

DIN EN 14169-5

ICS 03.160; 35.040; 35.240.15

Einsprüche bis 2010-10-16

Entwurf

**Schutzprofile für Sichere Signaturerstellungseinheiten –
Teil 5: Erweiterung für Einheiten mit Schlüsselgenerierung und
vertrauenswürdigen Kanal zur Signatur von
Generierungsanwendungen;
Deutsche Fassung prEN 14169-5:2010**

Protection Profiles for Secure Signature Creation Device –
Part 5: Device with key generation and trusted communication with signature-creation
application;
German version prEN 14169-5:2010

Profils de protection pour dispositif sécurisé de création électronique –
Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée
avec l'application de création de signature;
Version allemande prEN 14169-5:2010

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 25 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (prEN 14169-5:2010) 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 5: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigen Kanal zur Signatur von Generierungsanwendungen

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

Protection profiles for secure signature creation device — Part 5: Device with key generation and trusted communication with signature-creation 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.....	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 Bedrohungen.....	10
6.2 Organisatorische Sicherheitsvorgaben	11
6.3 Annahmen	11
7 Sicherheitsziele.....	11
7.1 Sicherheitsziele für den EVG	11
7.2 Sicherheitsziele für die Einsatzumgebung	11
7.3 Begründung der Sicherheitsziele.....	12
8 IT-Sicherheitsanforderungen.....	14
8.1 Allgemeines	14
8.2 Funktionale EVG-Sicherheitsanforderungen	14
8.3 Anforderungen an die Vertrauenswürdigkeit der EVG-Sicherheit	18
9 Begründung.....	18
9.1 Begründung der Sicherheitsanforderungen	18
9.2 Begründung der Abhängigkeiten der funktionalen Sicherheitsanforderungen	20
9.3 Begründung für Vertrauenswürdigkeitsstufe 4 Augmentiert.....	22
Literaturhinweise	23

Vorwort

Dieses Dokument (prEN 14169-5:2010) 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 CWA 14169:2004.

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 vertrauenswürdigem Kanal zur Zertifizierung von Generierungsanwendungen;*
- *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 5: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigem Kanal zur Signatur von Generierungsanwendungen;*
- *Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigem 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 Schlüsselerzeugung) 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 und den öffentlichen Schlüssel in geschützter Weise exportieren 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 14169-1, *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.

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 EN 14169-1 [6].

1) Noch zu veröffentlichen.

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. Außerdem soll dieser Abschnitt Implementierern als Grundlage für den formlosen Beschreibungsteil in CC-Dokumenten auf der Basis dieses Schutzprofils dienen.

4.1 Schutzprofilreferenz

Titel:	Schutzprofil für Sichere Signaturerstellungseinheit mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung
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 für sichere Signaturerstellungseinheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal (SSCD/SCA) wurde vom CEN zur Anwendung durch die Europäische Kommission als allgemein anerkannte Norm für Produkte zur Erstellung von elektronischen Signaturen im Amtsblatt der Europäischen Gemeinschaften erstellt, gemäß des Verfahrens, das im Artikel 9 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen [1], im Folgenden als „die Richtlinie“ bezeichnet, dargelegt wurde.

Das Ziel dieses Schutzprofils ist es, die im Anhang III der Richtlinie [1] definierten funktionalen Sicherheitsanforderungen und die Anforderungen an die Vertrauenswürdigkeit für eine sichere Signaturerstellungseinheit (secure signature creation device, SSCD) festzulegen, die der Evaluationsgegenstand (EVG) ist. Die Mitgliedstaaten müssen 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 (Security Target, ST) diesem Schutzprofil entspricht.

Dieses Schutzprofil für sichere Signaturerstellungseinheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal SSCD/SCA (PP SSCD KG TCSCA) enthält die Sicherheitsanforderungen an SSCD mit Schlüsselerzeugung, die Signaturerstellungsdaten [signature-creation-data, SCD] und eine digitale Signatur erzeugen kann, um für die im Basis-Schutzprofil [7] beschriebenen (qualifizierten oder fortgeschrittenen) elektronischen Signaturen verwendet zu werden. Zusätzlich unterstützt der Evaluationsgegenstand (EVG) des aktuellen 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 [7]. Die eigentliche Bedeutung dieses Konformitätsanspruches wird im Unterabschnitt 5.3 „Begründung der Konformität“ erläutert.

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