SLOVENSKI STANDARD
SIST EN 419211-2:2013

01-september-2013

Profil zaščite sredstva za varno elektronsko podpisovanje - 2. del: Sredstvo za tvorjenje ključa

Protection Profile for Secure signature creation device - Part 2: Device with key generation

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 2: Geräte mit Schlüsselerzeugung

Profils de protection des dispositifs sécurisés de création de signature - Partie 2: Dispositif avec génération de clé

Ta slovenski standard je istoveten z: **EN 419211-2:2013**

ICS:

03.160	Pravo. Uprava	Law. Administration
35.040	Nabori znakov in kodiranje informacij	Character sets and information coding
35.100.05	Večslojne uporabniške rešitve	Multilayer applications

SIST EN 419211-2:2013 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-2

July 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 2: Device with key generation

Profils de protection des dispositifs sécurisés de création de signature - Partie 2: Dispositif avec génération de clé

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 2: Geräte mit Schlüsselerzeugung

This European Standard was approved by CEN on 8 May 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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 419211-2:2013: E

Contents

Page

Foreword

This document (EN 419211-2:2013) 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 January 2014, and conflicting national standards shall be withdrawn at the latest by January 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 document was submitted to the Enquiry procedure under reference prEN 14169-2.

The EN 419211 series 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*

Preparation of this document as a protection profile (PP) follows the rules of ISO/IEC 15408-1.

Correspondence and comments regarding this protection profile about secure signature creation device with key generation (PP SSCD KG) can be referred to the CEN/TC 224 Secretary.

According to the CEN-CENELEC Internal Regulations, the national standards organisations 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.

1 Scope

This European Standard specifies a protection profile for a secure signature creation device that may generate signing keys internally: secure signature creation device with key generation (SSCD KG).

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

ISO/IEC 15408-1:2009[2)] *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2[2)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3[2)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

3 Conventions and terminology

3.1 Conventions

The content and structure of this document follow the rules and conventions laid out in ISO/IEC 15408-1.

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

3.2 Terms and definitions

For the purposes of this document, the acronyms, terms and definitions given in prEN 419211-1 apply.

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 2: Device with key generation
Version:	2.0.1.
Author:	CEN (TC224/WG17)
Publication date:	2013
Registration:	BSI-CC-PP-0059-2009-MA-01
CC version:	3.1 Revision 3

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

2) ISO/IEC 15408-1, -2 and -3 respectively correspond to *Common Criteria for Information Technology Security Evaluation*, Parts 1, 2 and 3.

Editor:	Arnold Abromeit, TÜV Informationstechnik GmbH
General status:	final draft
Keywords:	secure signature creation device, electronic signature, digital signature

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 1999/93/EC[3] 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 Union as a generally recognised standard for electronic signature products.

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

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

This Protection Profile describes core security requirements for a secure device that can generate a signing key[4] (signature creation data, SCD) and operates to create electronic signatures with the generated key. A device evaluated according to this protection profile and used in the specified environments can be trusted to create any type of digital signature. As such, this PP can be used for any device that has been configured to create a digital signature. Specifically this PP allows the qualification of a product as a device for creating an advanced electronic signature as defined in the directive.

After an SSCD has generated a signing key, the corresponding public key (signature verification data, SVD) has to be provided as input to a certificate generation application (CGA). Security requirements for export of the SVD are described in a protection profile that extends this PP (prEN 419211-4, *Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application)*[5] and not in this document.

When operated in a secure environment for signature creation a signer may use an SSCD that fulfils only these core security requirements to create an advanced electronic signature.[6] Security requirements for an SSCD used in environments where the communication between SSCD and the signature creation application (SCA) is assumed to be protected by the SSCD and the SCA are described in a separate protection profile that extend this PP (prEN 419211-5, *Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application*)[7] and not in this document.

These extended Protection Profiles claim conformance to this PP.

---

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

4) An SSCD that can generate its own SCD/SVD was defined in the previous version of this PP (CWA 14169) as a Type 3 SSCD. The notion of types does not exist anymore in this series of ENs. In order to refer to the same functionality, a reference to EN 419211-2 (i.e. Part 2) should be used.

5) This document was submitted to the Enquiry procedure under reference prEN 14169-4.

6) An advanced electronic signature is defined as an electronic signature created by an SSCD using a public key with a public key certificate created as specified in the directive.

7) This document was submitted to the Enquiry procedure under reference prEN 14169-5.

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

— The preparation environment, where it interacts with a certification service provider through a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the SCD the TOE has generated. The initialisation environment interacts further with the TOE to personalise 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 digital signature[8)].

— The management environments where it interacts with the user or an SSCD-provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE. Figure 2 in Part 1 of this standard illustrates the operational environment.

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case, the TOE provides a function to identify each SCD and the 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 digital signature created by the TOE may be used to create an advanced electronic signature as defined in Article 5.1 of the directive. Determining the state of the certificate as qualified is beyond the scope of this standard.

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

The TOE stores signatory reference authentication data to authenticate a user as its signatory. The RAD is a password, e.g. PIN, a biometric template or a combination of these. The TOE protects the confidentiality and integrity of the RAD. The TOE may provide a user interface to directly receive verification authentication data (VAD) from the user; alternatively, the TOE receive the VAD from the signature creation application. If the signature creation application handles, is requesting or obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

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

---

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

— initialising the RAD;

— generating a key pair;

— storing personal information of the legitimate user.

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

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

The TOE may implement its function for digital signature creation to conform to the specifications in ETSI TS 101 733 (CAdES) [3], ETSI TS 101 903 (XAdES) [4] and ETSI TS 101 903 (PAdES) [5].

The TOE is prepared for the signatory's use by:

a) generating at least one SCD/SVD pair; and

b) personalising 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.

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

After preparation, the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, the means of providing this information is expected to protect the confidentiality and the integrity of the corresponding RAD.

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

4.3.3 TOE lifecycle

4.3.3.1 General

The TOE lifecycle distinguishes stages for development production, preparation and operational use. Note that other lifecycle definitions are possible; when this PP is claimed by other PPs (e.g. SCD/SVD generation in trusted environment after delivery to the signatory may be allowed when there is a trusted channel to the CGA).

The development phase comprises the development and production of the TOE. The development phase is subject of the evaluation according to the assurance lifecycle (ALC) class. The development phase ends with the delivery of the TOE to the SSCD-provisioning service.

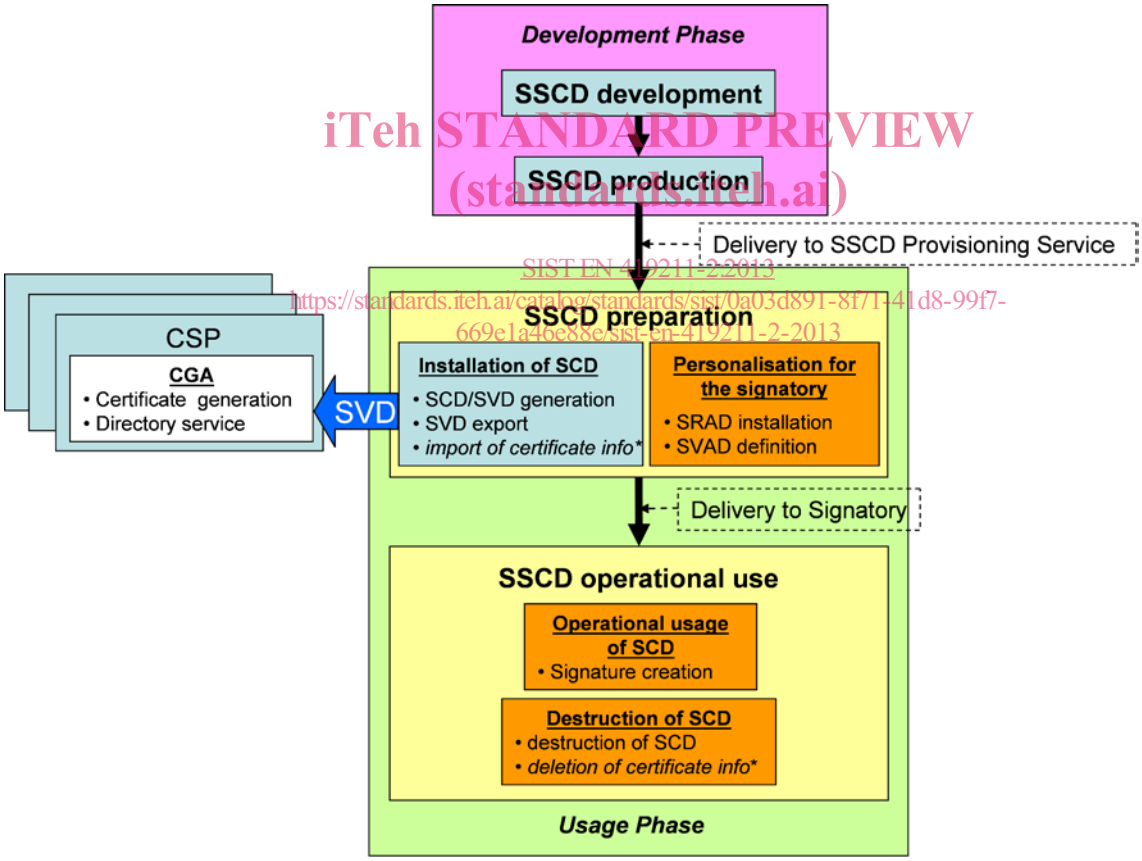

Figure 1 - Example of TOE lifecycle[9)]

9) The asterisks * mark the optional import of the SVD and certificate info during TOE preparation and certificate info deletion when SCD is destroyed.

The operational usage of the TOE comprises the preparation stage and the operational use stage. The TOE operational use stage begins when the signatory has obtained both the VAD and the TOE. Enabling the TOE for signing requires at least one set of SCD stored in its memory.

Figure 1 shows an example of the lifecycle where an SCD/SVD pair is generated on the TOE before delivery to the signatory. The lifecycle may allow generation of SCD or SCD/SVD key pairs after delivery to the signatory as well.

4.3.3.2 Preparation stage

An SSCD-provisioning service provider having accepted the TOE from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user has received the TOE from the SSCD-provisioning service and any SCD it might already hold have been enabled for use in signing.

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

a) Obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE.

b) Generate a PIN and/or obtain a biometric sample of the legitimate user, store this data as RAD in the TOE and prepare information about the VAD for delivery to the legitimate user.

c) Generate a certificate for at least one SCD either by:

   1) the TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE; or

   2) initialising security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving a protected request from the TOE.

d) Optionally, present certificate info to the SSCD.

e) Deliver the TOE and the accompanying VAD info to the legitimate user.

The SVD certification task (third item listed above) of an SSCD-provisioning service provider as specified in this PP may support a centralised, 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 (cf. [1], Annex II)

— the SVD which correspond to SCD under the control of the signatory;

— the name of the signatory or a pseudonym, which is to be identified as such;

— an indication of the beginning and end of the period of validity of the certificate.

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

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

a) establishing the sender as genuine SSCD;

b) establishing the integrity of the SVD to be certified as sent by the originating SSCD;

c) establishing that the originating SSCD has been personalised for the legitimate user;

d) establishing correspondence between SCD and SVD; and

e) an assertion 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 realised 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 [10)]. Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in a separate PP (see section 4.2).

Prior to generating the certificate the certification service provider asserts the identity of the signatory specified in the certification request as the legitimate user of the TOE.

4.3.3.3 Operational use stage

In this lifecycle stage the signatory can use the TOE to create advanced electronic signatures.

The TOE operational use stage begins when the signatory has obtained both the VAD and the TOE. Enabling the TOE for signing requires at least one set of SCD stored in its memory.

The signatory can also interact with the SSCD to perform management tasks, e.g. reset a RAD value or use counter if the password/PIN in the reference data has been lost or blocked. Such management tasks require a secure environment.

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

The TOE may support functions to generate additional signing keys. If the TOE supports these functions it will support further functions to securely obtain certificates for the new keys. 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 in the certificate request for instance to use a pseudonym instead of the legal name in the certificate [11)]. 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.

The TOE life cycle as SSCD ends when all set of SCD stored in the TOE are destructed. This may include deletion of the corresponding certificates.

---

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

11) The certificate request 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.

5 Conformance claims

5.1 CC conformance claim

This PP uses ISO/IEC 15408-3 (see Clause 10).

This PP is conforming to ISO/IEC 15408-2.

This PP is conforming to ISO/IEC 15408-3.

5.2 PP claim, Package claim

This PP does not claim conformance to any other PP.

This PP is conforming to assurance package EAL4 augmented with AVA_VAN.5 defined in ISO/IEC 15408-3..

5.3 Conformance rationale

This PP does not provide a conformance rationale because it does not claim conformance to any other PP.

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

ISO/IEC 15408 defines 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.

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:

a) 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.

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

c) 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.