BS EN 419211-5:2013

BSI Standards Publication

Protection profiles for secure signature creation device

Part 5: Extension for device with key generation and trusted channel to signature creation application

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 419211-5:2013.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 71699 7

ICS 03.160; 35.040; 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2013.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-5

December 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application

Profils de protection pour dispositif sécurisé de création de signature - Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature

Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Signaturerstellungsanwendung

This European Standard was approved by CEN on 12 October 2013.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (EN 419211-5:2013) 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 European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2014, and conflicting national standards shall be withdrawn at the latest by June 2014.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes CWA 14169:2004.

This series of European Standards, *Protection profiles for secure signature creation device* consists of the following parts:

— *Part 1: Overview*

— *Part 2: Device with key generation*

— *Part 3: Device with key import*

— *Part 4: Extension for device with key generation and trusted channel to certificate generation application*

— *Part 5: Extension for device with key generation and trusted channel to signature creation application*

— *Part 6: Extension for device with key import and trusted channel to signature creation application*

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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) 14169:2004, Annex B and Annex C on the protection profile secure signature creation devices, “EAL 4+”.

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

1 Scope

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

prEN 419211-1:2011, *Protection profiles for secure signature creation device — Part 1: Overview*[1)]

3 Conventions and terminology

3.1 Conventions

This document is drafted in accordance with the CEN-CENELEC Internal Regulations Part 3 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 prEN 419211-1:2011 apply.

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application
Version:	1.0.1
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	2012–11–14
Registration:	BSI-CC-PP-0072
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 signature creation application

1) To be published. This document was submitted to the Enquiry procedure under reference prEN 14169-1.

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[2)] 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 recognized 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 signature creation application (PP SSCD KG TCSCA) includes the security requirements for SSCD with key generation generating signature creation data (SCD) and creating digital signature to be used for (qualified or advanced) electronic signatures as described in the core PP [5]. 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 KG [5]. The implication of this conformance claim is explained in 5.3 hereinafter.

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

4.3 TOE overview

4.3.1 Operation of the TOE

This subclause 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 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 signature[3)]. 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.

---

2) This European Directive is referred to in this PP as “the Directive”.

3) 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.

The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE. Figure 5 in prEN 419211-1:2011 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 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:

— initializing 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 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:

a) to generate signature creation data (SCD) and the correspondent signature verification data (SVD);

b) to export the SVD for certification;

c) to, optionally, receive and store certificate info;

d) to switch the TOE from a non-operational state to an operational state; and

e) if in an operational state, to create electronic signatures for data with the following steps:

   1) select an SCD if multiple are present in the SSCD;

   2) authenticate the signatory and determine its intent to sign;

   3) receive data to be signed or a unique representation thereof (DTBS/R) through a trusted channel with SCA;

   4) 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) [7], ETSI/TS 101 903 (XAdES) [8] and ETSI/TS 101 903 (PAdES) [9].

4.3.3 TOE lifecycle

The TOE lifecycle is the same as defined in the PP SSCD KG [5], section 4.3.3.

5 Conformance claims

5.1 CC conformance claim

This PP uses the Common Criteria version 3.1 Revision 4 (see Bibliography).

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 [5] 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 TCSCA conforms to the core PP SSCD KG [5]. This implies for this PP:

a) The TOE type of this PP SSCD KG TCSCA 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.

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

c) The security objectives for the TOE in this PP SSCD KG TCSCA include all the security objectives for the TOE of the core PP SSCD KG 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).

d) The security objectives for the operational environment in this PP SSCD KG TCSCA include all security objectives for the operational environment of the core PP SSCD KG 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).

e) The SFRs specified in this PP SSCD KG TCSCA includes all security functional requirements (SFRs) specified in the core PP SSCD KG. Additional SFRs address trusted channel between the TOE and the SCA: FDP_UIT.1/DTBS, FTP_ITC.1/VAD and FTP_ITC.1/DTBS.

f) This PP SSCD KG TCSCA does not provide completion of all operations left to the ST writer in the core PP SSCD KG. This PP provides refinements for the SFR FIA_UAU.1 of the core PP.

g) The SARs specified in this PP SSCD KG TCSCA includes all SAR as 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 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 Type TCSCA are the same as of the core PP SSCD KG [7].

Assets and objects:

a) SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SCD shall be maintained.

b) SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported shall be maintained.

c) 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 shall be maintained.

Users and subjects acting for users:

d) 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.

e) Administrator: User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

f) 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:

g) 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 Organizational security policies

This PP includes all organizational 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 organizational security policies.

6.4 Assumptions

This PP includes all assumptions of the core PP SSCD KG [5]: 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_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 shall 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 includes the security objectives for the operational environment as defined in the core PP SSCD KG [5]: 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 OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

7.2.3 OE.SCA_TC_DTBS_Exp Trusted channel of SCA for DTBS export

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Application note 4: 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.

7.3 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 environment cover the threats, organizational security policies and assumptions. Take note that this PP describes the same threats, organizational security policies and assumptions as the core PP, with the following two exceptions:

OE.HID_VAD from the core PP has been split into the objectives OE.HID_TC_VAD_Exp and OT.TOE_TC_VAD_Imp in this PP, i.e. a part of a security objective for the environment (namely OE.HID_VAD from the core PP) will be met by the TOE itself, which is allowed according to CC.

OE.DTBS_Protect from the core PP has been split into OE.SCA_TC_DTBS_Exp and OT.TOE_TC_DTBS_Imp in this PP, i.e. a part of a security objective for the environment (namely OE.DTBS_Protect from the core PP) will be met by the TOE itself, which is allowed according to CC.

Table 1 - Mapping of security problem definition to security objectives

Threats, OSP's and assumptions	**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_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	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_Divulg					**X**															
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**						
P.QSign						**X**	**X**							**X**			**X**			
P.Sigy_SSCD	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**		**X**					**X**				
P.Sig_Non-	**X**		**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Threats, OSP's and assumptions	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_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	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
Repud																				
A.CGA														**X**	**X**					
A.SCA																	**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 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 threats T.DTBS_Forgery and T.SigF_Misuse and 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 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 initialization, personalization 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 form 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 generated with the TOE. OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service) ensures that the signatory uses an authentic TOE, initialized and personalized for the signatory. OE.CGA_QCert (Generation of qualified certificates) ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth (Authenticity of the SVD) and OE.CGA_QCert (Generation of qualified certificates) 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 (Correspondence between SVD and SCD) ensures that the SVD exported by the TOE corresponds to the SCD that is stored in the TOE. OT.SCD_Unique (Uniqueness of the signature creation data) provides that the signatory's SCD can practically occur just once.

OE.Signatory (Security obligation of the 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 (Signature creation function for the legitimate signatory only) 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 (SCA sends data intended to be signed), OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE), OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) and OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) 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 (Cryptographic security of the electronic signature) 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

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 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 SFR as described in the core PP SSCD KG [5]: 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:

9.1.2 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:

a) Self-test according to FPT_TST.1,

b) identification of the user by means of TSF required by FIA_UID.1,

c) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD,

d) [assignment: *list of additional TSF-mediated actions*][4)]

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 [5] by adding the establishment of a trusted channel to HID.

4) [assignment: *list of TSF mediated actions*]

9.1.3 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 SFP[5] to receive[6] user data in a manner protected from modification and insertion[7] errors.
FDP_UIT.1.2/DTBS	The TSF shall be able to determine on receipt of user data, whether modification and insertion[8] has occurred.

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

9.1.4 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 ensured 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 product[9] 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

a) User authentication according to FIA_UAU.1,

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

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.

---

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

6) [selection: *transmit, receive*]

7) [selection: *modification, deletion, insertion, replay*]

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

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

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

9.1.5 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 ensured 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 product[11] to initiate communication via the trusted channel.
FTP_ITC.1.3/DTBS	The TSF **or the SCA** shall initiate communication via the trusted channel for a) signature creation, b) [assignment: *list of other functions for which a trusted channel is required*][12].

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”.

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

12) [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 requirements coverage

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

Functional requirements	TOE 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_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
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												
FDP_ACC.1/Signature_Creation	X						X						
FDP_AFC.1/SCD/SVD_Generation	X	X											
FDP_AFC.1/SVD_Transfer	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_UIT.1/DTBS													X
FIA_AFL.1							X						
FIA_UAU.1		X					X						
FIA_UID.1		X					X						
FMT_MOF.1	X						X						
FMT_MSA.1/Admin	X	X											
FMT_MSA.1/Signatory	X						X						
FMT_MSA.2	X	X					X						

Functional requirements	TOE 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_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
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/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 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_TC_VAD_Imp, 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.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
FDR_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/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

Functional requirement	Dependencies	Satisfied by
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/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 specialised 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.

Bibliography

[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] EN 419211-2:2013, *Protection profiles for secure signature creation device — Part 2: Device with key generation*

[7] 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

[8] 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

[9] 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

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™