SLOVENSKI STANDARD
SIST EN 419211-4:2014

01-marec-2014

Profil zaščite sredstva za varno elektronsko podpisovanje - 4. del: Podaljšek za sredstvo, ki generira ključ in zaupno komunicira prek aplikacije z generiranjem certifikatov

Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 4: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigem Kanal zur Zertifizierung von Generierungsanwendungen

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats

Ta slovenski standard je istoveten z: **EN 419211-4:2013**

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 419211-4:2014 **en,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-4

November 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 4: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Zertifikaterzeugungsanwendung

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

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

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

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

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

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

Ref. No. EN 419211-4:2013 E

Contents

Foreword

This document (EN 419211-4:2013) 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 May 2014 and conflicting national standards shall be withdrawn at the latest by May 2014.

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

This document supersedes CWA 14169:2004.

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

— *Part 1: Overview*

— *Part 2: Device with key generation*

— *Part 3: Device with key import*

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

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

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

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

Introduction

This series of European Standards specifies Common Criteria protection profiles for secure signature creation devices and is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) as update of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14169:2004, Annex B and Annex C on the protection profile secure signature creation devices, “EAL 4+”.

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

1 Scope

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

2 Normative references

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

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

3 Conventions and terminology

3.1 Conventions

This document is drafted in accordance with the CEN/CENELEC Internal Regulations Part 3 and content and structure of this document follow the rules and conventions laid out in Common Criteria 3.1.

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

3.2 Terms and definitions

For the purposes of this document, the acronyms, terms and definitions given in prEN 419211-1:2011 apply.

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application
Version:	1.0.1
Author:	CEN/TC 224 (WG17)
Publication date:	2013-11-27
Registration:	BSI-CC-PP-0071
CC version:	3.1 Revision 4
Editor:	Arnold Abromeit, TÜV Informationstechnik GmbH
General status:	final
Keywords:	secure signature creation device, electronic signature, digital signature, key generation, trusted communication with certificate generation application

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

4.2 PP overview

This Protection Profile is established by CEN as a European Standard for products to create electronic signatures. It fulfils requirements of Directive[2] 1999/93/EC of the European parliament and of the council of 13 December 1999 on *a community framework for electronic signatures*.

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

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

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

This Protection Profile about secure signature creation device with key generation and trusted communication with certificate generation application (PP SSCD KG TCCGA) defines the security requirements for SSCD generating signature creation data (SCD) and creating advanced electronic signatures, which if based on valid qualified certificates are qualified electronic signatures, as described in the core PP SSCD KG [6]. Additionally the TOE of this PP supports its authentication as SSCD by the certificate generation application (CGA) of the Certification service provider (CSP) and a trusted communication with this CGA for protection of signature verification data (SVD) generated and exported by the TOE and imported by CGA. These security features allow a changed lifecycle of the TOE. This PP conforms to the core PP SSCD KG [6]. The implication of this conformance claim is explained in 0 hereinafter.

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

4.3 TOE overview

4.3.1 Operation of the TOE

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

— The preparation environment, where it interacts with a certification service provider through a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the signature creation data (SCD) the TOE has generated. The TOE exports the SVD through a trusted channel allowing the CGA to check the authenticity of the SVD. 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 or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting electronic signature[3].

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

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

- The 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 4 in prEN 419211-1:2011 illustrates the operational environment.

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case the TOE provides a function to identify each SCD and the signature creation application (SCA) can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The electronic signature created with the TOE is a *qualified electronic signature* as defined in **the Directive** if the certificate for the SVD is a qualified certificate (Annex I). Determining the state of the certificate as qualified is beyond the scope of this standard.

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

The TOE 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:

- initializing the RAD;
- generating a key pair;
- storing personal information of the legitimate user.

The TOE and the CGA communicate through a trusted channel in order to protect the integrity and authenticity of the SVD exported from the TOE.

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

4.3.2 Target of evaluation

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

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

The TOE provides the following functions:

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

b) to export the SVD for certification through a trusted channel to the CGA;

c) to prove the identity as SSCD to external entities;

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

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

f) 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 electronic signature creation to also conform to the specifications in ETSI/TS 101 733 (CAdES) [7], ETSI/TS 101 903 (XAdES) [8] and ETSI/TS 101 903 (PAdES) [9].

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

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

h) 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.

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

The TOE lifecycle is the same as defined in the PP SSCD KG [6], 4.3.3, except the following:

- In the preparation stage of the usage phase, the SSCD-provisioning provider additionally initialises the security functions in the TOE for the identification as SSCD, for the proof of this SSCD identity to external entities, and for the protected export of the SVD.

- In the preparation stage of the usage phase, the SSCD-provisioning provider additionally links the identity of the TOE as SSCD and the identity of the legitimate user as potential applicant for certificates for SVD generated by the TOE.

- In the usage phase, SCD/SVD generation by the TOE and SVD export from the TOE may take place in the preparation stage and/or in the operational use stage. The TOE then provides a trusted channel to the CGA protecting the integrity of the SVD.

- In the usage phase, before generating the certificate including the SVD exported from the TOE, the CGA additionally establishes (1) the identity of the TOE as SSCD, (2) that the originating SSCD has been personalized for the applicant for the certificate as legitimate user, and (3) the correspondence between SCD stored in the SSCD and the received SVD.

5 Conformance claims

5.1 CC conformance claim

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

This PP is conforming to Common Criteria Part 2 [3] extended.

This PP is conforming to Common Criteria Part 3 [4].

5.2 PP claim, Package claim

This PP is strictly conforming to the core PP SSCD KG [6] version 2.0.1 as dated of 2012-01-23.

This PP is conforming to assurance package EAL4 augmented with AVA_VAN.5 defined in CC part 3 [4].

5.3 Conformance rationale

This PP SSCD KG TCCGA conforms to the core PP SSCD KG [6]. This implies for this PP:

a) The TOE type of this PP SSCD KG TCCGA is the same as the TOE type of the core PP SSCD KG: the TOE is a combination of hardware and software configured to securely create, use and manage signature creation data.

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

c) The security objectives for the TOE in this PP SSCD KG TCCGA include all the security objectives for the TOE of the core PP SSCD KG and add the security objective OT.TOE_SSCD_Auth (Authentication proof as SSCD) and OT.TOE_TC_SVD_Exp (Trusted channel for SVD).

d) The security objectives for the operational environment in this PP SSCD KG TCCGA include all security objectives for the operational environment of the core PP SSCD KG except OE.SSCD_Prov_Service. This PP substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service and adds OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp in order to address the extended security functionality of the TOE and methods of use (cf. section 0 for details).

e) The SFRs specified in this PP SSCD KG TCCGA includes all security functional requirements (SFRs) specified in the core PP SSCD KG. This PP includes additional SFRs FIA_API.1, FDP_DAU.2/SVD and FTP_ITC.1/SVD.

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