BS EN 419211-1:2014

BSI Standards Publication

Protection profiles for secure signature creation device

Part 1: Overview

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 419211-1:2014.

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 74075 6

ICS 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 October 2014.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-1

October 2014

ICS 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 1: Overview

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 1: Présentation générale

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 1: Überblick

This European Standard was approved by CEN on 25 July 2014.

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

Ref. No. EN 419211-1:2014 E

Contents

Page

Foreword

This document (EN 419211-1:2014) 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 April 2015 and conflicting national standards shall be withdrawn at the latest by April 2015.

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.

Significant changes between this edition and CWA 14169:2004 can be found in Annex A.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

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 Protection Profiles for Secure Signature Creation Devices and is issued by the European Committee for Standardization (CEN) as an update of the Electronic Signatures (E-SIGN) CEN workshop agreement (CWA) 14169:2004, Annex C on the protection profile secure signature creation devices, “EAL 4+”.

This series of European Standards 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 communication with certificate generation application*

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

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

Preparation of the documents in this series of European Standards as protection profiles follows the rules of the Common Criteria version 3.1 ([2], [3] and [4]).

1 Scope

This European Standard:

— specifies terms used in specifying protection profiles for secure signature creation devices,

— specifies functional and operational requirements for secure signature creation devices,

— describes the targets of evaluation for these protection profiles.

2 Normative references

Not applicable.

3 Terminology

For the purposes of this document, the following terms and definitions apply.

3.1 Legislative references

This European Standard reflects the requirement of a European Directive in the technical terms of a protection profile. The following terms are used in the text to reference this Directive:

3.1.1
the Directive
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on "*a Community framework for electronic signatures"* [1]

Note 1 to entry: References in this document to a specific article and paragraph of Directive 1999/93/EC are of the form "(**the Directive:** n.m)".

3.1.2
annex
one of the annexes, Annex I, Annex II or Annex III of **the Directive**

3.2 Technical terms

3.2.1
administrator
user who performs TOE initialization, TOE personalization, or other TOE administrative functions

3.2.2
advanced electronic signature
digital signature which meets specific requirements in **the Directive: 2.2**

Note 1 to entry: According to **the Directive** a digital signature qualifies as an advanced electronic signature if it:

— is uniquely linked to the signatory;

— is capable of identifying the signatory;

— is created using means that the signatory can maintain under their sole control; and

— is linked to the data to which it relates in such a manner that any subsequent change of the data are detectable.

3.2.3
authentication data
information used to verify the claimed identity of a user

3.2.4
certificate
digital signature used as electronic attestation binding signature verification data to a person confirming the identity of that person as legitimate signer (**the directive: 2.9**)

3.2.5
certificate info
information associated with an SCD/SVD pair that may be stored in a secure signature creation device

Note 1 to entry: Certificate info may include:

— a signer's public key certificate, or

— one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values, or

— a public key certificate as defined in X.509.

Note 2 to entry: Certificate info may contain information to allow the user to distinguish between several certificates.

3.2.6
certificate generation application
CGA
collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate

3.2.7
certification service provider
CSP
entity that issues certificates or provides other services related to electronic signatures (**the Directive: 2.11**)

3.2.8
data to be signed
DTBS
all of the electronic data to be signed including a user message and signature attributes

3.2.9
data to be signed or its unique representation
DTBS/R
data received by a secure signature creation device as input in a single signature creation operation

Note 1 to entry: Examples of DTBS/R are:

— a hash value of the data to be signed (DTBS), or

— an intermediate hash value of a first part of the DTBS complemented with a remaining part of the DTBS, or

— the DTBS.

3.2.10
legitimate user
user of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory

3.2.11
qualified certificate
public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in **Annex II** (**the Directive: 2.10**)

3.2.12
qualified electronic signature
an advanced electronic signature which is based on a qualified certificate and which is created by an SSCD

3.2.13
reference authentication data
RAD
data persistently stored by the TOE for authentication of the signatory

3.2.14
secure signature creation device
SSCD
a signature-creation device which meets the requirements laid down in Annex III

Note 1 to entry: An SSCD may be evaluated according to the security target conforming to a PP as defined in the series of European Standards.

3.2.15
signatory
a person who holds (and is a legitimate user) of an SSCD and acts either on their own behalf or on behalf of the natural or legal person or entity they represent

3.2.16
signature creation application
SCA
application complementing an SSCD with a user interface with the purpose to create an electronic signature

3.2.17
signature creation data
SCD
unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

Note 1 to entry: For the PPs of this standard the SCD is held in the SSCD.

3.2.18
signature creation system
SCS
complete system that creates an electronic signature consisting of an SCA and an SSCD

3.2.19
signature verification data
SVD
data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature

3.2.20
SSCD-provisioning service
service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD

3.2.21
user
entity (human user or external IT entity) outside the TOE that interacts with the TOE

3.2.22
user message
data determined by the signatory as the correct input for signing

3.2.23
verification authentication data
VAD
data input to an SSCD for authentication of the signatory

4 Abbreviated terms

CC	Common Criteria [a]
CGA	certificate generation application
DTBS	data to be signed
DTBS/R	data to be signed or its unique representation
EAL	evaluation assurance level [a]
IT	information technology
PP	protection profile [a]
RAD	reference authentication data
SCA	signature creation application
SCD	signature creation data
SCS	signature creation system
SDO	signed data object
SFP	security Function Policy
SSCD	secure signature creation device
ST	security Target [a]
SVD	signature verification data
TOE	target of evaluation [a]
TSF	TOE security functionality [a]
VAD	verification authentication data
[a] See Bibliography [2, 3, 4] for details on the specification of Common Criteria.	

5 Protection Profile Overview

This series of documents constitutes a suite of protection profiles, which are established by CEN as European Standards for products to create electronic signatures. They fulfil requirements of Directive[1)] 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on *a Community framework for electronic signatures*.

[1)] This European Directive is referred to in this series of protection profiles as "**the Directive**".

In accordance with Article 9 of this European Directive these standards can be indicated by the European Commission in the Official Journal of the European Communities as generally recognized standards for electronic signature products.

These protection profiles formally specify the security functional and assurance requirements 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 the protection profiles.

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 one or more of the Protection Profiles (PPs) of this standard.

For an electronic signature product that has been evaluated according to Common Criteria (version 3.1) as conforming to a Security Target (ST) that is compliant with one or more of these Protection Profiles (PP) this European Standard implies that European Union Member States shall presume compliance with the requirements in Annex III of **the Directive** for that product.

Part 2 of this series of European Standards specifies a protection profile for an SSCD that performs its core operations including the generation of signature keys in the device. An SSCD that fulfils only the security requirements in this protection profile shall be operated by the signatory in a secure environment to create either an advanced electronic signature or a qualified electronic signature. The target of evaluation for this protection profile is defined in 7.2 and shown in Figure 2.

Part 3 of this series of European Standards specifies a protection profile for an SSCD that performs its core operations including import of the signature key generated in a trusted manner outside the device. An SSCD that fulfils only the security requirements in this protection profile shall be operated by the signatory in a secure environment to create either an advanced electronic signature or a qualified electronic signature. The target of evaluation for this protection profile is defined in 7.3 and shown in Figure 3.

Part 4 of this series of European Standards specifies an extension protection profile for an SSCD with key generation that support establishing a trusted channel with a certificate generation application. The target of evaluation for this extended protection profile is defined in 7.4 and shown in Figure 4.

Part 5 of this series of European Standards specifies an extension protection profile for an SSCD with key generation that additionally supports establishing a trusted channel with a signature creation application. The target of evaluation for this extended protection profile is defined in 7.5 and shown in Figure 5.

Part 6 of this series of European Standards specifies an extension protection profile for an SSCD with key import that additionally supports establishing a trusted channel with a signature creation application. The target of evaluation for this extended protection profile is defined in 7.5 and shown in Figure 6.

The assurance level for these protection profiles is EAL4 augmented with AVA_VAN.5.

NOTE The evaluation assurance level augmentation with AVA_VAN.5 means that the security evaluation includes a systematic, independent, comprehensive analysis of possible vulnerabilities followed by penetration testing to determine the resistance against attacks that attempt to exploit these vulnerabilities.

6 Target of Evaluation

6.1 General

The TOE for the protection profiles specified in this series of European Standards is a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The TOE protects the SCD during its whole life cycle for use in a signature creation process solely by its signatory.

NOTE In this clause the term **TOE** is used as reference to the target of evaluation for any of the protection profiles specified in this series of European Standards. The term **SSCD** is used to refer to a product that incorporates the TOE.

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

6.2 Functions of an SSCD

6.2.1 Core functions

An SSCD provides the following functions:

a) to generate signature creation data (SCD) and the correspondent signature verification data (SVD) or to import signature creation data (SCD),

b) to export the SVD for certification if this has been created by the device and optionally receive and store certificate info,

c) to initialize user authentication data (RAD),

d) to switch the SSCD from a non-operational state to an operational state, and

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

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

   2) receive data to be signed or a unique representation thereof (DTBS/R),

   3) authenticate the signatory and determine its intent to sign,

   4) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

An SSCD shall only be switched to an operational state if it is properly prepared for the signatory's use and sole control by:

f) generating at least one SCD/SVD pair, and

g) personalizing for the signatory by storing in the TOE:

   1) the signatory’s reference authentication data (RAD),

   2) optionally, certificate info for at least one SCD in the TOE.

Upon receiving an SSCD, the signatory shall verify that any SCD it contains is in a non-operational state.

If so configured an SSCD may provide management functions for key generation or import initiated by the user as specified in 6.2.2.3.

Each TOE in this series of European Standards shall support the functions of an SSCD specified in this subclause.

6.2.2 Additional functions

6.2.2.1 General

A part of this series of European Standards may define a TOE with support of one or more of the following optional functions in its operational-use stage (see Clause 7).

6.2.2.2 User authentication and identification

An SSCD may provide functions to enable the user to:

a) unblock the RAD,

b) change the value of the RAD,

c) add or modify user information to be included in signatory identification data in a SVD certificate.

6.2.2.3 User management of signing key

An SSCD may provide functions to enable the user to:

a) install an SCD, generated outside the device in a trusted environment and communicated over a secure communication link (6.2.2.4 b)),

b) generate an SCD,

c) disable an SCD it holds, e.g. by erasing it from memory,

d) create, extend or modify certificate info stored in the device, and

e) create SVD for an SCD stored and export it for certification by a certificate generation application protected by trusted communication (6.2.2.4 a)).

6.2.2.4 Secure communication

An SSCD may provide functions to establish a trusted, cryptographically protected communication with:

a) a certificate generation application,

b) an SVD generation application, and

c) a signature creation application.

The supported function may include functions for management of the cryptographic keys, parameters and configuration used to establish the trusted communication.

The certificate generation application and SVD generation application may be implemented as a single application.

6.2.2.5 Other standards

An SSCD may be used in context with a signature creation application (SCA) for creation of digital signatures which conform to one or more of the specifications in ETSI/TS 101 733 (CAdES) [5], ETSI/TS 101 903 (XAdES) [6] and ETSI/TS 102 778 (PAdES) [7]. Protection Profiles for such an SCA are being defined in a separate European Standard.

6.3 TOE life cycle

6.3.1 General

The TOE life cycle in Figure 1 distinguishes stages for development, production, preparation and operational use. Development and production of the TOE (cf. CC part 1, para.139) together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to an SSCD-provisioning service provider.

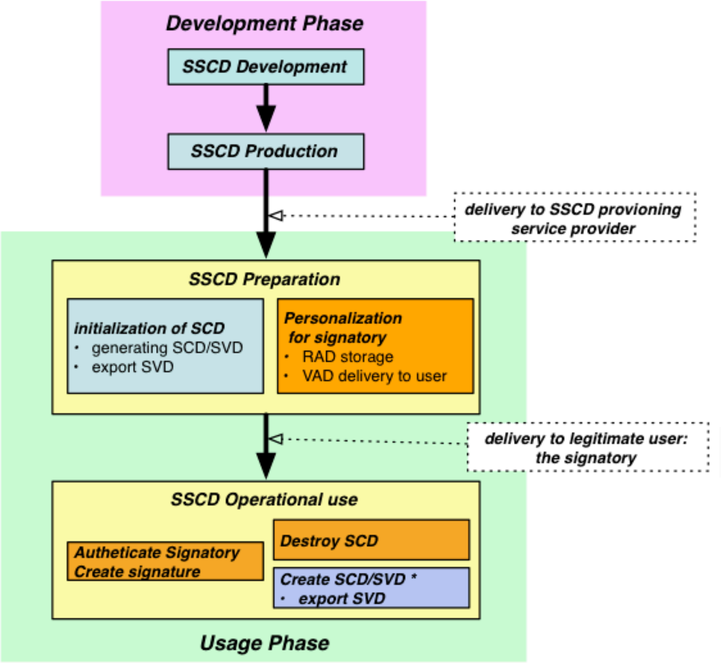

Figure 1 — TOE life cycle

The TOE operational use stage begins when the signatory performs the TOE operation to enable an SCD it contains for use in signing operations. The TOE life cycle ends when all SCD stored in it have been rendered permanently unusable. Rendering a key in the SSCD unusable may include deletion of the any stored corresponding certificate info.

NOTE The figure shows core operations in the usage phase that may be performed in the *SSCD preparation* or *SSCD operational* use stages. The figure does not indicate particular functions the TOE or the environment provide in support of these operations and to meet the required security.

6.3.2 Preparation stage

An SSCD-provisioning service provider having accepted it from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user of the TOE, having received it from an SSCD provisioning service enables an SCD it holds for use in signing.

During preparation of the TOE, an SSCD-provisioning service provider performs the following tasks:

— obtains information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE;

- generates a PIN and/or obtains a biometric sample of the legitimate user, stores this data as RAD in the TOE and prepares information about the VAD for delivery to the legitimate user;
- generates a certificate for at least one SCD either by:
  - the TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE; or
  - initializing security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving it from the TOE;
  - optionally, presenting certificate info to the SSCD.
- deliver the TOE and the accompanying VAD info to the legitimate user.

The SVD certification task (third list item above) of an SSCD-provisioning service provider as specified in this PP may support a centralized, pre-issuing key generation process, with at least one key generated and certified, before delivery to the legitimate user. Alternatively, or additionally, that task may support key generation by the signatory after delivery and outside the secure preparation environment. A TOE may support both key generation processes, for example with a first key generated centrally and additional keys generated by the signatory in the operational use stage.

Data required for inclusion in the SVD certificate at least includes (**Annex II**):

- the SVD;
- the name of the signatory, either
  - a legal name, or
  - a pseudonym together with an indication of this fact.

The data included in the certificate may have been stored in the SSCD during personalization.

Before initiating the actual certificate signature the certificate generation application verifies the SVD received from the TOE by asserting:

- the sender as genuine SSCD,
- the integrity of the SVD to be certified as sent by the originating SSCD,
- that the originating SSCD has been personalized for the legitimate user,
- correspondence between SCD and SVD, and
- that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Optionally, the TOE may support a function to provide an explicit proof of correspondence between an SCD it stores and an SVD realized by self-certification. Such a function may be performed implicitly in the SVD export function and may be invoked in the preparation environment without explicit consent of the signatory[2]. Security requirements to protect the SVD export function and the

[2] Self-certification of the SVD is effectively computing a digital signature with the corresponding SCD. A signing operation requires explicit sole signatory control, however this specific case, if supported, provides an exception to this rule as, before being delivered to the signatory, such control is evidently impossible.

certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in Part 4 of this series of European Standards.

Prior to generating the certificate, the certification service provider shall assert the identity of the signatory as the legitimate user of the TOE.

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, providing this information to the legitimate user shall protect the confidentiality of the corresponding RAD.

6.3.3 Operational-use stage

In the operational-use stage the signatory can use the TOE to create advanced electronic signatures.

The signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable may end the life of the TOE as SSCD.

NOTE An SSCD that supports key generation in the operational-use stage does not end its life when it no longer has a usable SCD.

The TOE may support functions to generate signing keys in the operational stage (6.2.2.3 b)). For an additional key the signatory may be allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory may also be allowed to choose some of the data to be incorporated in the certificate, for instance to use a pseudonym instead of the legal name[3)]. If the conditions to obtain a qualified certificate are met, the new key can also be used to create advanced electronic signatures. The optional TOE functions for additional key generation and certification may require additional security functions in the TOE and an interaction with the SSCD-provisioning service provider in an environment that is secure or using trusted communication.

6.4 Operations of the TOE

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

— The signing environment where it interacts with a user through a signature creation application (SCA) to sign data after authenticating the user 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 digital signature[4)];

— 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 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 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.

As shown in Figure 2 through Figure 6 the signing environment, the management environment and the preparation environment are secure and protect the data to be exchanged with the TOE. The protection of

[3)] The data provided as input to the CGA in this case will contain the name of the signatory as the requester, as for instance it may be signed by the signatory's existing SCD.

[4)] At a pure functional level the SSCD creates a *digital signature* as part of a signing process; for an implementation of the SSCD that meets the requirements of these protection profiles and with the key certificate created as specified in **Annex I**, the result of this signing process can be used as a *qualified electronic signature*.

data exchanged with the TOE may be realized by trusted communication, in which case the TOE may actually be operated in a non-secure environment for the functions thus protected.

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case, the TOE shall provide a function to identify each SCD and the 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 of the SCD and restricts its use in signature creation to its authenticated signatory. The digital signature created by the TOE is part of a *qualified electronic signature* (3.2.12) as described in **The Directive: 5.1** if the certificate for the SVD is a qualified certificate (**Annex I**). Determining the state of the certificate as qualified in beyond the scope of this standard.

The signature creation application shall 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 may receive the VAD from the signature creation application. If the signature creation application handles requesting obtaining a VAD from the user, it shall protect the confidentiality of this data.

A certification service provider and an 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.

NOTE 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 digital signature creation function of the smart card through the terminal.

7 TOE definitions

7.1 General

The Targets of Evaluation defined in this clause are the TOE for other parts of this series of European Standards.

7.2 TOE with key generation

The TOE with a function for key generation supports the core functions of an SSCD (6.2.1).

Figure 2 shows this TOE, its operational environments and the interactions with the environment.

The key generation function of this TOE shall be performed in a trusted preparation environment.

7.3 TOE with key import

The TOE with a function for key import supports the core functions of an SSCD (6.2.1).

Figure 3 shows this TOE, its operational environments and the interactions with the environment.

The key import function of this TOE shall be performed in a trusted preparation environment.

7.4 TOE with key generation and trusted channel to certificate generation application

The TOE with a function for key generation and trusted channel to certificate generation application supports

- core functions of an SSCD (6.2.1),
- functions to generate SCD in the operational-use stage (6.2.2.3 b)),
- functions to export SVD (6.2.2.3 e)), and
- functions to establish a secure connection with a certificate generation application (6.2.2.4 a)).

If this TOE supports generating multiple SCD it shall also support functions to specify certificate info (6.2.2.3 d)).

Figure 4 shows this TOE, its operational environments and the interactions with the environment.

The key generation function of this TOE may be performed in a non-trusted environment.

7.5 TOE with trusted channel to signature creation application

A TOE with a function to establish a trusted channel to certificate generation application supports:

- core functions of an SSCD (6.2.1), and
- functions to establish a secure connection with a signature creation application (6.2.2.4 c)).

Figure 5 shows a TOE supporting key generation with functions to establish a trusted channel with the signature creation application, its operational environments and the interactions with the environment.

Figure 6 shows a TOE supporting key import with functions to establish a trusted channel with the signature creation application, its operational environments and the interactions with the environment.

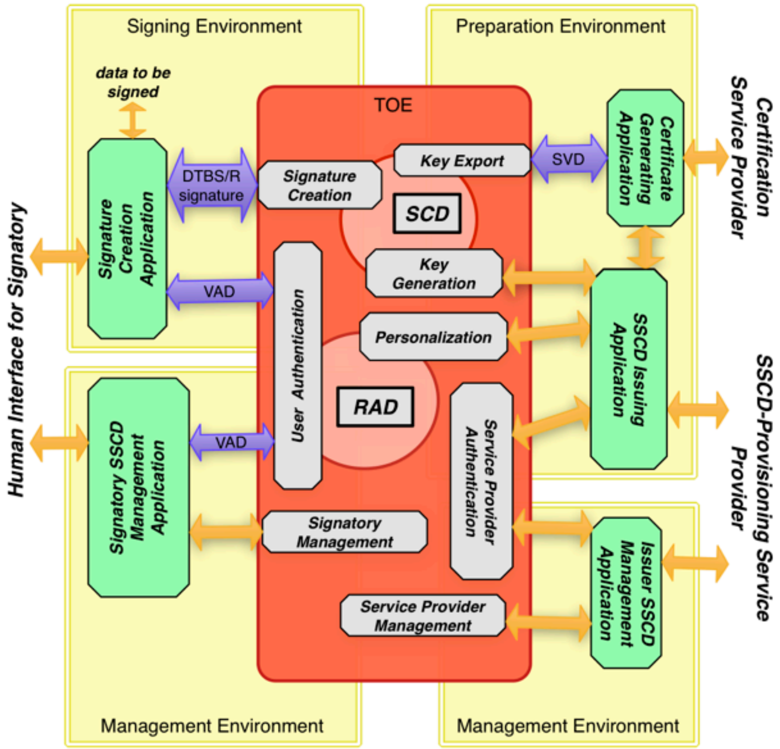
Signing Environment
Preparation Environment
data to be signed
TOE
Signature Creation Application
DTBS/R signature
Signature Creation
Key Export
SVD
Certificate Generating Application
Certification Service Provider
SCD
Key Generation
VAD
User Authentication
Personalization
SSCD Issuing Application
RAD
Human Interface for Signatory
Signatory SSCD Management Application
VAD
Service Provider Authentication
SSCD-Provisioning Service Provider
Signatory Management
Issuer SSCD Management Application
Service Provider Management
Management Environment
Management Environment

Figure 2 — TOE and operational environments with key generation

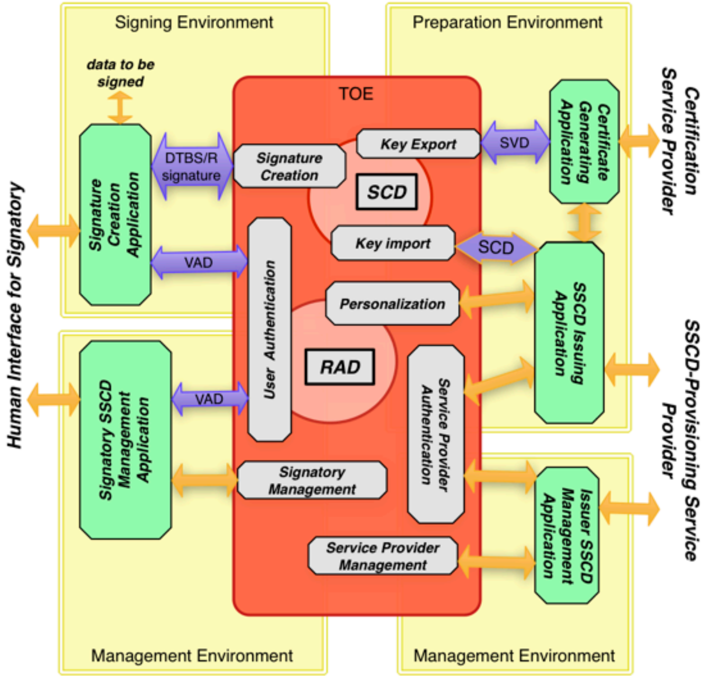
Signing Environment
Preparation Environment
data to be signed
TOE
Signature Creation Application
DTBS/R signature
Signature Creation
Key Export
SVD
Certificate Generating Application
Certification Service Provider
SCD
Key import
SCD
VAD
User Authentication
Personalization
SSCD Issuing Application
RAD
Human Interface for Signatory
Signatory SSCD Management Application
VAD
Service Provider Authentication
SSCD-Provisioning Service Provider
Signatory Management
Issuer SSCD Management Application
Service Provider Management
Management Environment
Management Environment

Figure 3 — TOE and operational environments with key import

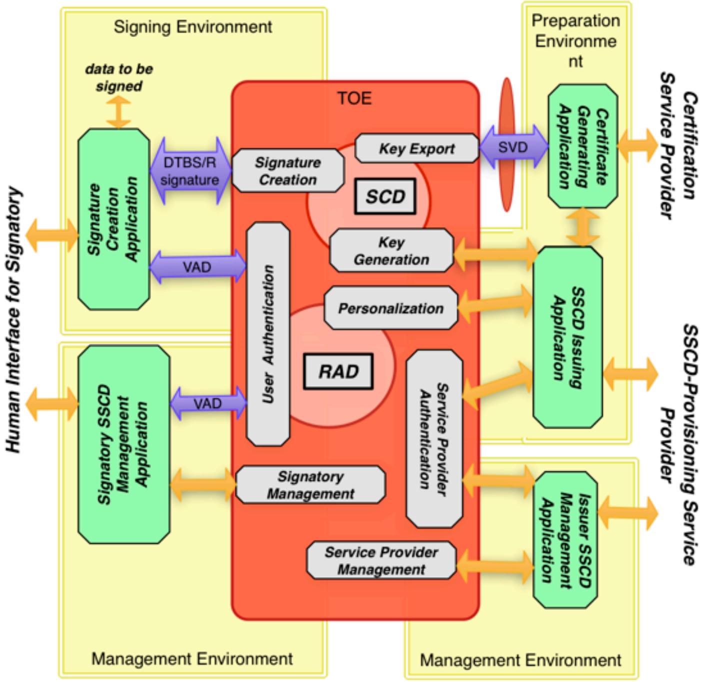
Signing Environment
data to be signed
Preparation Environme nt
TOE
Certification Service Provider
Certificate Generating Application
SVD
Key Export
Signature Creation
DTBS/R signature
SCD
Signature Creation Application
Human Interface for Signatory
VAD
Key Generation
SSCD Issuing Application
User Authentication
Personalization
SSCD-Provisioning Service Provider
RAD
Service Provider Authentication
Signatory SSCD Management Application
VAD
Signatory Management
Issuer SSCD Management Application
Service Provider Management
Management Environment
Management Environment

Figure 4 — TOE and operational environments with trusted channel to certificate generation application

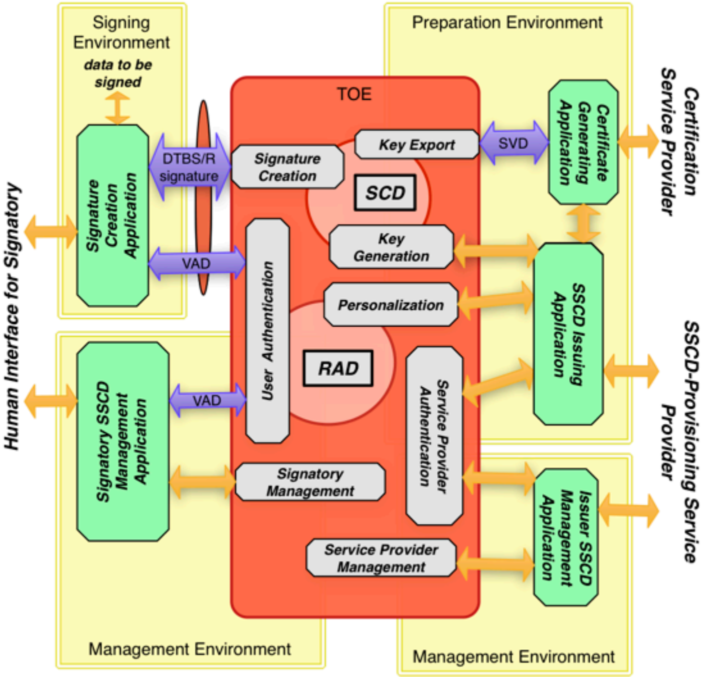
Signing Environment
data to be signed
Preparation Environment
TOE
Certification Service Provider
Certificate Generating Application
SVD
Key Export
Signature Creation
DTBS/R signature
SCD
Signature Creation Application
Human Interface for Signatory
VAD
Key Generation
SSCD Issuing Application
User Authentication
Personalization
SSCD-Provisioning Service Provider
RAD
Service Provider Authentication
Signatory SSCD Management Application
VAD
Signatory Management
Issuer SSCD Management Application
Service Provider Management
Management Environment
Management Environment

Figure 5 — TOE and operational environments with trusted channel to signature creation application and key generation

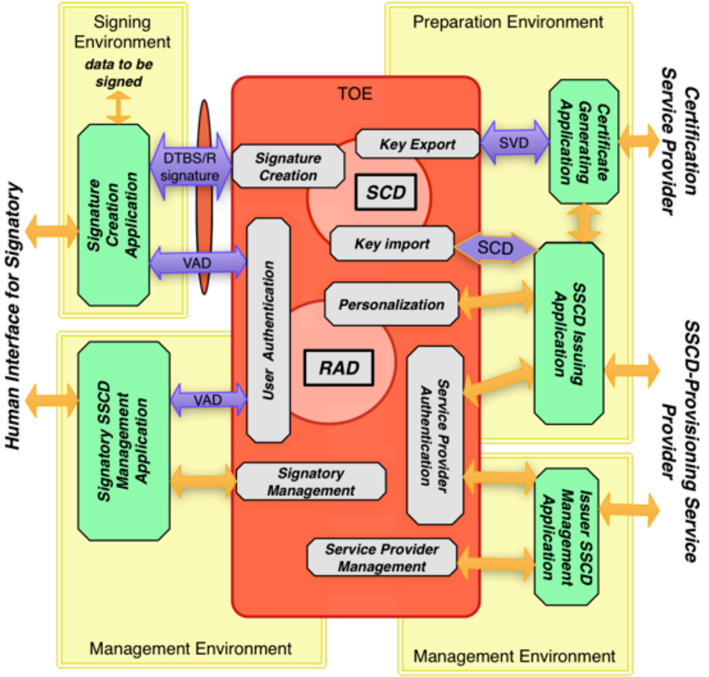
Signing Environment
data to be signed
Preparation Environment
TOE
Certification Service Provider
Human Interface for Signatory
Signature Creation Application
DTBS/R signature
VAD
Signature Creation
Key Export
SVD
Certificate Generating Application
SCD
Key import
SCD
User Authentication
Personalization
SSCD Issuing Application
RAD
Service Provider Authentication
SSCD-Provisioning Service Provider
Signatory SSCD Management Application
VAD
Signatory Management
Issuer SSCD Management Application
Service Provider Management
Management Environment
Management Environment

Figure 6 — TOE and operational environments with trusted channel to signature creation application and key import

Annex A
(informative)

Comparison with CWA 14169:2004, Annex C

A.1 General

This series of European Standards supersedes CWA 14169. This CEN workshop agreement established a number of protection profiles for an SSCD, each PP addressing different functional configuration of the device. In the CWA functional configurations where in part indicted by "*Type 1*", "*Type 2*" and "*Type 3*".

In this series of European Standards, different functional configurations for an SSCD are explicitly mentioned in the titles of its various parts. The functionality referred to as "*Type 2*" in CWA 14169 can be found in part 3 of this series of European Standards. The functionality referred to as "*Type 3*" in CWA 14169 can be found in part 2. The functionality referred to as "*Type 1*" is no longer supported.

A.2 Technical Differences

This series of European Standards supports the following product features not present in CWA 14169:2004:

Multiple signing keys in a device, the device can store certificate info, which can be presented to the user to select, or confirm, a particular key to be used in a signature creation process.

Off-line use, if so configured, an SSCD conforming to this series of European Standards can be used in an environment deemed "trusted" by the user to create an advanced (or qualified) electronic signature without a cryptographically protected communication with the signature creation application.

User-initiated device preparation, the issuer of an SSCD may offer the user the option to initiate key generation or import after receiving the device. If so configured, a device conforming to this series of European Standards may be delivered to a user without any signing keys, and additional signing keys may be created during the operational life of the device.

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 3, CCMB-2009-07-001, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, CCMB-2009-07-002, July 2009

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, CCMB-2009-07-003, July 2009

[5] 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.asp5

[6] 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.asp6

[7] 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.asp7

This page deliberately left blank

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.

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

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

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 Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™