

DIN EN 14169-1

ICS 35.240.15

Einsprüche bis 2011-07-16

Entwurf**Schutzprofile für Sichere Signaturerstellungseinheiten –
Teil 1: Überblick;
Deutsche Fassung prEN 14169-1:2011**

Protection Profile for Secure Signature Creation Device –
Part 1: Overview;
German version prEN 14169-1:2011

Dispositif sécurisé de signature électronique –
Partie 1: Présentation générale;
Version allemande prEN 14169-1:2011

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2011-05-09 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 24 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (prEN 14169-1:2011) 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 AA „IT-Sicherheitsverfahren“ im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN.

Schutzprofile für Sichere Signaturerstellungseinheiten — Teil 1: Überblick

Profiles de Protection pour Dispositif sécurisé de signature électronique — Partie 1 : Présentation générale

Protection Profiles for Secure Signature Creation Device — Part 1: Overview

ICS:

Deskriptoren

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

STD Version 2.4a

Inhalt

Seite

Vorwort	3
Einleitung.....	3
1 Anwendungsbereich	4
2 Normative Verweisungen.....	4
3 Begriffe	4
3.1 Verweisung auf EG-Richtlinie.....	4
3.2 Fachbegriffe	4
4 Abkürzungen	8
5 Schutzprofile im Überblick	8
6 Evaluationsgegenstand	9
6.1 Allgemeines.....	9
6.2 Funktionen einer SSCD	10
6.2.1 Kernfunktionen	10
6.2.2 Zusätzliche Funktionen	10
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.....	14
7 EVG-Definitionen	16
7.1 EVG mit Schlüsselerzeugung.....	16
7.2 EVG mit Schlüsselimport.....	16
7.3 EVG mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung	16
7.4 EVG mit vertrauenswürdigen Kanal zur Signaturerstellungsanwendung.....	17
Anhang A (informativ) Vergleich mit CWA 14168:2001, Anhang C	20
A.1 Allgemeines.....	20
A.2 Technische Unterschiede	20
Literaturhinweise	21
Stichwortverzeichnis	22

Vorwort

Dieses Dokument (prEN 14169-1:2011) 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:

- *Teil 1: Überblick;*
- *Teil 2: Geräte mit Schlüsselerzeugung;*
- *Teil 3: Geräte mit Schlüsselimport;*
- *Teil 4: Erweiterung für Geräte mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikat-erzeugungsanwendung;*
- *Teil 5: Erweiterung für Geräte mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Signatur-erstellungsanwendung;*
- *Teil 6: Erweiterung für Geräte mit Schlüsselimport und vertrauenswürdigen Kanal zur Signatur-erstellungsanwendung.*

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 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 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 eine 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 kann

ANMERKUNG 1 Zertifikatinformationen sind:

- entweder 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.

ANMERKUNG 2 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 bzw. deren eindeutige Darstellung

DTBS/R

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

ANMERKUNG DTBS/R sind:

- entweder 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-Bereitstellungsdiensteanbieter in den Besitz der sicheren Signaturerstellungseinheit gelangt und von der sicheren Signaturerstellungseinheit als deren Unterzeichner authentisiert werden kann

3.2.11

qualifiziertes Zertifikat

Public-Key-Zertifikat (Zertifikat über einen öffentlichen Schlüssel), das die Anforderungen des **Anhangs I** erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des **Anhangs II** erfüllt (**Richtlinie: 2.10**)

3.2.12

qualifizierte elektronische Signatur

fortgeschrittene elektronische Signatur, die mit einer sicheren Signaturerstellungseinheit mit einem Schlüssel mit qualifiziertem Zertifikat erstellt werden muss

ANMERKUNG Siehe **Richtlinie: 5.1**.

3.2.13

Referenz-Authentisierungsdaten

RAD

dauerhaft vom Evaluationsgegenstand gespeicherte Daten zur Authentisierung eines Benutzers als für eine bestimmte Rolle autorisiert

3.2.14

sichere Signaturerstellungseinheit

SSCD

SSEE

personalisierte Einheit, die die Anforderungen von **Anhang III** erfüllt, indem sie anhand eines Sicherheitsziels evaluiert wird, das einem Schutzprofil dieser Europäischen Normenreihe entspricht (**Richtlinie: 2.5** und **2.6**)

3.2.15

Unterzeichner

rechtmäßiger Benutzer einer sicheren Signaturerstellungseinheit, der dieser im Zertifikat der Signaturprüfdaten zugeordnet ist und der von der sicheren Signaturerstellungseinheit autorisiert ist, die Signaturerstellungsfunktion anzuwenden (**Richtlinie: 2.3**)

3.2.16

Signaturattribute

zusätzliche Informationen, die zusammen mit einer Benutzernachricht signiert werden

3.2.17

Signaturerstellungsanwendung

SCA

Anwendung, die eine sichere Signaturerstellungseinheit um eine Benutzerschnittstelle mit dem Zweck der Erstellung einer elektronischen Signatur ergänzt

ANMERKUNG Eine Signaturerstellungsanwendung ist Software, die aus einer Sammlung von Anwendungskomponenten besteht, die so konfiguriert sind, dass sie

- die zu signierenden Daten (DTBS) dem Unterzeichner zwecks Überprüfung anzeigen;
- vor dem Signiervorgang eine Entscheidung vom Unterzeichner einholen;
- eine eindeutige Darstellung der zu signierenden Daten (DTBS/R) an den Evaluationsgegenstand senden, wenn der Unterzeichner durch eine bestimmte eindeutige Eingabe oder Aktion seine Signierabsicht bekundet;
- die von der sicheren Signaturerstellungseinheit erzeugte elektronische Signatur auf geeignete Weise verarbeiten, z. B. als Anhang an die DTBS.