

DIN EN 419211-5

ICS 03.160; 35.040; 35.240.15

**Schutzprofile für sichere Signaturerstellungseinheiten –
Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und
vertrauenswürdigen Kanal zur Signaturerstellungsanwendung;
Deutsche Fassung EN 419211-5:2013**

Protection profiles for secure signature creation device –
Part 5: Extension for device with key generation and trusted channel to signature creation
application;
German version EN 419211-5:2013

Profils de protection pour dispositif sécurisé de création de signature –
Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée
avec l'application de création de signature;
Version allemande EN 419211-5:2013

Gesamtumfang 27 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (EN 419211-5:2013) 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.

Der zuständige deutsche Arbeitsausschuss ist der NA 043-01-17-04 UA „Austauschprotokolle bei Chip-Karten“ im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN.

Deutsche Fassung

Schutzprofile für sichere Signaturerstellungseinheiten —
Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und
vertrauenswürdigen Kanal zur Signaturerstellungsanwendung

Protection profiles for secure signature creation device —
Part 5: Extension for device with key generation and trusted
channel to signature creation application

Profils de protection pour dispositif sécurisé
de création de signature —
Partie 5: Extension pour un dispositif avec génération
de clé et communication sécurisée avec l'application
de création de signature

Diese Europäische Norm wurde vom CEN am 12. Oktober 2013 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.....	5
4.1 Schutzprofilreferenz	5
4.2 Überblick über das Schutzprofil.....	6
4.3 Überblick über den Evaluationsgegenstand.....	6
5 Konformität.....	9
5.1 CC-Konformität	9
5.2 Schutzprofil-Konformität, Paket-Konformität	9
5.3 Begründung der Konformität	9
5.4 Konformitätsangabe	9
6 Definition des Sicherheitsproblems	10
6.1 Zu schützende Werte, Benutzer und Bedrohungsagenten	10
6.2 Bedrohungen.....	10
6.3 Organisatorische Sicherheitsvorgaben	10
6.4 Annahmen	10
7 Sicherheitsziele.....	11
7.1 Sicherheitsziele für den EVG.....	11
7.2 Sicherheitsziele für die Einsatzumgebung	11
7.3 Begründung der Sicherheitsziele.....	12
8 Erweiterte Komponentendefinition	15
9 Sicherheitsanforderungen	15
9.1 Funktionale Sicherheitsanforderungen.....	15
9.2 Anforderungen an die Vertrauenswürdigkeit der EVG-Sicherheit	19
9.3 Begründung der Sicherheitsanforderungen.....	20
Literaturhinweise	25

Vorwort

Dieses Dokument (EN 419211-5:2013) 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.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juni 2014, und etwaige entgegenstehende nationale Normen müssen bis Juni 2014 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.

Diese Europäische Normenreihe, *Schutzprofile für sichere Signaturerstellungseinheiten* 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 Signaturstellungsanwendung
- Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur Signaturstellungsanwendung

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 vom CEN/ISSS (ISSS: Information Society Standardization System, Normungssystem für die Informationsgesellschaft) als aktualisierte Fassung des CEN/ISSS Workshop Agreements CWA 14169:2004 zu elektronischen Signaturen (E-SIGN), Anhang B und Anhang C, zu Schutzprofilen sicherer Signaturerstellungseinheiten, „EAL 4+“, herausgegeben.

Bei der Erstellung dieses Dokuments als Schutzprofil (Protection Profile, PP) wurden die Regeln der Common Criteria Version 3.1 [2], [3] und [4] befolgt.

1 Anwendungsbereich

Diese Europäische Norm legt ein Schutzprofil für eine sichere Signaturerstellungseinheit fest, die Signaturschlüssel intern erzeugen und mit der Signaturerstellungsanwendung in geschützter Weise kommunizieren kann: Sichere Signaturerstellungseinheit mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung (SSCD KG TCSCA).

2 Normative Verweisungen

Die folgenden zitierten Dokumente 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).

prEN 419211-1:2011, *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 1: Überblick*¹⁾

3 Übereinkünfte und Terminologie

3.1 Übereinkünfte

Dieses Dokument wurde in Übereinstimmung mit der CEN/CENELEC-Geschäftsordnung Teil 3 entworfen, und der Inhalt und die Struktur dieses Dokuments folgen den Regeln und Übereinkünften, die in den Common Criteria 3.1 festgelegt sind.

Normative Aspekte des Inhalts dieser Europäischen Norm wurden in Übereinstimmung mit den Regeln der Common Criteria spezifiziert und wurden nicht speziell durch die Verben „muss/müssen“ und „ist/sind zu“ kenntlich gemacht.

3.2 Begriffe

Für die Anwendung dieses Dokuments gelten die Akronyme und Begriffe nach prEN 419211-1:2011.

4 Einführung in Schutzprofile

4.1 Schutzprofilreferenz

Titel:	Schutzprofile für sichere Signaturerstellungseinheiten — Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung
Version:	1.0.1
Autor:	CEN/CENELEC (TC 224/WG 17)
Veröffentlichungsdatum:	2012-11-14
Registrierung:	BSI-CC-PP-0072
CC-Version:	3.1 Revision 4
Bearbeiter:	Arnold Abromeit, TÜV Informationstechnik GmbH
Allgemeiner Status:	final
Schlüsselwörter:	sichere Signaturerstellungseinheit, elektronische Signatur, digitale Signatur, Schlüsselerzeugung, vertrauenswürdiger Kanal zur Signaturerstellungsanwendung

1) Zu veröffentlichen. Dieses Dokument wurde zur CEN-Umfrage als prEN 14169-1 vorgelegt.

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 Richtlinie²⁾ 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

Gemäß 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 legt funktionale Sicherheitsanforderungen und Anforderungen an die Vertrauenswürdigkeit für eine sichere Signaturerstellungseinheit (en: secure signature creation device, SSCD) fest, 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 Übereinstimmung mit den Anforderungen von Anhang III der Richtlinie vorliegt, wenn die Evaluation für ein Produkt zur Erstellung sicherer Signaturen ergeben hat, dass das Sicherheitsziel (en: Security Target, ST) diesem Schutzprofil (en: protection profile, PP) entspricht.

Dieses Schutzprofil für sichere Signaturerstellungseinheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung (PP SSCD KG TCSCA) enthält die Sicherheitsanforderungen an SSCD mit Schlüsselerzeugung, die Signaturstellungsdaten [en: signature creation data, SCD] und eine digitale Signatur erzeugen kann, um für die im Basis-Schutzprofil [5] beschriebenen (qualifizierten oder fortgeschrittenen) elektronischen Signaturen verwendet zu werden. Zusätzlich unterstützt der Evaluationsgegenstand (EVG) dieses Schutzprofils eine vertrauenswürdige Kommunikation zu einer Signaturerstellungsanwendung zum Schutz von Authentisierungsdaten und von zu signierenden Daten. Diese Sicherheitsmerkmale erlauben es, den EVG in einer komplexeren Einsatzumgebung zu verwenden. Das entspricht dem Basis-Schutzprofil für SSCD mit Schlüsselerzeugung [5]. Die eigentliche Bedeutung dieses Konformitätsanspruches wird nachstehend in 5.3 erläutert.

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

4.3 Überblick über den Evaluationsgegenstand

4.3.1 Einsatz des EVG

Dieser Unterabschnitt bietet einen funktionsbezogenen Überblick über den EVG in seinen einzelnen Einsatzumgebungen:

- der Vorbereitungsumgebung, in der er durch eine Zertifikaterzeugungsanwendung (en: certificate generation application, CGA) mit einem Zertifizierungsdienstanbieter (en: certification service provider, CSP) interagiert, um ein Zertifikat für die Signaturprüfdaten (en: signature validation data, SVD) zu erhalten, die den vom EVG erzeugten Signaturstellungsdaten (en: signature creation data, SCD) entsprechen. Weiterhin interagiert die Initialisierungsumgebung mit dem EVG, um diesen mit dem Anfangswert der Referenz-Authentisierungsdaten (en: reference authentication data, RAD) zu personalisieren;
- der Signierumgebung, in der er durch eine Signaturerstellungsanwendung (SCA) mit einem Unterzeichner interagiert, um Daten zu signieren, nachdem der Unterzeichner als Unterzeichnender authentisiert wurde. Die Signaturerstellungsanwendung stellt die zu signierenden Daten (DTBS) oder eine eindeutige Darstellung derselben (DTBS/R) als Eingabe für die EVG-Signaturerstellungsfunktion bereit und bezieht die resultierende elektronische Signatur³⁾. Der Evaluationsgegenstand und die Signaturerstellungsanwendung kommunizieren über einen vertrauenswürdigen Kanal um die Integrität der DTBS bzw. DTBS/R sicherzustellen;

2) Diese Europäische Richtlinie wird in diesem Schutzprofil als „**die Richtlinie**“ bezeichnet.

3) Auf rein funktionaler Ebene erstellt die SSCD eine elektronische Signatur; für eine Implementierung der SSCD, die die Anforderungen dieses PP erfüllt und über ein nach Anhang I **der Richtlinie** erzeugtes Schlüsselzertifikat verfügt, kann das Ergebnis des Signierprozesses verwendet werden, um eine qualifizierte elektronische Signatur zu erstellen.

- der Managementumgebung, in der er mit dem Benutzer oder einem SSCD-Bereitstellungsdienstanbieter interagiert, um Managementoperationen auszuführen, z. B. damit der Unterzeichnende gesperrte RAD zurücksetzt. Ein einzelnes Gerät, z. B. ein Chipkartenendgerät, kann die erforderliche sichere Umgebung für das Management und die Signierung bereitstellen.

Die Signierumgebung, die Managementumgebung und die Vorbereitungsumgebung sind sicher und schützen die mit dem EVG ausgetauschten Daten. prEN 419211-1:2011, Bild 5, zeigt die Einsatzumgebung.

Der EVG speichert Signaturerstellungsdaten und Referenz-Authentisierungsdaten. Er kann mehrere Instanzen von privaten Schlüsseln (SCD) speichern. Ist dies der Fall, stellt der EVG eine Funktion zur Identifizierung sämtlicher privaten Schlüssel (SCD) bereit, und die Signaturerstellungsanwendung kann eine Schnittstelle zum Unterzeichner bereitstellen, damit dieser einen in der Signaturerstellungsfunktion der SSCD zu verwendenden privaten Schlüssel (SCD) auswählen kann. Der EVG schützt die Vertraulichkeit und Integrität der Signaturerstellungsdaten und beschränkt deren Verwendung bei der Signaturerstellung auf den jeweiligen Unterzeichner. Die mit dem EVG erstellte elektronische Signatur ist eine in **der Richtlinie** definierte *qualifizierte elektronische Signatur*, wenn das Zertifikat für die Signaturprüfdaten ein qualifiziertes Zertifikat ist (Anhang I **der Richtlinie**). Die Feststellung, ob es sich um ein qualifiziertes Zertifikat handelt, liegt außerhalb des Anwendungsbereichs dieser Norm.

Die Signaturerstellungsanwendung (SCA) übernimmt den Schutz der Integrität der Eingangsdaten, die sie der Signaturerstellungsfunktion des EVG bereitstellt, schützen und sicherstellen, dass diese den vom Unterzeichner zum Signieren freigegebenen Benutzerdaten entsprechen. Sofern dem EVG die Art der von der SCA bereitgestellten Signiereingangsdaten nicht bekannt ist, gibt die Signaturerstellungsanwendung diese an (als DTBS/R) und berechnet die erforderlichen Hash-Werte. Der EVG kann die DTBS/R um von ihm gespeicherte Signaturparameter erweitern und berechnet anschließend einen Hash-Wert über die Eingangsdaten, wie er von der Art der Eingangsdaten und vom verwendeten kryptographischen Algorithmus benötigt wird. Der EVG und die SCA kommunizieren über einen vertrauenswürdigen Kanal um die Integrität der DTBS/R zu schützen.

Der EVG speichert Referenz-Authentisierungsdaten des Unterzeichners, um einen Benutzer als den jeweiligen Unterzeichner zu authentisieren. Die RAD sind ein Passwort, z. B. eine PIN, eine biometrische Schablone oder eine Kombination daraus. Der EVG schützt die Vertraulichkeit und Integrität der RAD. Er kann eine Benutzerschnittstelle bereitstellen, um Prüfauthentisierungsdaten (verification authentication data, VAD) direkt vom Benutzer zu empfangen; alternativ kann er die VAD von der Signaturerstellungsanwendung empfangen. Wenn die Signaturerstellungsanwendung bei einer Anfrage VAD vom Benutzer bezieht, übernimmt sie den Schutz der Vertraulichkeit und Integrität dieser Daten.

Ein Zertifizierungsdienstanbieter und ein SSCD-Bereitstellungsdienstanbieter interagieren mit dem EVG in der sicheren Vorbereitungsumgebung, um Vorbereitungsfunktionen auszuführen, die erforderlich sind, bevor die Kontrolle über den EVG an den berechtigten Benutzer übergeben wird. Zu diesen Funktionen können gehören:

- Initialisieren der RAD;
- Erzeugen eines Schlüsselpaars;
- Speichern persönlicher Informationen des berechtigten Benutzers.

Ein typisches Beispiel für eine sichere Signaturerstellungseinheit ist eine Chipkarte. In diesem Fall kann ein Chipkartenendgerät vorhanden sein, das die erforderliche sichere Umgebung zur Behandlung einer Anfrage bezüglich einer Unterzeichnerautorisierung bereitstellt. Eine Signatur kann auf einem Dokument erhalten werden, das von einer Komponente einer Signaturerstellungsanwendung vorbereitet wird, die auf einem mit dem Kartenendgerät verbundenen PC läuft. Nachdem das Dokument dem Benutzer dargestellt und die Autorisierungs-PIN bezogen wurde, leitet die Signaturerstellungsanwendung durch das Endgerät die elektronische Signaturerstellungsfunktion der Chipkarte ein.