SLOVENSKI STANDARD
oSIST prEN 419111-1:2013

01-april-2013

Zaščitni profili za uporabo pri oblikovanju in preverjanju podpisov - 1. del: Predstavitev

Protection profiles for signature creation and verification application - Part 1: Introduction

Schutzprofile für eine Anwendung zum Erzeugen und Prüfen von Signaturen - Teil 1: Einführung in die europäische Norm

Profils de protection pour application de création et de vérification de signature - Partie 1 : Introduction

Ta slovenski standard je istoveten z: **prEN 419111-1**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

oSIST prEN 419111-1:2013 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 419111-1

February 2013

ICS 35.240.15

Will supersede CWA 14170:2004

English Version

Protection profiles for signature creation and verification application - Part 1: Introduction

Profils de protection pour application de création et de vérification de signature - Partie 1 : Introduction

Schutzprofile für eine Anwendung zum Erzeugen und Prüfen von Signaturen - Teil 1: Einführung in die europäische Norm

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-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.

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

Contents

Page

Figures

Foreword

This document (prEN 419111-1:2013) 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 document is currently submitted to the CEN Enquiry.

This document, together with prEN 41911-2:2013 and prEN 419111-3:2013, will supersede CWA 14170:2004.

EN 419111 consists of the following parts under the general title "*Protection profiles for signature creation and verification application*":

— *Part 1: Introduction.*
This part is an introduction to EN 419111;

— *Part 2: Signature creation application – Core PP.*
This part is a PP for the SCA, specifying only the core security functions;

— *Part 3: Signature creation application – Possible extensions.*
This part specifies possible additional security functions that can be added to the core SCA PP;

— *Part 4: Signature verification application – Core PP.*
This part is a PP for the SVA, specifying only the core security functions;

— *Part 5: Signature verification application – Possible extensions.*
This part specifies possible additional security functions that can be added to the core SVA PP.

1 Scope

This document is an introduction to EN 419111, the European Standard that contains Protection Profiles defining the security requirements for Signature Creation and Signature Verification applications.

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 419111-2:2013, *Protection profiles for signature creation and verification application – Part 2: Signature creation application – Core PP*

prEN 419111-3:2013, *Protection profiles for signature creation and verification application – Part 3: Signature creation application – Possible extensions*

prEN 419111-4:2013, *Protection profiles for signature creation and verification application – Part 4: Signature verification application – Core PP*

prEN 419111-5:2013, *Protection profiles for signature creation and verification application – Part 5: Signature verification application – Possible extensions*

[NR1] *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model – July 2009 – Version 3.1 Rev. 3 CCMB-2009-07-001*

[NR2] *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components – July 2009 – Version 3.1 Rev. 3 CCMB-2009-07-002*

[NR3] *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components – July 2009 – Version 3.1 Rev. 3 CCMB-2009-07-003*

[NR4] *Common Criteria for Information Technology Security Evaluation – Evaluation methodology – July 2009 – Version 3.1 Rev. 3 CCMB-2009-07-004*

3 Terms and definitions

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

3.1
advanced electronic signature
electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control; and

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

[SOURCE: Directive 1999/93/EC, Article 2, Definition 2 [1]]

Note 1 to entry: Within the context of this document, Signature is used to denote an Advanced Electronic Signature.

3.2
Attribute Authority
AA
authority that assigns privileges by issuing attributes certificates

3.3
Card Acceptance Device
CAD
card reader where the SSCD is plugged

3.4
card holder
legitimate holder of the SSCD

3.5
certificate
electronic attestation, which links the SVD to a person and confirms the identity of that person

[SOURCE: Directive 1999/93/EC, Article 2, Definition 9 [1]]

3.6
certificate revocation list
CRL
time stamped list identifying revoked certificates which is signed by a CA or CRL issuer and made freely available in a public repository

3.7
certification path
ordered set of certificates, certifying one another, starting from a root certificate that the TOE trusts, and ending with the signing certificate

3.8
certification service provider
CSP
entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

Note 1 to entry: See also 5.6.3.2.

3.9
digital signature
result of the cryptographic signature of the DTBSR, computed by the SSCD

3.10
driving application
DA
application that calls the SCA (resp. the SVA) in order to validate electronic signatures

Note 1 to entry: The SCA (resp. the SVA) returns the SDO (resp. the validation result) to the DA.

[SOURCE: ETSI TS 102 853 V1.1.1, modified [15]]

Note 2 to entry: In case of SVA, see ETSI TS 102 853 V1.1.1 [15].

3.11
electronic signature
data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

[SOURCE: Directive 1999/93/EC, Article 2, Definition 1 [1]]

3.12
interface device
ID
device that connects the SSCD to the SCP

3.13
local signature policy rules
local rules
set of rules as represented within the signature creation or verification application, under which the signature can be determined to be technically valid. These may be derived from an agreed signature policy established outside the scope of this EN.

Note 1 to entry: These rules are called validation constraints in ETSI TS 102 853 V1.1.1 [15].

3.14
protection profile
PP
implementation-independent statement of security needs for a TOE

[SOURCE: [NR1], Clause 4]

3.15
qualified certificate
certificate which meets the requirements laid down in Directive 1999/93/EC, Annex I, and is provided by a certification-service-provider who fulfils the requirements laid down in Directive 1999/93/EC, Annex II

[SOURCE: Directive 1999/93/EC, Article 2, Definition 10, modified [1]]

3.16
qualified electronic signature
QES
advanced electronic signature based on a qualified certificate and containing a digital signature computed by an SSCD

3.17
reference authentication data
RAD
This data is stored inside the SSCD. It is used as a reference to which the VAD will be compared to. This RAD can be biometrics data, a PIN, or a symmetric key. It can also be a combination of these factors. In some applications, the RAD can be transferred through the TOE.

3.18
secure signature creation device
SSCD
signature-creation device which meets the requirements laid down in Directive 1999/93/EC, Annex III

[SOURCE: Directive 1999/93/EC, Article 2, Definition 6, modified [1]]

3.19
signature attribute
signed or unsigned additional information that is associated with a signature

Note 1 to entry: A signature attribute can also be referred to as a signature property (see ETSI TS 102 853 V1.1.1 [15]).

3.20
signature policy
SP

3.20.1
formal signature policy
set of rules agreed or issued by a trusted authority for the creation and validation of an electronic signature, under which the signature can be determined to be valid

Note 1 to entry: A given legal/contractual context may recognise a particular signature policy as meeting its requirements. The signature policy may be explicitly identified or may be implied by the semantics of the data being signed and other external data like a contract being referenced which itself refers to a signature policy. Examples of formal signature policies are given in ETSI TR 102 038 V1.1.1 [10] and ETSI TR 102 272 V1.1.1 [11].

3.20.2
local signature policy
set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid in a particular transactions context

Note 1 to entry: In the rest of this document, SP always refers to the local signature policy.

3.21
signature creation application
SCA

application that creates an electronic signature, using the digital signature produced by an SSCD connected to the SCA

3.22
signature creation device
configured software or hardware used to implement the signature-creation data

[SOURCE: Directive 1999/93/EC, Article 2, Definition 5 [1]]

3.23
signature creation platform
SCP
set of hardware and software that contains and supports the SCA

3.24
signature creation system
SCS
overall system, consisting of the SCA and the SSCD, which creates an electronic signature

3.25
signed data object(s)
SDO
document(s) or parts of the document(s) for which an electronic signature has been generated, along with the electronic signature

3.26
signature type
specific format for encoding an advanced electronic signature including its attributes

3.27
signature validation
process of checking that a signature is valid including overall checks of the signature against local or shared signature policy requirements as well as certificate validation and signature verification

3.28
signature verification
process of checking the cryptographic value of a signature using signature verification data

3.29
time mark
information in an audit record from a trusted service provider that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

3.30
time stamp token
data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

3.31
time stamping authority
TSA
trusted third party that creates time-stamp tokens in order to indicate that a datum existed at a particular point in time

3.32
trusted service provider
TSP
entity that helps to build trust relationships by making available or providing some information upon request

3.33
user
current user of the TOE

Note 1 to entry: The user can be the issuer or the card holder.

3.34
validation data
additional data, collected by the signer and/or a verifier, needed to verify the electronic signature, and which may include certificates, revocation status information, time-stamps or time-marks

3.35
verification authentication data
VAD
This data is may be transferred to the SSCD. It will be compared to the RAD.

3.36
verification time
chosen time either present or in past that the verifier wants to check if the signing certificate was valid at this time

3.37
verifier
entity that validates or verifies an electronic signature, and that may be either a relying party or a third party, e.g. an arbitrator, interested in the validity of an electronic signature

4 Symbols and abbreviations

For the purposes of this document, the following symbols and abbreviations apply.

AA	Attribute Authority
AdES	Advanced Electronic Signature
BES	Basic Electronic Signature
CA	Certificate Authority
CAD	Card Acceptance Device
CB	Certification Body
CC	Common Criteria
CRL	Certificate Revocation List
CSP	Certificate Service Provider
DA	Driving Application
DHC	Data Hashing Component
DTBS	Data To Be Signed
DTBSR	Data To Be Signed Representation
DTBSR_DS	Data To Be Signed Representation Digital Signature
EPES	Explicit Policy-based Electronic Signature
ID	Interface Device
OCSP	Online Certificate Status Protocol
PC	Personal Computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
QES	Qualified Electronic Signature
RAD	Reference Authentication Data
SCA	Signature Creation Application
SCD	Signature Creation Data
SCP	Signature Creation Platform
SCS	Signature Creation System
SD	Signer's Document
SDO	Signed Data Object
SP	Signature Policy
SSCD	Secure Signature Creation Device
ST	Security Target
SVA	Signature Verification Application
SVD	Signature Verification Data
TOE	Target of Evaluation
TSA	Time Stamping Authority
TSP	Trusted Service Provider
VAD	Verification Authentication Data