

DIN EN 419211-1

ICS 35.240.15

**Schutzprofile für sichere Signaturerstellungseinheiten –
Teil 1: Überblick;
Deutsche Fassung EN 419211-1:2014**

Protection profiles for secure signature creation device –
Part 1: Overview;
German version EN 419211-1:2014

Profils de protection pour dispositif sécurisé de signature électronique –
Partie 1: Présentation générale;
Version allemande EN 419211-1:2014

Gesamtumfang 24 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 419211-1:2014) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR (Frankreich) gehalten wird.

Das zuständige deutsche Gremium ist der Unterausschuss NA 043-01-17-04 UA „Austauschprotokolle bei Chipkarten“ des Arbeitsausschusses NA 043-01-17 AA „Karten und persönliche Identifikation“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Deutsche Fassung

Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick

Protection profiles for secure signature creation device —
Part 1: Overview

Profils de protection pour dispositif sécurisé de
création de signature électronique —
Partie 1: Présentation générale

Diese Europäische Norm wurde vom CEN am 25. Juli 2014 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
3.1 Verweisung auf EG-Richtlinie.....	5
3.2 Fachbegriffe	5
4 Abkürzungen	8
5 Schutzprofile im Überblick	9
6 Evaluationsgegenstand	10
6.1 Allgemeines	10
6.2 Funktionen einer SSCD	10
6.2.1 Kernfunktionen	10
6.2.2 Zusätzliche Funktionen	11
6.3 EVG-Lebenszyklus.....	12
6.3.1 Allgemeines	12
6.3.2 Vorbereitungsstufe	12
6.3.3 Einsatzstufe	14
6.4 Einsatz des EVG.....	15
7 EVG-Definitionen	16
7.1 Allgemeines	16
7.2 EVG mit Schlüsselerzeugung.....	16
7.3 EVG mit Schlüsselimport.....	16
7.4 EVG mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung	17
7.5 EVG mit vertrauenswürdigen Kanal zur Signaturerstellungsanwendung.....	17
Anhang A (informativ) Vergleich mit CWA 14169:2004, Anhang C	21
A.1 Allgemeines	21
A.2 Technische Unterschiede	21
Literaturhinweise	22

Vorwort

Dieses Dokument (EN 419211-1:2014) 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.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis April 2015, und etwaige entgegenstehende nationale Normen müssen bis April 2015 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt CWA 14169:2004.

Die wesentlichen Änderungen zwischen dieser Ausgabe und CWA 14169:2004 sind in Anhang A angegeben.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Diese Europäische Normenreihe legt Schutzprofile für sichere Signaturerstellungseinheiten fest und wird von der Europäischen Normungsorganisation CEN als aktualisierte Fassung des CEN Workshop Agreements zu elektronischen Signaturen (E-SIGN) CWA 14169:2004, Anhang C, zu Schutzprofilen sicherer Signaturerstellungseinheiten, „EAL 4+“, herausgegeben.

Diese Europäische Normenreihe besteht aus den folgenden Teilen:

- *Teil 1: Überblick*
- *Teil 2: Einheiten mit Schlüsselerzeugung*
- *Teil 3: Einheiten mit Schlüsselimport*
- *Teil 4: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung*
- *Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung*
- *Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung*

Bei der Erstellung der Dokumente dieser Europäischen Normenreihe als Schutzprofile wurden die Regeln der Common Criteria Version 3.1 ([2], [3] und [4]) eingehalten.

1 Anwendungsbereich

Diese Europäische Norm

- legt die bei der Festlegung von Schutzprofilen für sichere Signaturerstellungseinheiten verwendeten Begriffe fest,
- legt funktionale und einsatzbezogene Anforderungen an sichere Signaturerstellungseinheiten fest,
- beschreibt den Evaluationsgegenstand für diese Schutzprofile.

2 Normative Verweisungen

Nicht zutreffend.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1 Verweisung auf EG-Richtlinie

Diese Europäische Norm spiegelt in den Fachbegriffen der Schutzprofile die Anforderungen einer Europäischen Richtlinie wider. Zur Verweisung auf diese Richtlinie werden im Text die folgenden Begriffe verwendet:

3.1.1

Richtlinie

Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über „gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“ [1]

Anmerkung 1 zum Begriff: Verweisungen in diesem Dokument auf einen bestimmten Artikel und Absatz der Richtlinie 1999/93/EG sind wie folgt angegeben: „(**Richtlinie: n.m**)“.

3.1.2

Anhang

einer der drei Anhänge der **Richtlinie**, d. h. Anhang I, Anhang II oder Anhang III

3.2 Fachbegriffe

3.2.1

Administrator

Benutzer, der die Initialisierung und Personalisierung des Evaluationsgegenstands vornimmt oder sonstige administrative EVG-Funktionen ausführt

3.2.2

fortgeschrittene elektronische Signatur

digitale Signatur, die bestimmte in der **Richtlinie: 2.2** angegebene Anforderungen erfüllt

Anmerkung 1 zum Begriff: Nach der **Richtlinie** ist eine digitale Signatur als fortgeschrittene elektronische Signatur anzusehen, wenn sie

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

3.2.3

Authentisierungsdaten

Informationen, die zur Überprüfung der behaupteten Identität eines Benutzers verwendet werden

3.2.4

Zertifikat

digitale Signatur, die als elektronische Bescheinigung verwendet wird, mit der Signaturprüfdaten einer Person zuordnet werden und so die Identität dieser Person als rechtmäßiger Unterzeichner bestätigt wird (**Richtlinie: 2.9**)

3.2.5

Zertifikatinformationen

Informationen, die einem SCD/SVD-Paar zugeordnet sind, das in einer sicheren Signaturerstellungseinheit gespeichert sein darf

Anmerkung 1 zum Begriff: Zertifikatinformationen dürfen enthalten:

- das Public-Key-Zertifikat (über den öffentlichen Schlüssel) eines Unterzeichners; oder
- ein oder mehrere Hash-Werte des Public-Key-Zertifikats eines Unterzeichners sowie ein Bezeichner der zur Berechnung der Hash-Werte verwendeten Hash-Funktion; oder
- das Public-Key-Zertifikat wie es in X.509 definiert ist.

Anmerkung 2 zum Begriff: Zertifikatinformationen dürfen Informationen enthalten, die es dem Benutzer erlauben, zwischen verschiedenen Zertifikaten zu unterscheiden.

3.2.6

Zertifikaterzeugungsanwendung

CGA

Sammlung von Anwendungskomponenten, die von der sicheren Signaturerstellungseinheit die Signaturprüfdaten erhalten, um ein Zertifikat zu erzeugen, indem sie in das Zertifikat aufzunehmende Daten beziehen, und um eine digitale Signatur des Zertifikats zu erstellen

3.2.7

Zertifizierungsdienstanbieter

CSP

Stelle, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen erbringt (**Richtlinie: 2.11**)

3.2.8

zu signierende Daten

DTBS

sämtliche zu signierenden elektronischen Daten, einschließlich Benutzernachricht und Signaturattribute

3.2.9

zu signierende Daten oder deren eindeutige Darstellung

DTBS/R

von einer sicheren Signaturerstellungseinheit empfangene Daten, die als Eingangsdaten für eine einzelne Signaturerstellungsoption verwendet werden

Anmerkung 1 zum Begriff: Beispiele von DTBS/R sind:

- ein Hash-Wert der zu signierenden Daten (DTBS); oder
- ein Zwischen-Hash-Wert eines ersten Teils der DTBS, ergänzt durch einen verbleibenden Teil der DTBS; oder
- die DTBS.

3.2.10

rechtmäßiger Benutzer

Benutzer einer sicheren Signaturerstellungseinheit, der durch einen SSCD-Bereitstellungsdienstleister in den Besitz der sicheren Signaturerstellungseinheit gelangt und von der sicheren Signaturerstellungseinheit als deren Unterzeichner authentisiert werden kann