SLOVENSKI STANDARD
SIST EN 419211-1:2014

01-december-2014

Profil zaščite sredstva za varno elektronsko podpisovanje - 1. del: Pregled

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

Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 1: Überblick

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: EN 419211-1:2014

SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

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 419211-1:2014 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN 419211-1:2014

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

SIST EN 419211-1:2014

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-1

October 2014

ICS 35.240.15

Supersedes CWA 14169:2004

English Version

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

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

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 1: Überblick

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

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

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

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

SIST EN 419211-1:2014

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3fb9fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

SIST EN 419211-1:2014

Foreword

This document (EN 419211-1:2014) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2015 and conflicting national standards shall be withdrawn at the latest by April 2015.

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

This document supersedes CWA 14169:2004.

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

SIST EN 419211-1:2014

Introduction

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

This series of European Standards consists of the following parts:

— *Part 1: Overview*

— *Part 2: Device with key generation*

— *Part 3: Device with key import*

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

SIST EN 419211-1:2014

1 Scope

This European Standard:

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

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

— describes the targets of evaluation for these protection profiles.

2 Normative references

Not applicable.

3 Terminology

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

3.1 Legislative references

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

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

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

3.2 Technical terms

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

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

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

— is uniquely linked to the signatory;

— is capable of identifying the signatory;

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

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

SIST EN 419211-1:2014

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

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

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

Note 1 to entry: Certificate info may include:

— a signer's public key certificate, or

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

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

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

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

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

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

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

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

— the DTBS.

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

SIST EN 419211-1:2014

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

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

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

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/5f89fedc-f05e-48a4-a524-d04fab09bc06/sist-en-419211-1-2014

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

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

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

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

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

SIST EN 419211-1:2014

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

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

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

4 Abbreviated terms

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-d04fab09bc06/sist-en-419211-1-2014

5 Protection Profile Overview

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

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

SIST EN 419211-1:2014

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

These protection profiles formally specify the security functional and assurance requirements defined in Annex III of **the Directive** for a secure signature creation device (SSCD). This secure signature creation device is the target of evaluation (TOE) for the protection profiles.

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

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419211-1:2014
https://standards.iteh.ai/catalog/standards/sist/3f69fcdd-50be-46a4-a554-a04fab09bc06/sist-en-419211-1-2014

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

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

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

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

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

6 Target of Evaluation

6.1 General

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