

DIN EN 419111-1

ICS 35.240.15

Einsprüche bis 2013-05-25

Entwurf**Schutzprofile für eine Anwendung zum Erzeugen und Prüfen von Signaturen –****Teil 1: Einführung;****Englische Fassung prEN 419111-1:2013**

Protection profiles for signature creation and verification application –

Part 1: Introduction;

English version prEN 419111-1:2013

Profils de protection pour application de création et de vérification de signature –

Partie 1: Introduction;

Version anglaise prEN 419111-1:2013

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2013-03-25 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 41 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

E DIN 419111-1 ist Teil der fünfteiligen Europäischen Normenreihe E DIN EN 419111 (entsprechend prEN 419111). Diese Normenreihe enthält Schutzprofile, welche die Sicherheitserfordernisse für das Erzeugen und das Prüfen von Signaturen definieren. DIN 419111-1 gibt eine Einführung in die Normenreihe.

Gemäß den Kriterien des DIN für den Verzicht auf die Erstellung einer deutschen Sprachfassung wurde auf eine deutsche Fassung verzichtet; E DIN 419111-1 enthält somit den englischen Originaltext, ergänzt um eine deutsche Übersetzung der verwendeten Begriffe und Definitionen.

Im IT-Sicherheitsbereich sind Schutzprofile (en: protection profiles) Bestandteil des Zertifizierungsprozesses gemäß der „Common Criteria“, d. h., der Allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie (en: Common Criteria for Information Technology Security Evaluation, CC). Es handelt sich um die Festlegung einer implementierungsunabhängigen Menge von Mindestsicherheitsanforderungen für IT-Produkte bei einer gegebenen Sicherheitslage. Auf Basis dieser Schutzprofile können IT-Produkte geprüft werden und bei positivem Ausgang ein Zertifikat erhalten.

Die Normenreihe E DIN EN 419111 (entsprechend prEN 419111) ist Bestandteil einer Familie von Schutzprofilen, die von CEN als Europäische Normen zur Entwicklung von gemeinsamen Rahmenbedingungen für elektronische Signaturen in Auftrag gegeben worden sind. Weiterer Bestandteil der gemeinsamen Rahmenbedingungen ist z. B. die Normenreihe E DIN EN 14169 „Schutzprofile für Sichere Signaturerstellungseinheiten“.

Die fünf Teile der Europäischen Normenreihe E DIN EN 419111 beinhalten:

- Eine Einführung in die Normenreihe (E DIN EN 419111-1);
- die Festlegung der grundlegenden Funktionen, die für eine Anwendung zum Erzeugen von Signaturen unabdingbar sind. Hierbei handelt es sich um ein Schutzprofil gemäß CC, welche lediglich die benötigten Kernfunktionen spezifiziert (E DIN EN 419111-2);
- mögliche Ergänzungen zu den Funktionen von E DIN EN 419111-2 (E DIN EN 419111-3);
- die Festlegung der grundlegenden Funktionen, die für eine Anwendung zum Prüfen von Unterschriften unabdingbar sind. Hierbei handelt es sich um ein Schutzprofil gemäß CC, welches lediglich die benötigten Kernfunktionen spezifiziert (E DIN EN 419111-4); sowie
- mögliche Ergänzungen zu den Funktionen von E DIN EN 419111-4 (E DIN EN 419111-5).

E DIN EN 419111-1:2013 wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird. Das deutsche Spiegelgremium ist der NA 043-01-17 AA „Karten und persönliche Identifikation“.

Nationaler Anhang NA (informativ)

Begriffe, Symbole und Abkürzungen

Siehe Abschnitte 3 und 4 des Originaltextes.

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

fortgeschrittene elektronische Signatur

elektronische Signatur, die folgende Anforderungen erfüllt:

- a) sie ist ausschließlich dem Unterzeichner zugeordnet;
- b) sie ermöglicht die Identifizierung des Unterzeichners;
- c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann; und
- d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass jede nachträgliche Veränderung der Daten erkannt werden kann

[QUELLE: Directive 1999/93/EG, Artikel 2, Definition 2 [1]]

Anmerkung 1 zum Begriff: Im Zusammenhang mit diesem Dokument bezeichnet der Begriff Signatur eine fortgeschrittene elektronische Signatur.

3.2

Attributertifizierungsstelle

AA

Stelle, die Attribute durch die Ausstellung von Attributsertifikaten vergibt

3.3

Kartenannahmegerät

CAD

(en: Card Acceptance Device)

Kartenlesegerät, an das die sichere Signaturerstellungseinheit (SSEE) angeschlossen ist

3.4

Karteninhaber

Rechtmäßiger Eigentümer der SSEE

3.5

Zertifikat

elektronische Bescheinigung, mit der Signaturprüfdaten (SVD) einer Person zugeordnet werden und die Identität dieser Person bestätigt wird

[QUELLE: Directive 1999/93/EG, Artikel 2, Definition 9 [1]]

3.6

Zertifikatsperrliste

CRL

(en: Certificate Revocation List)

mit einem Zeitstempel versehene Liste zur Identifizierung ungültiger Zertifikate, die von einer Zertifizierungsstelle oder dem Aussteller der CRL unterzeichnet ist und in einem öffentlichen Verzeichnis frei verfügbar ist

3.7

Zertifizierungspfad

geordnete Aneinanderreihung von sich gegenseitig zertifizierenden Zertifikaten, beginnend mit einem Wurzelzertifikat, dem der Evaluationsgegenstand (EVG) vertraut, und endend mit dem Signaturzertifikat

3.8

Zertifizierungsdiensteanbieter

CSP

(en: Certification Service Provider)

Stelle oder juristische oder natürliche Person, die Zertifikate ausstellt oder sonstige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt

Anmerkung 1 zum Begriff: Siehe auch 5.6.3.2

3.9

digitale Signatur

von der sicheren Signaturerstellungseinheit (SSEE) berechnete Ergebnis der kryptografischen Signatur der eindeutigen Darstellung der zu signierenden Daten (DTBSR)

3.10

Aufrufende Anwendung

DA

(en: Driving application)

Anwendung, die zur Validierung elektronischer Signaturen die Signaturerstellungsanwendung (SCA) (bzw. die Signaturprüfanwendung (SVA) aufruft.

Anmerkung 1 zum Begriff: Die SCA (bzw. SVA) sendet das signierte Datenobjekt (SDO) (bzw. das Validierungsergebnis) an die DA zurück.

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

Anmerkung 2 zum Begriff: Für SVA, siehe ETSI TS 102 853 V1.1.1 [15]

3.11

elektronische Signatur

Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die als Mittel zur Authentisierung dienen

[QUELLE: Richtlinie 1999/93/EG, Artikel 2, Definition 1 [1]]

3.12

Schnittstellengerät

ID

(en: Interface Device)

Gerät, das die sichere Signaturerstellungseinheit (SSEE) mit der Signaturerstellungsplattform (SCP) verbindet

3.13**Regeln für die lokale Signaturpolitik****lokale Regeln**

Reihe von in der Signaturerstellungsanwendung oder der Signaturprüfanwendung (lokal) angewandten Regeln, nach denen die technische Gültigkeit der Signatur bestimmt werden kann. Diese Regeln können aus einer vereinbarten Signaturpolitik abgeleitet werden, die außerhalb des Anwendungsbereiches dieser EN festgelegt wurde

Anmerkung 1 zum Begriff: In ETSI TS 102 853 V1.1.1 [15] werden diese Regeln als Validierungsregeln bezeichnet.

3.14**Schutzprofil****PP**

(en: Protection Profile)

implementierungsunabhängige Festlegung von Sicherheitsanforderungen an einen Evaluationsgegenstand (EVG)

[QUELLE: [NR1], Abschnitt 4]

3.15**qualifiziertes Zertifikat**

Zertifikat, das die Anforderungen von [12], Anhang I erfüllt und von einem Zertifizierungsdienstanbieter bereitgestellt wird, der die Anforderungen von [12], Anhang II erfüllt

[QUELLE: Directive 1999/93/EG, Artikel 2, Definition 10. modified [1]]

3.16**qualifizierte elektronische Signatur****QES**

(en: qualified electronic signature)

fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und eine digitale Signatur enthält, die von einer sicheren Signaturerstellungseinheit (SSEE) erstellt wurde

3.17**Repräsentation der Authentisierungsdaten****RAD**

(en: Reference Authentication Data)

innerhalb der sicheren Signaturerstellungseinheit (SSEE) gespeicherte Daten, die als Bezugsdaten verwendet werden, mit denen die VAD verglichen werden. Diese RAD können biometrische Daten, eine PIN oder ein symmetrischer Schlüssel sein. Es kann sich dabei auch um eine Kombination dieser Daten handeln. In einigen Anwendungen können die RAD über den EVG übertragen werden

3.18**sichere Signaturerstellungseinheit****SSEE**

Signaturerstellungseinheit, die die Anforderungen von [6], Anhang 3 erfüllt

[QUELLE: Directive 1999/93/EG, Artikel 2, Definition 6 modified [1]]

3.19**Signaturattribut**

zusätzliche Informationen, die mit einer Signatur zusammenhängen. Ein Signaturattribut kann signiert oder unsigniert sein

Anmerkung 1 zum Begriff: Ein Signaturattribut darf auch als Signatureigenschaft bezeichnet werden (siehe ETSI TS 102 853 V1.1.1 [15]).

3.20**Signaturpolitik****SP**

(en: Signature Policy)

3.20.1**formale Signaturpolitik**

Reihe von Regeln, die mit einer vertrauenswürdigen Stelle zur Erstellung und Validierung einer elektronischen Signatur vereinbart oder von dieser erstellt wurden, nach denen die Gültigkeit der Signatur ermittelt werden kann

Anmerkung 1 zum Begriff: In einem bestimmten gesetzlichen/vertraglichen Zusammenhang kann festgestellt werden, ob eine bestimmte Signaturpolitik die jeweiligen Anforderungen des Gesetzes/Vertrages erfüllt. Die Signaturpolitik kann explizit identifiziert oder in der Semantik der zu signierenden Daten oder anderer externer Daten enthalten sein, wie z. B. in einem in Bezug genommenen Vertrag, der sich selbst wiederum auf eine Signaturpolitik bezieht. Beispiele für formale Signaturpolitiken sind in ETSI TR 102 038 V1.1.1 [10] und ETSI TR 102 272 V1.1.1 [11] angegeben.

3.20.2**lokale Signaturpolitik**

Reihe von Regeln zur Erstellung und Validierung einer elektronischen Signatur, nach denen ermittelt werden kann, ob die Signatur in einem bestimmten Transaktionszusammenhang gültig ist

Anmerkung 1 zum Begriff: Im übrigen Teil dieses Dokumentes bezieht sich der Begriff Signaturpolitik (SP) immer auf die lokale Signaturpolitik.

3.21**Signaturerstellungsanwendung****SCA**

(en: Signature Creation Application)

Anwendung, die durch Verwendung der von einer an die SCA angeschlossenen sicheren Signaturerstellungseinheit (SSEE) erzeugten digitalen Signatur eine elektronische Signatur erstellt

3.22**Signaturerstellungseinheit**

konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird

[QUELLE: Direktive 1999/93/EG, Artikel 2, Definition 5 [1]]

3.23**Signaturerstellungsplattform****SCP**

(en: Signature Creation Platform)

Hardware und Software, die die SCA enthalten und unterstützen

3.24**Signaturerstellungssystem****SCS**

(en: Signature Creation System)

gesamtes System, das aus der Signaturerstellungsanwendung (SCA) und der sicheren Signaturerstellungseinheit (SSEE) besteht, und eine elektronische Signatur erstellt

3.25**signierte(s) Datenobjekt(e)****SDO**

(en: Signed Data Object(s))

Dokument(e) oder Teile des Dokuments/der Dokumente, für die eine elektronische Signatur erzeugt wurde, zusammen mit der elektronischen Signatur

3.26

Signaturtyp

spezielles Format zur Kodierung/Darstellung einer fortgeschrittenen elektronischen Signatur einschließlich ihrer Attribute

3.27

Signaturvalidierung

Prozess der Überprüfung, ob eine Signatur gültig ist, einschließlich der Überprüfung der Signatur gegen die Anforderungen einer lokalen oder gemeinsamen Signaturpolitik sowie Zertifikatsvalidierung und Signaturprüfung

3.28

Signaturprüfung

Prozess der Überprüfung des kryptografischen Wertes einer Signatur anhand von Signaturprüfdaten

3.29

Zeitmarke

Information in einem Prüfprotokoll eines vertrauenswürdigen Diensteanbieters, mit der die Darstellung eines Bezugswertes mit einem bestimmten Zeitpunkt verknüpft wird, wodurch der Nachweis erbracht wird, dass der Bezugswert vor diesem Zeitpunkt vorhanden war

3.30

Zeitstempel-Objekt

Datenobjekt, das die Darstellung eines Bezugswertes mit einem bestimmten Zeitpunkt verknüpft, und so den Beweis dafür liefert, dass der Bezugswert vor diesem Zeitpunkt vorhanden war

3.31

Zeitstempeldiensteanbieter

TSA

(en: Time Stamping Authority)

vertrauenswürdige Drittpartei, die Zeitstempel-Objekte erstellt, um nachzuweisen, dass ein bestimmter Bezugswert zu einem bestimmten Zeitpunkt bereits existiert hat

3.32

vertrauenswürdiger Diensteanbieter

TSP

(en: Trusted Service Provider)

Stelle, die dazu beiträgt, ein Vertrauensverhältnis zu schaffen, indem sie auf Anfrage einige Informationen verfügbar macht oder liefert

3.33

Benutzer

jeweiliger aktueller Benutzer des EVG.

Anmerkung 1 zum Begriff: Der Benutzer kann der Herausgeber oder Inhaber der Karte sein.

3.34

Validierungsdaten

vom Unterzeichner und/oder einem Prüfer gesammelte zusätzliche Daten, die für die Verifizierung der elektronischen Signatur benötigt werden, welche Zertifikate, Sperrstatusinformationen, Zeitstempel oder Zeitmarken umfassen können

3.35

Prüfauthentisierungsdaten

VAD

(en: Verification Authentication Data)

Daten, die an die sichere Signaturerstellungseinheit (SSEE) übertragen werden können. Sie werden mit den Referenz-Authentisierungsdaten (RAD) verglichen.

3.36**Prüfzeitpunkt**

vom Prüfer gewählter Zeitpunkt entweder in der Gegenwart oder in der Vergangenheit, für die er überprüfen will, ob das Signaturzertifikat zu diesem Zeitpunkt gültig war

3.37**Prüfer**

Stelle, die eine elektronische Signatur validiert oder verifiziert. Dabei kann es sich entweder um eine vertrauende Partei oder eine Drittpartei handeln, z. B. einen Schiedsgutachter, die an der Gültigkeit einer elektronischen Signatur interessiert ist

4 Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Symbole und Abkürzungen

AA	Attributertifizierungsstelle	(en: Attribute Authority)
AdES	fortgeschrittene elektronische Signatur	(en: Advanced Electronic Signature)
BES	Grundform der elektronischen Signatur	(en: Basic Electronic Signature)
CA	Zertifizierungsdiensteanbieter	(en: Certificate Authority)
CB	Zertifizierungsstelle	(en: Certification Body)
CAD	Kartenannahmegerät	(en: Card Acceptance Device)
CC	Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie	(en: Common Criteria)
CRL	Zertifikatsperrliste	(en: Certificate Revocation list)
CSP	Zertifizierungsdiensteanbieter	(en: Certificate Service Provider)
DA	Aufrufende Anwendung	(en: Driving Application)
DTBS	zu signierende Daten	(en: Data To Be Signed)
DTBSR	Darstellung der zu signierenden Daten	(en: Data To Be Signed Representation)
DTBSR_DS	digitale Signatur der Darstellung der zu signierenden Daten	(en: Data To Be Signed Representation Digital Signature)
DHC	Datenhashing-Komponente	(en: Data Hashing Component)
EPES	elektronische Signatur auf der Grundlage einer expliziten Politik	(en: Explicit Policy-based Electronic Signature)
ID	Schnittstellengerät	(en: Interface Device)
OCSP	Online-Zertifikatsstatusprotokoll	(en: Online Certificate Status Protocol)
PIN	persönliche Identifizierungsnummer	(en: Personal Identification Number)
PC	Personal Computer	(en: Personal Computer)
PKI	Public-Key-Infrastruktur	(en: Public Key Infrastructure)
PP	Schutzprofil	(en: Protection Profile)
QES	qualifizierte elektronische Signatur	(en: Qualified Electronic Signature)
RAD	Repräsentation der Authentisierungsdaten	(en: Reference Authentication Data)
SCA	Signaturerstellungsanwendung	(en: Signature Creation Application)
SCD	Signaturstellungsdaten (Signaturschlüssel)	(en: Signature Creation Data)
SCP	Signaturerstellungsplattform	(en: Signature Creation Platform)
SCS	Signaturerstellungssystem	(en: Signature Creation System)

SD	Dokument des Unterzeichners	(en: Signer's Document)
SDO	signiertes Datenobjekt	(en: Signed Data Object)
SP	Signaturpolitik	(en: Signature Policy)
SSCD (SSEE)	sichere Signaturerstellungseinheit (SSEE)	(en: Secure Signature Creation Device) (SSCD)
ST	Sicherheitsvorgaben	(en: Security Target)
SVA	Signaturprüfanwendung	(en: Signature Verification Application)
SVD	Signaturprüfdaten (Signaturprüfschlüssel)	(en: Signature Verification Data)
TSA	Zeitstempeldiensteanbieter	(en: Time Stamping Authority)
TSP	vertrauenswürdiger Diensteanbieter	(en: Trusted Service Provider)
EVG (TOE)	Evaluationsgegenstand (EVG)	(en: Target of Evaluation) (TOE)
VAD	Prüfauthentisierungsdaten	(en: Verification Authentication Data)

— Leerseite —

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

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	10
5 Signature Creation Application	11
5.1 General.....	11
5.2 Conformance claim.....	11
5.2.1 CC Conformance Claim.....	11
5.2.2 PP Claim	11
5.2.3 Package Claim.....	11
5.2.4 Conformance Rationale	11
5.2.5 Conformance Statement	11
5.3 Overview of the target of evaluation.....	11
5.3.1 TOE Type	11
5.3.2 TOE Usage.....	11
5.4 Subjects	11
5.4.1 Signatory	11
5.4.2 Administrator	11
5.5 Objects.....	12
5.5.1 Signature	12
5.5.2 Signature Policy.....	12
5.5.3 Certificate	12
5.5.4 Document	12
5.6 SCA environment.....	14
5.6.1 Overview	14
5.6.2 External entities	14
5.6.3 Other Entities	16
5.7 Operations	16
5.7.1 Introduction	16
5.7.2 TOE Operations.....	17
5.7.3 TOE/TOE-environment operations.....	20
5.7.4 TOE-environment operations	21
6 Signature Verification Application	22
6.1 General.....	22
6.2 Conformance	22
6.2.1 CC Conformance Claim.....	22
6.2.2 PP Claim	22
6.2.3 Package Claim.....	22
6.2.4 Conformance Rationale	22
6.2.5 Conformance Statement	22
6.3 Overview of the target of evaluation.....	22
6.3.1 TOE Type	22
6.3.2 TOE Usage.....	22
6.4 Subjects	23
6.4.1 Verifier.....	23
6.4.2 Administrator	23
6.5 Objects.....	23
6.5.1 Signature	23

6.5.2	Signature Policy	23
6.5.3	Certificate	23
6.6	SVA environment.....	24
6.6.1	Overview.....	24
6.6.2	External entities	24
6.6.3	Other Entities	25
6.7	Operations.....	26
6.7.1	Introduction.....	26
6.7.2	TOE Operations	26
6.7.3	TOE/TOE-environment operations	30
	Bibliography.....	31
	Index	32

Figures

Figure 1 — SCA Environment	14
Figure 2 — SCA features	17
Figure 3 — SDO minimum content	18
Figure 4 — Document processing main steps	19
Figure 5 — SVA Environment.....	24
Figure 6 — SVA Features.....	26
Figure 7 — Signature validation in the SVA	27