



SLOVENSKI STANDARD
oSIST prEN 419111-5:2013
01-april-2013

Zaščitni profili za uporabo pri oblikovanju in preverjanju podpisov - Aplikacija preverjanja podpisa - 5. del: Mogoče razširitve

Protection profiles for signature creation and verification application - Signature verification application - Part 5: Possible extensions

Schutzprofile für eine Anwendung zum Erzeugen und Prüfen von Signaturen - Signatur Verifikation Anwendung - Teil 5: Mögliche Extensionen

Profils de protection pour application de création et de vérification de signature - Application de vérification de signature - Partie 5: Extensions possibles

<https://standards.iteh.ai/catalog/standards/sist/00c12ef9-504e-4703-bd27-fac6162a8a3c/osist-pren-419111-5-2013>

Ta slovenski standard je istoveten z: prEN 419111-5

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices
-----------	---	--

oSIST prEN 419111-5:2013

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[oSIST prEN 419111-5:2013](#)

<https://standards.iteh.ai/catalog/standards/sist/00c12e9-504e-4703-bd27-fac6162a8a3c/osist-pren-419111-5-2013>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 419111-5

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 5: Possible extensions

Profils de protection pour application de création et de
vérification de signature - Application de vérification de
signature - Partie 5: Extensions possibles

Schutzprofile für eine Anwendung zum Erzeugen und
Prüfen von Signaturen - Signatur Verifikation Anwendung -
Teil 5: Mögliche Extensionen

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

Foreword.....	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Symbols and abbreviations	6
5 Extended component definition	6
5.1 Definition of the Family FDP_SVR	6
6 Checker package	8
6.1 Scope	8
6.1.1 Introduction	8
6.2 Conformance	8
6.2.1 CC Conformance Claim.....	8
6.2.2 EAL Claim	8
6.3 Security problem definition	8
6.3.1 Assets	8
6.3.2 Threats	8
6.3.3 Organisational security policies	9
6.3.4 Assumptions	9
6.4 Security objectives	9
6.4.1 Security objectives for the TOE	9
6.4.2 Security objectives for the operational environment.....	9
6.4.3 Rationale for Security objectives	9
6.5 Security requirements.....	9
6.5.1 Introduction	9
6.5.2 Security functional requirements.....	9
6.5.3 SFR / Security objectives.....	11
6.5.4 SFR Dependencies	12
7 Time stamp attribute package	14
7.1 Scope	14
7.1.1 Introduction	14
7.1.2 TS attribute computation	14
7.1.3 TS attribute verification.....	14
7.2 Conformance	15
7.2.1 CC Conformance Claim.....	15
7.2.2 EAL Claim	15
7.3 Security problem definition	15
7.3.1 Assets	15
7.3.2 Threats	15
7.3.3 Organisational security policies	15
7.3.4 Assumptions	15
7.4 Security objectives	15
7.4.1 Security objectives for the TOE	15
7.4.2 Security objectives for the operational environment.....	15
7.4.3 Rationale for Security objectives	15
7.5 Security requirements.....	16
7.5.1 Introduction	16
7.5.2 Security functional requirements.....	16
7.5.3 SFR / Security objectives.....	18

7.5.4	SFR Dependencies	18
8	Complete validation data attribute package	18
8.1	Scope	18
8.1.1	Introduction.....	18
8.1.2	Complete validation attribute computation	19
8.1.3	Complete validation attribute verification.....	19
8.2	Conformance	19
8.2.1	CC Conformance Claim	19
8.2.2	EAL Claim.....	19
8.3	Security problem definition.....	19
8.3.1	Assets	19
8.3.2	Threats.....	20
8.3.3	Organisational security policies	20
8.3.4	Assumptions.....	20
8.4	Security objectives.....	20
8.4.1	Security objectives for the TOE	20
8.4.2	Security objectives for the operational environment	20
8.4.3	Rationale for Security objectives.....	20
8.5	Security requirements.....	20
8.5.1	Introduction.....	20
8.5.2	Security functional requirements	21
8.5.3	SFR / Security objectives.....	23
8.5.4	SFR Dependencies	23
9	Explicit Policy-based ES package	23
9.1	Scope	23
9.1.1	Introduction.....	23
Bibliography	24
Index	26

[oSIST prEN 419111-5:2013](https://standards.iteh.ai/catalog/standards/sist/00c12e9-504e-4703-bd27-fac6162a8a3c/osist-pren-419111-5-2013)
<https://standards.iteh.ai/catalog/standards/sist/00c12e9-504e-4703-bd27-fac6162a8a3c/osist-pren-419111-5-2013>

Figures

Figure 1 — FDP_SVR component levelling	7
Figure 2 — Time stamp attribute TOE environment	14
Figure 3 — Complete validation data attribute TOE environment.....	19

prEN 416111-5:2013 (E)

Tables

Table 1 — Checker SFP – subjects, objects and attributes	9
Table 2 — Checker operation rules.....	10
Table 3 — security objective rationale - with Checker.....	11
Table 4 — SFR Dependencies	12
Table 5 — Time stamp - security objective rationale	15
Table 6 — Time stamp - object security attributes.....	16
Table 7 — Time stamp - attributes conditions and modifications	16
Table 8 — Time stamp - SFR/objectives rationale.....	18
Table 9 — Time stamp - SFR dependencies rationale	18
Table 10 — Complete validation data - security objective rationale	20
Table 11 — Complete validation data - object security attributes.....	20
Table 12.....	21
Table 13 — Complete validation data - attributes conditions and modifications	21
Table 14 — Complete Validation Data - SFR/objectives rationale	23
Table 15 — Complete Validation Data - SFR dependencies rationale.....	23

iTeh STANDARD PREVIEW
(standards.iteh.ai)

oSIST prEN 419111-5:2013
<https://standards.iteh.ai/catalog/standards/sist/00c12cd-504e-4703-bd27-fac6162a8a3c/osist-pren-419111-5-2013>

Foreword

This document (prEN 416111-5:2013) 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 419111-4:2013, 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.

prEN 416111-5:2013 (E)**1 Scope**

This document contains a set of packages. These packages describe security functions that may be added to the core SVA PP prEN 419111-4:2013 [4]. The following packages are available:

- Checker package
- Certificate management package
- Explicit SP management package

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 Extended component definition**5.1 Definition of the Family FDP_SVR**

In order to define the IT-security requirements of the TOE completely, an additional functional family (FDP_SVR) of class FDP (user data protection) is defined. This family describes the functional requirements for a secure viewer component of a signature application component.

Due to the complexity of a legal binding viewer component as required by the signature law this component could not be modelled from the components that are provided by the Common Criteria framework. Therefore the introduction of a separate functional family is necessary that covers the requirements to describe the TOE consistently as needed for a confirmation that is based on the results of the Common Criteria evaluation.

FDP_SVR Secure Viewer

Family behaviour

This family defines the functional requirements to a secure viewer component for electronic signature applications. Electronic signature applications require a viewer component, which ensures, that the displayed data is unambiguous. The user shall be informed about content, that may not be displayed but the electronic signature will refer to.

Component levelling



Figure 1 — FDP_SVR component levelling

FDP_SVR.1 Secure Viewer requires the TSF to display the documents content in an unambiguous way, which is free of hidden content. In addition, the ability to inform the user about hidden content is required.

FDP_SVR.2 Secure Viewer requires the TSF to display the results of the signature verification according to the signature policy.

Management: FDP_SVR.1, FDP_SVR.2

For this component no management activities are foreseen.

Audit: FDP_SVR.1, FDP_SVR.2

No actions are identified, that should be logged, if FAU_GEN is part of the PP/ST.

FDP_SVR.1 Secure viewer of data content

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SVR.1.1 The TSF shall ensure, that the displayed content of a document is unambiguous according to [assignment: *norms for displaying content*].

FDP_SVR.1.2 The TSF shall ensure that the displayed content of a document is free of active or hidden content. The TSF shall ensure that the user is informed about hidden or active content.

FDP_SVR.1.3 The TSF shall ensure, that the user is informed about content that cannot be displayed.

prEN 416111-5:2013 (E)**FDP_SVR.2 Secure viewer of signature verification results**

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SVR.2.1 The TSF shall ensure, that the displayed results of signature verification is unambiguous according to [assignment: *signature policy*].

FDP_SVR.2.2 The TSF shall inform the user about [assignment: *list of verification results*].

The assurance requirements that have been defined by the Common Criteria v3.1 Part 3 [NR3] are applicable to the functional family FDP_SVR. This functional family has been defined to meet the requirements of a secure viewer component in a signature application component.

Because this component is a software component with a well defined behaviour on its external interfaces, the assurance requirements that have been defined in Part 3 of Common Criteria [NR3] are applicable to this functional family.

Through its nature as a software component the assurance classes ACM, ADO, ADV, AGD, ALC, ATE and AVA are applicable in the evaluation process. It is not required to define a new assurance class or assurance family for a consistent and complete description to cover this SFR. This SFR does not define any behaviour that might require an extension of Part 3 of the Common Criteria Evaluation Framework [NR3].

iTeh STANDARD PREVIEW (standards.iteh.ai)

6 Checker package**6.1 Scope**

[oSIST prEN 419111-5:2013](https://standards.iteh.ai/catalog/standards/sist/00c12e9-504e-4703-bd27-fac6162a8a3c/osist-pren-419111-5-2013)

6.1.1 Introduction

<https://standards.iteh.ai/catalog/standards/sist/00c12e9-504e-4703-bd27-fac6162a8a3c/osist-pren-419111-5-2013>

This package includes the checker in the TOE. In the core PP, the checker is in the environment.

6.2 Conformance**6.2.1 CC Conformance Claim**

This package 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]).

6.2.2 EAL Claim

The evaluation assurance level for this package is EAL4 augmented with the assurance components ALC_FLR.1.

6.3 Security problem definition**6.3.1 Assets**

No additional asset

6.3.2 Threats

No additional threat

6.3.3 Organisational security policies

No modification in OSP

6.3.4 Assumptions

No modification in assumptions

6.4 Security objectives

6.4.1 Security objectives for the TOE

OT.Checker

The TSF shall provide a module able to determine if the semantics of the document to be signed is conformant to the rules defined for the determined format.

6.4.2 Security objectives for the operational environment

OE.Checker removed from core

6.4.3 Rationale for Security objectives

The modification consists in replacing **OE.Checker** by **OT.Checker** in the header row.

6.5 Security requirements (standards.iteh.ai)

6.5.1 Introduction

oSIST prEN 419111-5:2013

<https://standards.iteh.ai/catalog/standards/sist/00c12e9-504e-4703-bd27->

6.5.1.1 Subjects Objects and security attributes

6.5.1.2 Operations

6.5.2 Security functional requirements

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Checker The TSF shall enforce the [**Checker SFP**] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

Table 1 — Checker SFP – subjects, objects and attributes

Subject/Object	Attributes
S.Verifier	AT.Authenticated
O.SDO	AT.Status, AT.CheckerStatus, AT.CheckerOptional, AT.Type