SLOVENSKI STANDARD
oSIST prEN 14169-3:2010

01-oktober-2010

Zaščitni profili naprave za varno elektronsko podpisovanje - 3. del: Naprava 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: **prEN 14169-3**

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

oSIST prEN 14169-3:2010 **en,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 14169-3

July 2010

ICS 03.160; 35.040; 35.240.15

Will supersede CWA 14169:2004

English Version

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

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

Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 3: Einheiten mit Schlüsselimport

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 224.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. prEN 14169-3:2010: E

Contents

Page

Foreword

This document (prEN 14169-3:2010) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This document is currently submitted to the CEN Enquiry.

This document will supersede CWA 14169:2004.

Introduction

This series of European standards specifies Protection Profiles for Secure Signature-Creation Devices and issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) as update of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14169:2002, Annex C on the protection profile secure signature-creation devices, "EAL 4+".

This series of European standards consists of the following parts:

— *Protection Profiles for Secure Signature Creation Device — Part 1: Overview*

— *Protection Profiles for Secure Signature Creation Device — Part 2: Device with key generation*

— *Protection Profiles for Secure Signature Creation Device — Part 3: Device with key import*

— *Protection Profiles for Secure Signature Creation Device — Part 4: Extension for device with key generation and trusted channel to certificate-generation application;*

— *Protection Profiles for Secure Signature Creation Device — Part 5: Extension for device with key generation and trusted channel to signature-creation application;*

— *Protection Profiles for Secure Signature Creation Device — Part 6: Extension for device with key import and trusted channel to signature-creation application.*

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

Correspondence and comments to this secure signature-creation device protection profile (PP SSCD with key generation) should be referred to:

CONTACT ADDRESS

CEN/ISSS Secretariat
Avenue Marnix 17
1000 Brussels, Belgium

Tel +32 2 550 0813
Fax +32 2 550 0966

Email isss@cenorm.be

1 Scope

This European standard specifies a protection profile for a secure signature creation device that may generate signing keys internally: SSCD with key import.

2 Normative references

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

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, CCMB-2009-07-001, July 2009.

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

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

3 Terms and definitions

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

4 Protection Profile Introduction

4.1 Overview of this section

This section provides document management and overview information. Section 4.2 “Protection Profile Reference” gives the label and further descriptive information necessary to enter this Protection Profile in a register. Section 4.3 “PP Overview” presents the purpose of this protection profile in the context of additional protection profiles for extended security requirements. This section is intended to be used as independent abstract, e.g. for use in a PP register. Section 4.4 “TOE Overview” provides an informal description of the functions of the TOE and summarizes the security requirements. That section is further intended for implementers as the basis for the informal description part in CC documents based on this PP.

4.2 Protection Profile Reference

Title:	Protection Profile Secure Signature Creation Device with key import
Version:	0.7
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	(TBD)
Registration:	BSI-CC-PP-00xx
CC version:	3.1 Revision 3
Editor:	Wolfgang Killmann, T-System GEI GmbH
General status:	internal draft
Keywords:	secure signature-creation device, electronic signature, digital signature

4.3 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 formally specifies 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 this protection profile.

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 this Protection Profile (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.

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).

This EN14169-3 “Protection profiles for Secure signature creation device — Part 3: Device with key import” defines the core security requirements for all 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 fulfills 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.

---

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

[2] An SSCD that can create SCD/SVD for export into other SSCD but does not create signatures with is known as an SSCD Type 1 to be distinguished from type 1 and type 2 as defined in the previous version of this PP (CWI 14160). The protection profile for a SSCD type 2 is in “EN14169-2 *Protection Profile Secure signature creation device - Part 2: Device with import of key*”

4.4 TOE Overview

4.4.1 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 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 with this SCD the certification service provider has generated. The SCD/SVD generation application transmitts the SVD to the CGA. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference-authentication data (RAD);

— the signing environment where it interacts with a signer through a signature-creation application (SCA) to sign data after authenticating the signer as its signatory. The signature-creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature-creation function and obtains the resulting digital signature[3];

— 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 3 in Part 1 [6] of this standard illustrates the operational environment.

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case the TOE 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 signatory. The digital signature created with the TOE is a *qualified electronic signature* as defined in **The Directive** if the certificate for the SVD is a qualified certificate (Annex I). Determining the state of the certificate as qualified 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 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.

---

[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.

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 authorization. A signature can be obtained on a document prepared by a signature-creation application component running on personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorization PIN initiates the digital signature creation function of the smart card through the terminal.

4.4.2 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 life cycle 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:

— to import signature-creation data (SCD) and, optionally, the correspondent signature-verification data (SVD);

— to, optionally, receive and store certificate info;

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

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

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

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

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

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

The TOE may implement its function for digital signature creation to also conform to the specifications in ETSI TS 101 733 (CAdES) [7] and ETSI TS 101 903 (XAdES) [8]. In this case the TOE may provide additional supporting functions, e.g. to support receiving and/or validating a time stamp.

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

— import at least one SCD; and

— 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 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, providing this information shall protect the confidentiality of the corresponding RAD.

If continued use of an SCD is no longer required the TOE will disable an SCD it holds, e.g. by erasing it from memory.

4.4.3 TOE life cycle

4.4.3.1 General

The TOE life cycle consists of a development and the operational usage. Note that other life cycle 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).

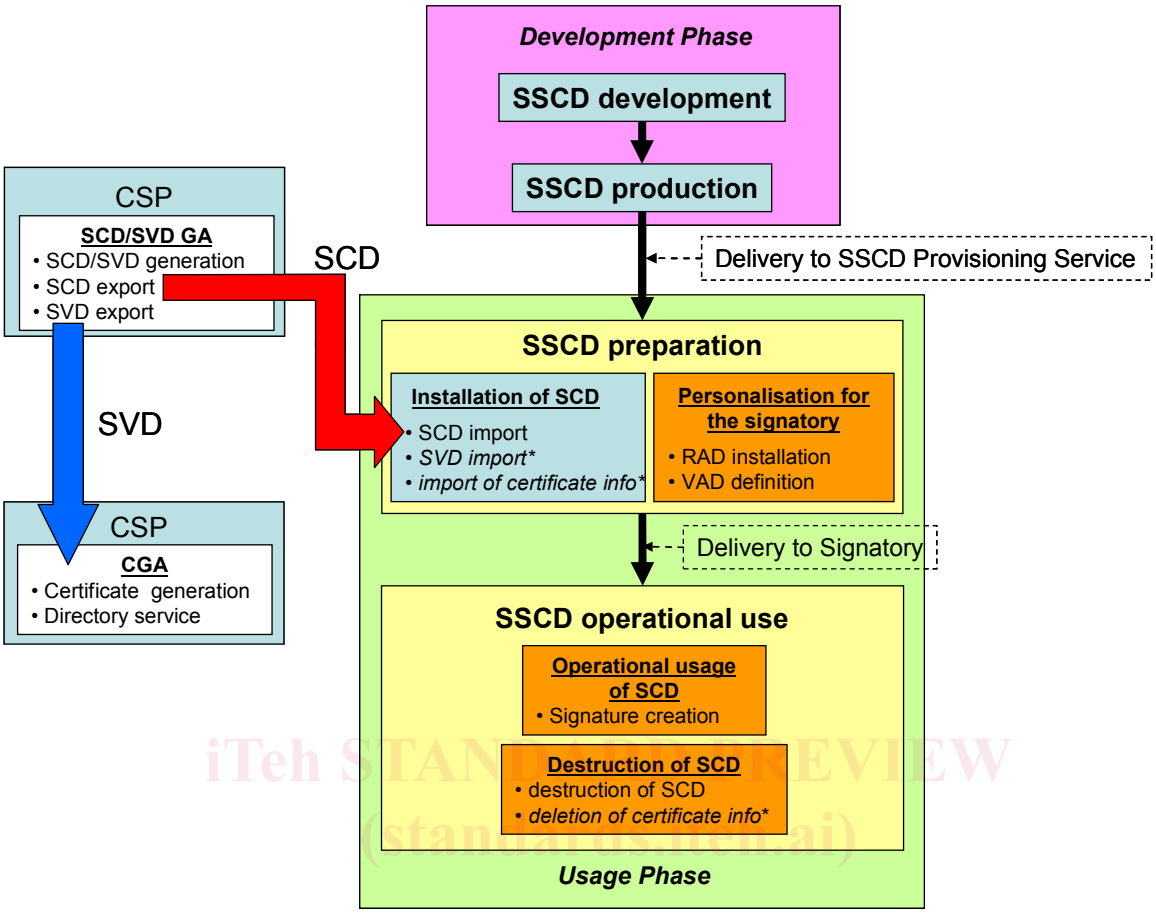

Figure 1 — Example of TOE life cycle[4]

The development phase comprises the development and production of the TOE (cf. CC part 1, para.139). The development phase is subject of the evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to the SSCD provision service.

The operational usage of the TOE comprises the preparation phase and the operation phase.

The Figure 1 shows example of the life cycle where an SCD or SCD/SVD pair is imported from SSCD Provisioning Service before delivery to the Signatory. The life cycle may allow import of SCD or SCD/SVD key pairs after delivery to the Signatory as well.

4.4.3.2 Preparation stage

The preparation phase of the TOE life cycle 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 provision service that prepares and provides the SSCD to subscribers. The preparation includes:

1) the personalization of TOE for use signatory i.e. the installation of the SRAD in the TOE and handover of SVAD to the signatory;

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

2) the initialization of the TOE i.e. the CSP generates the SCD/SVD pair by means of a SCD/SVD generation device (SCDGD, e.g. SSCD Type 1), loads the SCD to the TOE, and sends the SVD to the CGA. The TOE may import and store of 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 shall be identified as such;

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

The CGA generates a SCD / SVD pair and imports it into the SSCD. The CGA ensures the:

   a) the proof of correspondence between SCD and SVD;

   b) the algorithm and key size for the SVD are appropriate.

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 shall link the signature-verification data to the person (i.e. the signatory) and confirm 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 personalization. The environment shall 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).

The CSP will generate a (qualified) certificate only if the SCD is stored in a SSCD and if has verified the credentials presented by the signatory. An uninterrupted secured TOE delivery chain from the manufacturer through the SSCD delivery service to the signatory assures this property.

4.4.3.3 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 CGA 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 trustworthy SCA in secured environment only. The SCA shall protect the integrity of the DTBS 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.