SLOVENSKI STANDARD
SIST EN 419211-3:2014

01-marec-2014

Profil zaščite sredstva za varno elektronsko podpisovanje - 3. del: Sredstvo z vnosom ključa

Protection profiles for secure signature creation device - Part 3: Device with key import

Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 3: Einheiten mit Schlüsselimport

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 3: Dispositif avec import de clé

Ta slovenski standard je istoveten z: EN 419211-3:2013

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 419211-3:2014 **en,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-3

October 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 3: Device with key import

Profils de protection des dispositifs sécurisés de création de signature - Partie 3: Dispositif avec import de clé

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 3: Einheiten mit Schlüsselimport

This European Standard was approved by CEN on 14 September 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

Foreword

This document (EN 419211-3:2013) 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 April 2014, and conflicting national standards shall be withdrawn at the latest by April 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 CEN Enquiry under reference prEN 14169-3.

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.

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+".

This series of European Standards consists of the following parts:

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

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

1 Scope

This European Standard specifies a protection profile for a secure signature creation device with signing keys import possibility: SSCD with key import (SSCD KI).

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 14169-1:2011, *Protection profiles for secure signature creation device — Part 1: Overview*

3 Terms and definitions

For the purposes of this document, the acronyms, terms and definitions given in prEN 14169-1:2011 apply.

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 3: Device with key import
Version:	1.0.2
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	2012-07-24
Registration:	BSI-CC-PP-0075
CC version:	3.1 Revision 3
Editor:	Arnold Abromeit, TÜV Informationstechnik GmbH
General status:	final
Keywords:	secure signature creation device, electronic signature, digital signature, key import

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[1] 1999/93/ec of the European parliament and of the council of 13 December 1999 on *a community framework for electronic signatures*.

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

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

[1] This European Directive is referred to in this PP as “the directive”.

European Union Member States may presume that there is compliance with the requirements laid down in Annex III of **the Directive** [1] 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 import a signing key[2] (signature creation data, SCD) and operates to create electronic signatures with the imported 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**.

The intent of this Protection Profile is to specify security functional and assurance requirements defined in **the Directive** [1], Annex III for secure signature creation devices (SSCD), which is the target of evaluation (TOE). Member States shall presume that there is compliance with the requirements laid down in Annex III of **the Directive** [1] when an electronic signature product is evaluated to a Security Target (ST) that is compliant with this Protection Profile (PP).

EN 419211-3 defines the core security requirements for SSCD importing signature creation data (SCD) and creating advanced electronic signature, which if based on valid qualified certificates are qualified electronic signatures. A SSCD, which fulfils only these core security requirements, may be used by the signatory in a secure environment for signature creation. The CSP will generate SCD/SVD pair in a secure environment and import the SCD into the SSCD so that it can be delivered to the signer with at least one SCD and possibly Certificate info stored in the SSCD. The TOE may implement additional security functions e.g. to support integrity protection of imported data to be signed. The related security requirements are not subject of this core PP but extended PP EN14169-6 "Protection profiles for secure signature creation device — Part 6: Device with key import and Trusted Communication with Signature creation application" will address them claiming conformance to this core PP.

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 the TOE interacts with a certification service provider (CSP) through a SCD/SVD generation application to import the signature creation data (SCD) and a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding to the SCD the certification service provider has generated. The SCD/SVD generation application transmits the SVD to the CGA. 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 the TOE interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation

[2] An SSCD that can import SCD/SVD was defined in the previous version of this PP (CWA 14169) as a Type 2 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 419211-3 (i.e. Part 3) should be used.

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[3].

- The management environments where the TOE 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 preparation environment, the signing environment and the management environment are secure and protect data exchanged with the TOE. Figure 3 in prEN 14169-1:2011 illustrates the operational environment.

The TOE stores signature creation data (SCD) and reference authentication data (RAD). 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 value 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 (RAD) 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 (SCA). If the signature creation application handles, is requesting or obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

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

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

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.

[3] 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.

4.3.2 Target of evaluation

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

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

The TOE provides the following functions:

(1) to import signature creation data (SCD) and, optionally, the correspondent signature verification data (SVD),

(2) to, optionally, receive and store certificate info,

(3) to switch the TOE from a non-operational state to an operational state, and

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

  (a) select a set of SCD if multiple sets are present in the SSCD,

  (b) authenticate the signatory and determine its intent to sign,

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

  (d) 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) [6], ETSI TS 101 903 (XAdES) [7] and ETSI TS 102 778 (PAdES) [9].

The TOE is prepared for the signatory's use by

(1) import at least one set of SCD, and

(2) personalising for the signatory by storing in the TOE:

  (a) the signatory's reference authentication data (RAD)

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

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

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

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

4.3.3 TOE lifecycle

4.3.3.1 General

The TOE lifecycle distinguishes stages for development, preparation and operational use. Please take note that other lifecycle definitions are possible; when this PP is claimed by other PPs (e.g. for a SSCD providing additionally trusted communications with the signature creation application).

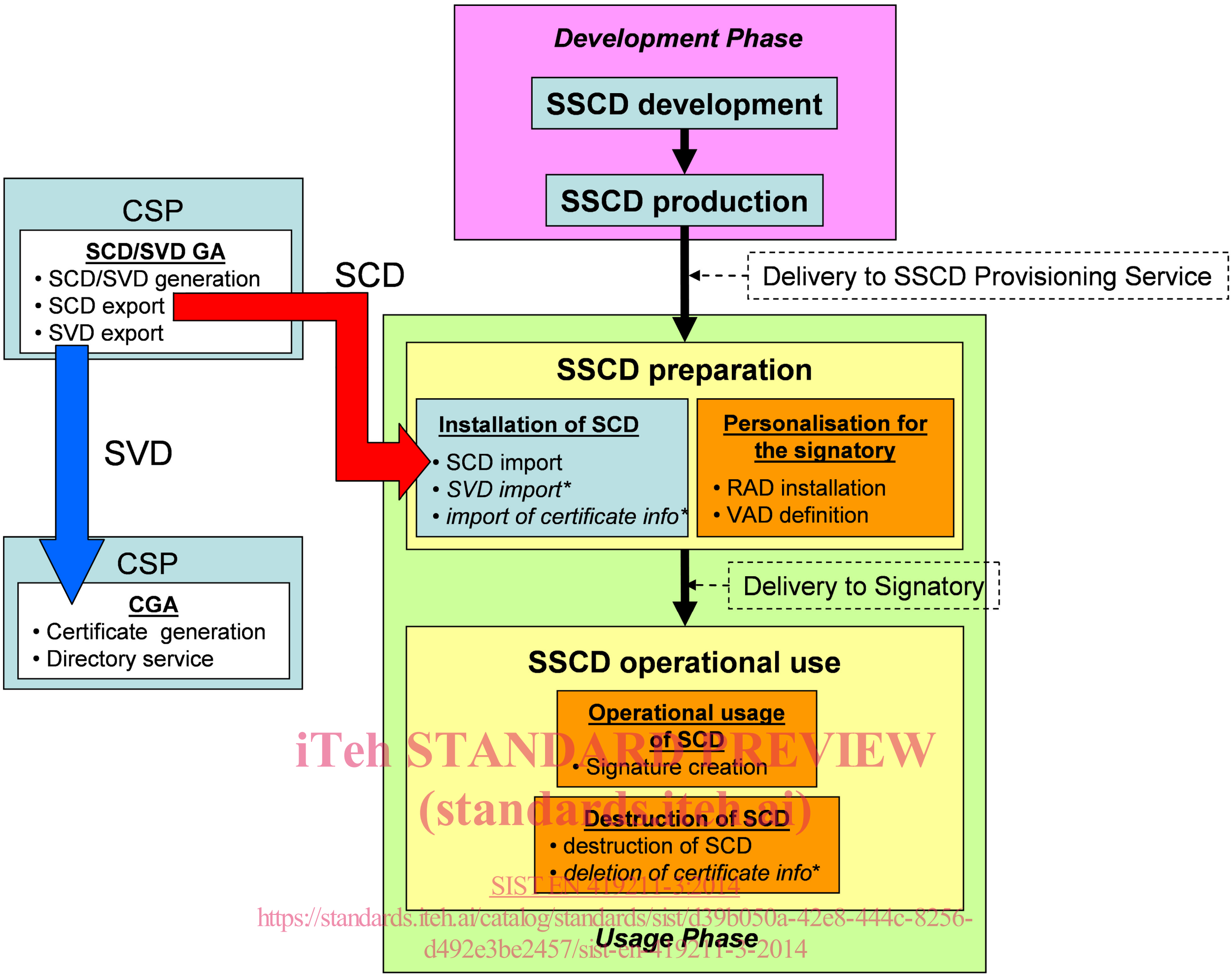

Figure 1 - Example of TOE lifecycle[4]

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.

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 or SCD/SVD pair is imported from SSCD-provisioning service before delivery to the signatory. The lifecycle may allow import of SCD or SCD/SVD key pairs after delivery to the signatory as well.

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

4.3.3.2 Preparation stage

The preparation phase of the TOE lifecycle is processing the TOE from the customer's acceptance of the delivered TOE to a state ready for operation by the signatory. The customer receiving the TOE from the manufacturer is the SSCD-provisioning service that prepares and provides the SSCD to subscribers. The preparation includes

(1) The personalisation of the TOE for use by the signatory, i.e. the installation of the RAD in the TOE and handover of VAD to the signatory.

(2) The initialisation of the TOE, i.e. the CSP generates the SCD/SVD pair by means of a SCD/SVD generation device, loads the SCD to the TOE, and sends the SVD to the CGA. The TOE may import and store the SCD/SVD pair.

(3) The generation of the (qualified) certificate containing among others (cf. [1], Annex II)
   (a) the SVD which correspond to SCD under the control of the signatory;
   (b) the name of the signatory or a pseudonym, which is to be identified as such,
   (c) an indication of the beginning and end of the period of validity of the certificate.

(4) The preparation may include optional loading of the certificate info into the SSCD for signatory convenience.

The CSP generates a SCD/SVD pair and imports SCD, and optionally also SVD, into the SSCD. The CSP ensures
(a) the correspondence between SCD and SVD,
(b) that algorithm and key size for the SVD are appropriate.

Please take note that verifying whether the claimed identity of the signer originates from that given SSCD has to be done by the CSP operating the CGA.

If the TOE is used for creation of advanced electronic signatures, the certificate links the signature verification data to the person (i.e. the signatory) and confirms the identity of that person (cf. [1], article 2, Clause 9).

This PP requires the TOE to provide mechanisms for import of SCD, implementation of the SCD and personalisation. The environment is assumed to protect all other processes for TOE preparation like SCD transfer between the SCD/SVD generation device and the TOE, and SVD transfer between the SCD/SVD generation device and the CGA. The CSP may export the SVD to the TOE for internal use by the TOE (e.g., self-test).

Before generating a (qualified) certificate, the CSP is expected to first store the SCD in a SSCD. A secure channel with the TOE may be used to support this, by ensuring integrity of the SCD during transmission to 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 operational phase of the TOE starts when at least one SCD/SVD pair is generated by the CSP and the SCD is imported into the SSCD and when the signatory takes control over the TOE and makes the SCD operational. The signatory uses the TOE with a trustworthy SCA in a secured environment only. The SCA is assumed to protect the DTBS/R during the transmission to the TOE.

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[5]. 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 SCD stored in the TOE are destructed. This may include deletion of the corresponding certificates.

5 Conformance claims

5.1 CC conformance claim

This PP uses the Common Criteria version 3.1 Revision 3 (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 does not claim conformance to any other PP.

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 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.

[5] 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.