

DIN EN 419211-6

ICS 03.160; 35.040; 35.240.15

**Schutzprofile für sichere Signaturerstellungseinheiten –
Teil 6: Erweiterung für Einheiten mit Schlüsselimport und
vertrauenswürdigen Kanal zur Signaturerstellungsanwendung;
Deutsche Fassung EN 419211-6:2014**

Protection profiles for secure signature creation device –
Part 6: Extension for device with key import and trusted channel to signature creation
application;
German version EN 419211-6:2014

Profils de protection pour dispositif sécurisé de création de signature électronique –
Partie 6: Extension pour un dispositif avec import de clé et communication sécurisée avec
l'application de création de signature;
Version allemande EN 419211-6:2014

Gesamtumfang 26 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 419211-6:2014) 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 6: Erweiterung für Einheiten mit Schlüsselimport und
vertrauenswürdigen Kanal zur Signaturerstellungsanwendung

Protection profiles for secure signature creation device —
Part 6: Extension for device with key import and trusted
channel to signature creation application

Profils de protection pour dispositif sécurisé de
création de signature électronique —
Partie 6: Extension pour un dispositif avec import de
clé et communication sécurisée avec l'application de
création de signature

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 Übereinkünfte und Terminologie	5
3.1 Übereinkünfte.....	5
3.2 Begriffe	5
4 Einführung in Schutzprofile.....	6
4.1 Schutzprofilreferenz	6
4.2 Überblick über das Schutzprofil.....	6
4.3 Überblick über den Evaluationsgegenstand.....	7
5 Konformität.....	9
5.1 CC-Konformität	9
5.2 Schutzprofil-Konformität, Paket-Konformität	9
5.3 Begründung der Konformität	9
5.4 Konformitätsangabe	10
6 Definition des Sicherheitsproblems	10
6.1 Zu schützende Werte, Benutzer und Bedrohungsagenten	10
6.2 Bedrohungen.....	11
6.3 Organisatorische Sicherheitsvorgaben	11
6.4 Annahmen	11
7 Sicherheitsziele	11
7.1 Sicherheitsziele für den EVG	11
7.2 Sicherheitsziele für die Einsatzumgebung	12
7.3 Begründung der Sicherheitsziele.....	13
8 Erweiterte Komponentendefinition	16
9 Sicherheitsanforderungen	16
9.1 Funktionale Sicherheitsanforderungen.....	16
9.2 Anforderungen an die Vertrauenswürdigkeit der Sicherheit	19
9.3 Begründung der Sicherheitsanforderungen	20
Literaturhinweise	24

Vorwort

Dieses Dokument (EN 419211-6:2014) 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.

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.

Im Vergleich zu CWA 14169 wurde das Dokument vollständig überarbeitet. Genauere Angaben zur Überarbeitung sind in EN 419211-1:2014, Anhang A zu finden.

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 Common Criteria 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 B und 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 vertrauenswürdigem Kanal zur Zertifikaterzeugungsanwendung*
- *Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Signaturstellungsanwendung*
- *Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigem Kanal zur Signaturstellungsanwendung*

Bei der Erstellung dieses Dokuments als Schutzprofil (Protection Profile, PP) wurden die Regeln von ISO/IEC 15408 befolgt.

1 Anwendungsbereich

Diese Europäische Norm legt ein Schutzprofil für eine sichere Signaturerstellungseinheit fest, die Signaturschlüssel importieren und in geschützter Weise mit der Signaturerstellungsanwendung kommunizieren darf: Sichere Signaturerstellungseinheit mit Schlüsselimport und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung (SSCD KI TCSCA).

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 419211-1:2014, *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick*

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*¹⁾

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

3 Übereinkünfte und Terminologie

3.1 Übereinkünfte

Dieses Dokument wurde in Übereinstimmung mit der CEN/CENELEC-Richtlinie entworfen, und der Inhalt und die Struktur dieses Dokuments folgen den Regeln und Übereinkünften, die in ISO/IEC 15408 festgelegt sind.

Die normativen Aspekte des Inhalts dieser Europäischen Norm wurden in Übereinstimmung mit den Regeln der Common Criteria festgelegt und nicht speziell durch die Verben „muss“ oder „ist zu“ gekennzeichnet.

3.2 Begriffe

Für die Anwendung dieses Dokuments gelten die Akronyme und Begriffe nach EN 419211-1.

1) ISO/IEC 15408-1, ISO/IEC 15408-2 und ISO/IEC 15408-3 entsprechen den *Common Criteria for Information Technology Security Evaluation*, Teil 1, 2 und 3.

4 Einführung in Schutzprofile

4.1 Schutzprofilreferenz

Titel:	Schutzprofile für sichere Signaturerstellungseinheiten — Teil 6: Schutzprofil für sichere Signaturerstellungseinheit mit Schlüsselimport und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung
Version:	1.0.4
Autor:	CEN/CENELEC (TC 224/WG 17)
Veröffentlichungsdatum:	2013-04-03
Registrierung:	BSI-CC-PP-0076
CC-Version:	3.1 Revision 4
Bearbeiter:	Arnold Abromeit, TÜV Informationstechnik GmbH
Allgemeiner Status:	final
Schlüsselwörter:	sichere Signaturerstellungseinheit, elektronische Signatur, digitale Signatur, Schlüsselimport, vertrauenswürdiger Kanal zur Signaturerstellungsanwendung

4.2 Überblick über das Schutzprofil

Dieses Schutzprofil wurde vom CEN als eine Europäische Norm für Produkte zur Erstellung elektronischer Signaturen erstellt. Sie erfüllt die Anforderungen der Richtlinie 1999/93/EG²⁾ des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über *gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*.

Nach Artikel 9 dieser Europäischen Richtlinie kann die vorliegende Norm von der Europäischen Kommission im Amtsblatt der Europäischen Gemeinschaften als allgemein anerkannte Norm für Produkte zur Erstellung elektronischer Signaturen angegeben werden.

Dieses Schutzprofil beschreibt funktionale Sicherheitsanforderungen und Sicherheitsanforderungen an die Vertrauenswürdigkeit für eine sichere Signaturerstellungseinheit (en: secure signature creation device, SSCD), die mit denen in Anhang III der Richtlinie übereinstimmen. Diese sichere Signaturerstellungseinheit ist der Evaluationsgegenstand (EVG) dieses Schutzprofils.

Die Mitgliedstaaten der EU dürfen davon ausgehen, dass eine Übereinstimmung mit den in Anhang III der Richtlinie festgelegten Anforderungen vorliegt, wenn ein Produkt zur Erstellung elektronischer Signaturen anhand eines Sicherheitsziels (en: security target, ST) evaluiert wurde, das diesem Schutzprofil (en: Protection Profile, PP) entspricht.

Dieses Schutzprofil für sichere Signaturerstellungseinheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung (PP SSCD KI TCSCA) enthält die Sicherheitsanforderungen an SSCD mit Schlüsselimport, die Signaturstellungsdaten [en: signature creation data, SCD] importieren und eine digitale Signatur erstellen können, um für die im Basis-Schutzprofil [6] beschriebenen (qualifizierten oder fortgeschrittenen) elektronischen Signaturen verwendet zu werden. Zusätzlich unterstützt der Evaluationsgegenstand (EVG) dieses Schutzprofils zum Schutz von Authentisierungsdaten und von zu signierenden Daten eine vertrauenswürdige Kommunikation mit einer Signaturerstellungsanwendung. Diese Sicherheitsmerkmale erlauben die Verwendung des EVG in einer komplexeren Einsatzumgebung. Es entspricht dem Basis-Schutzprofil für SSCD KI [3]. Die eigentliche Bedeutung dieses Konformitätsanspruches wird im Weiteren in 5.3 erläutert.

Die Vertrauenswürdigkeitsstufe für dieses Schutzprofil ist EAL4, augmentiert um AVA_VAN.5.

2) Diese Europäische Richtlinie wird im Folgenden als „die Richtlinie“ bezeichnet.