

DIN ISO 14533-2

ICS 35.240.60

Einsprüche bis 2015-01-12

Entwurf**Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung –****Langzeit-Signaturprofile –****Teil 2: Langzeit-Signaturprofile für XML-erweiterte elektronische Signaturen (XAdES) (ISO 14533-2:2012)**

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

Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)
(ISO 14533-2:2012)

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

Profils de signature à long terme –

Partie 2: Profils de signature à long terme pour les signatures électroniques avancées
XML (XAdES) (ISO 14533-2:2012)

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 20 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort	3
Nationaler Anhang NA (informativ) Literaturhinweise	4
Einleitung	5
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Symbole	6
5 Anforderungen	6
6 Langzeit-Signaturprofile	7
6.1 Definierte Profile	7
6.2 Darstellung der Anforderungsstufe	7
6.3 Vorgaben für die Festsetzung der Anforderungsstufe	8
6.4 Zu ergreifende Maßnahmen, wenn ein optionales Element nicht implementiert ist	8
6.5 XAdES-T-Profil	8
6.6 XAdES-A-Profil	10
6.7 Zeitstempel-Prüfdaten	12
Anhang A (normativ) Konformitätserklärung des Lieferanten mit den zugehörigen Anlagen	13
Anhang B (normativ) Struktur von Zeitstempel-Token	18
Literaturhinweise	20

Nationales Vorwort

Die vorliegende Norm enthält die deutsche Übersetzung der ISO 14533-2:2012, 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 14533-2 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.

Für die in diesem Dokument zitierte Internationale Norm wird im Folgenden auf die entsprechende Deutsche Norm hingewiesen:

ISO 14533-1 siehe DIN ISO 14533-1

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 (CAdES)
- Teil 2: Langzeit-Signaturprofile für XML-erweiterte elektronische Signaturen (XAdES)

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO 14533-1, *Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung — Langzeit-Signaturprofile — Teil 1: Langzeit-Signaturprofile für CMS-erweiterte elektronische Signaturen (CAAdES)*

Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung — Langzeit-Signaturprofile — Teil 2: Langzeit-Signaturprofile für XML-erweiterte elektronische Signaturen (XAdES)

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 XML-erweiterte elektronische Signaturen (en: XML Advanced Electronic Signatures, XAdES).

1 Anwendungsbereich

Der vorliegende Teil von ISO 14533 legt unter den in XML-erweiterten elektronischen Signaturen (XAdES) 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 XML-erweiterte elektronische Signaturen (XAdES) stellen die erweiterte Spezifikation der weit verbreiteten XML-Signatursyntax und –verarbeitung (en: XML-Signature Syntax and Processing) 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).

ISO 14533-1, *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 (CAAdES)*

ETSI TS 101 903 v1.4.1 (2009-06), *XML Advanced Electronic Signatures (XAdES)*¹⁾

3 Begriffe

Für die Anwendung dieses Dokuments gelten die in ISO 14533-1 angegebenen und die folgenden Begriffe.

3.1

XML-Signatur

Signatursyntax und –verarbeitung für eine gegebene Nachricht

ANMERKUNG Die XML-Signatur ist in *XML-Signature Syntax and Processing*, W3C Recommendation, 12 February 2002, definiert.

1) Zu beziehen unter <http://pda.etsi.org/pda/queryform.asp>

3.2

XML-erweiterte elektronische Signatur

XAdES (en: XML Advanced Electronic Signature)

Grundbegriff für XML-erweiterte elektronische Signaturen nach den Festlegungen in ETSI TS 101 903, für die der Unterzeichner identifiziert und jede unzulässige Änderung von Daten festgestellt werden können

3.3

XAdES mit Zeitangabe

XAdES-T (en: XAdES with Time)

XML-erweiterte elektronische Signatur nach den Festlegungen in ETSI TS 101 903 mit Informationen zur Ermittlung der Signierzeit (z. B. Signatur-Zeitstempel)

3.4

archivierte XAdES

XAdES-A (en: archival XAdES)

XML-erweiterte elektronische Signatur nach den Festlegungen in ETSI TS 101 903 mit Informationen zur Feststellung unzulässiger Änderungen betreffend der Signatur, einschließlich des Signaturgegenstandes und der Prüfdaten (z. B. Archiv-Zeitstempel)

3.5

Signaturelement

Element, welches als ein Leitweg für die XML-Signatur dient. Für einen Gegenstand einer Signatur kann es zwei oder mehr Signaturelemente geben

4 Symbole

Für die Anforderungsstufe werden folgende Kennbuchstaben benutzt:

- C Bedingt (en: Conditional)
- M Verbindlich (en: Mandatory)
- O Optional (en: Optional)

5 Anforderungen

5.1 Die Erzeugung oder Gültigkeitsprüfung von XAdES-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 XAdES-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 XAdES-T-Profil nach den Festlegungen im vorliegenden Teil von ISO 14533 als „Bedingt“ angegeben ist.

5.2 Die Erzeugung oder Gültigkeitsprüfung von XAdES-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 XAdES-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 XAdES-A-Profil nach den Festlegungen im vorliegenden Teil von ISO 14533 als „Bedingt“ angegeben ist.