



SLOVENSKI STANDARD
oSIST prEN 419111-3:2013
01-april-2013

Zaščitni profili za uporabo pri oblikovanju in preverjanju podpisov - 3. del: Mogoče razširitve

Protection profiles for signature creation and verification application - Signature creation application - Part 3: Possible extensions

Schutzprofile für eine Anwendung zum Erzeugen und Prüfen von Signaturen - Signatur Kreation Anwendung - Teil 3: Mögliche Extentionen

Profils de protection pour la création et la vérification de signatures électroniques - Application de création de signature - Partie 3: Extensions possibles

[https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491-](https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491-aac07f6a90ce/osist-pr-en-419111-3-2013)

Ta slovenski standard je istoveten z: prEN 419111-3

ICS:

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

oSIST prEN 419111-3:2013

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[oSIST prEN 419111-3:2013](https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491-aac07f6a90ce/osist-pren-419111-3-2013)

<https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491-aac07f6a90ce/osist-pren-419111-3-2013>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 419111-3

February 2013

ICS 35.240.15

Will supersede CWA 14170:2004

English Version

Protection profiles for signature creation and verification application - Signature creation application - Part 3: Possible extensions

Profils de protection pour la création et la vérification de
signatures électroniques - Application de création de
signature - Partie 3: Extensions possibles

Schutzprofile für eine Anwendung zum Erzeugen und
Prüfen von Signaturen - Signatur Kreation Anwendung -
Teil 3: 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.....	4
1 Scope	5
2 Normative references	5
3 Terms and definitions	5
4 Symbols and abbreviations	5
5 Extended component definition	5
5.1 Definition of the Family FDP_SVR	5
6 Checker package	7
6.1 Conformance	7
6.1.1 CC Conformance Claim.....	7
6.1.2 EAL Claim	7
6.2 Security problem definition	7
6.2.1 Assets	7
6.2.2 Threats	7
6.2.3 Organisational security policies	7
6.2.4 Assumptions	7
6.3 Security objectives	8
6.3.1 Security objectives for the TOE	8
6.3.2 Security objectives for the operational environment.....	8
6.3.3 Rationale for Security objectives	8
6.4 Security requirements.....	8
6.4.1 Introduction	8
6.4.2 Security functional requirements.....	8
6.4.3 Security Functional Requirement rationale	10
6.4.4 Rationale for SFR Dependencies	13
7 Secure channel with SSCD package.....	14
7.1 Conformance.....	14
7.1.1 CC Conformance Claim.....	14
7.1.2 EAL Claim	14
7.2 Security problem definition	14
7.2.1 Assets	14
7.2.2 Threats	15
7.2.3 Organisational security policies	15
7.2.4 Assumptions	15
7.3 Security objectives	15
7.3.1 Security objectives for the TOE	15
7.3.2 Security objectives for the operational environment.....	15
7.3.3 Rationale for Security objectives	15
7.4 Security requirements.....	15
7.4.1 Introduction	15
7.4.2 Security functional requirements.....	15
7.4.3 Security Functional Requirement rationale	16
7.4.4 Rationale for SFR Dependencies	20
Bibliography	22
Index.....	24

Figures

Figure 1 — FDP_SVR component levelling	6
---	----------

Tables

Table 1 — Checker SFP – Objects and Operations.....	8
Table 2 — Checker SFP – subjects, objects and attributes	9
Table 3 — Checker operation rules	9
Table 4 — SFR vs Objectives on the TOE.....	10
Table 5 — SFR dependencies	13
Table 6 — SFR vs Objectives on the TOE.....	16
Table 7 — SFR dependencies	20

iTeh STANDARD PREVIEW (standards.iteh.ai)

[oSIST prEN 419111-3:2013](https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491-aac07f6a90ce/osist-pren-419111-3-2013)

<https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491-aac07f6a90ce/osist-pren-419111-3-2013>

Foreword

This document (prEN 419111-3:2013) 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 419111-1:2013 and prEN 419111-2:2013, 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 contains a set of packages. These packages describe security functions that may be added to the core SCA PP prEN 419111-2:2013 [2]. The following packages are available:

- Checker package
- Certificate management package
- Secure channel with SSCD 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.

prEN 419111-3:2013 (E)**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

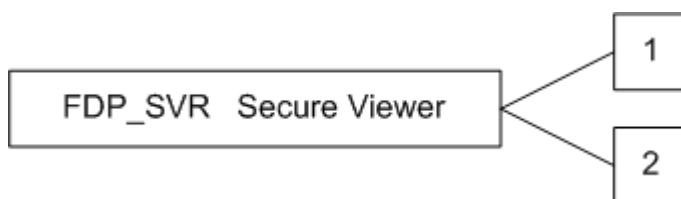


Figure 1 — FDP_SVR component levelling

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 document format*].

FDP_SVR.1.2 The TSF shall check 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 and its implications.

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

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].

6 Checker package

STANDARD PREVIEW
(standards.iteh.ai)

6.1 Conformance**6.1.1 CC Conformance Claim**

oSIST prEN 419111-3:2013

<https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491->

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]).

6.1.2 EAL Claim

The evaluation assurance level for this package is EAL3 augmented with the assurance components AVA_VAN.3.

6.2 Security problem definition**6.2.1 Assets**

No additional asset.

6.2.2 Threats

No additional threat.

6.2.3 Organisational security policies

No modification in OSP.

6.2.4 Assumptions

No modification in assumptions.

prEN 419111-3:2013 (E)

6.3 Security objectives

6.3.1 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.

6.3.2 Security objectives for the operational environment

OE.Checker removed from core

6.3.3 Rationale for Security objectives

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

6.4 Security requirements

6.4.1 Introduction

6.4.1.1 Subjects Objects and security attributes

6.4.1.2 Operations

iTeh STANDARD PREVIEW
(standards.iteh.ai)

6.4.2 Security functional requirements

FDP_SVR.1 is added to the Core SCA PP. [oSIST prEN 419111-3:2013](https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491-ae0710b0cc0e/osist-pr-en-419111-3-2013)

<https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491-ae0710b0cc0e/osist-pr-en-419111-3-2013>
FDP_IFC/Checker and FDP_IFF/Checker from the Core SCA PP are replaced by the following FDP_ACC/Checker and FDP_ACF/Checker.

FDP_ACC.1.1/Checker The TSF shall enforce the [**Checker SFP**] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

Table 1 — Checker SFP – Objects and Operations

Subject	Object	Operation
S.Signer	O.SDO	Check

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 2 — Checker SFP – subjects, objects and attributes

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

FDP_ACF.1.2/Checker The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

The following operations are allowed only when the rules are met:

Table 3 — Checker operation rules

Object	Operation	Conditions
O.SDO	Check	Type of document is supported by the Checker

FDP_ACF.1.3/Checker The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

iTeh STANDARD PREVIEW

FDP_ACF.1.4/Checker The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

oSIST prEN 419111-3:2013

<https://standards.iteh.ai/catalog/standards/sist/d67f8fc2-9fd2-4a49-b491->

FDP_SVR.1 **Secure viewer of data content** prEN-419111-3-2013

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 document format*].

FDP_SVR.1.2 The TSF shall check 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 and its implications.

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