SLOVENSKI STANDARD
oSIST prEN 419111-4:2013

01-april-2013

Zaščitni profili za uporabo pri oblikovanju in preverjanju podpisov - Aplikacija preverjanja podpisa - 4. del: Jedrni PP

Protection profiles for signature creation and verification application - Signature verification application - Part 4: Core PP

Schutzprofile zur Signatur Kreation Anwendung - Signatur Verifikation Anwendung - Teil 4: Core PP

Profils de protection pour application de création et de vérification de signature - Application de vérification de signature - Partie 4: Profils PP de base

Ta slovenski standard je istoveten z: **prEN 419111-4**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

oSIST prEN 419111-4:2013 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 419111-4

February 2013

ICS 35.240.15

Will supersede CWA 14171:2004

English Version

Protection profiles for signature creation and verification application - Signature verification application - Part 4: Core PP

Profils de protection pour application de création et de vérification de signature - Application de vérification de signature - Partie 4: Profils PP de base

Schutzprofile zur Signatur Kreation Anwendung - Signatur Verifikation Anwendung - Teil 4: Core PP

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

Tables

Foreword

This document (prEN 419111-4:2013) 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 document is currently submitted to the CEN Enquiry.

This document, together with prEN 419111-5:2013, will supersede CWA 14171:2004.

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 a Protection Profile that defines the security requirements for a Signature Verification Application.

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 419111-1:2013, *Protection profiles for signature creation and verification application – Part 1: Introduction*

[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 terms and definitions given in prEN 419111-1:2013 apply.

4 Symbols and abbreviations

For the purposes of this document, the symbols and abbreviations given in prEN 419111-1:2013 apply.

5 TOE overview

5.1 TOE Type

This PP aims at defining security requirements that an SVA shall conform to in the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to software, running on an operating system and hardware, the SCP. The TOE, using services provided by the SCP enables the verifier to verify an electronic signature.

This TOE is the minimum configuration for an SVA. Many features that belong to the environment in this TOE could be added inside the TOE as suggested in prEN 419111-1:2013.

5.2 TOE Usage

The TOE enables to verify electronic signatures.

Verifying an electronic signature means checking an SDO and the corresponding document in order to determine if the signature is

1) valid,

2) invalid,

3) indeterminate: the SVA is unable to issue a valid or invalid status.

5.3 TOE Environment

5.3.1 Overview

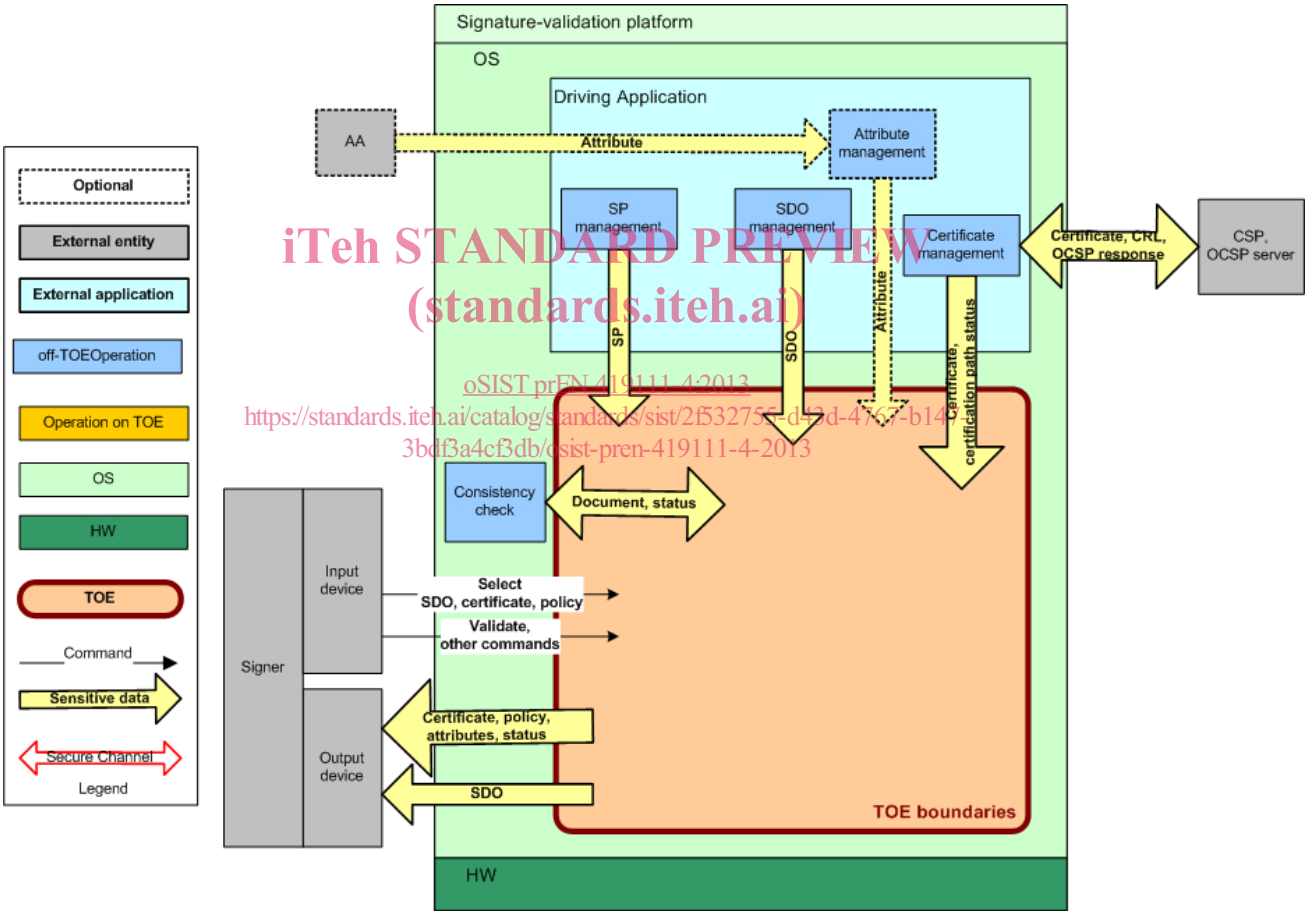

Figure 1 — Core SVA environment

Figure 1 — Core SVA environment is an illustration of what the environment of the SVA looks like. Its is provided as a help to understand this environment. It is not a mandated configuration.

5.3.2 External entities

The following entities are external entities of the TOE. They are connected to the TOE.

— driving application

— OS

— input device

— output device

A brief description of these external entities is given in prEN 419111-1:2013, 6.6.2.

5.3.3 Other Entities

The following entities are not directly external entities of the TOE, because they are not connected to the TOE, but to external entities of the TOE.

— CSP

— Attribute Authority

A brief description of these entities is given in prEN 419111-1:2013, 6.6.3.

5.4 TOE operations

5.4.1 Introduction

This section describes operations that are performed in the TOE or in its environment.

5.4.2 Pre-validation operations

These operations include:

— SDO (& SD) Selection and import

— Invoking SD checker

— Certificate Selection and import

— Signature policy selection and import

They are described in prEN 419111-1:2013, 6.7.2.2.

5.4.3 Validation operations

These operations include

— Extraction of data items from SDO (see prEN 419111-1:2013, 6.7.2.3),

— Certification path validation, (see prEN 419111-1:2013, 6.7.2.4),

— Cryptographic signature verification, (see prEN 419111-1:2013, 6.7.2.5),

— Verify other validation constraints, (see prEN 419111-1:2013, 6.7.2.6),

— Add Time stamp attribute, (see prEN 419111-1:2013, 6.7.2.7).

5.5 TOE-environment operations

These operations include:

— Checker

— Certificate management

— Signature Policy management

They are described in prEN 419111-1:2013, 6.7.3.

TOE-environment operations also include:

- Get information/commands from input device
- Send SD / attributes to output device

They are described in prEN 419111-1:2013, 6.7.4.

6 Conformance claims

6.1 CC Conformance Claim

This Protection Profile (PP) is CC Part 2 extended and CC Part 3 conformant and written according to the Common Criteria version 3.1R3 ([NR1], [NR2], [NR3], and [NR4]).

6.2 PP Claim

This PP does not claim conformance to any other Protection Profile

6.3 Package Claim

The evaluation assurance level for this PP is EAL4 augmented with the assurance component ALC_FLR.1.

CEN/TC 224 note: Different countries currently use different levels of EAL. So national bodies are requested to explicitly comment on this choice.

6.4 Conformance Rationale

Since this PP is not claiming conformance to any other protection profile, no rationale is necessary here.

6.5 Conformance Statement

The conformance required by this PP is the demonstrable-PP conformance. This will facilitate conformance claim to both this PP and other PP for Security Target (ST) authors.

7 Security problem definition

7.1 Assets

7.1.1 Validation status

The validation status, and its determination according to the SP selected by the verifier is the main asset of this PP.

The validation status and the process to determine it shall be protected in integrity.

7.1.2 Document

The document whose signature is to be verified is one asset that has to be protected in integrity. It is present in the TOE under the following forms:

— **SDO** Signed Data Object

— **SD** Signer's Document

— **DTBSR** Data To Be Signed Representation

— **DTBSR_DS** DTBSR Digital Signature

7.1.3 Signing certificate

The signing certificate needs to be protected in integrity. This can be achieved using the signature that it contains.

7.1.4 Root certificate

The root certificate is a certificate trusted by the SVA. It contains the root public key for the validation of the certification chain.

There may be more than one root certificate.

It shall be protected in integrity.

7.1.5 Certification path

The certification path is the set of certificates or certificate identifiers, signing one another, starting from a root certificate and ending with the signing certificate.

It needs to be protected in integrity.

7.1.6 Signature policy

The signature policy needs to be protected in integrity.

7.1.7 Signature attribute

The signature attributes need to be protected in integrity.

7.2 Threats

7.2.1 T.Document

Any data originally intended by the End-User to be verified are modified by an attacker after they are under TOE control. This manipulation can be done on the document under different forms: SDO, SD, DTBS, DTBSR.

7.2.2 T.SignaturePolicy

The Signature Policy can be modified by an attacker, e.g. by removing or modifying a signature attribute.

The verifier can mistakenly select a security policy after being fooled by an attacker.

7.2.3 T.Certificate

The Certificate can be modified by an attacker.

The signing certificate may have been provided by an untrusted provider..

7.2.4 T.RootCertificate

The root certificate can be modified by an attacker.

The root certificate may become obsolete.

All the above threats can lead to wrong the validation data.

7.3 Organisational security policies

OSP.Crypto

The cryptographic algorithms used on the TOE shall conform to the rules established by the relevant certification body.

7.4 Assumptions

7.4.1 A.Platform

The TOE is installed on a personal computer located in an admission restricted area ensuring that those resources the TOE is relying on cannot be manipulated without user notification.

It is assumed that the host platform on which the TOE is installed is either directly under the responsibility of the verifier or under the control of the organisation to which the verifier belongs or of which he is the customer.

The operation system of the host platform is supposed to provide low-level communication interface to the following external interfaces:

— Input device

— Output device.

The operation system of the host platform is supposed to provide separate execution contexts for the various processes executed.