

DIN EN 14169-4

ICS 03.160; 35.040; 35.240.15

Einsprüche bis 2010-10-16

Entwurf

**Schutzprofile für Sichere Signaturerstellungseinheiten –
Teil 4: Erweiterung für Einheiten mit Schlüsselgenerierung und
vertrauenswürdigen Kanal zur Zertifizierung von
Generierungsanwendungen;
Deutsche Fassung prEN 14169-4:2010**

Protection Profiles for Secure Signature Creation Device –
Part 4: Extension for device with key generation and trusted communication with certificate
generation application;
German version prEN 14169-4:2010

Profils de protection pour dispositif sécurisé de création de signature électronique –
Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée
avec l'application de génération de certificats;
Version allemande prEN 14169-4:2010

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2010-08-16 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 als Datei per E-Mail an nia@din.de 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 online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de, sofern dort wiedergegeben;
- 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 29 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (prEN 14169-4:2010) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR (Frankreich) gehalten wird.

Der zuständige deutsche Arbeitsausschuss ist der NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN.

Schutzprofile für sichere Signaturerstellungseinheiten — Teil 4: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigen Kanal zur Zertifizierung von Generierungsanwendungen

Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 4 : Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats

Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.3a

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	6
4.2 Überblick über das Schutzprofil.....	6
4.3 Überblick über den Evaluationsgegenstand.....	7
5 Konformität.....	13
5.1 CC-Konformität	13
5.2 Schutzprofil-Konformität, Paket-Konformität	13
5.3 Begründung der Konformität	13
5.4 Konformitätsangabe	14
6 EVG-Sicherheitsumgebung	14
6.1 Bedrohungen der Sicherheit	15
6.2 Organisatorische Sicherheitsvorgaben	15
6.3 Annahmen	15
7 Sicherheitsziele.....	15
7.1 Sicherheitsziele für den EVG	15
7.2 Sicherheitsziele für die Einsatzumgebung	15
7.3 Begründung der Sicherheitsziele.....	16
8 Erweiterte Komponentendefinition	18
8.1 Definition der Familie FIA_API	18
9 Sicherheitsanforderungen	19
9.1 Allgemeines	19
9.2 Funktionale Sicherheitsanforderungen	19
9.3 Anforderungen an die Vertrauenswürdigkeit der EVG-Sicherheit	22
10 Begründung.....	22
10.1 Begründung der Sicherheitsanforderungen	22
10.2 Begründung der Abhängigkeiten der funktionalen Sicherheitsanforderungen	24
10.3 Begründung für Vertrauenswürdigkeitsstufe 4 Augmentiert.....	26
Literaturhinweise	27

Vorwort

Dieses Dokument (prEN 14169-4:2010) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument ersetzt CEN/CWA 14169.

Einleitung

Diese Europäische Normenreihe legt 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 14169:2002, Anhang C, zu Schutzprofilen sicherer Signaturerstellungseinheiten, „EAL 4+“, herausgegeben.

Diese Europäische Normenreihe besteht aus den folgenden Teilen:

- *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 1: Überblick;*
- *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 2: Geräte mit Schlüsselerzeugung;*
- *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 3: Einheiten mit Schlüsselimport;*
- *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 4: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigen Kanal zur Zertifizierung von Generierungsanwendungen;*
- *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 5: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigen Kanal zur Signatur von Generierungsanwendungen;*
- *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur Signatur von Generierungsanwendungen.*

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

Schriftverkehr und Kommentare zu diesem Schutzprofil für sichere Signaturerstellungseinheiten (PP SSCD mit Schlüsselgenerierung) sollten an folgende Stelle gerichtet werden:

KONTAKTADRESSE

CEN/ISSS Secretariat
Avenue Marnix 17
1000 Brussels
Belgien

Tel +32 2 550 0813
Fax +32 2 550 0966

E-Mail iss@cenorm.be

1 Anwendungsbereich

Diese Europäische Norm legt ein Schutzprofil für eine sichere Signaturerstellungseinheit fest, die Signaturschlüssel intern erzeugen kann: Sichere Signaturerstellungseinheit mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung.

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).

EN 14169-1¹⁾, *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick*¹⁾

EN 14169-2, *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 2: Geräte mit Schlüsselerzeugung*¹⁾

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, CCMB-2009-07-001, July 2009

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, CCMB-2009-07-002, July 2009

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, CCMB-2009-07-003, July 2009

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 den Common Criteria 3.1 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/müssen“ oder „ist/sind zu“ gekennzeichnet.

3.2 Begriffe

Für die Anwendung dieses Dokuments gelten die Akronyme und Begriffe nach EN 14169-1 [6].

4 Einführung in Schutzprofile

Der vorliegende Abschnitt bietet Informationen zum Dokumentenmanagement und gibt einen Überblick. Unterabschnitt 4.2 „Schutzprofilreferenz“ nennt die Kennung und weitere beschreibende Informationen, die notwendig sind, um dieses Schutzprofil in ein Register einzutragen. Unterabschnitt 4.3 „Überblick über das Schutzprofil“ stellt den Zweck dieses Schutzprofils im Kontext zusätzlicher Schutzprofile für erweiterte Sicherheitsanforderungen vor. Dieser Abschnitt soll als unabhängiger Auszug verwendet werden können, zum Beispiel in einem PP-Register. Unterabschnitt 4.4 „Überblick über den EVG“ enthält eine formlose Beschreibung der Funktionen des EVG und fasst die Sicherheitsanforderungen zusammen. Weiterhin soll dieser Abschnitt Implementierern als Grundlage für den formlosen Beschreibungsteil in CC-Dokumenten auf der Basis dieses Schutzprofils dienen.

1) Noch zu veröffentlichen.

4.1 Schutzprofilreferenz

Titel:	Schutzprofil für sichere Signaturerstellungseinheit mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung
Version:	0.7
Autor:	CEN/CENELEC (TC 224/WG 17)
Veröffentlichungsdatum:	(noch nicht festgelegt)
Registrierung:	BSI-CC-PP-00xx
CC-Version:	3.1 Revision 3
Bearbeiter:	Wolfgang Killmann, T-System GEI GmbH
Allgemeiner Status:	interner Entwurf
Schlüsselwörter:	sichere Signaturerstellungseinheit, elektronische Signatur, digitale Signatur

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 die in Anhang III **der Richtlinie** definierten funktionalen Sicherheitsanforderungen und Anforderungen an die Vertrauenswürdigkeit für eine sichere Signaturerstellungseinheit (secure signature creation device, SSCD) auf formale Weise fest. Diese sichere Signaturerstellungseinheit ist der Evaluationsgegenstand (EVG) dieses Schutzprofils.

Für ein Produkt zur Erstellung sicherer Signaturen, für das die Evaluation nach den Common Criteria (Version 3.1) eine Übereinstimmung mit einem Sicherheitsziel (Security Target, ST) ergeben hat und das diesem Schutzprofil entspricht, müssen die Mitglieder der Europäischen Union nach dieser Europäischen Norm davon ausgehen, dass Übereinstimmung mit den Anforderungen von Anhang III **der Richtlinie** vorliegt.

Dieses Schutzprofil beschreibt die grundlegenden Sicherheitsanforderungen an eine sicheres Gerät, das einen Signaturschlüssel³⁾ erzeugen kann [Signaturstellungsdaten (signature creation data), SCD] und mit dem erzeugten Schlüssel elektronische Signaturen erstellt. Ein Gerät, das nach diesem Schutzprofil evaluiert wurde und das in den festgelegten Umgebungen eingesetzt wird, ist hinreichend vertrauenswürdig, um jede Art von digitaler Signatur zu erstellen. Somit kann dieses Schutzprofil für jedes Gerät verwendet werden, das für die Erstellung einer digitalen Signatur konfiguriert wurde. Speziell erlaubt dieses Schutzprofil, ein Produkt als ein Gerät zur Erstellung einer in **der Richtlinie** definierten fortgeschrittenen elektronischen Signatur zu qualifizieren.

2) Diese EG-Richtlinie wird im Folgenden als „**die Richtlinie**“ bezeichnet.

3) Eine sichere Signaturerstellungseinheit, die ihr eigenen SCD/SVD erstellen kann, wird als SSCD vom Typ 3 bezeichnet, um sie von dem in der vorherigen Version dieses Schutzprofils (CWI 14160) definierten Typ 1 und Typ 2 zu unterscheiden. Das Schutzprofil für eine SSCD vom Typ 2 findet sich in EN 14169-5, *Schutzprofil für sichere Signaturerstellungseinheiten — Teil 5: Einheiten mit Schlüsselimport*.

Dieses Schutzprofil für sichere Signaturerstellungseinheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung (PP SSCD KG TCCGA) definiert die grundlegenden Sicherheitsanforderungen an SSCD vom Typ 3 zur Erzeugung von Signaturerstellungsdaten (SCD) und zur Erstellung fortgeschrittener elektronischer Signaturen, die, sofern sie auf gültigen qualifizierten Zertifikaten basieren, als qualifizierte elektronische Signaturen gelten, wie im grundlegenden Schutzprofil beschrieben [7]. Zusätzlich unterstützt der EVG des aktuellen Schutzprofils dessen Authentisierung als SSCD durch die Zertifikaterzeugungsanwendung (certificate-creation application, CGA) des Zertifizierungsdiensteanbieters (Certification service provider, CSP) und einen vertrauenswürdigen Kanal mit dieser CGA zum Schutz der vom EVG erzeugten und exportierten und von der CGA importierten Signaturprüfdaten (Signature-verification data, SVD). Diese Sicherheitsmerkmale ermöglichen einen geänderten Lebenszyklus des EVG. Das aktuelle Schutzprofil entspricht dem Basis-Schutzprofil für SSCD mit Schlüsselerzeugung [7]. Die eigentliche Bedeutung dieser Konformität wird in 5.3 „Begründung der Konformität“ 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 Abschnitt bietet einen funktionsbezogenen Überblick über den EVG in seinen einzelnen Einsatzumgebungen:

- der Signierumgebung, in der er durch eine Signaturerstellungsanwendung (signature creation application, SCA) mit einem Unterzeichner interagiert, um Daten zu signieren, nachdem der Unterzeichner als Unterzeichnender authentisiert wurde. Die Signaturerstellungsanwendung stellt die zu signierenden Daten oder eine eindeutige Darstellung derselben (DTBS/R) als Eingabe für die EVG-Signaturerstellungsfunktion bereit und bezieht die resultierende digitale Signatur⁴⁾ durch einen vertrauenswürdigen Kanal;
- der Vorbereitungsumgebung, in der er durch eine Zertifikaterzeugungsanwendung (CGA) mit einem Zertifizierungsdiensteanbieter interagiert, um ein Zertifikat für die Signaturprüfdaten (SVD) zu erhalten, die den vom EVG erzeugten Signaturerstellungsdaten (SCD) entsprechen. Der EVG exportiert die Signaturprüfdaten durch einen vertrauenswürdigen Kanal, der es der Zertifikaterzeugungsanwendung ermöglicht die Authentizität der Signaturprüfdaten zu kontrollieren. Weiterhin interagiert die Initialisierungsumgebung mit dem EVG, um diesen mit dem Anfangswert der Referenz-Authentisierungsdaten (reference authentication data, RAD) zu personalisieren;
- der Managementumgebung, in der er mit dem Benutzer oder einem SSCD-Bereitstellungsdiensteanbieter 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. In Bild 4 in Teil 1 [6] dieser Norm ist die Einsatzumgebung dargestellt.

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