

Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application

Schutzprofile sichere Signaturerstellungseinheit — Teil 6: Erweiterung für ein Gerät mit Schlüsselimport und vertrauenswürdiger Kommunikation zur Signaturanwendungskomponente

Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 6: Extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature

ICS:

Descriptors:

Contents		Page
1	Scope	4
2	Normative references	4
3	Conventions and terminology	4
	3.1 Conventions	4
	3.2 Terms and definitions	4
4	PP introduction	5
	4.1 PP reference	5
	4.2 PP overview	5
	4.3 TOE overview	6
5	Conformance claims	8
	5.1 CC conformance claim	8
	5.2 PP claim, Package claim	8
	5.3 Conformance rationale	8
	5.4 Conformance statement	9
6	Security problem definition	9
	6.1 Assets, users and threat agents	9
	6.2 Threats	10
	6.3 Organisational security policies	10
	6.4 Assumptions	10
7	Security objectives	10
	7.1 Security objectives for the TOE	10
	7.2 Security objectives for the operational environment	11
	7.3 Security objectives rationale	12
8	Extended components definition	15
9	Security requirements	15
	9.1 Security functional requirements	15
	9.2 Security assurance requirements	18
	9.3 Security requirements rationale	19
10	References	23

Foreword

This document (prEN 14169-6:2013) has been prepared by Technical Committee CEN/TC 224 "Personal identification, electronic signature and cards and their related systems and operations", the secretariat of which is held by AFNOR.

This document is a working document.

Introduction

This series of European standards specifies Common Criteria protection profiles for secure signature creation devices and is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) as update of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14169:2002, Annex B and Annex C on the protection profile secure signature creation devices, "EAL 4+".

This series of European standards consists of the following parts:

- Protection profiles for secure signature creation device — Part 1: Overview;
- Protection profiles for secure signature creation device — Part 2: Device with key generation;
- Protection profiles for secure signature creation device — Part 3: Device with key import;
- Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application;
- Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application;
- Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application.

Preparation of this document as a protection profile (PP) follows the rules of the Common Criteria version 3.1 [2], [3] and [4].

Correspondence and comments to this protection profile about secure signature creation device with key import and trusted communication with signature creation application (PP SSCD KI TCSCA) should be referred to:

CONTACT ADDRESS

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

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

Email isss@cenorm.be

1 Scope

This European standard specifies a protection profile for a secure signature creation device that may import signing keys and communicate with the signature creation application in protected manner: secure signature creation device with key import and trusted communication with signature creation application (SSCD KI TCSCA).

2 Normative references

For the application of this European standard the following documents are indispensable:

EN 14169-1, Protection profiles for secure signature creation device — Part 1: Overview¹

EN 14169-3, Protection profiles for secure signature creation device — Part 2: Device with key import²

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 4, CCMB-2012-09-001, September 2012

Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 4, CCMB-2012-09-002, September 2012

Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 4, CCMB-2012-09-003, September 2012

3 Conventions and terminology

3.1 Conventions

This document is drafted in accordance with the CEN/CENELEC directive and content and structure of this document follow the rules and conventions laid out in Common Criteria 3.1.

Normative aspects of content in this European standard are specified according to the Common Criteria rules and not specifically identified by the verbs “*shall*” or “*must*”.

3.2 Terms and definitions

For the purposes of this document, the acronyms, terms and definitions given in EN 14169-1 apply [6].

¹ To be published].

² To be published].

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application
Version:	1.0.4
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	2013-04-03
Registration:	BSI-CC-PP-0076
CC version:	3.1 Revision 4
Editor:	Arnold Abromeit, TÜV Informationstechnik GmbH
General status:	final
Keywords:	secure signature creation device, electronic signature, digital signature, key import, trusted communication with signature creation application

4.2 PP overview

This Protection Profile is established by CEN as a European standard for products to create electronic signatures. It fulfils requirements of directive³ 1999/93/ec of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures.

In accordance with article 9 of this European directive this standard can be indicated by the European commission in the Official Journal of the European Communities as generally recognised standard for electronic signature products.

This protection profile defines security functional requirements and security assurance requirements that comply with those defined in Annex III of the directive for a secure signature creation device (SSCD). This secure signature creation device is the target of evaluation (TOE) for this protection profile.

European Union Member States may presume that there is compliance with the requirements laid down in Annex III of the directive when an electronic signature product is evaluated to a Security Target (ST) that is compliant with this Protection Profile (PP).

This Protection Profile about secure signature creation device with key import and trusted communication with signature creation application (PP SSCD KI TCSCA) includes the security requirements for SSCD with key import importing signature creation data (SCD) and creating digital signature to be used for (qualified or advanced) electronic signatures as described in the core PP [7]. Additionally, the TOE of this PP supports a trusted communication with a signature creation application for protection of authentication data and data to be signed. These security features allow using the TOE in a more complex operational environment. It conforms to the core PP SSCD KI [7]. The implication of this conformance claim is explained in section 5.3 hereinafter.

The assurance level for this PP is EAL4 augmented with AVA_VAN.5.

³ This European directive is referred to in this PP as “the directive”.

4.3 TOE overview

4.3.1 Operation of the TOE

This section presents a functional overview of the TOE in its distinct operational environments:

- The preparation environment, where it interacts with a certification service provider through a SCD/SVD generation application to import the signature creation data (SCD) and a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the signature creation data (SCD) the certification service provider has generated. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference-authentication data (RAD).
- The signing environment where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting electronic signature⁴. The TOE and the SCA communicate through a trusted channel to ensure the integrity of the DTBS respective DTBS/R.
- The management environments where it interacts with the user or an SSCD-provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE. Figure 5 in Part 1 [6] of this standard illustrates the operational environment.

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case the TOE provides a function to identify each SCD and the signature creation application (SCA) can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The electronic signature created with the TOE is a *qualified electronic signature* as defined in **the directive** if the certificate for the SVD is a qualified certificate (Annex I). Determining the state of the certificate as qualified is beyond the scope of this standard.

The SCA is assumed to protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash values required. The TOE may augment the DTBS/R with signature parameters it stores and then computes a hash value over the input as needed by the kind of input and the used cryptographic algorithm. The TOE and the SCA communicate through a trusted channel in order to protect the integrity of the DTBS/R.

The TOE stores signatory reference authentication data to authenticate a user as its signatory. The RAD is a password e.g. PIN, a biometric template or a combination of these. The TOE protects the confidentiality and integrity of the RAD. The TOE may provide a user interface to directly receive verification authentication data (VAD) from the user, alternatively, the TOE receive the VAD from the

⁴ At a pure functional level the SSCD creates an electronic signature; for an implementation of the SSCD, in that meeting the requirements of this PP and with the key certificate generated as specified in the directive, Annex I, the result of the signing process can be used as to create a qualified electronic signature.

signature creation application. If the signature creation application handles requesting obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

A certification service provider and a SSCD-provisioning service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions may include:

- initialising the RAD,
- generating a key pair,
- storing personal information of the legitimate user.

A typical example of an SSCD is a smart card. In this case a smart card terminal may be deployed that provides the required secure environment to handle a request for signatory authorization. A signature can be obtained on a document prepared by a signature creation application component running on personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorization PIN initiates the electronic signature creation function of the smart card through the terminal.

4.3.2 Target of evaluation

The TOE is a combination of hardware and software configured to securely import, use and manage signature creation data (SCD). The SSCD protects the SCD during its lifecycle beginning with import as to be used in a signature creation process solely by its signatory.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature.

The TOE provides the following functions:

- (1) to import signature creation data (SCD) and the correspondent signature verification data (SVD),
- (2) to, optionally, receive and store certificate info,
- (3) to switch the TOE from a non-operational state to an operational state, and
- (4) if in an operational state, to create electronic signatures for data with the following steps:
 - (a) select a set of SCD if multiple sets are present in the SSCD,
 - (b) authenticate the signatory and determine its intent to sign,
 - (c) receive data to be signed or a unique representation thereof (DTBS/R) through a trusted channel with SCA,
 - (d) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

The TOE may implement its function for electronic signature creation to also conform to the specifications in ETSI TS 101 733 (CAAdES) [8], ETSI TS 101 903 (XAdES) [9] and ETSI TS 102 778 (PAdES) [10].

The TOE is prepared for the signatory's use by

- (1) import at least one set of SCD, and
- (2) personalising for the signatory by storing in the TOE:
 - (a) the signatory's reference authentication data (RAD)
 - (b) optionally, certificate info for at least one SCD in the TOE.

After import the SCD is in a non-operational state. Upon receiving a TOE the signatory shall verify its non-operational state and change the SCD state to operational.

After preparation the intended legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, the

prEN 14169-6:2013 (E)

means of providing this information is expected to protect the confidentiality and the integrity of the corresponding RAD.

If the use of an SCD is no longer required, then it should be destroyed (e.g. by erasing it from memory) as well as the associated certificate info, if any exists.

4.3.3 TOE lifecycle

The TOE lifecycle is the same as defined in the PP SSCD KI [7], section 4.3.3.

5 Conformance claims

5.1 CC conformance claim

This PP uses the Common Criteria version 3.1 Revision 4 (see chapter 10 hereinafter).

This PP is conforming to Common Criteria Part 2 [3] extended.

This PP is conforming to Common Criteria Part 3 [4].

5.2 PP claim, Package claim

This PP is strictly conforming to the core PP SSCD KI [7] version 1.0.2 as dated of 2012-07-24.

This PP is conforming to assurance package EAL4 augmented with AVA_VAN.5 defined in CC part 3 [4].

5.3 Conformance rationale

This PP SSCD KI TCSCA conforms to the core PP SSCD KI [7]. This implies for this PP:

- (1) The TOE type of this PP SSCD KI TCSCA is the same as the TOE type of the core PP SSCD KI: the TOE is a combination of hardware and software configured to securely create, use and manage signature creation data.
- (2) The security problem definition (SPD) of this PP SSCD KI TCSCA contains the security problem definition of the core PP SSCD KI. The SPD for the SSCD KI TCSCA is described by the same threats, organisational security policies and assumptions as for the TOE in core PP SSCD KI.
- (3) The security objectives for the TOE in this PP SSCD KI TCSCA include all the security objectives for the TOE of the core PP SSCD KI and add the security objective OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) and OT.TOE_TC_DTBS_Imp (Trusted channel for DTBS).
- (4) The security objectives for the operational environment in this PP SSCD KI TCSCA include all security objectives for the operational environment of the core PP SSCD KI except

OE.HI_VAD and OE.DTBS_Protect. This PP adapts OE.HI_VAD and OE.DTBS_Protect to the support provided by the TOE by new security functionality (cf. OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp) provided by the TOE and changes them into OE.HID_TC_VAD_Exp and OE.SCA_TC_DTBS_Exp (cf. 7.2 for details).

- (5) The SFRs specified in this PP SSCD KI TCSCA includes all security functional requirements (SFRs) specified in the core PP SSCD KI. Additional SFRs address trusted channel between the TOE and the SCA: FDP_UIT.1/DTBS, FTP_ITC.1/VAD and FTP_ITC.1/DTBS.
- (6) This PP SSCD KI TCSCA does not provide completion of all operations left to the ST writer in the core PP SSCD KI. This PP provides refinements for the SFR FIA_UAU.1 of the core PP.
- (7) The SARs specified in this PP SSCD KI TCSCA includes all SAR as specified in the core PP SSCD KI. It does not include additional SAR not included in the core PP SSCD KI.

Further information about the relation of this PP and the core PP are given in sections 6.2, 6.3, 6.4, 7.1.1 and 7.2.1.

5.4 Conformance statement

This PP requires **strict** conformance of the ST or PP claiming conformance to this PP.

6 Security problem definition

6.1 Assets, users and threat agents

The Common Criteria define assets as entities that the owner of the TOE presumably places value upon. The term "asset" is used to describe the threats in the operational environment of the TOE. The assets of this PP SSCD KI TCSCA are the same as of the core PP SSCD KI [7].

Assets and objects:

1. SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.
2. SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.
3. DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

Users and subjects acting for users:

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

prEN 14169-6:2013 (E)

2. Administrator: User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.
3. Signatory: User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

Threat agents:

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

6.2 Threats

This PP includes all threats of the core PP SSCD KI [7]: T.SCD_Divulg, T.SCD_Derive, T.Hack_Phys, T.SVD_Forgery, T.SigF_Misuse, T.DTBS_Forgery and T.Sig_Forgery.

This PP does not define any additional threats.

6.3 Organisational security policies

This PP includes all organisational security policies of the core PP SSCD KI [7]: P.CSP_Qcert, P.Qsign, P.Sigy_SSCD and P.Sig_Non-Repud.

This PP does not define any additional organisational security policies.

6.4 Assumptions

This PP includes all assumptions of the core PP SSCD KI [7]: A.CGA, A.SCA and A.CSP.

This PP does not define any additional assumptions about the operational environment.

7 Security objectives

7.1 Security objectives for the TOE

7.1.1 Relation to core PP

This PP SSCD KI TCSCA includes all security objectives for the TOE as defined in the core PP SSCD KI [7]: OT.Lifecycle_Security, OT.SCD_Auth_Imp, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance.

This PP defines the following additional security objectives for the TOE:

7.1.2 OT.TOE_TC_VAD_Imp *Trusted channel of TOE for VAD import*

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

Application note 1: This security objective for the TOE is partly covering OE.HID_VAD from the core PP. While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore this PP re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

7.1.3 OT.TOE_TC_DTBS_Imp *Trusted channel of TOE for DTBS import*

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

Application note 2: This security objective for the TOE is partly covering OE.DTBS_Protect from the core PP. While OE.DTBS_Protect in the core PP requires only the operational environment to protect DTBS, this PP requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this PP re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

7.2 Security objectives for the operational environment

7.2.1 Relation to core PP

This PP SSCD KI TCSCA includes the security objectives for the operational environment as defined in the core PP SSCD KI [7]: OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp, OE.SVD_Auth, OE.CGA_Qcert, OE.SSCD_Prov_Service, OE.DTBS_Intend and OE.Signatory.

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

7.2.2 OE.HID_TC_VAD_Exp *Trusted channel of HID for VAD export*

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

Application note 3: This security objective for the TOE is partly covering OE.HID_VAD from the core PP. While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore this PP re-assigns partly the VAD protection from the operational environment as described by

	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.DTBS_Intend	OE.Signatory	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
T.SCD_Derive				X										X								
T.Hack_Phys			X				X	X	X													
T.SVD_Forgery															X		X					
T.SigF_Misuse	X				X	X				X	X								X	X	X	X
T.DTBS_Forgery						X					X								X			X
T.Sig_Forgery				X										X		X						
P.CSP_Qcert	X	X										X			X	X						
P.Qsign				X	X											X			X			
P.Sigy_SSCD	X	X	X	X	X	X	X		X			X	X	X				X				
P.Sig_Non-Repud	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.CGA																X	X					
A.SCA																			X			
A.CSP												X	X	X	X							

7.3.2 Security objectives sufficiency

The rationale for T.Hack_Phys, T.SCD_Divulg, T.SCD_Derive, T.Sig_Forgery, T.SVD_Forgery, P.CSP_Qcert, P.Qsign, P.Sigy_SSCD, A.CGA, A.SCA and A.CSP remains unchanged as given in the core PP SSCD KI [7], section 4.3.2. The rationale how security objectives address the threats T.DTBS_Forgery and T.SigF_Misuse and the organisational security policy P.Sig_Non-Repud changes as described below.

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 an electronic

prEN 14169-6:2013 (E)

signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of **Annex III**. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign. The combination of OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission from the SCA to the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). OE.Signatory (Security obligation of the signatory) ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory (Security obligation of the signatory) ensures also that the signatory keeps their VAD confidential.

T.DTBS_Forgery (*Forgery of the DTBS/R*) addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE. The TOE counters internally this threat by the means of OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensuring the integrity of the DTBS/R inside the TOE. The TOE IT environment also addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE.

P.Sig_Non-Repud (Non-repudiation of signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE.

OE.SSCD_Prov_Service ensures that the signatory uses an authentic copy of the TOE, initialised and personalised for the signatory.

OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy and OE.SCD_Unique ensure the security of the SCD in the CSP environment. OE.SCD_Secrecy ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. OE.SCD_Unique provides that the signatory's SCD can practically occur just once. OE.SCD_SVD_Corresp ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory.

OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure the authenticity of the SVD included in the certificate and to ensure correspondence of the SVD to the SCD stored in the SSCD. OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD-provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory (Security obligation of the signatory) ensures that the signatory keeps their VAD confidential. The confidentiality of VAD is protected during the

transmission between the HI device and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). OE.DTBS_Intend, OE.SCA_TC_DTBS_Exp, OT.TOE_TC_DTBS_Imp and OT.DTBS_Integrity_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

8 Extended components definition

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in the core PP SSCD KI [7]. This PP uses the extended component FPT_EMS.1 as defined in [7].

9 Security requirements

9.1 Security functional requirements

9.1.1 Use of requirement specifications

Common Criteria allow several operations to be performed on functional requirements; refinement, selection, assignment, and iteration. Each of these operations is used in this PP. Operations not performed in this PP are identified in order to enable instantiation of the PP into a Security Target (ST).

A **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is (i) denoted by the word “refinement” in **bold** text and the added or changed words are in **bold** text, or (ii) included in text as **bold** text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

A **selection** operation is used to select one or more options provided by the CC in stating a requirement. A selection that has been made in this European standard is indicated as underlined text and the original text of the component is given by a footnote. Selections left to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

An **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment that that has been made in this European standard is indicated as underlined text and the original text of the component is given by a footnote. Assignments left to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*.

An **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

This PP requires the following SFRs as described in the core PP SSCD KI [7]: FCS_CKM.4, FCS_COP.1, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FDP_ACC.1/Signature_Creation,

prEN 14169-6:2013 (E)

FDP_ACF.1/Signature_Creation, FDP_ITC.1/SCD, FDP_UCT.1/SCD, FDP_RIP.1, FDP_SDI.2/Persistent, FDP_SDI.2/DTBS, FIA_AFL.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMR.1, FMT_SMF.1, FPT_EMS.1, FPT_FLS.1, FPT_PHP.1, FPT_PHP.3, FPT_TST.1, FTP_ITC.1/SCD.

This PP adds an operation of FIA_UAU.1, as follows:

9.1.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow
(1) Self-test according to FPT_TST.1,
(2) identification of the user by means of TSF required by FIA_UID.1,
(3) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD,
(4) [assignment: list of additional TSF-mediated actions]⁵
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 5: The ST writer shall perform the missing operation in the element FIA_UAU.1.1. The list of additional TSF-mediated actions may be empty (i.e. assignment “none”). This PP performed the operation of the bullet (3) in the element FIA_UAU.1.1 of the core PP [7] by adding the establishment of a trusted channel to HID.

This PP adds the following SFRs FDP_UIT.1/DTBS, FTP_ITC.1/VAD and FTP_ITC.1/DTBS:

9.1.2 FDP_UIT.1/DTBS Data exchange integrity

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1/DTBS The TSF shall enforce the Signature Creation SFP⁶ to receive⁷ user data in a manner protected from modification and insertion⁸ errors.

FDP_UIT.1.2/DTBS The TSF shall be able to determine on receipt of user data, whether

⁵ [assignment: *list of TSF mediated actions*]

⁶ [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

⁷ [selection: *transmit, receive*]

⁸ [selection: *modification, deletion, insertion, replay*]

modification and insertion⁹ has occurred.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

- FTP_ITC.1.1/VAD The TSF shall provide a communication channel between itself and another trusted IT product **HID** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
- FTP_ITC.1.2/VAD The TSF shall permit the remote trusted IT product¹⁰ to initiate communication via the trusted channel.
- FTP_ITC.1.3/VAD The TSF **or the HID** shall initiate communication via the trusted channel for
- (1) User authentication according to FIA UAU.1.
 - (2) [assignment: list of other functions for which a trusted channel is required]¹¹.

Application note 6: The component FTP_ITC.1/VAD requires the TSF to support a trusted channel established by the HID to send the VAD. The ST writer shall perform the missing operations in the element FTP_ITC.1.3. If the TSF does not enforce the use of trusted channel for other functions the operation in the element FTP_ITC.1.3 is “none”. Note the VAD needs protection depending on the authentication methods employed: VAD for authentication by knowledge needs protection in confidentiality; VAD for biometric authentication may need protection in integrity only.

9.1.4 FTP_ITC.1/DTBS Inter-TSF trusted channel – Signature creation Application

Hierarchical to: No other components.

Dependencies: No dependencies.

- FTP_ITC.1.1/DTBS The TSF shall provide a communication channel between itself and another trusted IT product **SCA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
- FTP_ITC.1.2/DTBS The TSF shall permit the remote trusted IT product¹² to initiate communication via the trusted channel.

⁹ [selection: *modification, deletion, insertion, replay*]

¹⁰ [selection: *the TSF, another trusted IT product*]

¹¹ [assignment: *list of functions for which a trusted channel is required*]

¹² [selection: *the TSF, another trusted IT product*]

prEN 14169-6:2013 (E)

FTP_ITC.1.3/DTBS

The TSF **or the SCA** shall initiate communication via the trusted channel for

- (1) signature creation,
- (2) [assignment: list of other functions for which a trusted channel is required]¹³.

Application note 7: The component FTP_ITC.1/DTBS requires the TSF to support a trusted channel established by the SCA to send the DTBS. The ST writer shall perform the missing operations in the element FTP_ITC.1.3. If the TSF does not enforce the use of trusted channel for other functions the operation in the element FTP_ITC.1.3 is “none”.

9.2 Security assurance requirements

Table 2 Assurance requirements: EAL4 augmented with AVA_VAN.5

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing

¹³ [assignment: list of functions for which a trusted channel is required]

Assurance class	Assurance components
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

9.3 Security requirements rationale

9.3.1 Security requirements coverage

Table 3 Mapping of functional requirements to security objectives for the TOE

Functional requirements	TOE security objectives										
	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FCS_CKM.4	X		X								
FCS_COP.1	X			X							
FDP_ACC.1/SCD_Import	X	X									
FDP_ACC.1/Signature_Creation	X				X						
FDP_AFC.1/SCD_Import	X	X									
FDP_AFC.1/Signature_Creation	X				X						
FDP_ITC.1/SCD	X										
FDP_UCT.1/SCD	X		X								
FDP_RIP.1			X		X						
FDP_SDI.2/Persistent			X	X							
FDP_SDI.2/DTBS					X	X					
FDP_UIT.1/DTBS											X
FIA_AFL.1					X						
FIA_UAU.1		X			X						
FIA_UID.1		X			X						
FMT_MOF.1	X				X						

Functional requirements	TOE security objectives											
	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	
FMT_MSA.1/Admin	X											
FMT_MSA.1/Signatory	X				X							
FMT_MSA.2	X				X							
FMT_MSA.3	X				X							
FMT_MSA.4	X				X							
FMT_MTD.1/Admin	X				X							
FMT_MTD.1/Signatory	X				X							
FMT_SMR.1	X				X							
FMT_SMF.1	X				X							
FPT_EMS.1			X			X						
FPT_FLS.1			X									
FPT_PHP.1							X					
FPT_PHP.3			X					X				
FPT_TST.1	X		X	X								
FTP_ITC.1/SCD	X		X									
FTP_ITC.1/VAD									X			
FTP_ITC.1/DTBS											X	

9.3.2 TOE security requirements sufficiency

The table demonstrates that each security objective for the TOE is covered by at least one security functional requirement.

The rationale in the core PP SSSD KI, section 9.3.2, is still valid. It explains how the security functional requirements cover the security objectives for the TOE OT.Lifecycle_Security, OT.SCD_Auth_Imp, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance. The rationale for the security objectives OT.TOE_TC_VAD_Imp and OT.TOE_TC_DTBS_Imp is given below.

OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) is provided by FTP_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

9.3.3 Satisfaction of dependencies of chosen security requirements

Table 4 Satisfaction of dependencies of security functional requirements

Functional requirement	Dependencies	Satisfied by
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/SCD
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FDP_ITC.1/SCD, FCS_CKM.4
FDP_ACC.1/SCD_Import	FDP_ACF.1	FDP_ACF.1/SCD_Import
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACF.1/SCD_Import	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ITC.1/SCD	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FDP_ITC.1/SCD, FDP_ACC.1/SCD_Import
FDP_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FDP_UIT.1/DTBS	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	No dependencies	n/a
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1

prEN 14169-6:2013 (E)

Functional requirement	Dependencies	Satisfied by
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_MSA.1	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD_Import, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_EMS.1	No dependencies	n/a
FPT_FLS.1	No dependencies	n/a
FPT_PHP.1	No dependencies	n/a
FPT_PHP.3	No dependencies	n/a
FPT_TST.1	No dependencies	n/a
FTP_ITC.1/SCD	No dependencies	n/a
FTP_ITC.1/VAD	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a

Table 5 Satisfaction of dependencies of security assurance requirements

Assurance requirement(s)	Dependencies	Satisfied by
EAL4 package	(dependencies of EAL4 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1 (all are included in EAL4 package)

9.3.4 Rationale for chosen security assurance requirements

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_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to function in a variety of signature creation 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. 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.

10 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] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 4, CCMB-2012-09-001, September 2012
- [3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 4, CCMB-2012-09-002, September 2012
- [4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 4, CCMB-2012-09-003, September 2012
- [5] Protection Profile Secure Signature Creation Device Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0006-2002, also short SSCD-PP or CWA14169
- [6] CEN prEN 14169-1:2012, Protection profiles for secure signature creation device — Part 1: Overview
- [7] CEN prEN 14169-3:2012, Protection profiles for secure signature creation device — Part 3: Device with key import
- [8] ETSI Technical Specification 101 733, CMS Advanced Electronic Signatures (CAAdES), the latest version may be downloaded from the ETSI download page <http://pda.etsi.org/pda/queryform.asp>
- [9] ETSI Technical Specification 101 903, XML Advanced Electronic Signatures (XAdES), the latest version may be downloaded from the ETSI download page <http://pda.etsi.org/pda/queryform.asp>

prEN 14169-6:2013 (E)

- [10] ETSI Technical Specification 102 778: PDF Advanced Electronic Signatures (PAdES), the latest version may be downloaded from the ETSI download page <http://pda.etsi.org/pda/queryform.asp>