CEN/TC 224

Date: 2012-11

prEN 14169-4:2012

CEN/TC 224

Secretariat: AFNOR

Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application

Schutzprofile sichere Signaturerstellungseinheit — Teil 4: Erweiterung für ein Gerät mit Schlüsselerzeugung und vertrauenswürdiger Kommunikation zur Zertifikatserstellungsanwendung

Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats

ICS:

Descriptors:

Document type: European Standard
Document subtype:
Document stage: final
Document language: E

WD1 EN_14169-4_(E)_v1.0.1_KGTCCGA.doc

Contents

Foreword

This document (prEN 14169-4:2012) 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 channel to certificate generation application;
- Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application;
- Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to 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 generation and trusted communication with certificate generation application (PP SSCD KG TCCGA) 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 generate signing keys internally and export the public key in protected manner: secure signature creation device with key generation and trusted communication with certificate generation application (SSCD KG TCCGA).

2 Normative references

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

EN 14169-1, Protection profiles for secure signature creation device — Part 1: Overview[1]

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

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 4: Extension for device with key generation and trusted communication with certificate generation application
Version:	1.0.1
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	2012-11-14
Registration:	BSI-CC-PP-0071
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 generation, trusted communication with certificate generation 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 directive[3] 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 generation and trusted communication with certificate generation application (PP SSCD KG TCCGA) defines the security requirements for SSCD generating signature creation data (SCD) and creating advanced electronic signatures, which if based on valid qualified certificates are qualified electronic signatures, as described in the core PP SSCD KG [7]. Additionally the TOE of this PP supports its authentication as SSCD by the certificate generation application (CGA) of the Certification service provider (CSP) and a trusted communication with this CGA for protection of signature verification data (SVD) generated and exported by the TOE and imported by CGA. These security features allow a changed lifecycle of the TOE. This PP conforms to the core PP SSCD KG [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 certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the signature creation data (SCD) the TOE has generated. The TOE exports the SVD through a trusted channel allowing the CGA to check the authenticity of the SVD. 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 or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting electronic signature[4].
- 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 4 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 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, is requesting or 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.

The TOE and the CGA communicate through a trusted channel in order to protect the integrity and authenticity of the SVD exported from the TOE.

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 create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole lifecycle 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 generate signature creation data (SCD) and the correspondent signature verification data (SVD),
(2) to export the SVD for certification through a trusted channel to the CGA,
(3) to prove the identity as SSCD to external entities,
(4) to, optionally, receive and store certificate info,
(5) to switch the TOE from a non-operational state to an operational state, and
(6) if in an operational state, to create digital signatures for data with the following steps:
    (a) select an SCD if multiple 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),
    (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 (CAdES) [8], ETSI TS 101 903 (XAdES) [9] and ETSI TS 101 903 (PAdES) [10].

The TOE is prepared for the signatory's use by

(1) generating at least one SCD/SVD pair, 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 preparation the SCD shall be 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 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 shall 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 KG [7], section 4.3.3, except the following:

- In the preparation stage of the usage phase, the SSCD-provisioning provider additionally initializes the security functions in the TOE for the identification as SSCD, for the proof of this SSCD identity to external entities, and for the protected export of the SVD.

- In the preparation stage of the usage phase, the SSCD-provisioning provider additionally links the identity of the TOE as SSCD and the identity of the legitimate user as potential applicant for certificates for SVD generated by the TOE.

- In the usage phase, SCD/SVD generation by the TOE and SVD export from the TOE may take place in the preparation stage and/or in the operational use stage. The TOE then provides a trusted channel to the CGA protecting the integrity of the SVD.

- In the usage phase, before generating the certificate including the SVD exported from the TOE, the CGA additionally establishes (1) the identity of the TOE as SSCD, (2) that the originating SSCD has been personalized for the applicant for the certificate as legitimate user, and (3) the correspondence between SCD stored in the SSCD and the received SVD.

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 KG [7] version 2.0.1 as dated of 2012-01-23.

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 KG TCCGA conforms to the core PP SSCD KG [7]. This implies for this PP:

(1) The TOE type of this PP SSCD KG TCCGA is the same as the TOE type of the core PP SSCD KG: 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 KG TCCGA contains the security problem definition of the core PP SSCD KG. The SPD for the SSCD KG TCSCA is described by the same threats, organisational security policies and assumptions as for the TOE in core PP SSCD KG.

(3) The security objectives for the TOE in this PP SSCD KG TCCGA include all the security objectives for the TOE of the core PP SSCD KG and add the security objective OT.TOE_SSCD_Auth (Authentication proof as SSCD) and OT.TOE_TC_SVD_Exp (Trusted channel for SVD).

(4) The security objectives for the operational environment in this PP SSCD KG TCCGA include all security objectives for the operational environment of the core PP SSCD KG except OE.SSCD_Prov_Service. This PP substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service and adds OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp in order to address the extended security functionality of the TOE and methods of use (cf. section 0 for details).

(5) The SFRs specified in this PP SSCD KG TCCGA includes all security functional requirements (SFRs) specified in the core PP SSCD KG. This PP includes additional SFRs FIA_API.1, FDP_DAU.2/SVD and FTP_ITC.1/SVD.

(6) This PP SSCD KG TCCGA does not provide completion of all operations left to the ST writer in the core PP SSCD KG. This PP provides operation of the SFR FIA_UAU.1 of the core PP.

(7) The SARs specified in this PP SSCD KG TCSCA includes all SAR specified in the core PP SSCD KG. It does not include additional SAR not included in the core PP SSCD KG.

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 are the same as of the core PP SSCD KG [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.

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 KG [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 KG [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 KG [7]: A.CGA and A.SCA.

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 SSCD KG

This PP includes all security objectives for the TOE as defined in the core PP SSCD KG [7]: OT.Lifecycle_Security, OT.SCD/SVD_Gen, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance.

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

7.1.2 OT.TOE_SSCD_Auth *Authentication proof as SSCD*

The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate itself as SSCD.

7.1.3 OT.TOE_TC_SVD_Exp *TOE trusted channel for SVD export*

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

7.2 Security objectives for the operational environment

7.2.1 Relation to core PP SSCD KG

This PP includes the following security objectives for the operational environment as defined in the core PP SSCD KG [7]: OE.SVD_Auth, OE.CGA_Qcert, OE.HID_VAD, OE.DTBS_Intend, OE.DTBS_Protect, and OE.Signatory.

This PP substitutes OE.SSCD_Prov_Service from the core PP by OE.Dev_Prov_Service and adds security objectives for the operational environment OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp in order to address the additional method of use as SCD/SVD pair generation after delivery to the signatory and outside the secure preparation environment.

7.2.2 OE.Dev_Prov_Service *Authentic SSCD provided by SSCD Provisioning Service*

The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalises the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory. Note: This objective replaces OE.SSCD_Prov_Service from the core PP, which is possible as it does not

imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).

7.2.3 OE.CGA_SSCD_Auth *Pre-initialisation of the TOE for SSCD authentication*

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

7.2.4 OE.CGA_TC_SVD_Imp *CGA trusted channel for SVD import*

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

The developer prepares the TOE by pre-initialisation for the delivery to the customer (i.e. the SSCD provisioning service) in the development phase not addressed by a security objective for the operational environment. The SSCD Provisioning Service performs initialisation and personalisation as TOE for the legitimate user (i.e. the Device holder). If the TOE is delivered to the Device holder with SCD the TOE is a SSCD. This situation is addressed by OE.SSCD_Prov_Service except the additional initialisation of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the Device holder without a SCD the TOE will be a SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the signatory in the operational use stage the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialised by the SSCD Provisioning Service as described in OE.Dev_Prov_Service. Therefore this PP substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service allowing generation of the first SCD/SVD pair after delivery of the TOE to the Device holder and requiring initialisation of security functionality of the TOE. Nevertheless the additional security functionality must be used by the operational environment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore it does not conflict with the CC conformance claim to the core PP SSCD KG [7].

7.3 Security objectives rationale

7.3.1 Security objectives backtracking

The following table shows how the security objectives for the TOE and the security objectives for the operational environment cover the threats, organizational security policies and assumptions. Take note that this PP describes the same threats, organisational security policies and assumptions as for the TOE in core PP SSCD KG but it adds security objectives for the TOE (OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) and for the operational environment (OE.Dev_Prov_Service, OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp).

Table 1 Mapping of security problem definition to security objectives

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OE.CGA_QCert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp
T.SCD_Divulg					X																	
T.SCD_Derive		X				X																
T.Hack_Phys					X				X	X	X											
T.SVD_Forgery				X									X		X							X
T.SigF_Misuse	X						X	X									X	X	X	X		
T.DTBS_Forgery								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					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
A.CGA														X	X							
A.SCA																		X				

7.3.2 Security objectives sufficiency

The rationale for T.SCD_Divulg, T.SCD_Derive, T.Hack_Phys, T.SigF_Misuse, T.DTBS_Forgery, T.Sig_Forgery, P.QSign, A.CGA and A.SCA remains unchanged as given in the core PP SSCD KG [7], section 7.3.2. The rationale how security objectives address the threat T.SVD_Forgery and policies P.CSP_QCert, P.Sigy_SSCD and P.Sig_Non-Repud changes as described below.

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.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous

reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP. Additionally T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

P.CSP_QCert (*CSP generates qualified certificates*) 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 OE.CGA_QCert addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According to OT.TOE_SSCD_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The OE.CGA_SSCD_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD. The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory. The OT.Lifecycle_Security ensures that the TOE detects flaws during the initialisation, personalisation and operational usage.

P.Sigy_SSCD (*TOE as secure signature creation device*) requires the TOE to meet Annex III of **the directive**. The paragraph 1(a) of Annex III is ensured by OT.SCD_Unique requiring that the SCD used for signature creation can practically occurs only once. The OT.SCD_Secrecy OT.Sig_Secure and OT.EMSEC_Design and OT.Tamper_Resistance address the secrecy of the SCD (cf. paragraph 1(a) of Annex III). OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE. OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others. OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE must not alter the DTBS/R. The usage of SCD under sole control of the signatory is ensured by OT.Lifecycle_Security, OT.SCD/SVD_Gen and OT.Sigy_SigF.

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

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, that ensure the aspects of signatory's sole control over and responsibility for the electronic signatures generated with the TOE. OE.Dev_Prov_Service ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory. OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure

authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique provides that the signatory's SCD can practically occur just once.

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). The TOE security feature addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp supported by OE.Dev_Prov_Service enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA_SSCD_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp. OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may generate 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

8.1 Definition of the family FPT_EMS

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

8.2 Definition of the family FIA_API

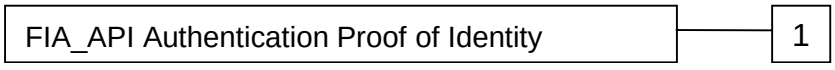
To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling:



FIA_API.1 Authentication Proof of Identity.

Management:	FIA_API.1
	The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

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 KG [7]:
FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_ACC.1/SCD/SVD_Generation, FDP_AFC.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_AFC.1/SVD_Transfer, FDP_ACC.1/Signature_Creation, FDP_AFC.1/Signature_Creation, 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

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 CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,
(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 1: 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 the CGA.

This PP adds the following SFRs:

9.1.2 FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the SSCD[6].

Application note 2: The ST writer shall perform the missing operation in the element FIA_API.1.1. Via the authentication mechanism to be assigned here the TOE has to be able to authenticate itself as SSCD to the CGA, using authentication data implemented in the TOE during pre-initialisation phase.

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

[6] [assignment: *authorized user or rule*]

9.1.3 FDP_DAU.2/SVD Data Authentication with Identity of Guarantor

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1/SVD The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD[7].

FDP_DAU.2.2/SVD The TSF shall provide CGA[8] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

9.1.4 FTP_ITC.1/SVD Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/SVD The TSF shall provide a communication channel between itself and another 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 The TSF shall permit another trusted IT product[9] to initiate communication via the trusted channel.

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

(1) data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD,

(2) [assignment: *list of other functions for which a trusted channel is required*][10].

Application note 3: The component FPT_ITC.1/SVD requires the TSF to enforce a trusted channel established by the CGA to export the SVD to the CGA. 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”.

Application note 4: If the ST writer requires the TSF to support (not to enforce) a trusted channel established by the CGA to export the SVD to the CGA than he or she shall use the core PP SSCD KG and include a similar component FPT_ITC.1/SVD with assignment “none” in the element FPT_ITC.1.3/SVD.

---

[7] [assignment: *list of objects or information types*]

[8] [assignment: *list of subjects*]

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

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

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
	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 requirement coverage

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

TOE security objectives / Functional requirements	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp
FCS_CKM.1	X		X	X	X								
FCS_CKM.4	X				X								
FCS_COP.1	X					X							
FDP_ACC.1/SCD/SVD_Generation	X	X											
FDP_ACC.1/SVD_Transfer	X												X
FDP_ACC.1/Signature_Creation	X						X						
FDP_AFC.1/SCD/SVD_Generation	X	X											
FDP_AFC.1/SVD_Transfer	X												X
FDP_AFC.1/Signature_Creation	X						X						
FDP_RIP.1					X		X						
FDP_SDI.2/Persistent				X	X	X							
FDP_SDI.2/DTBS							X	X					
FDP_DAU.2/SVD													X
FIA_AFL.1							X						
FIA_UAU.1		X					X					X	
FIA_API.1												X	
FIA_UID.1		X					X						
FMT_MOF.1	X						X						
FMT_MSA.1/Admin	X	X											
FMT_MSA.1/Signatory	X						X						

TOE security objectives / Functional requirements	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp
FMT_MSA.2	X	X					X						
FMT_MSA.3	X	X					X						
FMT_MSA.4	X	X					X						
FMT_MTD.1/Admin	X						X						
FMT_MTD.1/Signatory	X						X						
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/SVD													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 SSCD KG, 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/SVD_Gen, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance. The rationale for the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp is given below.

OT.TOE_SSCD_Auth (Authentication proof as SSCD) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication Proof of Identity). The SFR FIA_UAU.1 allows (additionally to the core PP SSCD KG) establishment of the trusted channel before (human) user is authenticated.

OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export) requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer.
- FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- FTP_ITC.1/SVD Inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

9.3.3 Satisfaction of dependencies of security requirements

Table 4 Satisfaction of dependencies of security functional requirements

Functional requirement	Dependencies	Satisfied by
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_DAU.2/SVD	FIA_UID1.	FIA_UID.1
FDR_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_API.1	No dependencies	n/a
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1

Functional requirement	Dependencies	Satisfied by
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, 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
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
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/SVD_Generation, 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/SVD	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

Assurance requirement(s)	Dependencies	Satisfied by
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 14169-2:2012, Protection profiles for secure signature creation device — Part 2: Device with key generation

[8] ETSI Technical Specification 101 733, CMS Advanced Electronic Signatures (CAdES), 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

[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