addressing the SSCD types, as illustrated in Figure 3. A SSCD Type 3 combines the major tasks of a SSCD (i.e., signature-creation and SCD/SVD generation). This approach allows for the

minimum set of measures to be taken in order to meet the general security requirements as set out in the EU Directive.

When a SSCD is deploying Type 2 (i.e., not Type 3) additional security functionality for the generation of the imported SCD is required. The PP as defined in Annex A (Type°1) is applicable in that case.

4.3 Scope of SSCD Protection Profile application

The SSCD PPs given in Annexes A, B and C refer to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is implemented by the TOE.

While the main application scenario of a SSCD will assume such a qualified certificate to be used in combination with a SSCD, there still is a large benefit in the security when such SSCD is applied in other areas and such application is encouraged. The SSCD PPs may as well be applied to environments where the certificates expressed as 'qualified certificates' in the SSCD PPs do not fulfil the requirements laid down in Annex I and Annex II of the EU Directive.

With this respect the notion of qualified certificates in the PPs refers to the fact that when an instance of a SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive, article 5, paragraph 1. As a consequence, this standard does not prevent a device itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

4.4 Requirements for signature algorithms and their parameters

Algorithms for secure electronic signature devices are to some extent independent from the device itself. The security requirements and assumptions are clearly separated and in general of a very different nature than those relevant to the device itself. Approved algorithms and parameters for SSCDs are addressed by a separate document.

The list of approved algorithms and parameters is relevant to the security requirements of the SSCD, the trusted systems of the CSP, and the signature-creation environment and the signature-verification environment. The cryptographic algorithms supported by the SSCD are part of the TOE’s security functional requirements addressed by the PPs. The relevant CC functional requirements classes are cryptographic support (FCS) including families cryptographic key management (FCS_CKM) and cryptographic operation (FCS_COP) [cc212]. The PPs shall specify the functional requirements from this class, so that a certification report shall identify the supported cryptographic algorithms and show that they satisfy the requirements.

4.5 Evaluation assurance level of the SSCD Protection Profile

The CC evaluation assurance level (EAL) [cc213] defined in the SSCD PPs is EAL4 augmented with strength of function (SOF) high. The augmentations are as follows:

Vulnerability assessment:	AVA_MSU.3	(analysis and testing of insecure states)
Vulnerability assessment:	AVA_VLA.4	(highly resistant)

4.6 Protection Profile Review

The Secure Signature-Creation Device Protection Profiles (SSCD-PP) are in the normative Annexes A, B and C of this CWA. They shall be subject to periodic review in order to adapt the CWA to technological progresses.

5 List of corrections to the Protection Profiles

5.1 Common corrections

The security functional requirements FCS_CKM.1 (Type 1 and Type 3), FCS_CKM.2/ CGA, FCS_COP.1/SIGNING (Type 2 and 3) FCS_COP.1/SCA_HASH (Type 2 and 3), FCS_COP.1/CORRESP assign the list of standards to a List of approved algorithms and parameters. The protection profiles refer under [5] to "Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the Directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive". The security target writer should instead consult [ALGO], the national certification body and the designated body according to the Directive 1999/93/EC, article 3, paragraph 4, for advice which algorithms and parameters that are approved to fulfil the protection profile.

Note that a protection profile conformance claim is required to include all security objective and all security requirements defined in the protection profile in the security target (for details see Common Criteria, part 1, section C.2.8). The corrigenda addresses errors in the protection profile parts outside the security objective and all security requirements which a security target writer like to reuse from the Protection profile text.

Document part	Correction	Comment
Foreword	CONTACT ADDRESS CEN/ISSS Secretariat	Misprint (instead of "CEC")
Terminology: CEN Workshop Agreement	This Protection Profile represents an Annex to the CWA...	All PPs represent different Annexes.
Terminology, p. 2, Signature-creation application, bullet b	b) to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intent to sign,	Misprint (instead of "intend")
section 2.2, 5th paragraph	"The TOE implements all" shall read "functionality which **is** necessary"	Grammatical error
section 3, paragraph S.OFFCARD	The attacker has a high attack potential and knows no secret.	Replace "high level potential attack" by "high attack potential" (as official term see CEM Annex B, section 8.1)
section 3.2, T.SCD_Derive	An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.	Misprint (instead of "public")
section 3.2 T.Sig_Repud	If an attacker can successfully threaten any of the assets, then the non-repudiation of the electronic signature is compromised.	Misprint (instead of "non repudation")
section 4.1, OT.SCD_Unique	In that context 'practically occur once' means that the probability of equal SCDs is negligible.	Instead of "In that context 'practically occur once' means that the probability of equal SCDs is negligible low."
section 5.2, table 5.1	Table 5.1 Assurance Requirements: EAL4 augmented by AVA_MSU.3	The table 5.1 shows correctly the assurance requirements

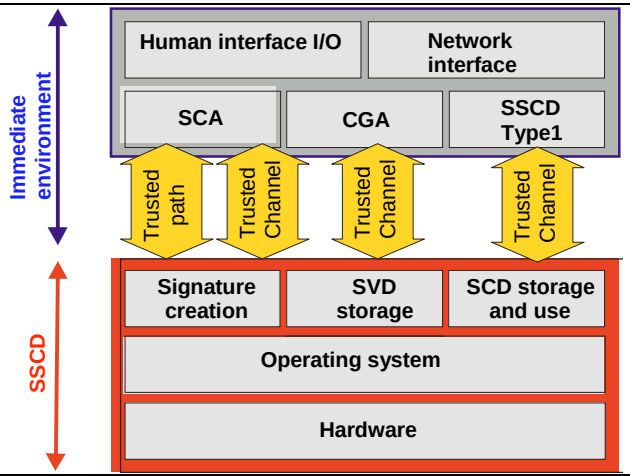
Document part	Correction	Comment
	and AVA_VLA.4	which are EAL4 augmented by AVA_MSU.3 and AVA_VLA.4.
section 6.4.2 FCS_CKM.3/ CGA	The CGA imports SVD via trusted channel implemented by FTP_ITC.1/ SVD import.	Misprint (instead of “cannel”)

5.2 Corrections for PP SSCD Type 1 - BSI-PP-0004-2002

Document part	Correction	Comment
Section 2.2	Paragraph starting "Figure 2 shows...": Delete "and signature-creation functionality".	Not correct for Type 1
section 3.2 T.Sig_Repud	The signatory is able to deny to have signed data using the SCD in the SSCD Type 2 or Type 3 under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.	The TOE is a SSCD Type 1 which does not generate signatures.
section 5.3.1.4 FTP_ITC.1.3/ SVD Transfer	Refinement: The mentioned remote trusted IT product is a SSCD of type 1 for SVD import and the CGA for the SVD export.	Misprint (remove “.” between “type 1” and “for”).
section 5.3.1.4 FTP_ITC.1.3/ SVD Transfer	Application Note: Change "TOE" to "SSCD Type 2".	

5.3 Corrections for PP SSCD Type 2 - BSI-PP-0005-2002

Document part	Correction	Comment
section 2.2	Consequently, there is an interdependence where a SSCD Type 1 constitutes the environment of the TOE.	Misprint (substitute “,” by “.”).
Section 2.2	Paragraph starting with "Figure 2 shows....": Delete "SCD/SVD generation".	Type 2 does not generate SCD/SVD.

Document part	Correction	Comment
section 2.2, figure 2		The TOE does not generate SCD/SVD pair but receives the SCD from SSCD Type 1 in the TOE environment.
section 6.2.1, table 6.1	Change column title OE_SCD_Unique to OE.SCD_Unique	Misprint
section 6.2.1, table 6.1	Add a “x” in row T.Sig_Repud and column OE.SCD_Unique	The rationale in section 6.2.2.2, paragraph T.Sig_Repud, explains that the TOE environment (i.e. the SSCD Type 1) ensures that the signatory’s SCD can practically occur just once.
section 6.2.2.2, paragraph T.SCD_Divulg, last sentence	OT.SCD_Transfer and OE.SCD_Transfer ensures the confidentiality of the SCD transferred between SSCDs.	Misprint (“ensures” occurs twice)
section 6.2.2.2, paragraph T.Sig_Forgery	This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp / OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.SCD_Transfer in combination with OE.SCD_Transfer (Secure transfer of SCD between SSCD), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows: … The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp,	The threat T.Sig_Forgery may be performed by a certificate assigned to the signatory for a SVD which does not correspond to the SCD in the SSCD of the signatory. This is addressed by security objectives protecting the SCD transfer from SSCD Type 1 to SSCD Type 2 and checking the SCD/SVD correspondence e.g. before the certificate will be generated. OT.SCD_Transfer and OE.SCD_Transfer work together to ensure secure transfer of SCD between these SSCD. OE.SCD_SVD_Corresp address the checking the correspondence by the SSCD Type 1 generating the SCD/SVD pair and sending the SCD to the TOE and CGA. OT.SCD_SVD_Corresp address the checking the correspondence of the stored SCD with the received SVD.

Document part	Correction	Comment
	OE.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process.	
section 6.2.2.2, paragraph T.Sig_Repud	This threat is in general addressed by OE.CGA_QCert (Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp / OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), OE.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Transfer in combination with OE.SCD_Transfer (Secure transfer of SCD between SSCD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity). OE.SCD_Unique provides that the signatory's SCD can practically occur just once.	Misprint, replace "OT.SCD_Unique" by "OE.SCD_Unique". OT.SCD_Transfer and OE.SCD_Transfer work together to ensure secure transfer of SCD from the SSCD Type 1 to SSCD Type 2 to prevent discloser and manipulation of the SCD. OE.SCD_SVD_Corresp address the checking the correspond-dence by the SSCD Type 1 generating the SCD/SVD pair and sending the SCD to the TOE and CGA. OT.SCD_SVD_Corresp address the checking the correspondence of the stored SCD with the received SVD.

5.4 Corrections for PP SSCD Type 3 - BSI-PP-0006-2002

Document part	Correction	Comment
section 6.2.2.2 T.Sig_Forgery	OT.Sig_Secure, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD.	Remove "OT.SCD_Transfer" which is not defined in the PP SSCD Type 3 because no SCD is transferred.

—— this page was intentionally left blank ——

Annex A

This Annex A, with the exception of its pagination, is deemed to be identical to the PP that has been certified by BSI and which is available at http://www.bsi.de/cc/pplist/PP0004b.pdf.

Nevertheless, in case of any discrepancies between the PP available from the BSI web-site and the PP in this Annex A, it is the PP published by BSI that is the normative one.

Protection Profile — Secure Signature-Creation Device Type1

Version: 1.05, EAL 4+

Saterday, 28 July 2001

Prepared By: ESIGN Workshop - Expert Group F

Prepared For: CEN/ISSS

Note: **This Protection Profile (PP) has been prepared for the European Electronic Signature Standardisation Initiative EESSI by CEN/ISSS area F on secure signature-creation devices (SSCDs). In its present form it represents one of two documents that the CEN/ISSS E-Sign Workshop decided at its Brussels meeting 21st November 2000 to forward to the EESSI Steering Committee—one defining evaluation assurance level *EAL 4 augmented* and one defining *EAL 4*.**

The actual PP is EAL 4 augmented by AVA_VLA.4 and AVA_MSU.3, strength of function high.

Foreword

This ‘Protection Profile — Secure Signature-Creation Device’ is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) Electronic Signatures (E-SIGN) workshop. The document represents Annex A of the CEN/ISSS workshop agreement (CWA) on secure signature-creation devices.

The document is for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

The document has been prepared as a Protection Profile (PP) following the rules and formats of ISO 15408, as known as the Common Criteria version 2.1 [2] [3] [4].

The set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is given in a separate document in [5].

Correspondence and comments to this secure signature-creation device protection profile (SSCD-PP) should be referred to:

CONTACT ADDRESS

CEC/ISSS Secretariat
Rue de Stassart 36
1050 Brussels, Belgium

Tel +32 2 550 0813
Fax +32 2 550 0966

Email isss@cenorm.be

—— this page was intentionally left blank ——

Revision History

v1.0-draft	22.09.00	submitted to CEN/ISSS WS/E-Sign Workshop
v1.0-final	16.11.00	for ballot by WS/E-Sign at Brussels meeting (11/00)
v1.0, EAL4+	28.11.00	for submission to European Commission by EESSI
v1.01, EAL4+	01.02.01	for ballot by WS/E-Sign at Brussels meeting (12/01)
v1.02, EAL4+	14.02.01	for ballot by WS/E-Sign as decided at Brussels meeting.
V1.03-EAL4+	15.06.01	Type1 PP extracted from SSCD approved by WS/E-Sign ballot to comply with the request of the evaluator.
V1.04-EAL4+	28.06.01	Type1 PP revised to comply with the request of the evaluator.
V1.05-EAL4+	28.07.01	final version after evaluation

—— this page was intentionally left blank ——

Table Of Contents

—— this page was intentionally left blank ——

List of Tables

—— this page was intentionally left blank ——

Conventions and Terminology

Conventions

The document follows the rules and conventions laid out in Common Criteria 2.1, part 1 [2], Annex B "Specification of Protection Profiles". Admissible algorithms and parameters for algorithms for secure signature-creation devices (SSCD) are given in a separate document [5]. Therefore, the Protection Profile (PP) refers to [5].

Terminology

Administrator means an user that performs TOE initialisation, TOE personalisation, or other TOE administrative functions.

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Authentication data is information used to verify the claimed identity of a user.

CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardisation (CEN). This Protection Profile (PP) represents Annex A to the CWA that has been developed by the European Electronic Signature Standardisation Initiative (EESSI) CEN/ISSS electronic signature (E-SIGN) workshop, Area F on secure signature-creation devices (SSCD).

Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)

Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of

(a) the SSCD proof of correspondence between SCD and SVD and
(b) checking the sender and integrity of the received SVD.

Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. (defined in the Directive [1], article 2.11)

Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).

Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is

(a) a hash-value of the DTBS or
(b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
(c) the DTBS.

The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.

Directive The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] is also referred to as the 'Directive' in the remainder of the PP.

Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], article 2.10)

Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by a SSCD according to the Directive [1], article 5, paragraph 1.

Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).

Signatory means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (defined in the Directive [1], article 2.3)

Signature attributes means additional information that is signed together with the user message.

Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements

(a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision,
(b) to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intend to sign,
(c) to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.

Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive [1], article 2.4)

Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.

Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [1], article 2.7)

Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.

SSCD provision service means a service that prepares and provides a SSCD to subscribers.

User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

Document Organisation

Section 1 provides the introductory material for the Protection Profile.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

A reference section is provided to identify background material.

An acronym list is provided to define frequently used acronyms.

1 Introduction

This section provides document management and overview information that is required to carry out protection profile registry. Therefore, section 1.1 “Identification” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Section 1.2 “Protection Profile Overview” summarises the PP in narrative form. As such, the section gives an overview to the potential user to decide whether the PP is of interest. It is usable as stand-alone abstract in PP catalogues and registers.

1.1 Identification

Title:	Protection Profile — Secure Signature-Creation Device Type1
Authors:	Wolfgang Killmann, Herbert Leitold, Reinhard Posch, Patrick Sallé
Vetting Status:	
CC Version:	2.1 Final
General Status:	Final Ballot Draft
Version Number:	1.05
Registration:	
Keywords:	secure signature-creation device, electronic signature

1.2 Protection Profile Overview

This Protection Profile (PP) is established by CEN/ISSS for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1], also referred to as the ‘Directive’ in the remainder of the PP, as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

The intent of this Protection Profile is to specify functional and assurance requirements for the generation of the SCD in conformance with the Directive [1], Annex III for secure signature-creation devices. Member States shall presume that there is compliance with the requirements laid down in Annex III of the Directive [1] when electronic signature products are evaluated according to Security Targets (ST) that are compliant with this PP and the PP for SSCD type 2 or a PP for SSCD type 3

The Protection Profile defines the security requirements of a SSCD for the generation of signature-creation data (SCD).

The assurance level for this PP is EAL4 augmented. The minimum strength level for the TOE security functions is 'SOF high' (Strength of Functions High).

2 TOE Description

2.1 Secure Signature Creation Devices

The present document assumes a well defined process signature-creation to take place. The present chapter defines three possible SSCD implementations, referred to as 'SSCD types', as illustrated in Figure 1.

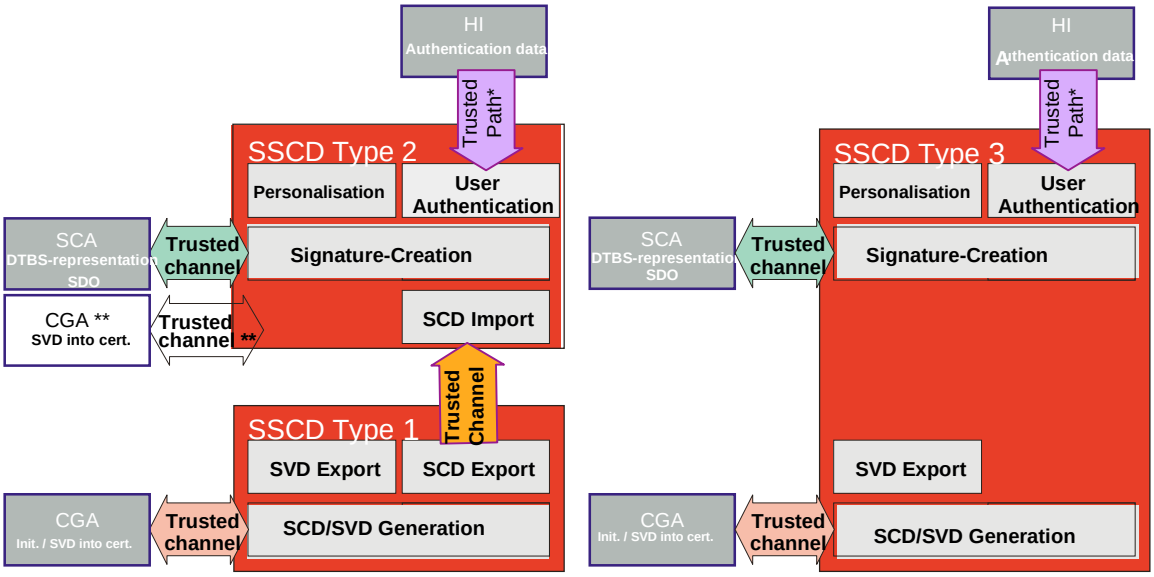
The left part of Figure 1 shows two SSCD components: A SSCD of Type 1 representing the SCD/SVD generation component, and a SSCD of Type 2 representing the SCD storage and signature-creation component. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel. The right part of Figure 1 shows a SSCD Type 3 which is analogous to a combination of Type 1 and Type 2, but no transfer of the SCD between two devices is provided.

If the SSCD holds the SVD and exports the SVD to a CGA for certification, a trusted channel is to be provided. The CGA initiates SCD/SVD generation ("Init.") and the SSCD exports the SVD for generation of the corresponding certificate ("SVD into cert.").

The signatory must be authenticated to create signatures that he sends his authentication data (e.g., a PIN) to the SSCD Type 2 or Type 3 (e.g., a smart card). If the human interface (HI) for such signatory authentication is not provided by the SSCD, a trusted path (e.g., a encrypted channel) between the SSCD and the SCA implementing the HI is to be provided. The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be transferred by the SCA to the SSCD only over a trusted channel. The same shall apply to the signed data object (SDO) returned from a SSCD to the SCA.

SSCD Type 1 is not a personalized component in the sense that it may be used by a specific user only, but the SCD/SVD generation and export shall be initiated by authorized persons only (e.g., system administrator).

SSCD Type 2 and Type 3 are personalized components which means that they can be used for signature creation by one specific user – the signatory - only.



* The trusted path for user authentication will be required if the HI is not provided by the TOE itself (e. g., it is provided by a SCA outside the SSCD)
** The trusted channel between the SSCD Type 2 and the CGA is required for cases where the SSCD type 2 holds the SVD and export of the SVD to the CGA for certification is provided.

Figure 1: SSCD types and modes of operation

2.2 Limits of the TOE

The TOE is a secure signature-creation device (SSCD Type1) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1]. A SSCD is configured software or hardware used to generate the signature-creation data (SCD).

The TOE provides the following function necessary for devices involved in qualified electronic signatures:

(1) Generation of the SCD and the correspondent signature-verification data (SVD)

The generation of the SCD/SVD pair by means of the TOE (Type1) requires the export the SCD into a SSCD of Type 2. Vice versa, signature generation by means of a SSCD Type 2 requires that the SCD/SVD pair has been generated by and imported from the TOE. Consequently, there is an interdependence where a SSCD Type 2 forms the environment of the TOE.

The TOE implements all IT security functionality which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control.

The SSCD protects the SCD during the whole life cycle as to be solely used in the signature-creation process by the legitimate signatory. The TOE (Type1) generates signatory's SCD and exports it into a SSCD of Type 2 in a secure manner.

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). The TOE will destroy the SCD after export.

Figure 2 shows the PP scope from the structural perspective. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the SCD/SVD generation, and signature-creation functionality. The SSCD Type2 and the CGA (and possibly other applications) are part of the immediate environment of the TOE. They shall communicate with the TOE over a trusted channel.

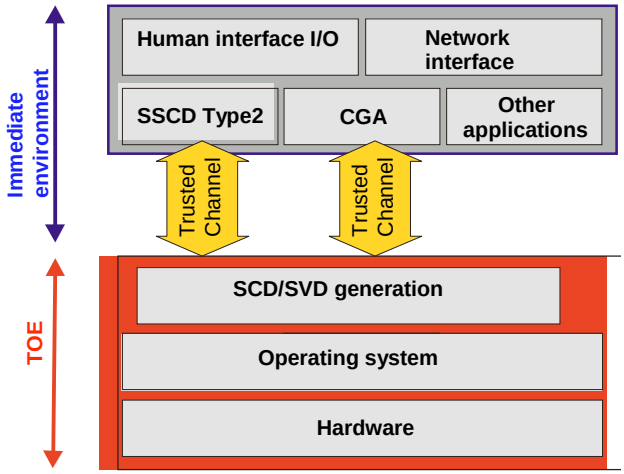


Figure 2: Scope of the SSCD, structural view

The TOE life cycle is shown in Figure 3. Basically, it consists of a development phase and the operational phase. This document refers to the operational phase which starts with personalisation including SCD/SVD generation and SCD export. This phase represents installation, generation, and start-up in the CC terminology. The main functionality in the usage phase is SCD/SVD creation including all supporting functionality. The life cycle ends with the destruction of the SSCD.

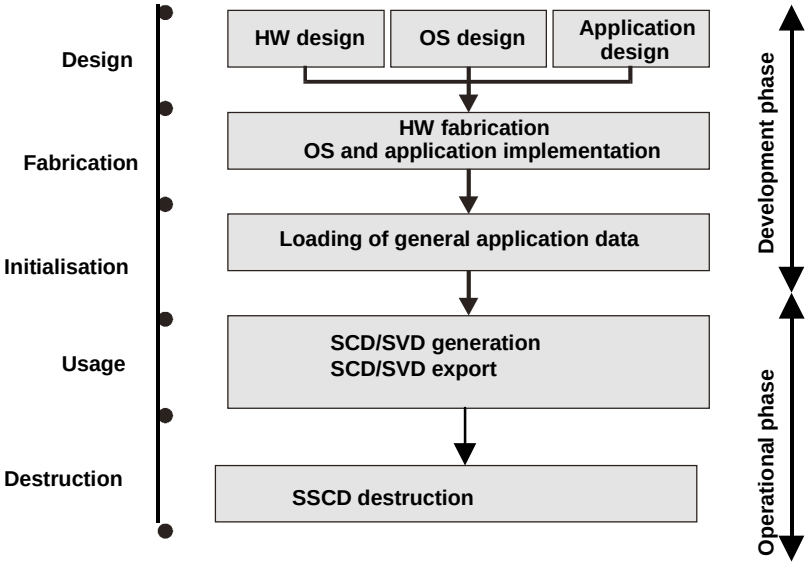


Figure 3. SSCD life cycle

Application note: Scope of SSCD PP application

This SSCD PP refers to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is created by the TOE.

While the main application scenario of a SSCD will assume a qualified certificate to be used in combination with a SSCD, there still is a large benefit in the security when such SSCD is applied in other areas and such application is encouraged. The SSCD PP may as well be applied to environments where the certificates expressed as 'qualified certificates' in the SSCD PP do not fulfil the requirements laid down in Annex I and Annex II of the Directive [1].

With this respect the notion of qualified certificates in the PP refers to the fact that when an instance of a SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive [1], article 5, paragraph 1. As a consequence, this standard does not prevent a device itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

3 TOE Security Environment

Assets:

1. SCD. confidentiality of the SCD must be maintained.
2. SVD: integrity of the SVD when it is exported must be maintained.
3. VAD: PIN code or biometrics data entered by the End User to perform a generation operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)
4. RAD: Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)

Subjects

Subject	**Definition**
S.User	End user of the TOE which can be identified as S.Admin
S.Admin	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.

Threat agents

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

3.1 Assumptions

A.SCD_Import *Trustworthy SCD import*

The party using the SCD/SVD-pair generated by the TOE will ensure that the confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and

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.

3.2 Threats to Security

T.Hack_Phys *Exploitation of vulnerabilities in the physical environment*

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.SCD_Rel *Release of the signature-creation data*

The SCD are released during generation in the TOE. 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_Forgery *Forgery of the electronic signature*

An attacker forges the signed data object maybe together with its electronic signature, created by a SSCD Type2 using the SCD generated by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties.

T.Sig_Repud *Repudiation of signatures*

If an attacker can successfully threaten any of the assets, then the non repudation of the electronic signature is compromised.

The signatory is able to deny to have 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 to the CGA. This result in loss of SVD integrity in the certificate of the signatory.

3.3 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 TOE. 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 generated by the TOE. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

P.SCD_Generate *TOE as SCD/SVD-generator of the SSCD provision service*

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.

4 Security Objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

4.1 Security Objectives for the TOE

OT.EMSEC_Design *Provide physical emanations security*

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

OT.Lifecycle_Security *Lifecycle security*

The TOE shall detect flaws during the initialisation, and operational usage. The TOE shall provide safe destruction techniques for the SCD after exportation.

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 exported SCD and SVD.

OT.SVD_Auth_TOE *TOE ensures authenticity of the SVD*

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

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. The SCD shall be deleted from the TOE whenever it is exported from that TOE into a SSCD Type 2.

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.

4.2 Security Objectives for the Environment

OE.SCD_Transfer *Secure transfer of SCD between SSCD*

The SSCD Type2 shall ensure the confidentiality of the SCD transferred from the TOE. In case the SVD is also transferred from the TOE to the SSCD Type2, it shall ensure its integrity.

OE.SVD_Auth_Type2 SSCD Type2 *ensures authenticity of the SVD*

The SSCD Type2 provides means to enable the CGA to verify the authenticity of the SVD that has been first exported by the TOE to the SSCD Type2 then exported by the SSCD Type2 to the CGA.

Note: This objective is applied only if SSCD Type2 imports the SVD from the TOE then exports it to the CGA. In case the TOE exports the SVD directly to the CGA, this Objective is not applicable.

OE.CGA_QCert *Generation of qualified certificates*

The CGA generates qualified certificates which include inter alias

(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 proves 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.

5 IT Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE and the environment.

Security functional requirements components given in section 5.1 “TOE security functional requirements” excepting FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 [3]. Some security functional requirements represent extensions to [3]. Operations for assignment, selection and refinement have been made. Operations not performed in this PP are identified in order to enable instantiation of the PP to a Security Target (ST).

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [4].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

5.1 TOE Security Functional Requirements

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

5.1.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

Application notes:

The cryptographic key SCD will be destroyed automatically after export.

5.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ Initialisation SFP	The TSF shall enforce the Initialisation SFP on generation of SCD/SVD pair by Administrator.
FDP_ACC.1.1/ SVD Export SFP	The TSF shall enforce the SVD Export SFP on export of SVD by Administrator.
FDP_ACC.1.1/ SCD Export SFP	The TSF shall enforce the SCD Export SFP on export of SCD by Administrator.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

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

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator
Initialisation attribute		
User	SCD / SVD management	authorised, not authorised

Note: The Signatory can be a user role if the evaluated product includes a Type2 or a Type3 SSCD.

Initialisation SFP

FDP_ACF.1.1/ Initialisation SFP	The TSF shall enforce the Initialisation SFP to objects based on security attributes “role” and “SCD / SVD management”.
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” 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: none

SVD Export SFP

FDP_ACF.1.1/ SVD Export SFP	The TSF shall enforce the SVD Export SFP to objects based on General attribute group.
FDP_ACF.1.2/ SVD Export 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” is allowed to export SVD.
FDP_ACF.1.3/ SVD Export SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ SVD Export SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none.

SCD Export SFP

FDP_ACF.1.1/ SCD Export SFP	The TSF shall enforce the SCD Export SFP to objects based on General attribute group and Initialisation attribute group.
FDP_ACF.1.2/ SCD Export 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" whose security attribute "SCD / SVD management" is set to "authorised" is allowed to export a SCD.
FDP_ACF.1.3/ SCD Export SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ SCD Export 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" whose security attribute "SCD / SVD management" is set to "not authorised" is not allowed to export a SCD.

5.1.2.3 Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1/ SCD Export	The TSF shall enforce the SCD Export SFP when exporting user data, controlled under the SFP(s),outside of the TSC.
FDP_ETC.1.2/ SCD Export	The TSF shall export the user data without the user data's associated security attributes.
FDP_ETC.1.1/ SVD Export	The TSF shall enforce the SVD Export SFP when exporting user data, controlled under the SFP(s), outside of the TSC.
FDP_ETC.1.2/ SVD Export	The TSF shall export the user data without the user data's associated security attributes.

5.1.2.4 Subset residual information protection (FDP_RIP.1)

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, RAD.

5.1.2.5 Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1/ Sender — The TSF shall enforce the SCD Export SFP to be able to transmit objects in a manner protected from unauthorised disclosure.

5.1.2.6 Data exchange integrity (FDP_UIT.1)

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

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

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 — The TSF shall detect when [*assignment: number*] 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.

5.1.3.2 User attribute definition (FIA_ATD.1)

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

5.1.3.3 Timing of authentication (FIA_UAU.1)

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 2 by means of TSF required by FTP_ITC.1/SCD export. 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.

5.1.3.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1 — The TSF shall allow establishing a trusted channel between the TOE and a SSCD of Type 2 by means of TSF required by FTP_ITC.1/SCD export on behalf of the user to be performed before the user is identified.

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the Initialisation SFP and SCD Export SFP to restrict the ability to modify [*assignment: other operations*] the security attributes SCD / SVD management to Administrator.

5.1.4.2 Secure security attributes (FMT_MSA.2)

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

5.1.4.3 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the Initialisation SFP and SCD Export 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 to specify alternative initial values to override the default values when an object or information is created.

5.1.4.4 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles Administrator.

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1 The TSF shall run a suite of tests [*selection: during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.5.2 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [*assignment: specified limits*] enabling access to RAD and SCD.

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 RAD and SCD.

Application note:

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation**,** simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

5.1.5.3 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*assignment: list of types of failures in the TSF*].

5.1.5.4 Passive detection of physical attack (FPT_PHP.1)

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.

5.1.5.5 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist [*assignment: physical tampering scenarios*] to the [*assignment: list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

5.1.5.6 TSF testing (FPT_TST.1)

FPT_TST.1.1	The TSF shall run a suite of self tests [*selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*][*assignment: conditions under which self test should occur*] 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 Trusted path/channels (FTP)

5.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCD export	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SCD export	The TSF shall permit [*selection: the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCD export	The TSF or the SSCD Type2 shall initiate communication via the trusted channel for SCD export.

Refinement: The mentioned remote trusted IT product is a SSCD of type 2.

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

Refinement: The mentioned remote trusted IT product is the CGA or a SSCD Type2

5.2 TOE Security Assurance Requirements

Table 5.1 Assurance Requirements: EAL(4)

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4

5.2.1 Configuration management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

5.2.1.3 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1D The developer shall provide CM documentation.

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is

completely represented.

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.2.3.3 Implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP

that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible

security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5 Life cycle support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.2.5.2 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

5.2.5.3 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.1D The developer shall identify the development tools being used for

the TOE.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.2.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

5.2.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Analysis and testing for insecure states (AVA_MSU.3)

AVA_MSU.3.1D The developer shall provide guidance documentation.

AVA_MSU.3.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.3.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.3.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.3.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.3.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.3.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.2.7.3 Highly resistant (AVA_VLA.4)

AVA_VLA.4.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.4.2D The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.4.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.4C The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

5.3 Security Requirements for the IT Environment

5.3.1 SCD import (SSCD type2)

5.3.1.1 Subset access control (FDP_ACC.1)

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/ SVD Transfer SFP The TSF shall enforce the SVD Transfer SFP on import and on export of SVD by User.

Application note:
FDP_ACC.1/SVD Transfer SFP will be required only, if the SSCD Type2 is to import the SVD from the TOE so it will be exported to the CGA for certification.

5.3.1.2 Import of user data without security attributes (FDP_ITC.1)

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.

5.3.1.3 Basic data exchange confidentiality (FDP_UCT.1)

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

5.3.1.4 Inter-TSF trusted channel (FTP_ITC.1)

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 [selection: the TSF, the remote trusted IT product] to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCD Import	The TSF or the remote trusted IT 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 [*selection: the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3/ SVD Transfer	The TSF or the trusted IT shall initiate communication via the trusted channel for transfer of SVD.

Refinement: The mentioned remote trusted IT product is a SSCD of type 1.for SVD import and the CGA for the SVD export.

Application note:
FTP_ITC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

5.3.2 Certification generation application (CGA)

5.3.2.1 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1/ CGA — The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method qualified certificate that meets the following: List of approved algorithms and parameters.

5.3.2.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA — The TSF shall perform import the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following: [*assignment: list of standards*].

5.3.2.3 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SVD import — The TSF shall enforce the SVD import SFP to be able to receive user data in a manner protected from modification and insertion errors.

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

5.3.2.4 Inter-TSF trusted channel (FTP_ITC.1)

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

FTP_ITC.1.2/ SVD import — The TSF shall permit [*selection: the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SVD import — The TSF shall initiate communication via the trusted channel for import SVD.

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 ensures the ongoing compliance.

6 Rationale

6.1 Introduction

The tables in sub-sections 6.2.1 “Security Objectives Coverage” and 6.3.1 “Security Requirement Coverage” provide the mapping of the security objectives and security requirements for the TOE.

6.2 Security Objectives Rationale

6.2.1 Security Objectives Coverage

Table 6.1 : Security Environment to Security Objectives Mapping

Threats - Assumptions - Policies / Security objectives	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.Init	OT.SCD_Unique	OE.SCD_Transfer	OE.SVD_Auth_Type2	OE.CGA_QCert	OE.SVD_Auth_CGA
T.Hack_Phys	x			x			x	x						
T.SCD_Divulg			x	x					x		x			
T.SCD_Derive										x				
T.SCD_Rel				x										
T.SVD_Forgery						x						x		x
T.Sig_Forgery	x	x	x	x	x	x	x	x			x	x	x	x
T.Sig_Repud	x	x	x	x	x	x	x	x		x	x	x	x	x
A.SCD_Import											x			
A.CGA													x	x
P.CSP_Qcert					x								x	
P.SCD_Generate			x		x				x					

6.2.2 Security Objectives Sufficiency

6.2.2.1 Policies and Security Objective Sufficiency

P.CSP_QCert (CSP generates qualified certificates) establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD

under sole control of this signatory. P.CSP_QCert is addressed by the TOE by OT.SCD_SVD_Corresp concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by OE.CGA_QCert for generation of qualified certificates by the CGA, respectively.

P.SCD_Generate (TOE as SCD/SVD-generator of the SSCD provision service) addresses the requirement of confidentiality of the signatory's SCD during the generation process. This requirement is derived form the Directive [1], Annex II, literal (g). OT.SCD_Secrecy and OT.SCD_Transfer address the confidentiality of the SCD during generation and, if applicable, the transfer between the SSCD of the CSP and the SSCD of the signatory. OT.Init provides that SSCD initialisation is restricted to authorised users. Threats and Security Objective Sufficiency

6.2.2.2 Threats and Security Objective Sufficiency

T.Hack_Phys (Exploitation of vulnerabilities in the physical environment) deals with physical attacks exploiting vulnerabilities in the environment of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. Physical attacks through the TOE interfaces are countered by OT.EMSEC_Design. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tamper attacks.

T.SCD_Divulg (Storing and copying and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by OT.SCD_Secrecy which assures the secrecy of the SCD used by Type2 SSCD for signature generation. OT.SCD_Transfer and OE.SCD_Transfer insure the confidentiality of the SCD during it's transfer between the TOE and a SSCD Type2. OT.SCD_Transfer ensures that the SCD is deleted by TOE after it is exported TOE Type 2. OT.Init ensures that only authorized users cabn generate the SCD so to counteract it's divulgation.

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OT.SCD_Unique that provides cryptographic secure generation of the SCD/SVD-pair.

T.SCD_Rel (Release of the signature-creation data) addresses the threat of compromising the SCD during generation in the TOE. This threat is addressed by OT.SCD_Secrecy in order to reasonably assure the secrecy of the SCD used for signature generation.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.SCD_Transfer and OE_SCD_Transfer (Secure transfer of SCD between SSCD), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows:

The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, OT.SCD_Transfer,

OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD sent to the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

If the SVD is exported to a SSCD Type2, OE.SVD_Auth_Type2 participates to the provision of the integrity and authenticity of the SVD

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert **(**Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Transfer and OE.SCD_Transfer (Secure transfer of SCD between SSCD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security),

If the SVD is exported to a SSCD Type2, OE.SVD_Auth_Type2 addresses also the threat (SSCD Type2 ensures authenticity of the SVD)

OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. If the SVD is exported to a SSCD Type2, OE.SVD_Auth_Type2 also participates to ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OT.Sig_Secure, OT.SCD_Transfer, OE.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD sent to the signatory's SSCD.

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SVD_Auth_TOE which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by OE.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA. In case the SVD is first exported a SSCD Type2, T.SVD_Forgery is also addressed by OE.SVD_Auth_Type2 which ensures that the TOE sends the SVD in a verifiable form to the CGA.

6.2.2.3 Assumptions and Security Objective Sufficiency

A.SCD_Import (Trustworthy SCD import) protects the confidentiality of the SCD while it is imported into the SSCD Type2. This is addressed by OE_SCD_Transfer which ensures the confidentiality of the SCD while it is transferred to the SSCD Type2. In case the SVD is also exported to the SSCD type2 (for re-exportation to the CGA), the integrity of the SVD must be maintained. This is also ensured by OE.SCD_Transfer.

A.CGA (Trustworthy certification-generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation

of qualified certificates) which ensures the generation of qualified certificates and by OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) which ensures the verification of the integrity of the received SVD and the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

Table 6.2 : Functional Requirement to TOE Security Objective Mapping

TOE Security Functional Requirement / TOE Security objectives	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.Init	OT.SCD_Unique
FCS_CKM.1					x					x
FCS_CKM.4		x	x	x						
FCS_COP.1/CORRESP					x					
FDP_ACC.1/Initialisation SFP				x					x	
FDP_ACC.1/SVD Export SFP						x				
FDP_ACC.1/SCD Export SFP			x							
FDP_ACF.1/Initialisation SFP				x					x	
FDP_ACF.1/SVD Export SFP						x				
FDP_ACF.1/SCD Export SFP			x							
FDP_ETC.1/SVD Export						x				
FDP_ETC.1/SCD Export			x							
FDP_RIP.1				x						
FDP_UCT.1/Sender			x							
FDP_UIT.1/SVD Export						x				
FIA_AFL.1									x	
FIA_ATD.1									x	
FIA_UAU.1									x	
FIA_UID.1									x	
FMT_MSA.1				x					x	
FMT_MSA.2			x							
FMT_MSA.3			x	x					x	
FMT_SMR.1			x	x						
FPT_AMT.1		x		x						
FPT_EMSEC.1	x									
FPT_FLS.1				x						
FPT_PHP.1							x			
FPT_PHP.3								x		
FPT_TST.1		x								
FTP_ITC.1/SCD Export			x							
FTP_ITC.1/SVD Export						x				

Table 6.3: IT Environment Functional requirement to Environment Security Objective Mapping

Environment Security Requirement / Environment Security objectives	OE.SCD_Transfer	OE.SVD_Auth_Type2	OE.CGA_QCert	OE.SVD_Auth_CGA
FDP_ACC.1/SCD Import SFP	x			
FDP_ACC.1/SVD Transfer SFP		x		
FDP_ITC.1/SCD	x			
FDP_UCT.1/Receiver	x			
FTP_ITC.1/SCD Import	x			
FTP_ITC.1/SVD Transfer		x		
FCS_CKM.2/CGA			x	
FCS_CKM.3/CGA			x	
FDP_UIT.1/SVD Import				x
FTP_ITC.1/SVD Import				x

Table 6.4 : Assurance Requirement to Security Objective Mapping

Objectives	Requirements
Security Assurance Requirements	
OT.Lifecycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ADO_DEL.2, ADO_IGS.1
OT.SCD_Secrecy	AVA_MSU.3, AVA_SOF.1, AVA_VLA.4
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_IGS.1, ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

6.3.2 Security Requirements Sufficiency

6.3.2.1 TOE Security Requirements Sufficiency

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1.

OT.Init (SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_ATD.1 define RAD as the corresponding user attribute. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The attributes of the authenticated user are provided by FMT_MSA.1, FMT_MSA.3, for static attribute initialisation. Access control is provided by FDP_ACC.1/Initialisation SFP and FDP_ACF.1/Initialisation SFP. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1 and FPT_AMT.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD to conclude the operational usage of the TOE as SSCD.

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functions specified by FDP_ACC.1/Initialisation SFP and FDP_ACF.1/Initialisation SFP that ensure that only authorised user can initialise the TOE and create or load the SCD. The authentication and access management functions specified by FMT_MSA.1, and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

FPT_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. Cryptographic correspondence is provided by FCS_COP.1/CORRESP

OT.SCD_Transfer (Secure transfer of SCD between SSCD) is provided by FDP_UCT.1/Sender that ensures that a trusted channel is provided and that confidentiality is maintained.

Security functions specified by FDP_ACC.1/SCD Export SFP, FMT_MSA.2; FMT_MSA.3, FMT_SMR.1, FDP_ACF.1/SCD Export SFP, and FDP_ETC.1/SCD Export ensure that transfer of SCDs is restricted to administrators. This supports the confidentiality-oriented functions.

Security functions complying with FDP_ETC.1/SCD Export and FTP_ITC.1/ SCD Export ensure that only TOE may export the SCD. Security function specified by FCS_CKM.4 destroy the SCD, once exported from the TOE.

OT.SCD_Unique (Uniqueness of the signature-creation data) implements the requirement of practically unique SCD as laid down in the Directive [1], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD) is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD Export and FDP_UIT.1/SVD Export. The cryptographic algorithms specified by FDP_ACC.1/SVD Export SFP, FDP_ACF.1/SVD Export SFP and FDP_ETC.1/SVD Export ensure that only authorised user can export the SVD to the CGA.

OT.Tamper_ID (Tamper detection) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

6.3.2.2 TOE Enviroment Security Requirements Sufficiency

OE.SCD_Transfer (Secure transfer of SCD between SSCD) is provided by FDP_ITC.1/SCD , FDP_UCT.1/Receiver and FTP_ITC.1/SCD Import that ensure that a trusted channel is provided and that confidentiality is maintained.

Security functions specified by FDP_ACC.1/SCD Import SFP ensures that transfer of SCDs is restricted to administrators. This supports the confidentiality-oriented functions.

OE.SVD_Auth_Type2 (SSCD Type2 ensures authenticity of the SVD) is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD Transfer. FDP_ACC.1/SVD Transfer SFP ensures that only authorised user can Import the SVD from the TOE and Export the SVD to the CGA.

OE.CGA_QCert (Generation of qualified certificates) addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA and FTP_ITC.1/SVD Import ensure that the CGA imports the SVD using a secure channel and a secure key access method.

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD.Import which assures identification of the sender and by FDP_UIT.1/ SVD Import. which guarantees it’s integrity

6.4 Dependency Rationale

6.4.1 Functional and Assurance Requirements Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled. The functional requirements dependencies for the TOE environment are not completely fulfilled (see section 6.4.2 for justification).

Table 6.5 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1/CORRESP, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1/ CORRESP	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1/ Initialisation SFP	FDP_ACF.1/Initialisation SFP
FDP_ACC.1/ SCD Export SFP	FDP_ACF.1/SCD Export SFP
FDP_ACC.1/ SVD Export SFP	FDP_ACF.1/SVD Export SFP
FDP_ACF.1/ Initialisation SFP	FDP_ACC.1/Initialisation SFP, FMT_MSA.3
FDP_ACF.1/ SCD Export SFP	FDP_ACC.1/SCD Export SFP, FMT_MSA.3
FDP_ACF.1/ SVD Export SFP	FDP_ACC.1/SVD Export SFP, FMT_MSA.3
FDP_ETC.1/ SCD Export SFP	FDP_ACC.1/ SCD Export SFP
FDP_ETC.1/ SVD Export SFP	FDP_ACC.1/ SVD Export SFP
FDP_RIP.1	None
FDP_UCT.1/ Sender	FTP_ITC.1/SCD Export, FDP_ACC.1/ SCD Export SFP
FDP_UIT.1/ SVD Export	FTP_ITC.1/SVD Export, FDP_ACC.1/SVD Export
FIA_AFL.1	FIA_UAU.1
FIA_ATD.1	None
FIA_UAU.1	FIA_UID.1
FIA_UID.1	None
FMT_MSA.1	FDP_ACC.1/Initialisation SFP, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1/Personalisation SFP, FMT_SMR.1 FMT_MSA.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_SMR.1	FIA_UID.1
FPT_AMT.1	None
FPT_EMSEC.1	None

Requirement	Dependencies
FPT_FLS.1	ADV_SPM.1
FPT_PHP.1	unsupported dependencies, see sub-section 6.4.2 for justification.
FPT_TST.1	FPT_AMT.1
FTP_ITC.1/ SCD Export	FTP_ITC.1/SCD Import
FTP_ITC.1/ SVD Export	FTP_ITC.1/SVD Import
Assurance Requirements	
ACM_AUT.1	ACM_CAP.3
ACM_CAP.4	ACM_SCP.1, ALC_DVS.1
ACM_SCP.2	ACM_CAP.3
ADO_DEL.2	ACM_CAP.3
ADO_IGS.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1
ADV_IMP.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1
ADV_SPM.1	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_TAT.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.3	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.4	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1
Functional Requirement for SSCD Type2	
FDP_ACC.1/ SCD Import SFP	unsupported dependencies, see sub-section 6.4.2 for justification
FDP_ACC.1/ SVD Transfer SFP	unsupported dependencies, see sub-section 6.4.2 for justification
FDP_ITC.1/ SCD Import	FDP_ACC.1/ SCD Import, unsupported dependencies, see sub-section 6.4.2 for justification
FDP_UCT.1/Receiver	FDP_ACC.1/ SCD Import, FTP_ITC.1/SCD Import
FTP_ITC.1/ SVD Transfer	None
FTP_ITC.1/ SCD Import	None

Functional Requirements for Certification generation application (GGA)	
FCS_CKM.2/CGA	unsupported dependencies, see sub-section 6.4.2 for justification
FCS_CKM.3/CGA	unsupported dependencies, see sub-section 6.4.2 for justification
FDP_UIT.1/ SVD Import	FTP_ITC.1/SVD Import, unsupported dependencies, see sub-section 6.4.2 for justification
FTP_ITC.1/ SVD Import	None

6.4.2 Justification of Unsupported Dependencies

FPT_PHP.1	Upon detection of physical tampering that might compromise the TSF, the SCD creation function must be disabled with no restriction. This is why FMT_MOF.1 is not applicable.

The security functional dependencies for the TOE environment SSCD Type2 and CGA are not completely supported by security functional requirements in section 5.3.

FDP/ACC.1/ SCD Import SFP	The SSCD Type2 will follow the SCD Import SFP when importing the SCD. The access control required by this SFP, FDP_ACF.1 Security attribute based access control, is outside the scope of this PP.
FDP/ACC.1/ SVD Transfer SFP	The SSCD Type2 will follow the SVD Transfer SFP when importing and then exporting the SVD. The access control required by this SFP, FDP_ACF.1 Security attribute based access control, is outside the scope of this PP.
FDP_ITC.1/ SCD Import	The SSCD Type2 importing the SCD must maintain it's confidentiality. The SFP used including The Static attribute initialisation FMT_MSA.3 is outside the scope of this PP.
FCS_CKM.2/ CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FCS_CKM.3/ CGA	The CGA imports SVD via trusted cannel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FDP_UIT.1/ SVD IMPORT	The access control policy (FDP_ACC.1) for the CGA is out of the scope of this PP.

6.5 Security Requirements Grounding in Objectives

Table 6.6 Assurance and Functional Requirement to Security Objective Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.1	EAL 4
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL 4, OT.Lifecycle_Security
ALC_LCD.1	EAL 4, OT.Lifecycle_Security
ALC_TAT.1	EAL 4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	OT.SCD_Secrecy
AVA_SOF.1	EAL 4, OT.SCD_Secrecy
AVA_VLA.4	OT.SCD_Secrecy
Security requirements	
R.Administrator_Guide	AGD_ADM.1

6.6 Rationale for Extensions

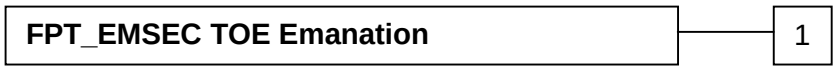
The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations.

6.6.1 FPT_EMSEC TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

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 RAD and SCD.

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 RAD and SCD.

Hierarchical to: No other components.

Dependencies: No other components.

6.7 Rationale for Strength of Function High

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the security objective OT.SCD_Secrecy. The protection against attacks with a high attack potential dictates a strength of function high rating for functions in the TOE that are realised by probabilistic or permutational mechanisms.

6.8 Rationale for Assurance Level 4 Augmented

The assurance level for this protection profile is EAL4 augmented.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. Augmentation results from the selection of:

AVA_MSU.3 Vulnerability Assessment - Misuse - Analysis and testing for insecure states

AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE is intended to generate SCD/SVD pairs by the CSP on behalf of the signatories in large quantities. The guidance shall allow the CSP to apply administrative and management procedures which are adequate and correspond to recognised standards and to prevent insecure states endangering the confidentiality of the SCD and authenticity of the SVD.

In **AVA_MSU.3**, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing by the evaluator. AVA_MSU.3 has the following dependencies:

ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy. AVA_VLA.4 has the following dependencies:

ADV_FSP.1 Informal functional specification
ADV_HLD.2 Security enforcing high-level design
ADV_IMP.1 Subset of the implementation of the TSF
ADV_LLD.1 Descriptive low-level design
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

References

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

[2] International Organization for Standardization, ISO/IEC 15408-1:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, 1999.

[3] International Organization for Standardization, *ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[4] International Organization for Standardization, *ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.

[5] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.

Appendix A - Acronyms

CC Common Criteria

EAL Evaluation Assurance Level

IT Information Technology

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSFI TSF Interface

TSP TOE Security Policy

—— this page was intentionally left blank ——

Annex B

This Annex B, with the exception of its pagination, is deemed to be identical to the PP that has been certified by BSI and which is available at http://www.bsi.de/cc/pplist/PP0005b.pdf.

Nevertheless, in case of any discrepancies between the PP available from the BSI web-site and the PP in this Annex B, it is the PP published by BSI that is the normative one.

Protection Profile — Secure Signature-Creation Device Type2

Version: 1.04, EAL 4+

Wednesday, 25 July 2001

Prepared By: ESIGN Workshop - Expert Group F

Prepared For: CEN/ISSS

Note: **This Protection Profile (PP) has been prepared for the European Electronic Signature Standardisation Initiative EESSI by CEN/ISSS area F on secure signature-creation devices (SSCDs). In its present form it represents one of two documents that the CEN/ISSS E-Sign Workshop decided at its Brussels meeting 21st November 2000 to forward to the EESSI Steering Committee—one defining evaluation assurance level *EAL 4 augmented* and one defining *EAL 4*.**

The actual PP is EAL 4 augmented by AVA_VLA.4 and AVA_MSU.3, strength of function high.

—— this page was intentionally left blank ——

Foreword

This ‘Protection Profile — Secure Signature-Creation Device’ is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) Electronic Signatures (E-SIGN) workshop. The document represents Annex A of the CEN/ISSS workshop agreement (CWA) on secure signature-creation devices.

The document is for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

The document has been prepared as a Protection Profile (PP) following the rules and formats of ISO 15408, as known as the Common Criteria version 2.1 [2] [3] [4].

The set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is given in a separate document in [5].

Correspondence and comments to this secure signature-creation device protection profile (SSCD-PP) should be referred to:

CONTACT ADDRESS

CEC/ISSS Secretariat
Rue de Stassart 36
1050 Brussels, Belgium

Tel +32 2 550 0813
Fax +32 2 550 0966

Email isss@cenorm.be

—— this page was intentionally left blank ——

Revision History

v1.0-draft	22.09.00	submitted to CEN/ISSS WS/E-Sign Workshop
v1.0-final	16.11.00	for ballot by WS/E-Sign at Brussels meeting (11/00)
v1.0-EAL4+	28.11.00	for submission to European Commission by EESSI
v1.01-EAL4+	01.02.01	for ballot by WS/E-Sign at Brussels meeting (12/01)
v1.02-EAL4+	14.02.01	for ballot by WS/E-Sign as decided at Brussels meeting.
V1.03-EAL4+	15.06.01	Type2 PP extracted from SSCD approved by WS/E-Sign ballot to comply with the request of the evaluator.
V1.04-EAL4+	25.07.01	Type2 PP revised to comply with the request of the evaluator.

—— this page was intentionally left blank ——

Table Of Contents

—— this page was intentionally left blank ——

List of Tables

—— this page was intentionally left blank ——

Conventions and Terminology

Conventions

The document follows the rules and conventions laid out in Common Criteria 2.1, part 1 [2], Annex B "Specification of Protection Profiles". Admissible algorithms and parameters for algorithms for secure signature-creation devices (SSCD) are given in a separate document [5]. Therefore, the Protection Profile (PP) refers to [5].

Terminology

Administrator means an user that performs TOE initialisation, TOE personalisation, or other TOE administrative functions.

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Authentication data is information used to verify the claimed identity of a user.

CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN). This Protection Profile (PP) represents Annex A to the CWA that has been developed by the European Electronic Signature Standardisation Initiative (EESSI) CEN/ISSS electronic signature (E-SIGN) workshop, Area F on secure signature-creation devices (SSCD).

Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)

Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of

(a) the SSCD proof of correspondence between SCD and SVD and
(b) checking the sender and integrity of the received SVD.

Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. (defined in the Directive [1], article 2.11)

Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).

Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is

(a) a hash-value of the DTBS or
(b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
(c) the DTBS.

The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.

Directive The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] is also referred to as the 'Directive' in the remainder of the PP.

Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], article 2.10)

Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by a SSCD according to the Directive [1], article 5, paragraph 1.

Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).

Signatory means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (defined in the Directive [1], article 2.3)

Signature attributes means additional information that is signed together with the user message.

Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements

(a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision,
(b) to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intend to sign,
(c) to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.

Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive [1], article 2.4)

Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.

Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [1], article 2.7)

Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.

SSCD provision service means a service that prepares and provides a SSCD to subscribers.

User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

Document Organisation

Section 1 provides the introductory material for the Protection Profile.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

A reference section is provided to identify background material.

An acronym list is provided to define frequently used acronyms.

1 Introduction

This section provides document management and overview information that is required to carry out protection profile registry. Therefore, section 1.1 “Identification” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Section 1.2 “Protection Profile Overview” summarises the PP in narrative form. As such, the section gives an overview to the potential user to decide whether the PP is of interest. It is usable as stand-alone abstract in PP catalogues and registers.

1.1 Identification

Title:	Protection Profile — Secure Signature-Creation Device Type2
Authors:	Wolfgang Killmann, Herbert Leitold, Reinhard Posch, Patrick Sallé, Bruno Baronnet
Vetting Status:	
CC Version:	2.1 Final
General Status:	Final Ballot Draft
Version Number:	1.04
Registration:	
Keywords:	secure signature-creation device, electronic signature

1.2 Protection Profile Overview

This Protection Profile (PP) is established by CEN/ISSS for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1], also referred to as the ‘Directive’ in the remainder of the PP, as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

The intent of this Protection Profile is to specify functional and assurance requirements defined in the Directive [1], Annex III for secure signature-creation devices (SSCD) which is the target of evaluation (TOE). Member States shall presume that there is compliance with the requirements laid down in Annex III of the Directive [1] when an electronic signature product is evaluated to a Security Target (ST) that is compliant with this Protection Profile.

The Protection Profile defines the security requirements of a SSCD for the creation of qualified electronic signatures. The TOE may implement additional functions and security requirements e.g. for editing and displaying the data to be signed (DTBS), but these additional functions and security requirements are not subject of this Protection Profile.

The assurance level for this PP is EAL4 augmented. The minimum strength level for the TOE security functions is 'SOF high' (Strength of Functions High).

2 TOE Description

2.1 Secure Signature Creation Devices

The present document assumes a well defined process signature-creation to take place. The present chapter defines three possible SSCD implementations, referred to as 'SSCD types', as illustrated in Figure 1.

The left part of Figure 1 shows two SSCD components: A SSCD of Type 1 representing the SCD/SVD generation component, and a SSCD of Type 2 representing the SCD storage and signature-creation component. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel. The right part of Figure 1 shows a SSCD Type 3 which is analogous to a combination of Type 1 and Type 2, but no transfer of the SCD between two devices is provided.

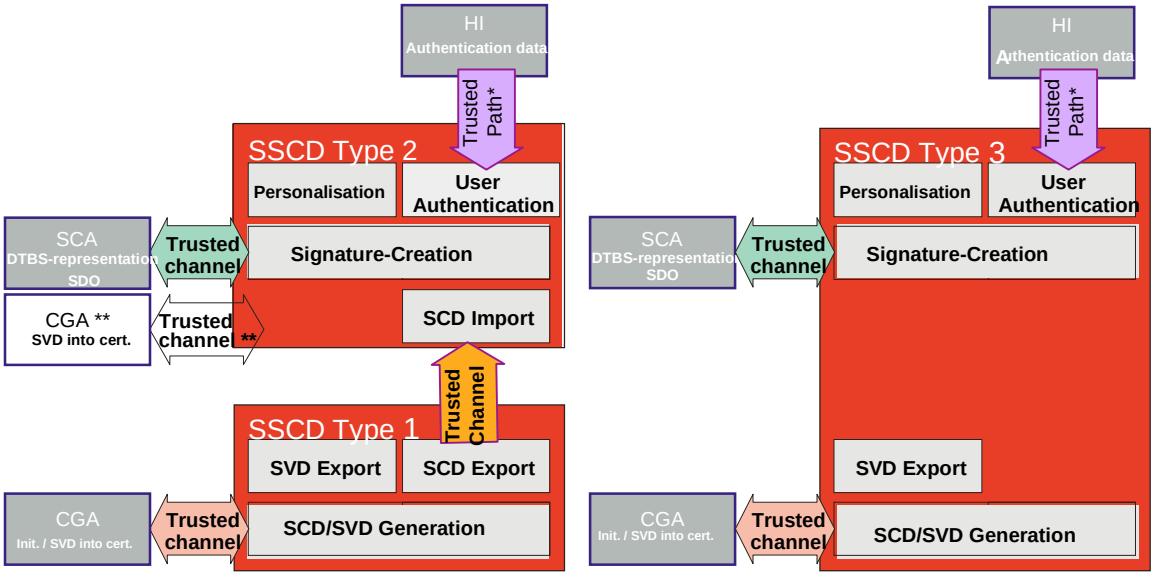
If the SSCD holds the SVD and exports the SVD to a CGA for certification, a trusted channel is to be provided. The CGA initiates SCD/SVD generation ("Init.") and the SSCD exports the SVD for generation of the corresponding certificate ("SVD into cert.").

The signatory must be authenticated to create signatures that he sends his authentication data (e.g., a PIN) to the SSCD Type 2 or Type 3 (e.g., a smart card). If the human interface (HI) for such signatory authentication is not provided by the SSCD, a trusted path (e.g., a encrypted channel) between the SSCD and the SCA implementing to HI is to be provided. The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be transferred by the SCA to the SSCD only over a trusted channel. The same shall apply to the signed data object (SDO) returned from a SSCD to the SCA.

SSCD Type 1 is not a personalized component in the sense that it may be used by a specific user only, but the SCD/SVD generation and export shall be initiated by authorized persons only (e.g., system administrator).

SSCD Type 2 and Type 3 are personalized components which means that they can be used for signature creation by one specific user – the signatory - only.

Type 2 and Type 3 are not necessarily to be considered mutually exclusive.



* The trusted path for user authentication will be required if the HI is not provided by the TOE itself (e. g., it is provided by a SCA outside the SSCD)
** The trusted channel between the SSCD Type 2 and the CGA is required for cases where the SSCD type 2 holds the SVD and export of the SVD to the CGA for certification is provided.

Figure 1: SSCD types and modes of operation

2.2 Limits of the TOE

The TOE is a secure signature-creation device (SSCD Type2) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1]. The destruction of the SCD is mandatory before the TOE loads a new pair SCD/SVD.

A SSCD is configured software or hardware used to implement the signature-creation data (SCD).

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:

(a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function may either be provided by the TOE itself or by appropriate environment
(b) using appropriate hash functions that are, according to [5], agreed as suitable for qualified electronic signatures
(c) after appropriate authentication of the signatory by the TOE.
(d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable according to [5].

The generation of the SCD/SVD pair by means of a SSCD Type 1 requires the export the SCD into the TOE (Type 2). Vice versa, signature generation by means of the TOE (Type2) requires that the SCD/SVD pair has been generated by and imported from a SSCD Type 1.

Consequently, there is an interdependence where a SSCD Type 1 constitutes the environment of the TOE,

The TOE implements all IT security functionality which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The TOE may provide an interface for user authentication by its own or implements IT measures to support a trusted path to a trusted human interface device.

In addition to the functions of the SSCD, the TOE may implement the signature-creation application (SCA). The SCA presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. But this PP assumes the SCA as environment of the TOE because the PP describes the SCD-related security objectives and requirements, whereas the SCA does not implement the SCD. If a SSCD implements a SCA than it will fulfil the security objective and requirements for the TOE, as well as for the SCA as specific TOE environment in the actual PP.

The SSCD protects the SCD during the whole life cycle as to be solely used in the signature-creation process by the legitimate signatory. The SSCD of Type 1 generates signatory's SCD and exports it into a TOE of Type 2 in a secure manner. The TOE of Type 2 will be initialised for the signatory's use by

(1) import of the SCD
(2) personalisation for the signatory by means of the signatory's verification authentication data (VAD).

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). The TOE will destroy the SCD if the SCD is no longer used for signature generation.

The TOE allows to implement a human interface for user authentication:

(i) by the TOE itself or
(ii) by a trusted human interface device connected via a trusted channel with the TOE.

The human interface device is used for the input of VAD for authentication by knowledge or for the generation of VAD for authentication by biometric characteristics. The TOE holds RAD to check the provided VAD. The human interface implies appropriate hardware. The second approach allows to reduce the TOE hardware to a minimum e. g. a smart card.

Figure 2 shows the PP scope from the structural perspective. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the SCD/SVD generation, SCD storage and use, and signature-creation functionality. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE. They shall communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively.

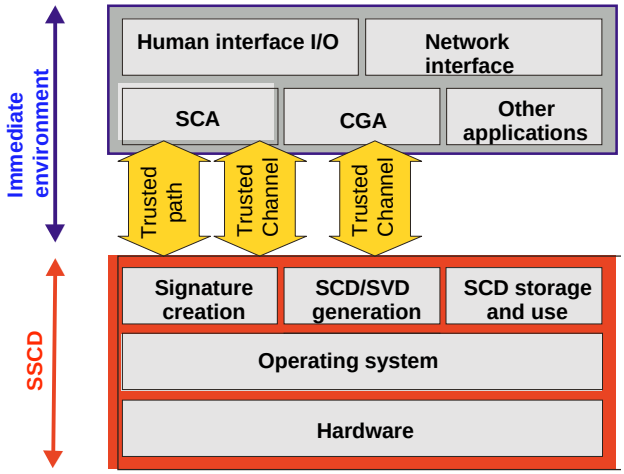


Figure 2: Scope of the SSCD, structural view

The TOE life cycle is shown in Figure 3. Basically, it consists of a development phase and the operational phase. This document refers to the operational phase which starts with personalisation including SCD import. This phase represents installation, generation, and start-up in the CC terminology. The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., SCD storage and SCD use). The life cycle ends with the destruction of the SSCD.

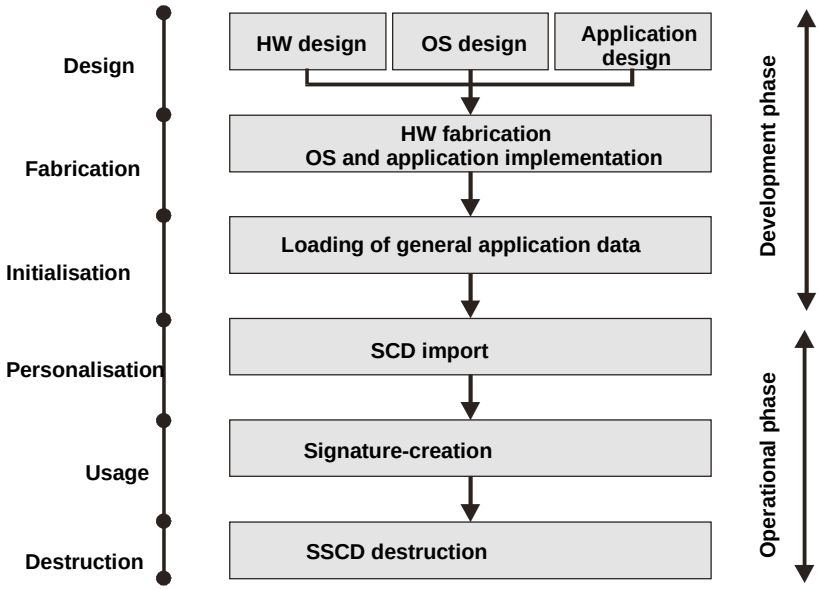


Figure 3. SSCD life cycle

Application note: Scope of SSCD PP application

This SSCD PP refers to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is implemented by the TOE.

While the main application scenario of a SSCD will assume a qualified certificate to be used in combination with a SSCD, there still is a large benefit in the security when such SSCD is applied in other areas and such application is encouraged. The SSCD PP may as well be applied to environments where the certificates expressed as 'qualified certificates' in the SSCD PP do not fulfil the requirements laid down in Annex I and Annex II of the Directive [1].

With this respect the notion of qualified certificates in the PP refers to the fact that when an instance of a SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive [1], article 5, paragraph 1. As a consequence, this standard does not prevent a device itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

3 TOE Security Environment

Assets:

1. SCD: private key used to perform an electronic signature operation(confidentiality of the SCD must be maintained).

2. 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).

3. DTBS and DTBS-representation: set of data, or its representation which is intended to be signed (Their integrity must be maintained).

4. VAD: PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)

5. RAD: Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)

6. 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)

7. Electronic signature: (Unforgeabilty of electronic signatures must be assured).

Subjects

Subject	**Definition**
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory
S.Admin	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

Threat agents

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

3.1 Assumptions

A.CGA *Trustworthy certification-generation application*

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

A.SCA *Trustworthy signature-creation application*

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

A.SCD_Generate *Trustworthy SCD/SVD generation*

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

(a) this party will use a SSCD for SCD/SVD-generation,

(b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and

(c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.

(d) The generation of the SCD/SVD is invoked by authorised users only

(e) The SSCD Type1 ensures the authenticity of the SVD it has created an exported

3.2 Threats to Security

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 repudation of the electronic signature is compromised.

The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

T.SVD_Forgery *Forgery of the signature-verification data*

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

T.DTBS_Forgery *Forgery of the DTBS-representation*

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

T.SigF_Misuse *Misuse of the signature-creation function of the TOE*

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

3.3 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 Security Objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

4.1 Security Objectives for the TOE

OT.EMSEC_Design *Provide physical emanations security*

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

OT.Lifecycle_Security *Lifecycle security*

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

OT.SCD_Secrecy *Secrecy of the signature-creation data*

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

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

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

OT.SVD_Auth_TOE *TOE ensures authenticity of the SVD*

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

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.DTBS_Integrity_TOE *Verification of the DTBS-representation integrity*

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

OT.Sigy_SigF *Signature generation function for the legitimate signatory only*

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

OT.Sig_Secure *Cryptographic security of the electronic signature*

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

4.2 Security Objectives for the Environment

OE.SCD_SVD_Corresp *Correspondence between SVD and SCD*

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

OE.SCD_Transfer *Secure transfer of SCD between SSCD*

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

OE.SCD_Unique *Uniqueness of the signature-creation data*

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

OE.CGA_QCert *Generation of qualified certificates*

The CGA generates qualified certificates which include inter alia
(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,
(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA *CGA verifies the authenticity of the SVD*

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

OE.HI_VAD *Protection of the VAD*

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

OE.SCA_Data_Intend *Data intended to be signed*

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

5 IT Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE and the environment.

Security functional requirements components given in section 5.1 “TOE security functional requirements”, excepting FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 [3]. Some security functional requirements represent extensions to [3]. Operations for assignment, selection and refinement have been made. Operations not performed in this PP are identified in order to enable instantiation of the PP to a Security Target (ST).

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [4].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

5.1 TOE Security Functional Requirements

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in case of re-importation of the SCD in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

Application notes:

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator.
The destruction of the SCD is mandatory before the SCD is re-imported into the TOE.

5.1.1.2 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP — The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key *sizes [assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

FCS_COP.1.1/ SIGNING — The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ SVD Transfer SFP — The TSF shall enforce the SVD Transfer SFP on import and on export of SVD by User.

Application note:
FDP_ACC.1/SVD Transfer SFP will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

FDP_ACC.1.1/ 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

1. sending of DTBS-representation by SCA,
2. signing of DTBS-representation by Signatory.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

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

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
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

SVD Transfer SFP

FDP_ACF.1.1/ SVD Transfer SFP: The TSF shall enforce the SVD Transfer SFP to objects based on General attribute.

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

The user with the security attribute “role” set to “Administrator” or 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.

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.

SCD Import SFP

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

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

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 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.

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 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 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 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 authorised 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 authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “no”.

5.1.2.3 Export of user data without security attributes (FDP_ETC.1)

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

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

Application note:

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

5.1.2.4 Import of user data without security attributes (FDP_ITC.1)

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

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

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

Application note:

A SSCD of Type 1 is authorised to send SCD to a SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorised SSCD of Type 1 are able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FTP_ITC.1.3/SCD export.

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

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

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

Application note:

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

5.1.2.5 Subset residual information protection (FDP_RIP.1)

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, RAD.

5.1.2.6 Stored data integrity monitoring and action (FDP_SDI.2)

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

1. SCD
2. RAD
3. SVD (if persistent 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.

The DTBS-representation temporarily stored by TOE has 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 Basic data exchange confidentiality (FDP_UCT.1)

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

5.1.2.8 Data exchange integrity (FDP_UIT.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_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.1.1/ TOE DTBS	The TSF shall enforce the Signature-creation SFP to be able to receive the DTBS-representation 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.

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [*assignment: number*] 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.

5.1.3.2 User attribute definition (FIA_ATD.1)

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

5.1.3.3 Timing of authentication (FIA_UAU.1)

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.

5.1.3.4 Timing of identification (FIA_UID.1)

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.

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (FMT_MOF.1)

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

5.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ Administrator The TSF shall enforce the SCD Import SFP to restrict the ability to modify [*assignment: other operations*] 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.

5.1.4.3 Secure security attributes (FMT_MSA.2)

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

5.1.4.4 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 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 import of the SCD.

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

5.1.4.5 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to modify [*assignment: other operations*] the RAD to Signatory.

5.1.4.6 Security roles (FMT_SMR.1)

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 Protection of the TSF (FPT)

5.1.5.1 Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1 The TSF shall run a suite of tests [*selection: during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.5.2 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [*assignment: specified limits*] enabling access to RAD and SCD.

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 RAD and SCD.

Application note:

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation**,** simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

5.1.5.3 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*assignment: list of types of failures in the TSF*].

5.1.5.4 Passive detection of physical attack (FPT_PHP.1)

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.

5.1.5.5 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist [*assignment: physical tampering scenarios*] to the [*assignment: list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

5.1.5.6 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests [*selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*][*assignment: conditions under which self test should occur*] 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 Trusted path/channels (FTP)

5.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

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 [*selection: the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SCD Import The TSF or the remote trusted IT 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 [*selection: the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SVD Transfer The TSF or the trusted IT shall initiate communication via the trusted channel for transfer of SVD.

Refinement: The mentioned remote trusted IT product is a SSCD of type 1.for SVD import and the CGA for the SVD export.

Application note:
FTP_ITC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

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

5.1.6.2 Trusted path (FTP_TRP.1)

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

FTP_TRP.1.1/ TOE	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ TOE	The TSF shall permit [*selection: the TSF, 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 *[selection: initial user authentication] [assignment: other services for which trusted path is required]*.

5.2 TOE Security Assurance Requirements

Table 5.1 Assurance Requirements: EAL(4)

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4

5.2.1 Configuration management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the

TOE.

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

5.2.1.3 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1D The developer shall provide CM documentation.

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is

completely represented.

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.2.3.3 Implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP

that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible

security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5 Life cycle support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.2.5.2 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

5.2.5.3 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.1D The developer shall identify the development tools being used for

the TOE.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.2.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

5.2.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Analysis and testing for insecure states (AVA_MSU.3)

AVA_MSU.3.1D The developer shall provide guidance documentation.

AVA_MSU.3.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.3.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.3.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.3.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.3.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.3.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.2.7.3 Highly resistant (AVA_VLA.4)

AVA_VLA.4.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.4.2D The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.4.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.4C The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

5.3 Security Requirements for the IT Environment

5.3.1 Signature key generation (SSCD Type1)

5.3.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

5.3.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1/Type1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

Application notes:

The cryptographic key SCD will be destroyed automatically after export .

5.3.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

5.3.1.4 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ SCD Export SFP	The TSF shall enforce the SCD Export SFP on export of SCD by Administrator.

5.3.1.5 Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1/ Sender	The TSF shall enforce the SCD Export SFP to be able to transmit objects in a manner protected from unauthorised disclosure.

5.3.1.6 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCD Export	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SCD Export	The TSF shall permit [*selection: the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCD Export	The TSF or the SSCD Type2 shall initiate communication via the trusted channel for SCD export.

Refinement: The mentioned remote trusted IT product is a SSCD Type2

Application note:

If the SSCD Type 1 exports the SVD to a SSCD Type2 and the SSCD Type 2 holds the SVD then the trusted channel between the SSCD Type 1 and the SSCD Type 2 will be required .

5.3.2 Certification generation application (CGA)

5.3.2.1 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1/ CGA — The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method qualified certificate that meets the following: List of approved algorithms and parameters.

5.3.2.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA — The TSF shall perform import the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following: [*assignment: list of standards*].

5.3.2.3 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SVD Import — The TSF shall enforce the SVD import SFP to be able to receive user data in a manner protected from modification and insertion errors.

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

5.3.2.4 Inter-TSF trusted channel (FTP_ITC.1)

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

5.3.3 Signature creation application (SCA)

5.3.3.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ SCA Hash	The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes none that meet the following: List of approved algorithms and parameters.

5.3.3.2 Data exchange integrity (FDP_UIT.1)

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

5.3.3.3 Inter-TSF trusted channel (FTP_ITC.1)

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

5.3.3.4 Trusted path (FTP_TRP.1)

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

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

FTP_TRP.1.2/ SCA — The TSF shall permit [*selection: the TSF, local users*] to initiate communication via the trusted path.

FTP_TRP.1.3/ SCA — The TSF shall require the use of the trusted path for [*selection: initial user authentication*] [*assignment: other services for which trusted path is required*].

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 ensures 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 stores the SCD corresponding to the SVD to be included in the qualified certificate.

6 Rationale

6.1 Introduction

The tables in sub-sections 6.2.1 “Security Objectives Coverage” and 6.3.1 “Security Requirement Coverage” provide the mapping of the security objectives and security requirements for the TOE.

6.2 Security Objectives Rationale

6.2.1 Security Objectives Coverage

Table 6.1 : Security Environment to Security Objectives Mapping

Threats – Assumptions - Policies / Security objectives	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.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OE.SCD_SVD_Corresp	OE.SCD_Transfer	OE_SCD_Unique	OE.CGA_QCert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend
T.Hack_Phys	x			x			x	x										
T.SCD_Divulg			x	x									X					
T.SCD_Derive											x			x				
T.SVD_Forgery						x										x		
T.DTBS_Forgery									x									x
T.SigF_Misuse									x	x							x	x
T.Sig_Forgery	x	x	x	x	x	x	x	x			x	x	x		x	x		x
T.Sig_Repud	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x		x
A.SCD_Generate												x	x	x				
A.CGA															x	x		
A.SCA																		x
P.CSP_Qcert					x							x			x			
P.Qsign										x	x				x			x
P.Sigy_SSCD										x				x				

6.2.2 Security Objectives Sufficiency

6.2.2.1 Policies and Security Objective Sufficiency

P.CSP_QCert (CSP generates qualified certificates) establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by the TOE by OT.SCD_SVD_Corresp and OE.SCD_SVD_Corresp concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by OE.CGA_QCert for generation of qualified certificates by the CGA, respectively.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by OT.Sigy_SigF ensuring that the SCD is under sole control of the signatory and OE.SCD_Unique ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature.

6.2.2.2 Threats and Security Objective Sufficiency

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. Physical attacks through the TOE interfaces or observation of TOE emanations are countered by OT.EMSEC_Design. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tamper attacks.

T.SCD_Divulg (Storing and copying and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by OT.SCD_Secrecy which assures the secrecy of the SCD used for signature generation. OT.SCD_Transfer and OE.SCD_Transfer ensures ensures the confidentiality of the SCD transferred between SSCDs.

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OE.SCD_Unique that provides cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which then does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent.

T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create SDO for data the signatory has not decided to sign, as required by the Directive [1], Annex III, paragraph 1, literal (c). This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of OT.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.SCD_Transfer (Secure transfer of SCD between SSCD), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows:

OT.Sig_Secure ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. OE.SCA_Data_Intend provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, OT.SCD_Transfer, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert **(**Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-

creation data), OT.SCD_Transfer (Secure transfer of SCD between SSCD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity).

OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OT.Sig_Secure, OT.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. OE.SCA_Data_Intend and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SVD_Auth_TOE which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by OE.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA.

6.2.2.3 Assumptions and Security Objective Sufficiency

A.SCD_Generate *Trustworthy SCD/SVD* generation establishes a trustworthy SCD/SVD pair. This that the SCD must be unique, objective met by OE.SCD_Unique, that the SCD and the SVD must correspond, objective met by OE.SCD_SVD_Corresp. The secrecy of the SCD must be maintained while it is transferred to the TOE before being deleted, OE.SCD_Transfer.

A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by OE.SCA_Data_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE

A.CGA (Trustworthy certification-generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates) which ensures the generation of qualified certificates and by OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) which ensures the verification of the integrity of the received SVD and the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

Table 6.2 : Functional Requirement to TOE Security Objective Mapping

TOE Security Functional Requirement / TOE Security objectives	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.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FCS_CKM.4		x	x	x							
FCS_COP.1/CORRESP					x						
FCS_COP.1/SIGNING											x
FDP_ACC.1/SVD Transfer SFP						x					
FDP_ACC.1/Personalisation SFP										x	
FDP_ACC.1/SCD Import SFP			x								
FDP_ACC.1/Signature-creation SFP									x	x	
FDP_ACF.1/SVD Transfer SFP						x					
FDP_ACF.1/Personalisation SFP										x	
FDP_ACF.1/SCD Import SFP			x								
FDP_ACF.1/Signature-creation SFP									x	x	
FDP_ETC.1/SVD Transfer						x					
FDP_ITC.1/SCD			x								
FDP_ITC.1/DTBS									x		
FDP_RIP.1				x						x	
FDP_SDI.2/DTBS									x		
FDP_SDI.2/Persistent				x	x					x	x
FDP_UCT.1/Receiver			x								
FDP_UIT.1/SVD Transfer						x					
FDP_UIT.1/TOE DTBS									x		
FIA_AFL.1										x	
FIA_ATD.1										x	
FIA_UAU.1										x	
FIA_UID.1										x	
FMT_MOF.1				x						x	
FMT_MSA.1/Administrator				x							
FMT_MSA.1/Signatory										x	
FMT_MSA.2			x							x	

TOE Security Functional Requirement / TOE Security objectives	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.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FMT_MSA.3			x	x						x	
FMT_MTD.1										x	
FMT_SMR.1			x	x						x	
FPT_AMT.1		x		x							x
FPT_EMSEC.1	x										
FPT_FLS.1				x							
FPT_PHP.1							x				
FPT_PHP.3								x			
FPT_TST.1		x									x
FTP_ITC.1/SCD Import			x								
FTP_ITC.1/SVD Transfer						x					
FTP_ITC.1/DTBS Import									x		
FTP_TRP.1/TOE										x	

Table 6.3: IT Environment Functional requirement to Environment Security Objective Mapping

Environment Security Requirement / Environment Security objectives	OE.SCD_SVD_Corresp	OE.SCD_Transfer	OE.SCD_Unique	OE.CGA_QCert	OE.HI_VAD	OE.SCA_Data_Intend	OE.SVD_Auth_CGA
FCS_CKM.1	x		x				
FCS_CKM.4/Type1		x					
FCS_COP.1/CORRESP	x						
FDP_ACC.1/SCD Export SFP		X					
FDP_UCT.1/Sender		X					
FTP_ITC.1/SCD Export		X					
FCS_CKM.2/CGA				x			
FCS_CKM.3/CGA				x			
FDP_UIT.1/SVD Import							x
FTP_ITC.1/SVD Import							x
FCS_COP.1/SCA HASH						x	
FDP_UIT.1/SCA DTBS						x	
FTP_ITC.1/SCA DTBS						x	
FTP_TRP.1/SCA					x		
R.Sigy_Name				x			

Table 6.4 : Assurance Requirement to Security Objective Mapping

Objectives	Requirement
Security Assurance Requirements	
OT.Lifecycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, ADO_IGS.1
OT.SCD_Secrecy	ADV_IMP.1, AVA_SOF.1, AVA_VLA.4
OT.Sig_Secure	AVA_VLA.4
OT.Sigy_SigF	AVA_MSU.3, AVA_SOF.1, AVA.VLA.4
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_IGS.1, ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

6.3.2 Security Requirements Sufficiency

6.3.2.1 TOE Security Requirements Sufficiency

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1 and FPT_AMT.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD to conclude the operational usage of the TOE as SSCD.

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1/Administrator, FMT_MSA.3, and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Cryptographic correspondence is provided by FCS_COP.1/CORRESP

OT.SCD_Transfer (Secure transfer of SCD between SSCD) is provided by FDP_ITC.1/SCD Import and FDP_UCT.1/Receiver that ensure that a trusted channel is provided and that confidentiality is maintained.

Security functions specified by FDP_ACC.1/SCD Import SFP, FMT_MSA.2, FMT_MSA.3, FMT_SMR.1, and FDP_ACF.1/SCD Import SFP ensure that transfer of SCDs is restricted to administrators. This supports the confidentiality-oriented functions.

Security function FCS_CKM.4 destroys the SCD before a SCD is re-imported into the TOE.

OT.DTBS_Integrity_TOE (Verification of DTBS-representation integrity) covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS Import, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/Signature-creation SFP and FDP_ACF.1/Signature-creation SFP keeps unauthorised parties off from altering the DTBS-representation.

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated.

The security functions specified by FDP_ACC.1/Personalisation SFP, FDP_ACC.1/Signature-creation SFP, FDP_ACF.1/Personalisation SFP, FDP_ACF.1/Signature-creation SFP, FMT_MTD.1 and FMT_SMR.1 ensure that the signature process is restricted to the signatory.

The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and MSA.3 ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as FMT_MSA.1/Signatory provides that the control of corresponding security attributes is under signatory's control.

The security functions specified by FDP_SDI.2/Perssistent and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored.

The security functions specified by FDP_RIP.1 and FIA_AFL.1 provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

The assurance measures specified by AVA_MSU.3 by requesting analysis of misuse of the TOE implementation, AVA_SOF.1 by requesting high strength level for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1/SIGNING which ensures the cryptographic robustness of the signature algorithms. The security functions specified by FPT_AMT.1 and FPT_TST.1 ensure that the security functions are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE.

OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD) is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD Transfer and FDP_UIT.1/SVD Transfer. The cryptographic algorithms specified by FDP_ACC.1/SVD Transfer SFP, FDP_ACF.1/SVD Transfer SFP and FDP_ETC.1/SVD Transfer ensure that only authorised user can Import the SVD from a SSCD Type1 and Export the SVD to the CGA.

OT.Tamper_ID (Tamper detection) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

6.3.2.2 TOE Enviroment Security Requirements Sufficiency

OE.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. Cryptographic correspondence is provided by FCS_COP.1/CORRESP

OE.SCD_Transfer (Secure transfer of SCD between SSCD) is provided by FDP_UCT.1/Sender, that ensure that a trusted channel is provided and that confidentiality is maintained.

Security functions complying with FDP_ACC.1/Export SFP and FTP_ITC.1/ SCD Export ensure that only TOE may export the SCD. Security function specified by FCS_CKM.4/Type1 destroy the SCD, once exported from the TOE.

OE.SCD_Unique (Uniqueness of the signature-creation data) stores the requirement of practically unique SCD as laid down in the Directive [1], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

OE.CGA_QCert (Generation of qualified certificates) addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA ensure that the CGA imports the SVD using a secure channel and a secure key access method.

OE.HI_VAD (Protection of the VAD) covers confidentiality and integrity of the VAD which is provided by the trusted path FTP_TRP.1/SCA.

OE.SCA_Data_Intend (Data intended to be signed) is provided by the functions specified by FTP_ITC.1/SCA DTBS and FDP_UIT.1/SCA DTBS that ensure that the DTBS can be checked by the TOE, and FCS_COP.1/SCA HASH that provides that the hashing function corresponds to the approved algorithms.

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD.Import which assures identification of the sender and by FDP_UIT.1/ SVD Import. which guarantees it’s integrity

6.4 Dependency Rationale

6.4.1 Functional and Assurance Requirements Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled. The functional requirements dependencies for the TOE environment are not completely fulfilled (see section 6.4.2 for justification).

Table 6.5 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.4	FDP_ITC.1/SCD, FMT_MSA.2
FCS_COP.1/ CORRESP	FDP_ITC.1/DTBS, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ SIGNING	FDP_ITC.1/SCD, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1/ PERSONALISATION SFP	FDP_ACF.1/PERSONALISATION SFP
FDP_ACC.1/ SCD Import SFP	FDP_ACF.1/SCD IMPORT SFP
FDP_ACC.1/ SIGNATURE-CREATION SFP	FDP_ACF.1/SIGNATURE CREATION SFP
FDP_ACC.1/ SVD Transfer SFP	FDP_ACF.1/SVD Transfer SFP
FDP_ACF.1/ PERSONALISATION SFP	FDP_ACC.1/PERSONALISATION SFP, FMT_MSA.3
FDP_ACF.1/ SCD Import SFP	FDP_ACC.1/SCD Import SFP, FMT_MSA.3
FDP_ACF.1/ SIGNATURE-CREATION SFP	FDP_ACC.1/SIGNATURE-CREATION SFP, FMT_MSA.3
FDP_ACF.1/ SVD Transfer SFP	FDP_ACC.1/SVD Transfer SFP, FMT_MSA.3
FDP_ETC.1/ SVD Transfer SFP	FDP_ACC.1/ SVD Transfer SFP
FDP_ITC.1/SCD	FDP_ACC.1/ SCD Import SFP, FMT_MSA.3
FDP_ITC.1/DTBS	FDP_ACC.1/ SIGNATURE-CREATION SFP, FMT_MSA.3
FDP_UCT.1/ RECEIVER	FTP_ITC.1/SCD Import, FDP_ACC.1/ SCD Import SFP
FDP_UIT.1/ SVD Transfer	FTP_ITC.1/SVD Transfer, FDP_ACC.1/SVD Transfer SFP
FDP_UIT.1/ TOE DTBS	FDP_ACC.1/SIGNATURE_CREATION SFP, FTP_ITC.1/DTBS Import
FIA_AFL.1	FIA_UAU.1

Requirement	Dependencies
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1/ Administrator	FDP_ACC.1/SCD import SFP, FMT_SMR.1
FMT_MSA.1/ Signatory	FDP_ACC.1/SIGNATURE_CREATION SFP, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1/PERSONALISATION SFP, FMT_SMR.1 FMT_MSA.1/Administrator, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1/Administrator, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1
FPT_FLS.1	ADV_SPM.1
FPT_PHP.1	FMT_MOF.1
FPT_TST.1	FPT_AMT.1
Assurance Requirements	
ACM_AUT.1	ACM_CAP.3
ACM_CAP.4	ACM_SCP.1, ALC_DVS.1
ACM_SCP.2	ACM_CAP.3
ADO_DEL.2	ACM_CAP.3
ADO_IGS.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1
ADV_IMP.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1
ADV_SPM.1	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_TAT.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.3 AVA_SOF.1	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1 ADV_FSP.1, ADV_HLD.1
AVA_VLA.4	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1
Functional Requirement for SSCD Type1	
FCS_CKM.1	FCS_CKM.4/Type1, FCS_COP.1/CORRESP, unsupported dependencies, see sub-section 6.4.2 for justification
FCS_CKM.4/Type1	FCS_CKM.1, unsupported dependencies, see sub-section 6.4.2 for justification
FCS_COP.1/CORRESP	FCS_CKM.1, FCS_CKM.4/Type1, unsupported dependencies, see sub-section 6.4.2 for justification
FDP/ACC.1/ SCD Export SFP	unsupported dependencies, see sub-section 6.4.2 for justification

Requirement	Dependencies
FDP_UCT.1/ Sender	FDP/ACC.1/SCD Export, FTP_ITC.1/SCD Export
FTP_ITC.1/ SCD Export	None
Functional Requirements for Certification generation application (GGA)	
FCS_CKM.2/CGA	unsupported dependencies, see sub-section 6.4.2 for justification
FCS_CKM.3/CGA	unsupported dependencies, see sub-section 6.4.2 for justification
FDP_UIT.1/ SVD Import	FTP_ITC.1/SVD Import, unsupported dependencies, see sub-section 6.4.2 for justification
FTP_ITC.1/ SVD Import	None
Functional Requirements for Signature creation application (SCA)	
FCS_COP.1/ SCA HASH	Unsupported dependencies, see sub-section 6.4.2 for justification
FDP_UIT.1/ SCA DTBS	FTP_ITC.1/SCA DTBS, unsupported dependencies on FDP_ACC.1, see sub-section 6.4.2 for justification
FTP_ITC.1/ SCA DTBS	None
FTP_TRP.1/ SCA	None

6.4.2 Justification of Unsupported Dependencies

The security functional dependencies for the TOE environment SSCD Type1, CGA and SCA are not completely supported by security functional requirements in section 5.3.

FCS_CKM.1	The SSCD Type1 generates the SCD/SVD pair. The dependency for cryptographic secure key generation is supported by FCS_COP.1/CORRESP, verification of SCD/SVD correspondence, and the key destruction by FCS_CKM.4/Type1. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FCS_CKM.4/Type1	The SSCD Type1 destroys the SCD once it has been exported. The dependency for key generation is supported by FCS_CKM.1. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FCS_COP.1/ CORRESP	The SSCD Type1 does a cryptographic operation when creating the SCD/SVD pair, FCS_CKM.1 and when destroying it, FCS_CKM.4/Type1. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FDP/ACC.1/ SCD Export SFP	The SSCD Type1 will follow the SCD export SFP when exporting the SCD. The access control required by this SFP, FDP_ACF.1 Security attribute based access control, is outside the scope of this PP.

FCS_CKM.2/ CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FCS_CKM.3/ CGA	The CGA imports SVD via trusted cannel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FDP_UIT.1/ SVD Import (CGA)	The access control (FDP_ACC.1) for the CGA is outside the scope of this PP.
FCS_COP.1/ SCA HASH	The hash algorithm implemented by FCS_COP.1/SCA HASH does not require any key or security management. Therefore FDP_ITC.1, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 are not required for FCS_COP.1/SCA HASH in the SCA.
FDP_UIT.1/ SCA DTBS	Access control (FDP_ACC.1.1) for the SCA are outside of the scope of this PP.

6.5 Security Requirements Grounding in Objectives

This chapter covers the grounding that have not been done in the precedent chapter.

Table 6.6: Assurance and Functional Requirement to Security Objective Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.1	EAL 4
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL4, OT.Lifecycle_Security
ALC_LCD.1	EAL4, OT.Lifecycle_Security
ALC_TAT.1	EAL4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	OT.Sigy_SigF
AVA_SOF.1	EAL 4, OT.SCD_Secrecy, OT.Sigy_SigF
AVA_VLA.4	OT.SCD_Secrecy, OT.Sig_Secure,
Security Objectives for the Environment	
R.Administrator_Guide	AGD_ADM.1
R.Sigy_Guide	AGD_USR.1
R.Sigy_Name	OE.CGA_QCert

6.6 Rationale for Extensions

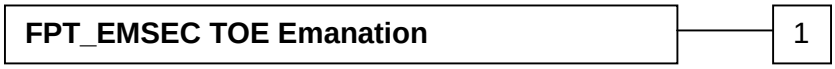
The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations.

6.6.1 FPT_EMSEC TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE Emanation has two constituents:

- FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

- FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

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]*.

Hierarchical to: No other components.

Dependencies: No other components.

6.7 Rationale for Strength of Function High

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The protection against attacks with a high attack potential dictates a strength of function high rating for functions in the TOE that are realised by probabilistic or permutational mechanisms.

6.8 Rationale for Assurance Level 4 Augmented

The assurance level for this protection profile is EAL4 augmented.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. Augmentation results from the selection of:

AVA_MSU.3 Vulnerability Assessment - Misuse - Analysis and testing for insecure states
AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE is intended to function in a variety of signature generation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

In **AVA_MSU.3**, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing by the evaluator. AVA_MSU.3 has the following dependencies:

ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. AVA_VLA.4 has the following dependencies:

ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

All of these are met or exceeded in the EAL4 assurance package.

References

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

[2] International Organization for Standardization, ISO/IEC 15408-1:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, 1999.

[3] International Organization for Standardization, *ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[4] International Organization for Standardization, *ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.

[5] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.

Appendix A - Acronyms

CC Common Criteria

EAL Evaluation Assurance Level

IT Information Technology

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSFI TSF Interface

TSP TOE Security Policy

—— this page was intentionally left blank ——

Annex C

This Annex C, with the exception of its pagination, is deemed to be identical to the PP that has been certified by BSI and which is available at http://www.bsi.de/cc/pplist/PP0006b.pdf.

Nevertheless, in case of any discrepancies between the PP available from the BSI web-site and the PP in this Annex C, it is the PP published by BSI that is the normative one.

Protection Profile — Secure Signature-Creation Device Type 3

Version: 1.05, EAL 4+

Wednesday, 25 July 2001

Prepared By: ESIGN Workshop - Expert Group F

Prepared For: CEN/ISSS

Note: **This Protection Profile (PP) has been prepared for the European Electronic Signature Standardisation Initiative EESSI by CEN/ISSS area F on secure signature-creation devices (SSCDs). In its present form it represents one of two documents that the CEN/ISSS E-Sign Workshop decided at its Brussels meeting 21st November 2000 to forward to the EESSI Steering Committee—one defining evaluation assurance level *EAL 4 augmented* and one defining *EAL 4*.**

The actual PP is EAL 4 augmented by AVA_VLA.4 and AVA_MSU.3, strength of function high.

—— this page was intentionally left blank ——

Foreword

This ‘Protection Profile — Secure Signature-Creation Device’ is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) Electronic Signatures (E-SIGN) workshop. The document represents Annex A of the CEN/ISSS workshop agreement (CWA) on secure signature-creation devices.

The document is for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

The document has been prepared as a Protection Profile (PP) following the rules and formats of ISO 15408, as known as the Common Criteria version 2.1 [2] [3] [4].

The set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is given in a separate document in [5].

Correspondence and comments to this secure signature-creation device protection profile (SSCD-PP) should be referred to:

CONTACT ADDRESS

CEC/ISSS Secretariat
Rue de Stassart 36
1050 Brussels, Belgium

Tel +32 2 550 0813
Fax +32 2 550 0966

Email isss@cenorm.be

—— this page was intentionally left blank ——

Revision History

v1.0-draft	22.09.00	submitted to CEN/ISSS WS/E-Sign Workshop
v1.0-final	16.11.00	for ballot by WS/E-Sign at Brussels meeting (11/00)
v1.0-EAL4+	28.11.00	for submission to European Commission by EESSI
v1.01-EAL4+	01.02.01	for ballot by WS/E-Sign at Brussels meeting (12/01)
v1.02-EAL4+	14.02.01	for ballot by WS/E-Sign as decided at Brussels meeting.
V1.03-EAL4+	15.06.01	Type3 PP extracted from SSCD approved by WS/E-Sign ballot to comply with the request of the evaluator.
V1.04-EAL4+	10.07.01	Type3 PP revised to comply with the request of the evaluator.
V1.05-EAL4+	25.07.01	Type3 PP revised to comply with the request of the evaluator.

—— this page was intentionally left blank ——

Table Of Contents

—— this page was intentionally left blank ——

List of Tables

—— this page was intentionally left blank ——

Conventions and Terminology

Conventions

The document follows the rules and conventions laid out in Common Criteria 2.1, part 1 [2], Annex B "Specification of Protection Profiles". Admissible algorithms and parameters for algorithms for secure signature-creation devices (SSCD) are given in a separate document [5]. Therefore, the Protection Profile (PP) refers to [5].

Terminology

Administrator means an user that performs TOE initialisation, TOE personalisation, or other TOE administrative functions.

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Authentication data is information used to verify the claimed identity of a user.

CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN). This Protection Profile (PP) represents Annex A to the CWA that has been developed by the European Electronic Signature Standardisation Initiative (EESSI) CEN/ISSS electronic signature (E-SIGN) workshop, Area F on secure signature-creation devices (SSCD).

Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)

Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of

(a) the SSCD proof of correspondence between SCD and SVD and
(b) checking the sender and integrity of the received SVD.

Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. (defined in the Directive [1], article 2.11)

Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).

Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is

(a) a hash-value of the DTBS or
(b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
(c) the DTBS.

The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.

Directive The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] is also referred to as the 'Directive' in the remainder of the PP.

Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], article 2.10)

Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by a SSCD according to the Directive [1], article 5, paragraph 1.

Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).

Signatory means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (defined in the Directive [1], article 2.3)

Signature attributes means additional information that is signed together with the user message.

Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements

(a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision,
(b) to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intend to sign,
(c) to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.

Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive [1], article 2.4)

Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.

Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [1], article 2.7)

Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.

SSCD provision service means a service that prepares and provides a SSCD to subscribers.

User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

Document Organisation

Section 1 provides the introductory material for the Protection Profile.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

A reference section is provided to identify background material.

An acronym list is provided to define frequently used acronyms.

1 Introduction

This section provides document management and overview information that is required to carry out protection profile registry. Therefore, section 1.1 “Identification” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Section 1.2 “Protection Profile Overview” summarises the PP in narrative form. As such, the section gives an overview to the potential user to decide whether the PP is of interest. It is usable as stand-alone abstract in PP catalogues and registers.

1.1 Identification

Title:	Protection Profile — Secure Signature-Creation Device Type 3
Authors:	Wolfgang Killmann, Herbert Leitold, Reinhard Posch, Patrick Sallé, Bruno Baronnet
Vetting Status:	
CC Version:	2.1 Final
General Status:	Final Ballot Draft
Version Number:	1.05
Registration:	
Keywords:	secure signature-creation device, electronic signature

1.2 Protection Profile Overview

This Protection Profile (PP) is established by CEN/ISSS for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1], also referred to as the ‘Directive’ in the remainder of the PP, as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

The intent of this Protection Profile is to specify functional and assurance requirements defined in the Directive [1], Annex III for secure signature-creation devices (SSCD) which is the target of evaluation (TOE). Member States shall presume that there is compliance with the requirements laid down in Annex III of the Directive [1] when an electronic signature product is evaluated to a Security Target (ST) that is compliant with this Protection Profile.

The Protection Profile defines the security requirements of a SSCD for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures. The TOE may implement additional functions and security requirements e.g. for editing and displaying the data to be signed (DTBS), but these additional functions and security requirements are not subject of this Protection Profile.

The assurance level for this PP is EAL4 augmented. The minimum strength level for the TOE security functions is 'SOF high' (Strength of Functions High).

2 TOE Description

2.1 Secure Signature Creation Devices

The present document assumes a well defined process signature-creation to take place. The present chapter defines three possible SSCD implementations, referred to as 'SSCD types', as illustrated in Figure 1.

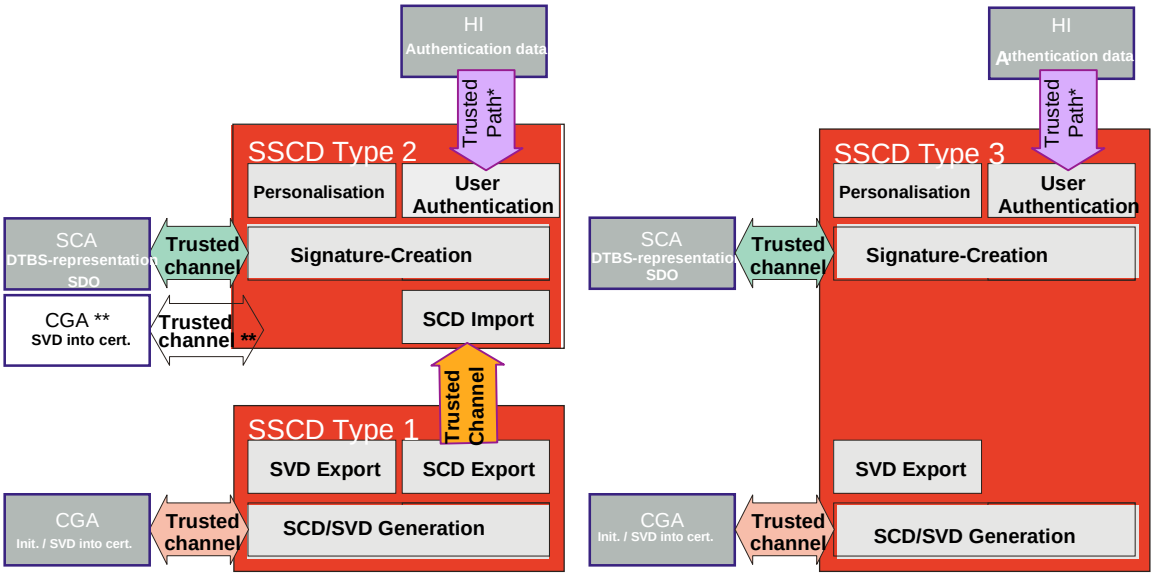
The left part of Figure 1 shows two SSCD components: A SSCD of Type 1 representing the SCD/SVD generation component, and a SSCD of Type 2 representing the SCD storage and signature-creation component. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel. The right part of Figure 1 shows a SSCD Type 3 which is analogous to a combination of Type 1 and Type 2, but no transfer of the SCD between two devices is provided.

If the SSCD holds the SVD and exports the SVD to a CGA for certification, a trusted channel is to be provided. The CGA initiates SCD/SVD generation ("Init.") and the SSCD exports the SVD for generation of the corresponding certificate ("SVD into cert.").

The signatory must be authenticated to create signatures that he sends his authentication data (e.g., a PIN) to the SSCD Type 2 or Type 3 (e.g., a smart card). If the human interface (HI) for such signatory authentication is not provided by the SSCD, a trusted path (e.g., a encrypted channel) between the SSCD and the SCA implementing to HI is to be provided. The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be transferred by the SCA to the SSCD only over a trusted channel. The same shall apply to the signed data object (SDO) returned from a SSCD to the SCA.

SSCD Type 1 is not a personalized component in the sense that it may be used by a specific user only, but the SCD/SVD generation and export shall be initiated by authorized persons only (e.g., system administrator).

SSCD Type 2 and Type 3 are personalized components which means that they can be used for signature creation by one specific user – the signatory - only.



* The trusted path for user authentication will be required if the HI is not provided by the TOE itself (e. g., it is provided by a SCA outside the SSCD)
** The trusted channel between the SSCD Type 2 and the CGA is required for cases where the SSCD type 2 holds the SVD and export of the SVD to the CGA for certification is provided.

Figure 1: SSCD types and modes of operation

2.2 Limits of the TOE

The TOE is a secure signature-creation device (SSCD type3) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1]. The destruction of the SCD is mandatory before the TOE generate a new pair SCD/SVD.
A SSCD is configured software or hardware used to implement the signature-creation data (SCD).

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:

(1) to generate the SCD and the correspondent signature-verification data (SVD) and
(2) to create qualified electronic signatures
  (a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function may either be provided by the TOE itself or by appropriate environment
  (b) using appropriate hash functions that are, according to [5], agreed as suitable for qualified electronic signatures
  (c) after appropriate authentication of the signatory by the TOE.
  (d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable according to [5].

The TOE implements all IT security functionality which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The TOE may provide an interface for user authentication by its own or implements IT measures to support a trusted path to a trusted human interface device.

In addition to the functions of the SSCD, the TOE may implement the signature-creation application (SCA). The SCA presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. But this PP assumes the SCA as environment of the TOE because the PP describes the SCD-related security objectives and requirements, whereas the SCA does not implement the SCD. If a SSCD implements a SCA than it will fulfil the security objective and requirements for the TOE, as well as for the SCA as specific TOE environment in the actual PP.

The SSCD protects the SCD during the whole life cycle as to be solely used in the signature-creation process by the legitimate signatory. The TOE will be initialised for the signatory's use by

(1) generating a SCD/SVD pair
(2) personalisation for the signatory by means of the signatory's verification authentication data (SVAD).

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). The TOE will destroy the SCD it is no longer used for signature generation.

The TOE allows to implement a human interface for user authentication:

(i) by the TOE itself or
(ii) by a trusted human interface device connected via a trusted channel with the TOE.

The human interface device is used for the input of VAD for authentication by knowledge or for the generation of VAD for authentication by biometric characteristics. The TOE holds RAD to check the provided VAD. The human interface implies appropriate hardware. The second approach allows to reduce the TOE hardware to a minimum e. g. a smart card.

Figure 2 shows the PP scope from the structural perspective. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the SCD/SVD generation, SCD storage and use, and signature-creation functionality. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE. They shall communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively.

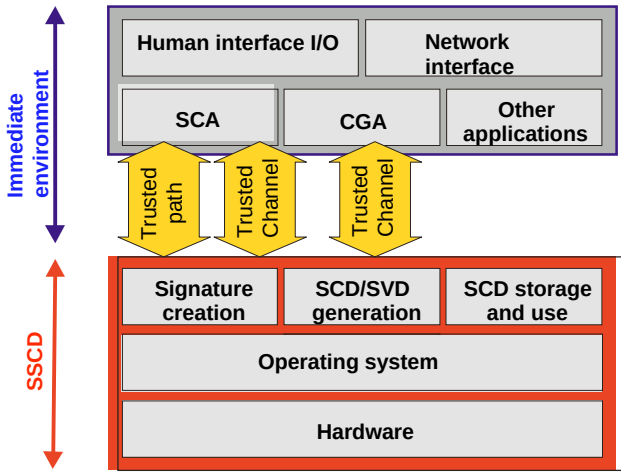


Figure 2: Scope of the SSCD, structural view

The TOE life cycle is shown in Figure 3. Basically, it consists of a development phase and the operational phase. This document refers to the operational phase which starts with personalisation including SCD/SVD generation and SCD import if necessary. This phase represents installation, generation, and start-up in the CC terminology . The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., SCD storage and SCD use). The life cycle ends with the destruction of the SSCD.

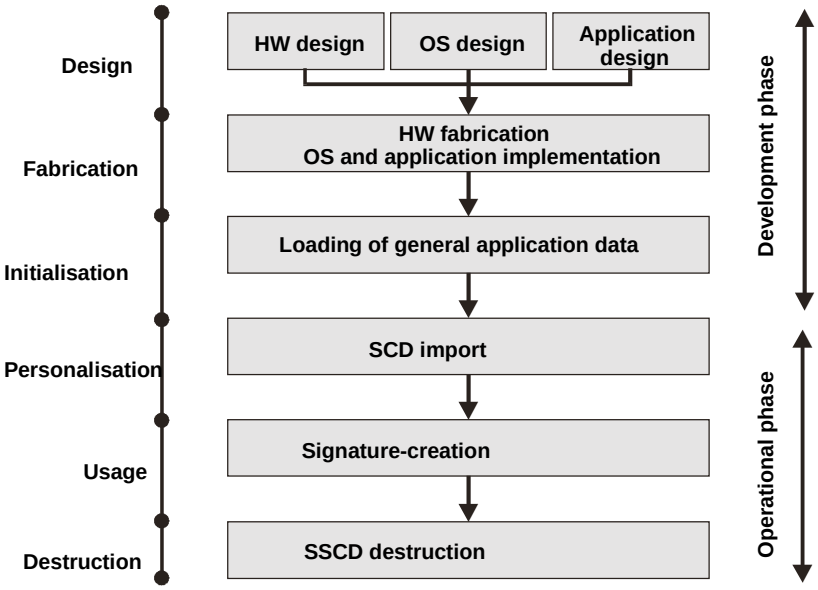


Figure 3. SSCD life cycle

Application note: Scope of SSCD PP application

This SSCD PP refers to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is implemented by the TOE.

While the main application scenario of a SSCD will assume a qualified certificate to be used in combination with a SSCD, there still is a large benefit in the security when such SSCD is applied in other areas and such application is encouraged. The SSCD PP may as well be applied to environments where the certificates expressed as 'qualified certificates' in the SSCD PP do not fulfil the requirements laid down in Annex I and Annex II of the Directive [1].

With this respect the notion of qualified certificates in the PP refers to the fact that when an instance of a SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive [1], article 5, paragraph 1. As a consequence, this standard does not prevent a device itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

3 TOE Security Environment

Assets:

1. SCD: private key used to perform an electronic signature operation(confidentiality of the SCD must be maintained).

2. 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).

3. DTBS and DTBS-representation: set of data, or its representation which is intended to be signed (Their integrity must be maintained).

4. VAD: PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)

5. RAD: Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)

6. 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)

7. Electronic signature: (Unforgeabilty of electronic signatures must be assured).

Subjects

Subjects	**Definition**
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory
S.Admin	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

Threat agents

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

3.1 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.

3.2 Threats to Security

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 atacker 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 repudation of the electronic signature is compromised. This results in 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 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*

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.

3.3 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 (according to directive Annex 1) 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

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

4.1 Security Objectives for the TOE

OT.EMSEC_Design *Provide physical emanations security*

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

OT.Lifecycle_Security *Lifecycle security*

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

OT.SCD_Secrecy *Secrecy of the signature-creation data*

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

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

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

OT.SVD_Auth_TOE *TOE ensures authenticity of the SVD*

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

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.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.DTBS_Integrity_TOE *Verification of the DTBS-representation integrity*

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

OT.Sigy_SigF *Signature generation function for the legitimate signatory only*

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

OT.Sig_Secure *Cryptographic security of the electronic signature*

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

4.2 Security Objectives for the Environment

OE.CGA_QCert *Generation of qualified certificates*

The CGA generates qualified certificates which include inter alia
(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,
(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA *CGA verifies the authenticity of the SVD*

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

OE.HI_VAD *Protection of the VAD*

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

OE.SCA_Data_Intend *Data intended to be signed*

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

5 IT Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE and the environment.

Security functional requirements components given in section 5.1 “TOE security functional requirements” excepting FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 [3]. Some security functional requirements represent extensions to [3]. Operations for assignment, selection and refinement have been made. Operations not performed in this PP are identified in order to enable instantiation of the PP to a Security Target (ST).

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [4].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

5.1 TOE Security Functional Requirements

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

5.1.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

Application notes:

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 by the TOE.

5.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.
FCS_COP.1.1/ SIGNING	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

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/ Initialisation SFP	The TSF shall enforce the Initialisation SFP on generation of SCD/SVD pair 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 1. sending of DTBS-representation by SCA, 2. signing of DTBS-representation by Signatory.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

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

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
Initialisation attribute		
User	SCD / SVD management	authorised, not authorised
Signature-creation attribute group		
SCD	SCD operational	no, yes
DTBS	sent by an authorised SCA	no, yes

Initialisation SFP

FDP_ACF.1.1/ Initialisation SFP — The TSF shall enforce the Initialisation SFP to objects based on 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 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

FDP_ACF.1.1/ SVD Transfer SFP — The TSF shall enforce the SVD Transfer SFP to objects based on General attribute.

FDP_ACF.1.2/ SVD Transfer SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute “role” set to “Administrator” or 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.

Personalisation SFP

FDP_ACF.1.1/ Personalisation SFP	The TSF shall enforce the Personalisation SFP to objects based on 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: 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 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 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 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 authorised 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 authorised SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

5.1.2.3 Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1/ SVD Transfer — The TSF shall enforce the SVD Transfer 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 Import of user data without security attributes (FDP_ITC.1)

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

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

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

Application note:

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

5.1.2.5 Subset residual information protection (FDP_RIP.1)

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, RAD.

5.1.2.6 Stored data integrity monitoring and action (FDP_SDI.2)

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

1. SCD
2. RAD
3. SVD (if persistent 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.

The DTBS-representation temporarily stored by TOE has 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 Data exchange integrity (FDP_UIT.1)

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.1.1/ TOE DTBS	The TSF shall enforce the Signature-creation SFP to be able to receive the DTBS-representation 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.

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1	The TSF shall detect when [*assignment: number*] 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.

5.1.3.2 User attribute definition (FIA_ATD.1)

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

5.1.3.3 Timing of authentication (FIA_UAU.1)

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 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 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.

5.1.3.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow
1. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.
2. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import.]

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

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (FMT_MOF.1)

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

5.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ Administrator — The TSF shall enforce the Initialisation SFP to restrict the ability to modify [*assignment: other operations*] the security attributes SCD / SVD management 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.

5.1.4.3 Secure security attributes (FMT_MSA.2)

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

5.1.4.4 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 — 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 — The TSF shall allow the Administrator to specify alternative initial values to override the default values when an object or information is created.

5.1.4.5 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 — The TSF shall restrict the ability to modify [*assignment: other operations*] the RAD to Signatory.

5.1.4.6 Security roles (FMT_SMR.1)

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 Protection of the TSF (FPT)

5.1.5.1 Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1 — The TSF shall run a suite of tests [*selection: during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.5.2 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [*assignment: specified limits*] enabling access to RAD and SCD.

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 RAD and SCD.

Application note:

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation**,** simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

5.1.5.3 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*assignment: list of types of failures in the TSF*].

5.1.5.4 Passive detection of physical attack (FPT_PHP.1)

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.

5.1.5.5 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist [*assignment: physical tampering scenarios*] to the [*assignment: list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

5.1.5.6 TSF testing (FPT_TST.1)

FPT_TST.1.1	The TSF shall run a suite of self tests [*selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*][*assignment: conditions under which self test should occur*] 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 Trusted path/channels (FTP)

5.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SVD Transfer	The TSF shall provide a communication channel between itself and a remote trusted IT product **CGA** 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 [*selection: the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3/ SVD Transfer	The TSF **or the CGA** shall initiate communication via the trusted channel for export SVD.
.	
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 **SCA** to initiate communication via the trusted channel.
FTP_ITC.1.3/ DTBS import	The TSF **or the SCA** shall initiate communication via the trusted channel for signing DTBS-representation.

5.1.6.2 Trusted path (FTP_TRP.1)

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

FTP_TRP.1.1/ TOE	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ TOE	The TSF shall permit [*selection: the TSF, 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 [*selection: initial user authentication*][*assignment: other services for which trusted path is required*].

5.2 TOE Security Assurance Requirements

Table 5.1 Assurance Requirements: EAL(4)

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4

5.2.1 Configuration management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1D	The developer shall use a CM system.
ACM_AUT.1.2D	The developer shall provide a CM plan.
ACM_AUT.1.1C	The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.
ACM_AUT.1.2C	The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3C	The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4C	The CM plan shall describe how the automated tools are used in the CM system.

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1D	The developer shall provide a reference for the TOE.
ACM_CAP.4.2D	The developer shall use a CM system.
ACM_CAP.4.3D	The developer shall provide CM documentation.
ACM_CAP.4.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2C	The TOE shall be labelled with its reference.
ACM_CAP.4.3C	The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.5C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.4.6C	The CM system shall uniquely identify all configuration items.
ACM_CAP.4.7C	The CM plan shall describe how the CM system is used.
ACM_CAP.4.8C	The evidence shall demonstrate that the CM system is operating

in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

5.2.1.3 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1D The developer shall provide CM documentation.

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.2.3.3 Implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into

TSP-enforcing and other modules.

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5 Life cycle support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the

physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.2.5.2 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

5.2.5.3 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional

specification and the tests identified in the test documentation is complete.

5.2.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

5.2.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Analysis and testing for insecure states (AVA_MSU.3)

AVA_MSU.3.1D The developer shall provide guidance documentation.

AVA_MSU.3.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.3.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.3.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.3.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.3.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.3.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.2.7.3 Highly resistant (AVA_VLA.4)

AVA_VLA.4.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.4.2D The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.4.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.4C The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

5.3 Security Requirements for the IT Environment

5.3.1 Certification generation application (CGA)

5.3.1.1 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1/ CGA The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method qualified certificate that meets the following: List of approved algorithms and parameters.

5.3.1.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA The TSF shall perform import the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following: [*assignment: list of standards*].

5.3.1.3 Data exchange integrity (FDP_UIT.1)

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

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

5.3.1.4 Inter-TSF trusted channel (FTP_ITC.1)

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

FTP_ITC.1.2/ SVD import The TSF shall permit [*selection: the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SVD import The TSF **or the TOE** shall initiate communication via the trusted channel for import SVD.

5.3.2 Signature creation application (SCA)

5.3.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ SCA Hash	The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes none that meet the following: List of approved algorithms and parameters.

5.3.2.2 Data exchange integrity (FDP_UIT.1)

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

5.3.2.3 Inter-TSF trusted channel (FTP_ITC.1)

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

5.3.2.4 Trusted path (FTP_TRP.1)

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

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

initial user authentication][*assignment: other services for which trusted path is required*].

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 ensures 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 Rationale

6.1 Introduction

The tables in sub-sections 6.2.1 “Security Objectives Coverage” and 6.3.1 “Security Requirement Coverage” provide the mapping of the security objectives and security requirements for the TOE .

6.2 Security Objectives Rationale

6.2.1 Security Objectives Coverage

Table 6.1-: Security Environment to Security Objectives Mapping

Error! Not a valid link.

6.2.2 Security Objectives Sufficiency

6.2.2.1 Policies and Security Objective Sufficiency

P.CSP_QCert (CSP generates qualified certificates) establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by the TOE by OT.SCD_SVD_Corresp concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by OE.CGA_QCert for generation of qualified certificates by the CGA, respectively.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by OT.Sigy_SigF ensuring that the SCD is under sole control of the signatory and OT.SCD_Unique ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. OT.Init provides that generation of the SCD/SVD pair is restricted to authorised users.

6.2.2.2 Threats and Security Objective Sufficiency

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. Physical attacks through the TOE interfaces or observation of TOE emanations are countered by OT.EMSEC_Design. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tamper attacks.

T.SCD_Divulg (Storing,copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by OT.SCD_Secrecy which assures the secrecy of the SCD used for signature generation.

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OT.SCD_Unique that provides cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which than does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent.

T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create SDO for data the signatory has not decided to sign, as required by the Directive [1], Annex III, paragraph 1, literal (c). This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of OT.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data),, OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows:

OT.Sig_Secure ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. OE.SCA_Data_Intend provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, , OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert **(**Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-creation data), , OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity).

OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OT.Sig_Secure, OT.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. OE.SCA_Data_Intend and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SVD_Auth_TOE which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by OE.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA.

6.2.2.3 Assumptions and Security Objective Sufficiency

A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by OE.SCA_Data_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE

A.CGA (Trustworthy certification-generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates) which ensures the generation of qualified certificates and by OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) which ensures the verification of the integrity of the received SVD and the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

Table 6.2 : Functional Requirement to TOE Security Objective Mapping

Error! Not a valid link.

Table 6.3 : IT Environment Functional requirements to Environment Security Objective Mapping

Error! Not a valid link.

Table 6.4: Assurances Requirement to Security Objective Mapping

Objectives	Requirements
Security Assurance Requirements	
OT.Lifecycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, ADO_IGS.1
OT.SCD_Secrecy	AVA_SOF.1, AVA_VLA.4
OT.Sigy_SigF	AVA_MSU.3, AVA_SOF.1
OT.Sig_Secure	AVA_VLA.4
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_IGS.1, ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

6.3.2 Security Requirements Sufficiency

6.3.2.1 TOE Security Requirements Sufficiency

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1.1.

OT.Init (SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_ATD.1 define RAD as the corresponding user attribute. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The attributes of the authenticated user are provided by FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3 for static attribute initialisation. Access control is provided by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1 and FPT_AMT.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD.

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functions specified by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP that ensure that only authorised user can initialise the TOE and create or load the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1, FMT_MSA.3 corresponding to the actual TOE (i.e., FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3), and

FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Cryptographic correspondence is provided by FCS_COP.1/CORRESP

OT.SCD_Unique (Uniqueness of the signature-creation data) implements the requirement of practically unique SCD as laid down in the Directive [1], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

OT.DTBS_Integrity_TOE (Verification of DTBS-representation integrity) covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS IMPORT, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/SIGNATURE CREATION SFP and FDP_ACF.1/SIGNATURE CREATION SFP keeps unauthorised parties off from altering the DTBS-representation.

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated.

The security functions specified by FDP_ACC.1/PERSONALISATION SFP, FDP_ACC.1/SIGNATURE-CREATION SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE-CREATION SFP, FMT_MTD.1 and FMT_SMR.1 ensure that the signature process is restricted to the signatory.

The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and FMT_MSA.3 ensure that the access to the signature generation functions remain under the sole control of

the signatory, as well as FMT_MSA.1/SIGNATORY provides that the control of corresponding security attributes is under signatory's control.

The security functions specified by FDP_SDI.2 and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored.

The security functions specified by FDP_RIP.1 and FIA_AFL.1 provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

The assurance measures specified by AVA_MSU.3 by requesting analysis of misuse of the TOE implementation, AVA_SOF.1 by requesting high strength level for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1/SIGNING which ensures the cryptographic robustness of the signature algorithms. The security functions specified by FPT_AMT.1 and FPT_TST.1 ensure that the security functions are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE.

OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD) is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD TRANSFER and FDP_UIT.1/SVD TRANSFER. The cryptographic algorithms specified by FDP_ACC.1/SVD TRANSFER SFP, FDP_ACF.1/SVD TRANSFER SFP and FDP_ETC.1/SVD TRANSFER ensure that only authorised user can export the SVD to the CGA.

OT.Tamper_ID (Tamper detection) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

6.3.2.2 TOE Environment Security Requirements Sufficiency

OE.CGA_QCert (Generation of qualified certificates) addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA ensure that the CGA imports the SVD using a secure channel and a secure key access method.

OE.HI_VAD (Protection of the VAD) covers confidentiality and integrity of the VAD which is provided by the trusted path FTP_TRP.1/SCA.

OE.SCA_Data_Intend (Data intended to be signed) is provided by the functions specified by FTP_ITC.1/SCA DTBS and FDP_UIT.1/SCA DTBS that ensure that the DTBS can be checked by the TOE, and FCS_COP.1/SCA HASH that provides that the hashing function corresponds to the approved algorithms.

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD.IMPORT which assures identification of the sender and by FDP_UIT.1/ SVD IMPORT. which guarantees it's integrity

6.4 Dependency Rationale

6.4.1 Functional and Assurance Requirements Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled. The functional requirements dependencies for the TOE environment are not completely fulfilled (see section 6.4.2 for justification).

Table 6.5 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1/SIGNING, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1/ CORRESP	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ SIGNING	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1/ Initialisation SFP	FDP_ACF.1/Initialisation SFP
FDP_ACC.1/ Personalisation SFP	FDP_ACF.1/Personalisation SFP
FDP_ACC.1/ Signature-Creation SFP	FDP_ACF.1/Signature Creation SFP
FDP_ACC.1/ SVD Transfer SFP	FDP_ACF.1/SVD Transfer SFP
FDP_ACF.1/ Initialisation SFP	FDP_ACC.1/Initialisation SFP, FMT_MSA.3
FDP_ACF.1/ Personalisation SFP	FDP_ACC.1/Personalisation SFP, FMT_MSA.3
FDP_ACF.1/ Signature-Creation SFP	FDP_ACC.1/Signature-Creation SFP, FMT_MSA.3
FDP_ACF.1/ SVD Transfer SFP	FDP_ACC.1/SVD Transfer SFP, FMT_MSA.3
FDP_ETC.1/ SVD Transfer SFP	FDP_ACC.1/ SVD Transfer SFP
FDP_ITC.1/DTBS	FDP_ACC.1/ Signature-Creation SFP, FMT_MSA.3
FDP_UIT.1/ SVD Transfer	FTP_ITC.1/SVD Transfer, FDP_ACC.1/SVD Transfer SFP
FDP_UIT.1/ TOE DTBS	FDP_ACC.1/Signature_Creation SFP, FTP_ITC.1/DTBS Import
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1/Administrator	FDP_ACC.1/Initialisation SFP, FMT_SMR.1

Requirement	Dependencies
FMT_MSA.1/ Signatory	FDP_ACC.1/ Signature_Creation SFP, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1/Personalisation SFP, FMT_SMR.1 FMT_MSA.1/Administrator, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1/Administrator, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1
FPT_FLS.1	ADV_SPM.1
FPT_PHP.1	FMT_MOF.1
FPT_TST.1	FPT_AMT.1
Assurance Requirements	
ACM_AUT.1	ACM_CAP.3
ACM_CAP.4	ACM_SCP.1, ALC_DVS.1
ACM_SCP.2	ACM_CAP.3
ADO_DEL.2	ACM_CAP.3
ADO_IGS.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1
ADV_IMP.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1
ADV_SPM.1	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_TAT.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.3	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.4	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1
Functional Requirements for Certification generation application (GGA)	
FCS_CKM.2/CGA	unsupported dependencies, see sub-section 6.4.2 for justification
FCS_CKM.3/CGA	unsupported dependencies, see sub-section 6.4.2 for justification
FDP_UIT.1/ SVD IMPORT	FTP_ITC.1/SVD IMPORT, unsupported dependencies, see sub-section 6.4.2 for justification ,
FTP_ITC.1/ SVD IMPORT	None
Functional Requirements for Signature creation application (SCA)	
FCS_COP.1/ SCA HASH	Unsupported dependencies, see sub-section 6.4.2 for justification
FDP_UIT.1/ SCA DTBS	FTP_ITC.1/ SCA DTBS, unsupported dependencies on FDP_ACC.1, see sub-section 6.4.2 for justification
FTP_ITC.1/ SCA DTBS	None
FTP_TRP.1/SCA	None

6.4.2 Justification of Unsupported Dependencies

The security functional dependencies for the TOE environment CGA and SCA are not completely supported by security functional requirements in section 5.3.

FCS_CKM.2/ CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FCS_CKM.3/ CGA	The CGA imports SVD via trusted cannel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FDP_UIT.1/ SVD Import (CGA)	The access control (FDP_ACC.1) for the CGA is outside the scope of this PP.
FCS_COP.1/ SCA HASH	The hash algorithm implemented by FCS_COP.1/SCA HASH does not require any key or security management. Therefore FDP_ITC.1, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 are not required for FCS_COP.1/SCA HASH in the SCA.
FDP_UIT.1/ SCA DTBS	Access control (FDP_ACC.1.1) for the SCA are outside of the scope of this PP.

6.5 Security Requirements Grounding in Objectives

This chapter covers the grounding that have not been done in the precedent chapter

Table 6.6 : Assurance Requirement to Security Objective Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.1	EAL 4
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL4, OT.Lifecycle_Security
ALC_LCD.1	EAL4, OT.Lifecycle_Security
ALC_TAT.1	EAL4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	OT.Sigy_SigF
AVA_SOF.1	EAL 4, OT.SCD_Secrecy, OT.Sigy_SigF
AVA_VLA.4	OT.SCD_Secrecy, OT.Sig_Secure,
Security Objectives for the Environment	
R.Administrator_Guide	AGD_ADM.1
R.Sigy_Guide	AGD_USR.1
R.Sigy_Name	OE.CGA_QCert

6.6 Rationale for Extensions

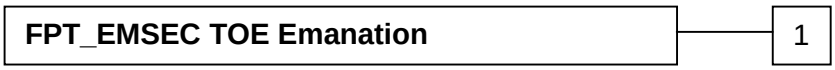
The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations.

6.6.1 FPT_EMSEC TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

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]*.

Hierarchical to: No other components.

Dependencies: No other components.

6.7 Rationale for Strength of Function High

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The protection against attacks with a high attack potential dictates a strength of function high rating for functions in the TOE that are realised by probabilistic or permutational mechanisms.

6.8 Rationale for Assurance Level 4 Augmented

The assurance level for this protection profile is EAL4 augmented.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. Augmentation results from the selection of:

AVA_MSU.3 Vulnerability Assessment - Misuse - Analysis and testing for insecure states
AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE is intended to function in a variety of signature generation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

In **AVA_MSU.3**, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing by the evaluator. AVA_MSU.3 has the following dependencies:

ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. AVA_VLA.4 has the following dependencies:

ADV_FSP.1 Informal functional specification
ADV_HLD.2 Security enforcing high-level design
ADV_IMP.1 Subset of the implementation of the TSF
ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

References

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

[2] International Organization for Standardization, ISO/IEC 15408-1:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, 1999.

[3] International Organization for Standardization, *ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[4] International Organization for Standardization, *ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.

[5] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.

Appendix A - Acronyms

CC Common Criteria

EAL Evaluation Assurance Level

IT Information Technology

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSFI TSF Interface

TSP TOE Security Policy

—— this page was intentionally left blank ——