

DIN ISO 14533-1

ICS 35.240.60

Einsprüche bis 2015-01-12

Entwurf**Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung –****Langzeit-Signaturprofile –****Teil 1: Langzeit-Signaturprofile für CMS-erweiterte elektronische Signaturen (CAeS) (ISO/DIS 14533-1:2014)**

Processes, data elements and documents in commerce, industry and administration –
Long term signature profiles –

Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAeS)
(ISO/DIS 14533-1:2014)

Processus, éléments d'informations et documents dans le commerce, l'industrie et
l'administration –

Profils de signature à long terme –

Partie 1: Profils de signature à long terme pour les signatures électroniques avancées
CMS (CAeS) (ISO/DIS 14533-1:2014)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-09-12 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 online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst 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 in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 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 23 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

Seite

Nationales Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	4
2 Normative Verweisungen	4
3 Begriffe	4
4 Symbole	7
5 Anforderungen	7
6 Langzeit-Signaturprofile	8
6.1 Definierte Profile	8
6.2 Darstellung der Anforderungsstufe	8
6.3 Vorgaben für die Festsetzung der Anforderungsstufe	8
6.4 Zu ergreifende Maßnahmen, wenn ein optionales Element nicht implementiert ist	9
6.5 CAdES-T-Profil	9
6.5.1 Allgemeines	9
6.5.2 Inhaltsinformation	10
6.5.3 Signierte Daten und Unterzeichnerinformation	10
6.5.4 Signiertes Attribut und unsigniertes Attribut	11
6.6 CAdES-A-Profil	12
6.6.1 Allgemeines	12
6.6.2 Struktur des CAdES-A-Profils	12
6.6.3 Zusätzliche unsignierte Attribute	12
6.7 Zeitstempel-Prüfdaten	14
Anhang A (normativ) Konformitätserklärung des Lieferanten mit den zugehörigen Anlagen	16
A.1 Allgemeines	16
A.2 Vordruck der Konformitätserklärung des Lieferanten	16
A.3 Vordruck der Anlage zur Konformitätserklärung des Lieferanten	17
A.3.1 Allgemeines	17
A.3.2 Zu zitierende Versionsnummer von ETSI TS 101 733	17
A.3.3 Anwendungsbereich der Profilimplementierung	17
A.3.4 Konformität mit dem CAdES-T-Profil	17
A.3.5 Konformität mit dem CAdES-A-Profil	19
A.3.6 Spezifikationen, auf die durch „bedingte“ Elemente zu verweisen ist	20
A.3.7 Bemerkungen	20
Anhang B (normativ) Struktur von Zeitstempel-Token	21
B.1 Allgemeines	21
B.2 Normative Spezifikationen	21
B.3 Anforderungsstufe von Einzelelementen	21
Literaturhinweise	23

Nationales Vorwort

Die vorliegende Norm enthält die deutsche Übersetzung der ISO/DIS 14533-1:2014, die vom Technischen Komitee ISO/TC 154 „Processes, data elements and documents in commerce, industry and administration“ unter Beteiligung deutscher Experten erarbeitet wurde. Im DIN Deutsches Institut für Normung e. V. ist hierfür der Normenausschuss Informationstechnik und Anwendungen (NIA), Arbeitsausschuss NA 043-03-03 AA „Elektronisches Geschäftswesen“ zuständig.

Die Festlegungen der ISO/DIS 14533-1 wurden sachlich unverändert in diese Deutsche Norm übernommen. Um eine Verfälschung der für die Signaturprofile festgelegten Elemente und/oder Attribute in der deutschen Übersetzung zu vermeiden, wurden diese in Englisch belassen. Zudem verfügt die mit dieser Norm angesprochene IT-Zielgruppe üblicherweise über ausreichende Englischkenntnisse.

Die Normenreihe DIN ISO 14533 unter dem allgemeinen Titel *Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung — Langzeit-Signaturprofile* besteht aus folgenden Teilen:

- Teil 1: Langzeit-Signaturprofile für CMS-erweiterte elektronische Signaturen (CAAdES)
- Teil 2: Langzeit-Signaturprofile für XML-erweiterte elektronische Signaturen (XAdES)

Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung — Langzeit-Signaturprofile — Teil 1: Langzeit-Signaturprofile für CMS-erweiterte elektronische Signaturen (CAAdES)

Einleitung

Der Zweck des vorliegenden Teils von ISO 14533 ist die Sicherstellung der Interoperabilität von Implementierungen in Bezug auf Langzeitsignaturen, mit denen elektronische Signaturen für eine lange Zeit nachprüfbar bleiben. Die in der jeweiligen Implementierung bezeichneten Spezifikationen von Langzeitsignaturen betreffen vom Europäischen Institut für Telekommunikationsnormen (en: European Telecommunications Standards Institute, ETSI) entwickelte CMS-erweiterte elektronische Signaturen (en: CMS Advanced Electronic Signatures, CAAdES).

1 Anwendungsbereich

Der vorliegende Teil von ISO 14533 legt unter den in CMS-erweiterten elektronischen Signaturen (CAAdES) definierten Elementen diejenigen Elemente fest, die die Prüfung einer digitalen Signatur über eine lange Zeitspanne möglich machen.

Es werden weder neue technische Spezifikationen für die digitale Signatur selbst noch neue Einschränkungen für die Anwendung der technischen Spezifikationen von bereits vorhandenen digitalen Signaturen angegeben.

ANMERKUNG CMS-erweiterte elektronische Signaturen (CAAdES) stellen die erweiterte Spezifikation der weit verbreiteten kryptografischen Nachrichtensyntax (en: Cryptographic Message Syntax, CMS) dar.

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).

ETSI TS 101 733 v2.2.1 (2013-04), *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)*¹⁾

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1 Langzeitsignatur
Signatur, die über eine lange Zeitspanne nachprüfbar ist, indem Mittel wie die Signierzeit, der Gegenstand der bezeichneten Signatur und die Prüfdaten implementiert werden, mit denen unzulässige Änderungen der Signaturinformation festgestellt werden können

¹⁾ Zu beziehen unter <http://pda.etsi.org/pda/queryform.asp> (siehe nachfolgende Versionen wie ETSI EN 319 122)

3.2

Profil

Vorschrift, mit der die Interoperabilität bezüglich der optionalen Elemente von zitierten Spezifikationen, der Wertebereiche, usw. sichergestellt wird

3.3

Anforderungsstufe

Stufe der Anforderung für die Implementierung der jeweiligen Elemente, die ein Profil bilden

3.4

kryptografische Nachrichtensyntax

CMS (en: Cryptographic Message Syntax)

Syntax für Signatur, Hashwert, Authentifizierung und Verschlüsselung einer gegebenen Nachricht

Anmerkung 1 zum Begriff: Die kryptografische Nachrichtensyntax ist in IETF RFC 5652 festgelegt.

3.5

CMS-erweiterte elektronische Signatur

CAdES (en: CMS Advanced Electronic Signature)

elektronische Signatur nach den Festlegungen in ETSI TS 101 733, für die der Unterzeichner identifiziert und jede unzulässige Änderung von Daten festgestellt werden können

3.6

CAdES mit Zeitangabe

CAdES-T (en: CAdES with Time)

CMS-erweiterte elektronische Signatur nach den Festlegungen in ETSI TS 101 733 mit Informationen zur Ermittlung der Signierzeit

BEISPIEL Signatur-Zeitstempel

3.7

archivierte CAdES

CAdES-A (en: archival CAdES)

CMS-erweiterte elektronische Signatur nach den Festlegungen in ETSI TS 101 733 mit Informationen zur Feststellung unzulässiger Änderungen betreffend der Signatur, einschließlich des Signaturgegenstandes und der Prüfdaten

BEISPIEL Archiv-Zeitstempel

3.8

Inhaltsinformation

Datenstruktur, die den Inhalt in CMS definiert

3.9

signierte Daten

Datenstruktur, die die signierten Daten in CMS oder zugehörige Daten definiert

3.10

Unterzeichnerinformation (en: signerinfo)

Datenstruktur, die die Signaturinformation für jeden Unterzeichner oder zugehörige Daten definiert

3.11

signiertes Attribut

Signaturinformationen, die der Gegenstand einer Signatur sind

3.12

unsigned Attribut

Signaturinformationen, die nicht der Gegenstand einer Signatur sind

Anmerkung 1 zum Begriff: Signatur-Zeitstempel und Archiv-Zeitstempel sind unsignierte Attribute.

3.13

Prüfdaten

Zertifikats- und Sperrinformationen, die für die Gültigkeitsprüfung einer Signatur und eines Zeitstempels genutzt werden

3.14

Zeitstempelstelle

TSA (en: Timestamping Authority)

vertrauenswürdiger Dritter, der damit beauftragt ist, einen Nachweis dafür zu erbringen, dass bestimmte Daten vor einem bestimmten Zeitpunkt vorhanden waren

3.15

Zeitstempel-Token

TST (en: Timestamp Token)

Datenobjekt, das die Darstellung einer Gegebenheit an einen bestimmten Zeitpunkt bindet und damit einen Nachweis dafür erbringt, dass die Gegebenheit vor diesem Zeitpunkt vorhanden war

3.16

Signatur-Zeitstempel

mit einem Signaturwert verknüpfter Zeitstempel zur Ermittlung des Zeitpunkts, seit dem die Signatur vorhanden ist

3.17

Archiv-Zeitstempel

Zeitstempel, der mit zu einer Signatur gehörenden Informationen verknüpft ist, einschließlich des Gegenstands der Signatur und der Prüfdaten, damit unzulässige Änderungen festgestellt werden können

3.18

Vertrauensanker

Ursprung des Vertrauens in Form eines Public-Key-Zertifikats (Zertifikat für einen öffentlichen Schlüssel) oder eines öffentlichen Schlüssels, das bzw. der vom Prüfer zur Prüfung einer elektronischen Signatur benutzt wird, und im Allgemeinen ein Public-Key-Zertifikat, das von einer vertrauenswürdigen Stelle für Wurzelzertifikate ausgegeben wird

3.19

vertrauenswürdige Dritte Partei

TTP (en: Trusted Third Party)

Sicherheitsinstanz oder deren Vertreter, die bzw. der von einer anderen Entität mit Aktivitäten in Bezug auf die Sicherheit betraut wurde

3.20

Zertifizierungsinstanz

CA (en: Certification Authority)

Zentrale, die mit der Erstellung und Zuweisung von Public-Key-Zertifikaten beauftragt ist

Anmerkung 1 zum Begriff: Zertifizierungsstellen können nach ihrem Ermessen Schlüssel erzeugen und diese Entitäten zuweisen.

3.21

Zertifikat

Information über den öffentlich weitergegebenen Schlüssel als Teil eines asymmetrischen Schlüsselpaars für eine Entität, die von einer Zertifizierungsstelle signiert wurde, um Fälschungen zu verhindern

3.22

Attributzertifikat

Zertifikat, das die Tätigkeit, die Qualifizierung, die Stellung und andere Attribute und Attributwerte enthält

3.23

Sperrinformation

von einer Zertifizierungsstelle ausgegebene Information über die Zurückziehung eines Zertifikats innerhalb der Laufzeit

Anmerkung 1 zum Begriff: Diese Information kann abgeglichen werden, um zu ermitteln, ob das Zertifikat noch gilt.

3.24

erweiterter Sicherheitsdienst

ESS (en: Enhanced Security Service)

optionaler erweiterter Dienst in Bezug auf eine Signatur, zu dem unter anderem Informationen zur Kennzeichnung des Unterzeichnerzertifikats (SigningCertificate) und Informationen mit der Angabe des Signaturtyps gehören

4 Symbole

Für die Anforderungsstufe werden folgende Kennbuchstaben benutzt:

- C Bedingt (en: Conditional)
- M Verbindlich (en: Mandatory)
- O Optional (en: Optional)
- P Verboten (Bildung oder Änderung) (en: Prohibited)

5 Anforderungen

5.1 Die Erzeugung oder Gültigkeitsprüfung von CAdES-T-Daten entspricht dem vorliegenden Teil von ISO 14533, sofern die folgenden Anforderungen erfüllt sind:

- a) bei der Verarbeitung müssen alle Elemente einbezogen werden, deren Anforderungsstufe im CAdES-T-Profil nach den Festlegungen im vorliegenden Teil von ISO 14533 als „Verbindlich“ angegeben ist;
- b) es müssen genaue Spezifikationen für die Verarbeitung von Elementen zur Verfügung gestellt werden, deren Anforderungsstufe im CAdES-T-Profil nach den Festlegungen im vorliegenden Teil von ISO 14533 als „Bedingt“ angegeben ist.

5.2 Die Erzeugung oder Gültigkeitsprüfung von CAdES-A-Daten entspricht dem vorliegenden Teil von ISO 14533, sofern die folgenden Anforderungen erfüllt sind:

- a) bei der Verarbeitung müssen alle Elemente einbezogen werden, deren Anforderungsstufe im CAdES-A-Profil nach den Festlegungen im vorliegenden Teil von ISO 14533 als „Verbindlich“ angegeben ist;
- b) es müssen genaue Spezifikationen für die Verarbeitung von Elementen zur Verfügung gestellt werden, deren Anforderungsstufe im CAdES-A-Profil nach den Festlegungen im vorliegenden Teil von ISO 14533 als „Bedingt“ angegeben ist.

5.3 Wenn eine „First-Party“-Konformitätsbewertung angewendet wird, muss der Implementierer eine Konformitätserklärung nach dem vorliegenden Teil von ISO 14533 abgeben, indem die Übereinstimmungserklärung des Lieferanten mit den zugehörigen Anlagen (siehe Anhang A) und einer Beschreibung des Status der Implementierung (und den Spezifikationen für alle mit „Bedingt“ bezeichneten Elemente) offengelegt wird.

ANMERKUNG Bild 1 zeigt die Aufstellung für die Erzeugung und Gültigkeitsprüfung von CAdES-T-Daten und CAdES-A-Daten.