

DIN ISO 14533-3



ICS 35.240.63

Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung –**Langzeit-Signaturprofile –****Teil 3: Langzeit-Signaturprofile für PDF-erweiterte elektronische Signaturen (PAdES) (ISO 14533-3:2017)**

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 14533-3:2017)

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 14533-3:2017)

Gesamtumfang 35 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Abkürzungen und Symbole	8
5 Anforderungen	8
6 Langzeit-Signaturprofile	9
6.1 Definition des PAdES-Profiles und Positionierung	9
6.2 Darstellung der Anforderungsstufe	10
6.3 Vorgaben für die Festsetzung der Anforderungsstufe	10
6.4 PAdES-T-Profil	11
6.4.1 Allgemeines	11
6.4.2 PAdES unter Verwendung des CAdES-Signaturprofils	12
6.4.3 Zeitstempel des PAdES-T-Profiles	15
6.5 PAdES-A-Profil	16
6.5.1 Allgemeines	16
6.5.2 Struktur des PAdES-A-Profiles	16
6.5.3 'Document Security Store'-Verzeichnis	16
6.5.4 'Signature VRI'-Verzeichnis	17
6.5.5 'Document Timestamp'	17
6.5.6 Aktualisierung von PAdES-A	17
6.5.7 Prüfdaten für Signatur und Zeitstempel	18
6.6 Mehrfache Signaturen	18
6.6.1 Allgemeines	18
6.6.2 Zeitstempel für mehrfache Signaturen	19
Anhang A (normativ) Konformitätserklärung des Bereitstellers mit den zugehörigen Anlagen . .	21
A.1 Allgemeines	21
A.2 Vordruck der Konformitätserklärung des Bereitstellers	21
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	22
A.3.5 Konformität mit dem PAdES-A-Profil	24
A.3.6 Konformität mit dem PAdES-DT-Profil (siehe Abschnitt B.2)	25
A.3.7 Konformität mit dem PAdES-DTA-Profil (siehe Abschnitt B.3)	25
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
Anhang C (normativ) Struktur von Zeitstempel-Token	28
C.1 Allgemeines	28
C.2 Normative Spezifikationen	28
C.3 Anforderungsstufe von Einzelelementen	28

Anhang D (informativ) Angewendete PAdES mit CMS-Signaturen	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	35

Bilder

Bild 1 — Beziehung zwischen PAdES-T-Daten und PAdES-A-Daten	10
Bild 2 — PAdES-T-Profil mit ‚Document Timestamp‘	11
Bild 3 — PAdES-T-Profil mit ‚Signature Timestamp‘-Attribut	12
Bild 4 — PAdES-T-Profil mit ‚Subsequent Signature‘ mit ‚Signature Timestamp‘-Attribut	12
Bild 5 — Zeitstempel für mehrfache Signaturen mit Dokument-Zeitstempel	19
Bild 6 — Zeitstempel für mehrfache Signaturen mit ‚Signature TimeStamp‘-Attribut	20
Bild B.1 — Struktur von PAdES-DT	26
Bild B.2 — Beziehung zwischen den PAdES-DT-Daten und den PAdES-DTA-Daten	27
Bild E.1 — Beispiel einer PDF-Datei konform zum PAdES-T-Profil	31
Bild E.2 — Beispiel einer PDF-Datei konform zum PAdES-A-Profil	32
Bild E.3 — Beispiel einer PDF-Datei konform zum PAdES-A-Profil (mit 2 Generationen)	33

Tabellen

Tabelle 1 — Signaturverzeichnis von PAdES unter Verwendung der CAdES-Signaturen	12
Tabelle 2 — Inhaltsinformation in der Signatur	13
Tabelle 3 — Signierte Daten in der Signatur	13
Tabelle 4 — Unterzeichnerinformation in der Signatur	14
Tabelle 5 — Signierte Attribute in der Signatur	14
Tabelle 6 — Unsignierte Attribute in der Signatur	15
Tabelle 7 — Zeitstempel des PAdES-T-Profiles	15
Tabelle 8 — Elemente des PAdES-A-Profiles	16
Tabelle 9 — Signaturverzeichnis von ‚DocTimeStamp‘	17
Tabelle 10 — Speicherelemente der Prüfdaten	18
Tabelle A.1 — Profilimplementierung	21
Tabelle A.2 — PAdES-T-Profilimplementierung	22
Tabelle A.3 — Signaturverzeichnis	22
Tabelle A.4 — ‚ContentInfo‘ in den Signaturdaten	22
Tabelle A.5 — ‚SignedData‘ in den Signaturdaten	23
Tabelle A.6 — ‚SignerInfo‘ in den Signaturdaten	23
Tabelle A.7 — Signierte Attribute in den Signaturdaten	23
Tabelle A.8 — Unsignierte Attribute in den Signaturdaten	24
Tabelle A.9 — Elemente des PAdES-A-Profiles	24
Tabelle A.10 — Prüfung der Speicherdaten	24
Tabelle A.11 — Elemente des PAdES-DT-Profiles	25
Tabelle A.12 — Elemente des PAdES-DTA-Profiles	25
Tabelle A.13 — „Bedingte“ Elemente	25
Tabelle C.1 — Anforderungsstufe für jedes Element des Zeitstempel-Tokens	28

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO 14533-3:2017, die vom Technischen Komitee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration* unter Beteiligung deutscher Experten erarbeitet wurde.

Für die deutsche Mitarbeit ist der Arbeitsausschuss NA 043-03-03 AA *Elektronisches Geschäftswesen* im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) verantwortlich.

Die Übernahme der ISO 14533-3 ins deutsche Normenwerk wurde u. a. beschlossen, da ein Bezug zur Technischen Richtlinie BASI/TR 03125, *Beweiswerterhaltung kryptographisch signierter Dokumente*, besteht.

Die Anforderungen der ISO 14533-3 wurden sachlich unverändert in dieses Dokument 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 den 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)*

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 14533-1	siehe	DIN ISO 14533-1
ISO/IEC 17050-1:2004	siehe	DIN EN ISO/IEC 17050-1:2010-08

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 17050-1:2010-08, *Konformitätsbewertung — Konformitätserklärung von Anbietern — Teil 1: Allgemeine Anforderungen (ISO/IEC 17050-1:2004, korrigierte Fassung 2007-06-15); Deutsche und Englische Fassung EN ISO/IEC 17050-1:2010*

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) (ISO 14533-1:2014)*

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von ISO Technischen Komitees durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Directives, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Directives, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration* erarbeitet.

Eine Auflistung aller Teile der Normenreihe ISO 14533 ist auf der ISO-Internetseite abrufbar.

Einleitung

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

1 Anwendungsbereich

Dieses Dokument legt unter den in PDF-erweiterten elektronischen Signaturen (PAdES, en: PDF Advanced Electronic Signatures) definierten Elementen diejenigen Elemente fest, die die Prüfung einer digitalen Signatur über eine lange Zeitspanne ermöglichen.

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 werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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 (CAdES)*

ISO 32000-2, *Document management — Portable document format — Part 2: PDF 2.0*

3 Begriffe

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

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

3.1

erweiterte elektronische Signatur

elektronische Signatur, die eindeutig mit dem Unterzeichner verknüpft ist, die den Unterzeichner identifizieren kann, die unter Verwendung von elektronischen Signaturerstellungsdaten erstellt wird, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann, und die mit den damit signierten Daten so verknüpft ist, dass jede spätere Änderung der Daten feststellbar ist

4 Abkürzungen und 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 Dokument, 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 Dokument 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 Dokument als „Bedingt“ angegeben ist.

5.2 Die Erzeugung oder Gültigkeitsprüfung von PAdES-A-Daten entspricht diesem Dokument, 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 Dokument 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 Dokument als „Bedingt“ angegeben ist.

5.3 Die Erzeugung oder Validierung von PAdES-DT- und PAdES-DTA-Daten entspricht diesem Dokument, vorausgesetzt, die Anforderungen aus Bild B.1 und Bild B.2 sind erfüllt. Siehe Anhang B.

5.4 Sofern eine „First-Party“-Konformitätsbewertung angewendet wird, muss der Implementierer eine Konformitätserklärung nach diesem Dokument 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 1 Siehe ISO/IEC 17050-1:2004.

ANMERKUNG 2 Bild 1 zeigt die Anordnung der Erzeugung und Validierung von PAdES-T-Daten und PAdES-A-Daten.

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,
- müssen jegliche unzulässigen Änderungen von zur Signatur gehörenden Informationen einschließlich des Gegenstands von Informationen und Prüfdaten erkennbar sein und
- muss die Interoperabilität sichergestellt sein.

Um diese Anforderungen zu erfüllen, werden in diesem Dokument 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.

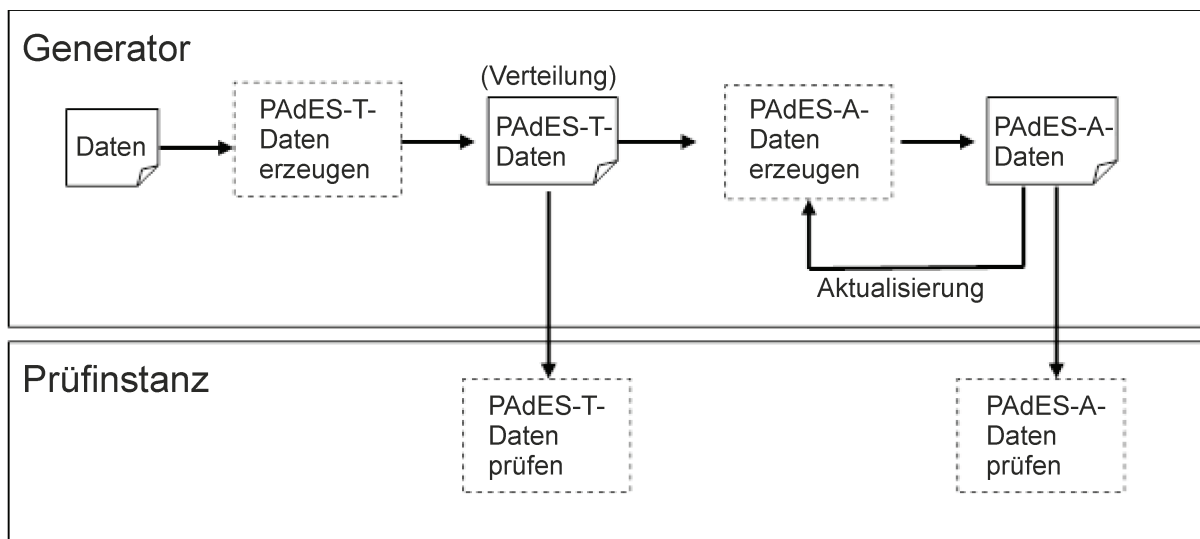


Bild 1 — Beziehung zwischen PAdES-T-Daten und PAdES-A-Daten

6.2 Darstellung der Anforderungsstufe

Dieses Dokument 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 aber 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 Einzelelemente 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 Bild 2 bis Bild 4 dargestellt.

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

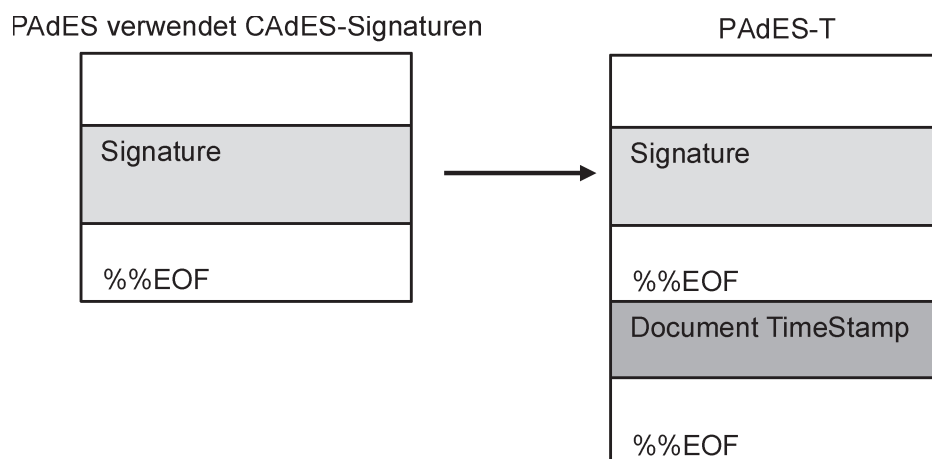


Bild 2 — PAdES-T-Profil mit ‚Document Timestamp‘