

DIN ISO 14533-3



ICS 35.240.63

Einsprüche bis 2017-01-04

Entwurf

**Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung –
Langzeit-Signaturprofile –
Teil 3: Langzeit-Signaturprofile für PDF-erweiterte elektronische Signaturen (PAdES) (ISO/DIS 14533-3:2016);
Text Deutsch und Englisch**

Processes, data elements and documents in commerce, industry and administration –
Long term signature profiles –
Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)
(ISO/DIS 14533-3:2016);
Text in German and English

Processus, éléments d'informations et documents dans le commerce, l'industrie et
l'administration –
Profils de signature à long terme –
Partie 3: Profils de signature à long terme pour les signatures électroniques avancées PDF
(PAdES) (ISO/DIS 14533-3:2016);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-11-04 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.din.de/go/entwuerfe 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/go/stellungnahmen-norm-entwuerfe 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, 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 66 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort.....	4
Einleitung	5
1 Anwendungsbereich.....	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Symbole.....	7
5 Anforderungen	7
6 Langzeit-Signaturprofile.....	8
6.1 Definition des PAdES-Profiles und Positionierung.....	8
6.2 Darstellung der Anforderungsstufe.....	9
6.3 Vorgaben für die Festsetzung der Anforderungsstufe.....	9
6.4 PAdES-T-Profil.....	10
6.4.1 Allgemeines	10
6.4.2 PAdES unter Verwendung des CAdES-Signaturprofils.....	11
6.4.3 Zeitstempel des PAdES-T-Profiles	14
6.5 PAdES-A-Profil.....	14
6.5.1 Allgemeines	14
6.5.2 Struktur des PAdES-A-Profiles.....	15
6.5.3 'Document Security Store'-Verzeichnis	15
6.5.4 'Signature VRI'-Verzeichnis	15
6.5.5 'Document Timestamp'	16
6.5.6 Aktualisierung von PAdES-A.....	16
6.5.7 Prüfdaten für Signatur und Zeitstempel	17
6.6 Mehrfache Signaturen.....	17
6.6.1 Zeitstempel für mehrfache Signaturen.....	18
Anhang A (normativ) Konformitätserklärung des Bereitstellers mit den zugehörigen Anlagen.....	20
A.1 Allgemeines	20
A.2 Vordruck der Konformitätserklärung des Bereitstellers.....	20
A.3 Vordruck der Anlage zur Konformitätserklärung des Bereitstellers	21
A.3.1 Allgemeines	21
A.3.2 Zu zitierende Versionsnummer des Standards	21
A.3.3 Anwendungsbereich der Profilimplementierung	21
A.3.4 Konformität mit dem PAdES-T-Profil.....	21
A.3.5 Konformität mit dem PAdES-A-Profil.....	23
A.3.6 Konformität mit dem PAdES-DT-Profil (Anhang B).....	24
A.3.7 Konformität mit dem PAdES-DTA-Profil (Anhang B)	24
A.3.8 Spezifikationen, auf die durch „Bedingte“ Elemente zu verweisen ist	25
A.3.9 Bemerkungen.....	25
Anhang B (normativ) Profil bei der ausschließlichen Nutzung eines Zeitstempels.....	26
B.1 Allgemeines	26
B.2 PAdES-DT-Profil.....	26
B.2.1 Allgemeines	26
B.2.2 Verzeichnis des Dokument-Zeitstempels	26

B.3	PAdES-DTA-Profil.....	26
B.3.1	Allgemeines	26
Anhang C (normativ) Struktur von Zeitstempel-Token		28
C.1	Allgemeines	28
C.2	Normative Spezifikationen	28
C.3	Anforderungsstufe von Einzelementen.....	28
Anhang D (informativ) Angewendete PAdES mit CMS-Signaturen.....		30
D.1	Allgemeines	30
Anhang E (informativ) Beispiele für mehrfache Signaturen.....		31
E.1	Allgemeines	31
E.2	Beispiel des PAdES-T-Profiles.....	31
E.3	Beispiel des PAdES-A-Profiles.....	32
Literaturhinweise.....		34

Nationales Vorwort

Der vorliegende Norm-Entwurf enthält die deutsche Übersetzung der ISO/DIS 14533-3:2016, der vom Technischen Komitee ISO/TC 154 „Processes, data elements and documents in commerce, industry and administration“ unter Beteiligung deutscher Experten erarbeitet wurde. Von deutscher Seite ist hierfür der DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), Arbeitsausschuss NA 043-03-03 AA „Elektronisches Geschäftswesen“ zuständig.

Die Übernahme der ISO 14533-3 als DIN ISO-Norm wurde u. a. deswegen beschlossen, da hier ein Bezug zur Technischen Richtlinie BSI* TR-03125, *Beweiswerterhaltung kryptographisch signierter Dokumente*, besteht.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der ISO/DIS 14533-3 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Die Festlegungen der ISO/DIS 14533-3 wurden sachlich unverändert in diesen Deutschen Norm-Entwurf 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.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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)*
- Teil 3: *Langzeit-Signaturprofile für PDF-erweiterte elektronische Signaturen (PAdES)*

* BSI = Bundesamt für Sicherheit in der Informationstechnik

Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung — Langzeit-Signaturprofile — Teil 3: Langzeit-Signaturprofile für PDF-erweiterte elektronische Signaturen (PAdES)

Einleitung

Der Zweck dieses 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 PMS-erweiterte elektronische Signaturen (en: PDF Advanced Electronic Signatures, PAdES).

1 Anwendungsbereich

Dieser Teil von ISO 14533 legt unter den in PDF-erweiterten elektronischen Signaturen (PAdES) 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.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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/DIS 32000-2, *Document Management — Portable document format — Part 2: PDF 2.0*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

erweiterte elektronische Signatur

elektronische Signatur, die die folgenden Anforderungen erfüllt:

- a) sie ist eindeutig mit dem Unterzeichner verlinkt;
- b) sie ist in der Lage, den Unterzeichner zu identifizieren;
- c) sie wird mit elektronischen Signaturerstellungsdaten erstellt, die mit hoher Sicherheit unter der alleinigen Kontrolle des Unterzeichners stehen; und
- d) sie wird mit den zu signierenden Daten verknüpft, derart dass eine nachträgliche Änderung der Daten erkannt werden kann.

3.2

Langzeitsignatur

elektronische 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

3.3

Profil

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

3.4

Anforderungsstufe

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

3.5

Prüfdaten

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

3.6

Zeitstempelstelle

TSA

(en: timestamping authority)

vertrauenswürdiger Dritter, dem vertraut wird, einen Zeitstempeldienst zu erbringen

[QUELLE: ISO/IEC 18014-1:2008, 3.17]

3.7

Zeitstempel-Token

TST

(en: timestamp token)

Datenstruktur, die eine überprüfbare Verbindung zwischen der Darstellung eines Datenelements und einem Zeitwert enthält

Anmerkung 1 zum Begriff: Ein Zeitstempel-Token kann auch weitere Datenelemente in der Verbindung enthalten.

[QUELLE: ISO/IEC 18014-1:2008, 3.15]

3.8

Vertrauensanker

Instanz, die von einer verlässlichen Partei betraut wird und die für die Validierung von Zertifikaten in Zertifizierungspfade verwendet wird

3.9

vertrauenswürdige Dritte Partei

TTP

(en: trusted third party)

Sicherheitsinstanz oder deren Vertreter, die bzw. der in Bezug auf einige Sicherheitsaktivitäten betraut wird (im Kontext einer Sicherheits-Policy)

[QUELLE: ISO/IEC 10181-1:1996, 3.3.30 [2]]

3.10

Zertifizierungsstelle

CA

(en: certification authority)

Behörde, die von einer oder mehreren Anwendern betraut ist, Public-Key-Zertifikate zu erzeugen und zuzuweisen

Anmerkung 1 zum Begriff: Wahlweise kann die Zertifizierungsstelle die Schlüssel der vertrauenden Parteien erzeugen.

[QUELLE: ISO/IEC 9594-8:2014, 3.5.16 [1]]

3.11

Zertifikat (Public-Key-Zertifikat)

öffentlicher Schlüssel eines Anwenders, der zusammen mit einigen anderen Informationen durch digitale Signatur mit dem privaten Schlüssel der Zertifizierungsstelle (en: certification authority, CA), von der er herausgegeben wurde, fälschungssicher gestaltet wird

[QUELLE: ISO/IEC 9594-8:2014, 3.5.53 [1]]

3.12

Attributzertifikat

von einer Attributinstanz digital signierte Datenstruktur, die einige Attributwerte mit den Identifikationsinformationen über den Halter verbindet

[QUELLE: ISO/IEC 9594-8:2014, 3.5.1 [1]]

3.13

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.

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 PAdES-T-Daten entspricht diesem Teil von ISO 14533, sofern die folgenden Anforderungen erfüllt sind:

- a) bei der Verarbeitung müssen alle Elemente einbezogen werden, deren Anforderungsstufe im PAdES-T-Profil nach den Festlegungen in diesem 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 PAdES-T-Profil nach den Festlegungen in diesem Teil von ISO 14533 als „Bedingt“ angegeben ist.

5.2 Die Erzeugung oder Gültigkeitsprüfung von PAdES-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 PAdES-A-Profil nach den Festlegungen in diesem 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 PAdES-A-Profil nach den Festlegungen in diesem Teil von ISO 14533 als „Bedingt“ angegeben ist.

5.3 Sofern eine „First-Party“-Konformitätsbewertung angewendet wird, muss der Implementierer eine Konformitätserklärung nach diesem Teil von ISO 14533 abgeben, indem die Übereinstimmungserklärung des Bereitstellers 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 Siehe ISO/IEC 17050-1:2004, Conformity assessment - Supplier's declaration of conformity - Part 1: General requirements.

6 Langzeit-Signaturprofile

6.1 Definition des PAdES-Profils und Positionierung

Um elektronische Signaturen für eine lange Zeit nachprüfbar zu machen, muss die Signierzeit feststellbar sein, jegliche unzulässigen Änderungen von zur Signatur gehörenden Informationen einschließlich des Gegenstands von Informationen und Prüfdaten müssen erkennbar sein und es muss die Interoperabilität sichergestellt sein. Um diese Anforderungen zu erfüllen, werden in diesem Teil von ISO 14533 die folgenden beiden Profile für PAdES definiert:

- a) das PAdES-T-Profil: ein Profil, welches die Erzeugung und Gültigkeitsprüfung der Signatur mit einem Zeitstempel für die Signatur betrifft. Der Zeitstempel wird in einem Zeitstempel-Attribut der Signatur oder in irgendein nachfolgendes Objekt gespeichert, das den Zeitstempel für die Signatur enthält. Das nachfolgende Objekt ist ein dokumentenbezogener Zeitstempel oder eine Signatur mit dem Zeitstempel-Attribut der Signatur.
- b) das PAdES-A-Profil: ein Profil, welches die Erzeugung und Gültigkeitsprüfung der Langzeit-Verfügbarkeit und Integrität des Prüfmaterials betrifft, die die PAdES-T-Daten einschließlich die Prüfdaten von jeder unzulässigen Änderung schützen.

Bild 1 zeigt die Beziehung zwischen PAdES-T-Daten und PAdES-A-Daten.

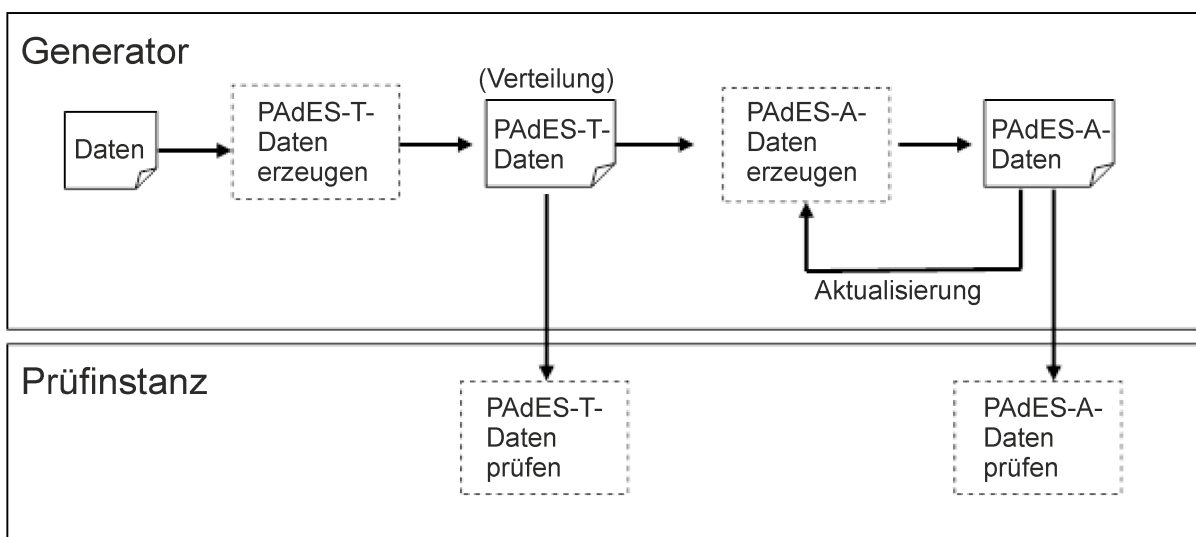


Bild 1 — Beziehung zwischen PAdES-T-Daten und PAdES-A-Daten

6.2 Darstellung der Anforderungsstufe

Dieser Teil von ISO 14533 legt die folgenden Darstellungsmethoden für die Anforderungsstufe (als ein Profil) für jedes Element fest, das PAdES-T-Daten und PAdES-A-Daten darstellt.

- a) Verbindlich (M): Elemente mit der Anforderungsstufe „Verbindlich“ müssen ausnahmslos implementiert werden. Besitzt ein solches Element optionale Unterelemente, muss wenigstens ein Unterelement ausgewählt werden. Jedes Element mit der Anforderungsstufe „Verbindlich“, welches ein Unterelement eines optionalen Elements ist, muss immer ausgewählt werden, wenn das optionale Element ausgewählt wird.
- b) Optional (O): Elemente mit der Anforderungsstufe „Optional“ dürfen nach dem Ermessen des Implementierers implementiert werden.
- c) Bedingt (C): Elemente mit der Anforderungsstufe „Bedingt“ dürfen nach dem Ermessen des Implementierers implementiert werden, sofern genaue Spezifikationen für die Verarbeitung dieser Elemente gesondert zur Verfügung gestellt werden.
- d) Verboten (P): Elemente mit der Anforderungsstufe „Verboten“ dürfen nicht gebildet oder geändert werden, sie dürfen nur gelesen werden.

6.3 Vorgaben für die Festsetzung der Anforderungsstufe

Die Anforderungsstufe für jedes Element, das PAdES-T-Daten und PAdES-A-Daten darstellt, muss nach folgenden Anforderungen festgesetzt werden:

- a) Die Anforderungsstufe muss für Elemente „Verbindlich“ sein, deren Anforderungsstufe in der Definition der PAdES „Verbindlich“ ist und die für die Erzeugung und Gültigkeitsprüfung von Langzeitsignaturen erforderlich sind. Die Elemente, deren Anforderungsstufe in der Definition der PAdES „Optional“ ist, werden als „Verbindlich“, „Optional“ oder „Bedingt“ definiert.

- b) Für alle extern definierten Elemente muss die Anforderungsstufe „Bedingt“ sein.

BEISPIEL 1 OtherCertificateFormat

- c) Für Elemente, die für eine Interaktion mit einer bestimmten Anwendung vorgesehen sind, muss die Anforderungsstufe „Bedingt“ sein.

BEISPIEL 2 CommitmentType

- d) Für Elemente mit einem einsatzabhängigen Faktor muss die Anforderungsstufe „Bedingt“ sein.

BEISPIEL 3 Attribute certificate, time mark

ANMERKUNG Der in ISO/IEC 18014-2 definierte Archivierungszeitstempel ist in „Time mark oder andere Methode“ enthalten.

- e) Für Elemente, die nur Referenzinformationen enthalten, muss die Anforderungsstufe „Optional“ sein.

6.4 PAdES-T-Profil

6.4.1 Allgemeines

Das PAdES-Profil ist als die Form einer elektronischen Signatur definiert, bei der der Signatur-Wert durch jedes nachfolgende Objekt geschützt wird, das vertrauenswürdige Belege als Beweis der Existenz enthält (z. B. document timestamp).

Das PAdES-T wird, wie in 6.4.2 festgelegt, durch PAdES unter Verwendung der CAdES-Signaturen erweitert. Die Anforderungsstufen der Einzelemente des ‚PAdES verwendet CAdES-Signaturen‘ sind ebenfalls in 6.4.2 festgelegt.

Die folgenden drei Typen sind definiert als Formen des PAdES-T-Profiles.

- PAdES-T mit ‚Document Timestamp‘
- PAdES-T mit ‚Signature Timestamp‘-Attribut
- PAdES-T mit ‚Subsequent Signature‘ mit ‚Signature Timestamp‘-Attribut

Diese Formen werden in den Bildern 2 bis 4 dargestellt.

Die Anforderungsstufen der PAdES-T-Profile werden in 6.4.3 festgelegt.

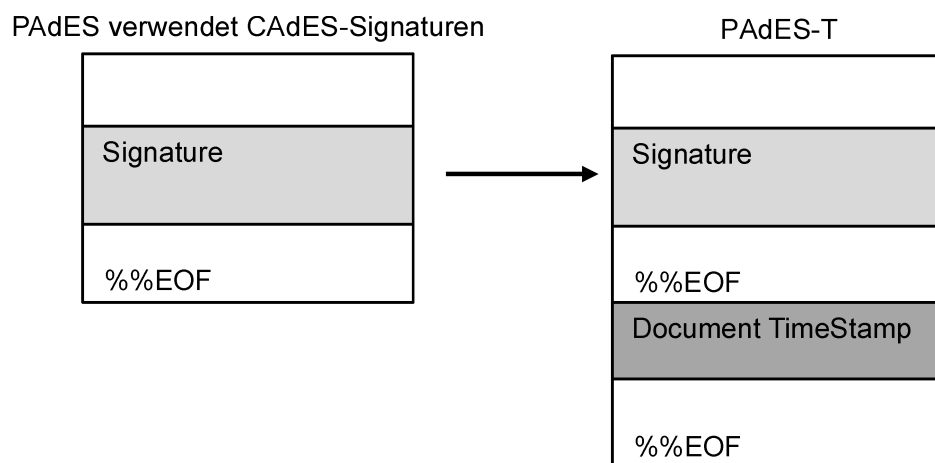


Bild 2 — PAdES-T-Profil mit ‚Document Timestamp‘

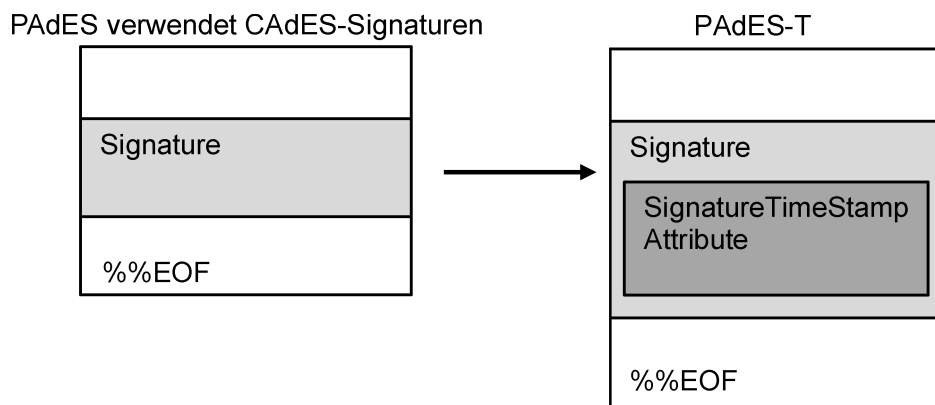


Bild 3 — PAdES-T-Profil mit ‚Signature Timestamp‘-Attribut

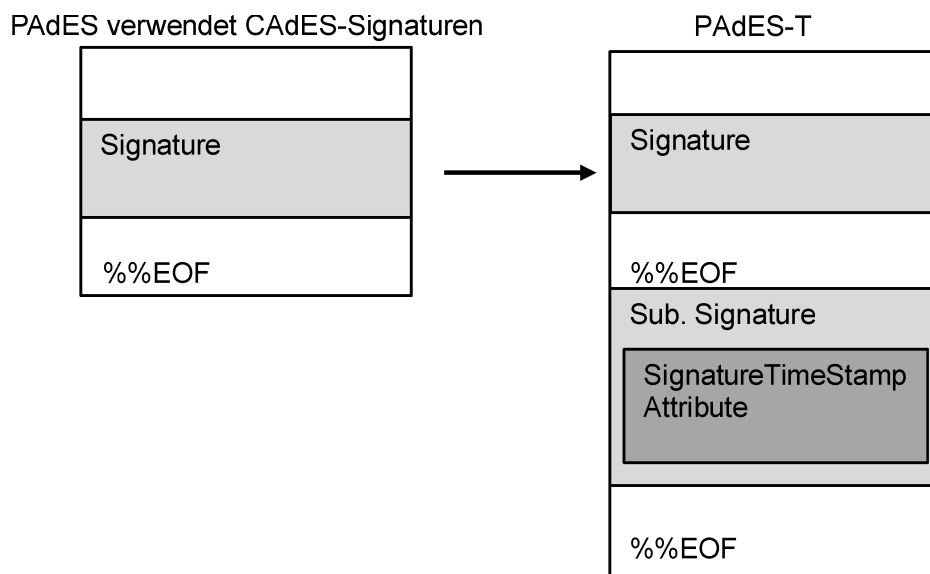


Bild 4 — PAdES-T-Profil mit ‘Subsequent Signature’ mit ‘Signature Timestamp’-Attribut

6.4.2 PAdES unter Verwendung des CAdES-Signaturprofils

In Tabelle 1 sind die Anforderungsstufen der Einträge festgelegt, die das Signaturverzeichnis von PAdES unter Verwendung des CAdES-Signaturprofils bilden. Das nicht angegebene Element wird mit C (Bedingt) angesetzt.

Tabelle 1 — Signaturverzeichnis von PAdES unter Verwendung der CAdES-Signaturen

Eintrag	Anforderungsstufe	Wert
Type	O	Sig
Filter	M	
SubFilter	M	ETSI.CAdES.detached
Contents	M	siehe Tabelle 2
ByteRange	M	
M	M ^a	
Cert	P	
Location	O	
Reason	O	
ContactInfo	O	

^a Auch wenn eine Signatur den M-Eintrag nicht enthält, darf die Signaturprüfanwendung diese Signatur nicht als ungültig betrachten. Die Zeit des M-Eintrages wird nicht grundsätzlich verwendet, um Zertifikate zu validieren. Wenn diese Information für die Validierung verwendet wird, ist es notwendig, eine eindeutige Nutzung dieser Information zu definieren (z. B. Beschreibung einer Verwendung in einer Signaturrichtlinie).

Tabelle 2 legt die Anforderungsstufen der Elemente fest, die die Inhaltsinformation in den Signaturdaten bilden.

Tabelle 2 — Inhaltsinformation in der Signatur

Element	Anforderungsstufe	Value
ContentType	M	id-signedData
Content	M	See Table 3

Tabelle 3 legt die Anforderungsstufen der Elemente fest, die die signierten Daten in den Signaturdaten bilden. Ein DER-verschlüsseltes 'SignedData'-Objekt, wie in CMS festgelegt, muss als PDF-Signatur im Eintrag mit dem Schlüssel 'Content' des Signaturverzeichnisses nach ISO 32000-2 enthalten sein.

Tabelle 3 — Signierte Daten in der Signatur

Element	Anforderungsstufe
CMSVersion	M
DigestAlgorithmIdentifiers	M
EncapsulatedContentInfo	M
- eContentType	M
- eContent	O
CertificateSet (Certificates)	M
- certificate	M ^a
- v2AttrCert	P
- other	C
RevocationInfoChoices (crls)	O
- crl	O
- other	C
SignerInfos	M ^b
- signerInfo	M
^a Zumindest eine Signaturgeneratoranwendung muss ein Unterzeichner-Zertifikat zur Interoperabilität enthalten. Auch wenn eine Unterschrift dieses Element nicht enthält, darf die Signaturprüfanwendung diese Signatur nicht als ungültig betrachten.	
^b Nur eine einzelne 'SignerInfo' darf in der PDF-Signatur auftreten.	

Tabelle 4 legt die Anforderungsstufen der Elemente fest, die die Unterzeichnerinformation in den Signaturdaten bilden.

Tabelle 4 — Unterzeichnerinformation in der Signatur

Element	Anforderungsstufe
CMSVersion	M
SignerIdentifier	M
- issuerAndSerialNumber	O
- subjectIdentifier	O
DigestAlgorithmIdentifier	M
SignedAttributes	M
SignatureAlgorithmIdentifier	M
SignatureValue	M
UnsignedAttributes	O

Tabelle 5 legt die Anforderungsstufen der Elemente fest, die die signierten Attribute bilden. Das nicht angegebene Element wird mit C (Bedingt) angesetzt.

Tabelle 5 — Signierte Attribute in der Signatur

Element	Anforderungsstufe
ContentType	M
MessageDigest	M
SigningCertificateReference	M
- ESS SigningCertificate	O
- ESS SigningCertificateV2	O ^a
- otherSigningCertificate	C
SignaturePolicyIdentifier	C ^b
CommitmentType	C ^b
SignerIdentifier	C
ContentTimestamp	C
SigningTime	P
ContentReference	P
ContentIdentifier	P
ContentHints	P
signer-attributes	C ^c
SignerLocation	O ^d

^a Wenn eine Signatur, die mit ‚PAdES verwendet CAdES-Signaturen‘ konform ist, erzeugt wird, muss das Attribut von ‚signingCertificateV2‘ in ‚signedAttrs.‘ auftreten.

^b Siehe ISO/DIS 32000-2, 12.8.3.4.4.

^c Siehe ISO/DIS 32000-2, 12.8.3.4.3.

^d Entweder das ‚SignerLocation‘-Attribut oder der ‚Location‘-Eintrag in Tabelle 1 darf verwendet werden.

Tabelle 6 legt die Anforderungsstufen der Elemente fest, die die unsignierten Attribute bilden. Das nicht angegebene Element wird mit C (Bedingt) angesetzt.

Tabelle 6 — Unsignierte Attribute in der Signatur

Element	Anforderungsstufe
CounterSignature	P

6.4.3 Zeitstempel des PAdES-T-Profiles

a) PAdES-T-Profil mit 'Document Timestamp'

Das PAdES-T-Profil mit 'Document Timestamp' ist als eine erweiterte Form von PAdES unter Verwendung der CAdES-Signaturen definiert, zu der das 'Document Timestamp'-Verzeichnis ergänzt wird.

b) PAdES-T-Profil mit 'Signature Timestamp'-Attribut

Das PAdES-T-Profil mit 'Signature Timestamp'-Attribut ist als eine erweiterte Form definiert, zu der das 'Signature Timestamp'-Attribut ergänzt wird.

c) PAdES-T-Profil mit 'Subsequent Signature' mit 'Signature Timestamp'-Attribut

Das PAdES-T-Profil mit 'Subsequent Signature' mit 'Signature Timestamp'-Attribut ist als eine erweiterte Form von PAdES unter Verwendung des CAdES-Signaturenprofils definiert, zu dem das 'Subsequent Signature'-Verzeichnis ergänzt wird, das die Signatur mit dem 'Signature Timestamp'-Attribut enthält.

Der Zeitwert von PAdES-T muss konform zum ältesten gültigen Zeitstempels sein, der die Signaturwerte nach a), b) oder c) abdeckt.

Tabelle 7 — Zeitstempel des PAdES-T-Profiles

Element	Anforderungsstufe
timestamp for signature	M
- Document TimeStamp dictionary	0
- Signature TimeStamp Attribute (unsigned attributes in signature data)	0
- Subsequent Signature with a Signature TimeStamp Attribute (unsigned attributes in signature data)	0

6.5 PAdES-A-Profil

6.5.1 Allgemeines

Die Anforderungsstufen der bildenden Elemente des PAdES-A-Profiles sind in 6.5.2 bis 6.5.7 festgelegt.

6.5.2 Struktur des PAdES-A-Profils

Das PAdES-A-Profil ist als die Form einer elektronischen Signatur definiert, bei der die PDF-Objekte durch vertrauenswürdige Belege als Beweis der Existenz geschützt sind (z. B. document timestamp). Die PDF-Objekte enthalten die folgende Objekte:

- zu signierende Daten;
- Signaturwert;
- vertrauenswürdiger Beleg, der den Signaturwert schützt;
- vertrauenswürdige Belege für PDF-Objekte der Vergangenheit;
- Prüfinformation aktualisiert (thisUpdate of CRL or OCSP response) nach dem Zeitwert von PAdES-T des Signaturwertes und der vertrauenswürdigen Belege.

ANMERKUNG Siehe Rec. ITU-T X.509|ISO/IEC 9594-8 oder RFC 6960.

Das PAdES-A-Profil ist eine erweiterte Form des PAdES-T-Profils, bei der die in Tabelle 8 festgelegten Elemente ergänzt werden. PAdES-A ermöglicht die Entdeckung jeder unzulässigen Änderung von Informationen betreffend der Signatur einschließlich dem Gegenstand der Signatur und den Prüfdaten.

Tabelle 8 — Elemente des PAdES-A-Profils

Element	Anforderungsstufe
Document Security Store (DSS) Dictionary	M
Document Timestamp dictionary	M

6.5.3 'Document Security Store'-Verzeichnis

Die Anforderungen der Einträge, die das 'Document Security Store (DSS)'-Verzeichnis bilden, sind in ISO/DIS 32000-2 festgelegt.

Das DSS darf die Zertifikats- und Sperrinformationen enthalten, die für die Gültigkeitsprüfung der Signaturen und der Signatur-Zeitstempel genutzt werden, wobei die Dokument-Zeitstempel vor dem DSS-Verzeichnis angehängen werden.

6.5.4 'Signature VRI'-Verzeichnis

Die Anforderungen der Einträge, die das 'Signature VRI'-Verzeichnis bilden, sind in ISO/DIS 32000-2 festgelegt.

6.5.5 'Document Timestamp'

Tabelle 9 — Signaturverzeichnis von 'DocTimeStamp'

Eintrag	Anforderungsstufe	Wert
Type	M	DocTimeStamp
Filter	M	
SubFilter	M	ETSI.RFC3161
Contents	M	TimeStampToken ^a
ByteRange	M ^b	
Reference	P	
Changes	P	
Name	P	
M	P	
Cert	P	
Location	P	
Reason	P	
ContactInfo	P	
R	P	
V	O	0
Prop_Build	O	
Prop_AuthTime	P	
Prop_AuthType	P	
^a wie in RFC 3161 festgelegt.		
^b 'ByteRange' muss die gesamte Datei berücksichtigen, einschließlich des Signatur-Verzeichnisses aber ohne den Inhaltswert.		

Der Dokument-Zeitstempel muss angebracht werden, nachdem das DSS-Verzeichnis angehängen worden ist.

Die Anforderungen der Einträge, die den Dokument-Zeitstempel bilden, sind in ISO/DIS 32000-2 festgelegt.

6.5.6 Aktualisierung von PAdES-A

Um die Gültigkeit der Signaturen und/oder der Zeitstempel langfristig sicherzustellen, muss ein neuer Dokument-Zeitstempel zu einem Zeitpunkt angebracht werden, wenn die im letzten Dokument-Zeitstempel verwendeten Verschlüsselungsalgorithmen als zuverlässig gelten und die Zertifikate des Dokument-Zeitstempels nicht abgelaufen sind. Die folgenden Vorgänge müssen durchgeführt werden:

- 1) Der für die Gültigkeitsprüfung des letzten Dokument-Zeitstempels verwendete Satz von Zertifikats- und Sperrinformationen wird erhalten;
- 2) Der Satz von Zertifikats- und Sperrinformationen wird in den PDF-Daten als Stream-Objekte gespeichert. Das DSS-Verzeichnis, das die Referenzen zu diesen Objekten beinhaltet, wird angehängen sowie, wenn notwendig, das VRI.
- 3) Der Dokument-Zeitstempel wird an die PDF-Daten aus Schritt 2 angebracht.

6.5.7 Prüfdaten für Signatur und Zeitstempel

Die Prüfdaten sind ein Satz von Zertifikaten bis hin zum Vertrauensanker und den Sperrinformationen, die für die Gültigkeitsprüfung von Signaturen und Zeitstempeln verwendet werden. Die Prüfdaten dürfen, wie weiter unten beschrieben, mit der PAdES-Signatur gespeichert werden. Wenn sie nicht mit der PAdES-Signatur gespeichert werden, müssen die Prüfdaten durch ein anderes Sicherungsmittel gespeichert werden, mindestens einschließlich der Speicherung durch CA als ein TTP oder durch TSA.

Tabelle 10 — Speicherelemente der Prüfdaten

Typen von Prüfdaten	Speicherelemente der Prüfdaten	Anforderungsstufe	Bevorzugte Reihenfolge
Prüfdaten für Signaturen	Felder innerhalb von 'SignedData' der Signatur	O	
	Stream-Objekte bezeichnet durch DSS	O	1
	Stream-Objekte bezeichnet durch VRI	O	2
Prüfdaten für Zeitstempel-Token des Signatur-Zeitstempel-Attributs	Felder innerhalb von 'SignedData' der zeitgestempelten Signatur	O	
	Felder innerhalb des Signatur-Zeitstempels	O ^a	
	Stream-Objekte bezeichnet durch DSS	O	1
	Stream-Objekte bezeichnet durch VRI	O	2
Prüfdaten für Zeitstempel-Token des Dokument-Zeitstempels	Felder innerhalb von 'SignedData' der zeitgestempelten Signatur	P	
	Felder innerhalb des Dokument-Zeitstempels	O ^a	
	Stream-Objekte bezeichnet durch DSS	O	1
	Stream-Objekte bezeichnet durch VRI	O	2
^a Sperrinformationen sollten unter Verwendung von DSS oder VRI gespeichert werden.			

6.6 Mehrfache Signaturen

Mehrfache Signaturen dürfen an eine PDF-Datei unter Verwendung einer inkrementellen Aktualisierung angehängen werden.

Im Fall von mehrfachen Signaturen wird die Konformität einer ganzen PDF-Datei wie folgt definiert:

- Wenn alle Signaturen in einer PDF-Datei zu einem PAdES-A-Profil konform sind, dann ist diese PDF-Datei konform zum PAdES-A-Profil;
- Wenn zum PAdES-T-Profil und zum PAdES-A-Profil konforme Signaturen in einer PDF-Datei koexistieren, dann ist diese PDF-Datei konform zum PAdES-T-Profil.

Beispiele mehrfacher Signaturen sind im Anhang E beschrieben.

6.6.1 Zeitstempel für mehrfache Signaturen

Wenn ein Zeitstempel von PAdES-T auf eine PDF-Datei angewendet wird, die mehrfache Signaturen enthält, kann dieser Zeitstempel alle in der PDF-Datei bereits enthaltenen Signaturen schützen. Ein Zeitstempel kann daher als Zeitstempel für mehrfache Signaturen verwendet werden, wenn eine Zeitdifferenz zwischen Signaturen annehmbar ist.

Bild 5 zeigt ein Beispiel eines Zeitstempels für mehrfache Signaturen mit 'Document Timestamp'. Da dieser 'Document Timestamp' aus einem Byte-Bereich erzeugt wird, der sowohl 'Signature1' und 'Signature2' enthält, ist ein Beweis der Existenz beider Signaturen gegeben.

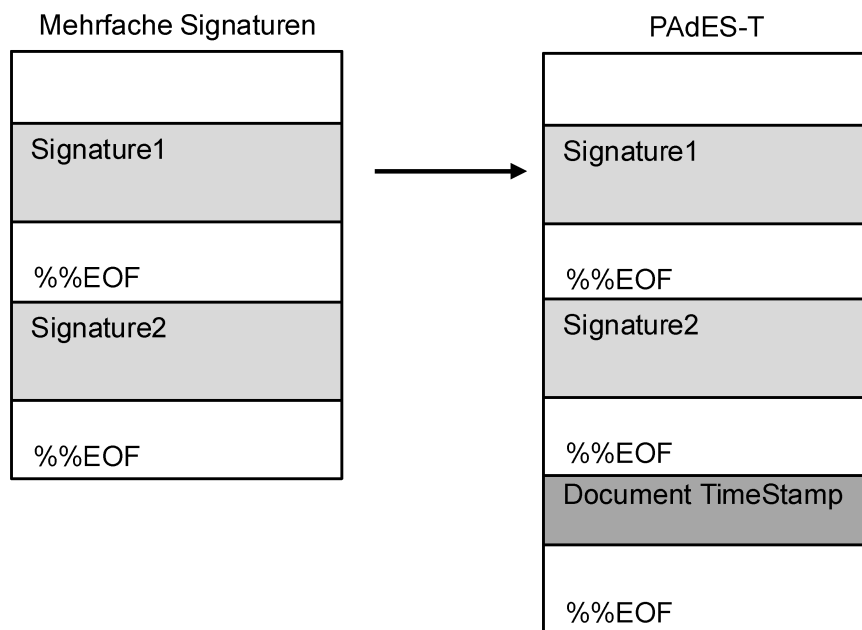


Bild 5 — Zeitstempel für mehrfache Signaturen mit Dokument-Zeitstempel

Bild 6 zeigt ein Beispiel eines Zeitstempels für mehrfache Signaturen mit 'Signature Timestamp'-Attribut. Dieses 'Signature TimeStamp'-Attribut in 'Signature2' wird aus dem Signaturwert von 'Signature2' erzeugt und der Signaturwert von 'Signature2' aus einem Byte-Bereich, der 'Signature1' einschließt. Daher folgert, dass dieses 'Signature TimeStamp'-Attribut sowohl 'Signature2' als auch 'Signature1' schützt. Das 'Signature TimeStamp'-Attribut kann als Zeitstempel für beide Signaturen verwendet werden.

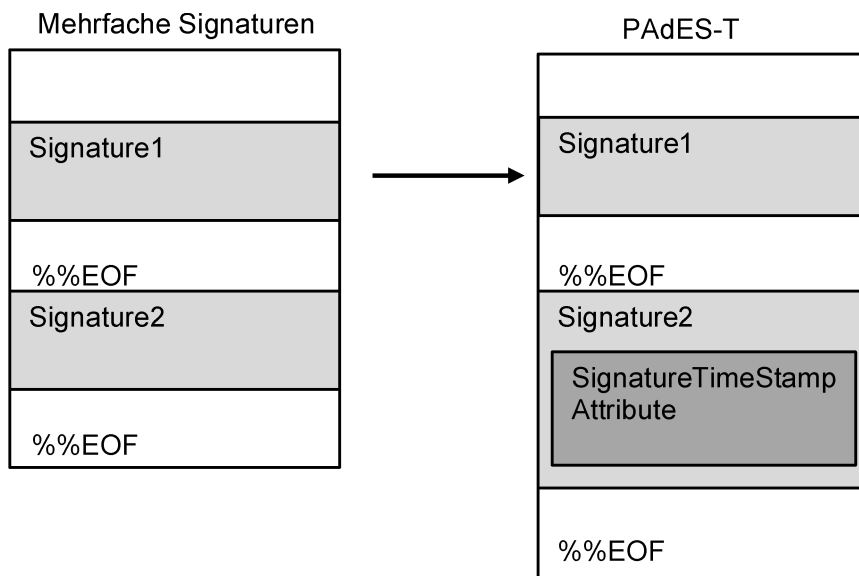


Bild 6 — Zeitstempel für mehrfache Signaturen mit 'Signature TimeStamp'-Attribut

ANMERKUNG Sofern nicht alle Signaturen und ein Zeitstempel sofort erzeugt werden können und eine Zeitdifferenz zwischen allen Signaturen und einem Zeitstempel annehmbar ist, muss ein Zeitstempel von PAdES-T für jede Signatur sofort nach ihrer Ausstellung erzeugt werden.

Anhang A (normativ)

Konformitätserklärung des Bereitstellers mit den zugehörigen Anlagen

A.1 Allgemeines

Dieser Anhang legt den Vordruck der Konformitätserklärung des Bereitstellers für das PAdES-Langzeit-Signaturprofil fest.

A.2 Vordruck der Konformitätserklärung des Bereitstellers

Konformitätserklärung des Bereitstellers für das Langzeit-Signaturprofil

Nr.

Name des Ausstellers:

Adresse des Ausstellers:

Gegenstand der Konformitätserklärung:

Der vorstehende Gegenstand der angegebenen Konformitätserklärung erfüllt die Anforderungen der folgenden Langzeit-Signaturprofile:

PAdES-T-Profil und/oder **PAdES-A-Profil**

PAdES-DT-Profil (Anhang B) und/oder **PAdES-DTA-Profil (Anhang B)**

Die implementierten Elemente entsprechen den Festlegungen in A.3.

Weitere Informationen:

(An dieser Stelle dürfen die Ergebnisse von Betriebs-/Funktionsprüfungen usw. eingefügt werden.)

Signiert für und im Auftrag von:

(Ort und Datum der Ausstellung)

(Name, Titel)