

DIN ISO 14533-3:2023-05 (D)

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)

Inhalt	Seite
Nationales Vorwort	5
Nationaler Anhang NA (informativ) Literaturhinweise	6
Vorwort	7
Einleitung	8
1 Anwendungsbereich.....	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Abkürzungen und Symbole	9
5 Anforderungen	10
6 Langzeit-Signaturprofile	10
6.1 Definition des PAdES-Profiles und Positionierung.....	10
6.2 Darstellung der Anforderungsstufe	11
6.3 Vorgaben für die Festsetzung der Anforderungsstufe	11
6.4 PAdES-T-Profil.....	12
6.4.1 Allgemeines.....	12
6.4.2 PAdES unter Verwendung des CAdES-Signaturprofils	13
6.4.3 Zeitstempel des PAdES-T-Profiles.....	16
6.5 PAdES-A-Profil.....	17
6.5.1 Allgemeines.....	17
6.5.2 Struktur des PAdES-A-Profiles	17
6.5.3 'Document Security Store'-Verzeichnis	17
6.5.4 'Signature VRI'-Verzeichnis.....	17
6.5.5 'Document Timestamp'.....	17
6.5.6 Aktualisierung von PAdES-A.....	18
6.5.7 Prüfdaten für Signatur und Zeitstempel	19
6.6 Mehrfache Signaturen.....	19
6.6.1 Allgemeines.....	19
6.6.2 Zeitstempel für mehrfache Signaturen	20
Anhang A (normativ) Konformitätserklärung des Bereitstellers mit den zugehörigen Anlagen.....	22
A.1 Allgemeines.....	22
A.2 Vordruck der Konformitätserklärung des Bereitstellers	22
A.3 Vordruck der Anlage zur Konformitätserklärung des Bereitstellers	22
A.3.1 Allgemeines.....	22
A.3.2 Zu zitierende Versionsnummer des Standards	22
A.3.3 Anwendungsbereich der Profilimplementierung.....	23
A.3.4 Konformität mit dem PAdES-T-Profil	23
A.3.5 Konformität mit dem PAdES-A-Profil	25
A.3.6 Konformität mit dem PAdES-DT-Profil (siehe Abschnitt B.2).....	26
A.3.7 Konformität mit dem PAdES-DTA-Profil (siehe Abschnitt B.3).....	26
A.3.8 Spezifikationen, auf die durch „Bedingte“ Elemente zu verweisen ist.....	26
A.3.9 Bemerkungen	27

Anhang B (normativ) Profil bei der ausschließlichen Nutzung eines Zeitstempels	28
B.1 Allgemeines.....	28
B.2 PAdES-DT-Profil.....	28
B.2.1 Allgemeines.....	28
B.2.2 Verzeichnis des Dokument-Zeitstempels.....	28
B.3 PAdES-DTA-Profil.....	28
Anhang C (normativ) Struktur von Zeitstempel-Token	30
C.1 Allgemeines.....	30
C.2 Normative Spezifikationen	30
C.3 Anforderungsstufe von Einzelementen.....	30
Anhang D (informativ) Angewendete PAdES mit CMS-Signaturen	32
Anhang E (informativ) Beispiele für mehrfache Signaturen	33
E.1 Allgemeines.....	33
E.2 Beispiel des PAdES-T-Profiles	33
E.3 Beispiel des PAdES-A-Profiles	34
Literaturhinweise	37

Bilder

Bild 1 — Beziehung zwischen PAdES-T-Daten und PAdES-A-Daten.....	11
Bild 2 — PAdES-T-Profil mit ‚Document Timestamp‘.....	13
Bild 3 — PAdES-T-Profil mit ‚Signature Timestamp‘-Attribut.....	13
Bild 4 — PAdES-T-Profil mit ‚Subsequent Signature‘ mit ‚Signature Timestamp‘-Attribut	13
Bild 5 — Zeitstempel für mehrfache Signaturen mit Dokument-Zeitstempel	20
Bild 6 — Zeitstempel für mehrfache Signaturen mit ‚Signature TimeStamp‘-Attribut.....	20
Bild B.1 — Struktur von PAdES-DT	28
Bild B.2 — Beziehung zwischen den PAdES-DT-Daten und den PAdES-DTA-Daten.....	29
Bild E.1 — Beispiel einer PDF-Datei konform zum PAdES-T-Profil.....	33
Bild E.2 — Beispiel einer PDF-Datei konform zum PAdES-A-Profil.....	34
Bild E.3 — Beispiel einer PDF-Datei konform zum PAdES-A-Profil (mit 2 Generationen)	35

Tabellen

Tabelle 1 — Signaturverzeichnis von PAdES unter Verwendung der CAdES-Signaturen	13
Tabelle 2 — Inhaltsinformation in der Signatur.....	14
Tabelle 3 — Signierte Daten in der Signatur.....	14
Tabelle 4 — Unterzeichnerinformation in der Signatur	15
Tabelle 5 — Signierte Attribute in der Signatur	15

Tabelle 6 — Unsignierte Attribute in der Signatur	16
Tabelle 7 — Zeitstempel des PAdES-T-Profiles	16
Tabelle 8 — Elemente des PAdES-A-Profiles	17
Tabelle 9 — Signaturverzeichnis von 'DocTimeStamp'	18
Tabelle 10 — Speicherelemente der Prüfdaten	19
Tabelle A.1 — Profilimplementierung	23
Tabelle A.2 — PAdES-T-Profilimplementierung	23
Tabelle A.3 — Signaturverzeichnis	23
Tabelle A.4 — 'ContentInfo' in den Signaturdaten	24
Tabelle A.5 — 'SignedData' in den Signaturdaten	24
Tabelle A.6 — 'SignerInfo' in den Signaturdaten	24
Tabelle A.7 — Signierte Attribute in den Signaturdaten.....	25
Tabelle A.8 — Unsignierte Attribute in den Signaturdaten.....	25
Tabelle A.9 — Elemente des PAdES-A-Profiles	25
Tabelle A.10 — Prüfung der Speicherdaten	25
Tabelle A.11 — Elemente des PAdES-DT-Profiles.....	26
Tabelle A.12 — Elemente des PAdES-DTA-Profiles.....	26
Tabelle A.13 — „Bedingte“ Elemente.....	26
Tabelle C.1 — Anforderungsstufe für jedes Element des Zeitstempel-Tokens.....	30