# eCH-0250 – Die Bewahrung der Gültigkeit von Signaturen in einem PDF

| | |
|---|---|
| **Name** | Die Bewahrung der Gültigkeit von Signaturen in einem PDF |
| **eCH-Nummer** | eCH-0250 |
| **Kategorie** | Standard |
| **Reifegrad** | Definiert |
| **Version** | 1.0.0 |
| **Status** | Genehmigt |
| **Beschluss am** | 2023-03-07 |
| **Ausgabedatum** | 2023-02-13 |
| **Ersetzt Version** | – |
| **Voraussetzungen** | ETSI TS 102 778-1 bis -6<br>ETSI EN 319 142-1 bis -2<br>ISO 32000-1 und -2, Document Management — Portable document format<br>Adobe ® XFA: XML Forms Architecture (XFA) Specification Version 2.5<br>eCH-0220 und CH-0230 |
| **Beilagen** | - |
| **Sprachen** | Deutsch (Original), Französisch (Übersetzung) |
| **Autoren** | Fachgruppe Technologie (in alphabetischer Reihenfolge)<br>Georg Büchler (Kost)<br>Daniel Muster (it-rm IT-Riskmanagement GmbH)<br>Marcel Niederberger (ESTV)<br>Michael von Niederhäusern (BIT)<br>Hubert Rötzer<br>Erich Vogt |
| **Herausgeber / Vertrieb** | Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich<br>T 044 388 74 64, F 044 388 71 80<br>www.ech.ch / info@ech.ch |

# Zusammenfassung

Der hier vorliegende Standard gibt eine Anleitung zur Bewahrung der Gültigkeit elektronischer Signaturen in einem PDF-Dokument, so dass die elektronische Signatur in den aufzubewahrenden PDF-Dokumenten während dieser Zeit verlässlich geprüft werden kann. Langzeit meint, dass die Signatur z.B. auch noch nach Ablauf der Gültigkeitsdauer des zur Signatur korrespondierenden Zertifikats entsprechend verifiziert und bei erfolgreicher Prüfung allgemein anerkannt werden kann. Die Gültigkeit eines Zertifikats kann z.B. nach seiner Laufzeit oder nach beantragter Revokation des Eigentümers des Zertifikats verfallen.

Der hier vorliegende Standard berücksichtigt das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) und ist ein Profil der folgenden zugrunde liegenden Standards und Empfehlungen:

- ETSI EN 319 142-1
- ETSI EN 319 142-2
- ISO-32000-1 und ISO 32000-2
- KOST (https://kost-ceco.ch/cms/willkommen.html)

Bei der hier vorgenommenen Auswahl an Attributen, Elementen und Objekten wurde darauf geachtet, dass das ganze Konstrukt der «Konservierung» elektronischer Signaturen in einem PDF-Dokument oder deren Komponenten - wenn möglich - auf Informationen von allgemein anerkannten Institutionen basiert und dabei möglichst einfach bleibt. Informationen von allgemein anerkannten Institutionen sind z.B. Angaben, welche in Bundesvorschriften geregelt sind, wie:

- nach ZertES geregelte Zertifikate
- Zeitstempeldienste, welche von nach ZertES anerkannten Zertifizierungsdiensten erbracht werden.

Oder:

- Empfehlungen der Europäischen Union (https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/Standards+and+specifications) Die Empfehlungen der EU zu dem hier behandelten Thema verweisen auf die oben aufgeführten ETSI-Standards.
- Empfehlungen der KOST

Für die Prüfung elektronisch signierter Dokumente sei auch auf den Standard ETSI EN 319 102-1 verwiesen. Hierzu besteht jedoch kein Bundeserlass und ist nicht Bestandteil dieses Standards.

# Inhaltsverzeichnis

# 1 Einleitung

## 1.1 Status

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

## 1.2 Anwendungsgebiet

Das Anwendungsgebiet ist: Überall dort, wo Signaturen in einem PDF-Dokument oder deren Bestandteile noch über Tage, Wochen oder gar Jahre hinweg aufbewahrt werden sollen, so dass deren elektronische Signatur auch nach dieser Zeitspanne verlässlich geprüft und bei erfolgreicher Prüfung akzeptiert werden kann.

Bei der Bewahrung der Gültigkeit elektronisch signierter Dokumente soll die zugrundeliegende Signatur auch nach Jahren als gültig akzeptiert werden, wenn sie früher (zum Zeitpunkt der Erstellung) als gültig taxiert worden ist. Zwischen dem Leisten der elektronischen Signatur und der späteren nochmaligen Prüfung der Signatur des aufbewahrten, elektronisch signierten Dokumentes können z.B. folgende Ereignisse eintreten, welche die Akzeptanz der elektronischen Signaturen zu einem späteren Zeitpunkt erschweren:

- Das Zertifikat mit dem öffentlichen Schlüssel zur Verifikation der elektronischen Signatur, kurz das Prüfzertifikat, ist nicht mehr gültig.
- Das Root-Zertifikat zum Prüfzertifikat ist nicht mehr gültig.
- Der private Signaturschlüssel wurde kompromittiert, und das Zertifikat wurde dann revoziert.
- Das Zertifikat ist aus anderen Gründen revoziert worden.
- Die für die Signatur verwendeten kryptografischen Algorithmen können als weniger sicher erklärt werden, was zur Revokation der bestehenden Schlüssel führen kann und vermutlich Anlass dazu sein wird, die Schlüssellänge zu erhöhen.

In [1] sind diese und weitere Fälle und ihre Auswirkungen auf die nachträgliche Prüfung der elektronischen Signatur erläutert.

## 1.3 Ziel(e) und Abgrenzung

### 1.3.1 Ziel

Mit dem hier vorliegenden Dokument und den zugrundeliegenden ETSI-Standards wird Folgendes ermöglicht.

| |
|---|
| Bei einem nach ZertES geregelten elektronisch signierten Dokument und bei einem nach ZertES geregelten Siegel soll verlässlich festgestellt werden können, ob bei der Erstellung dessen Signatur das dazu entsprechende Signaturzertifikat gültig war. Siehe auch Art. 2 Abs. c und d ZertES. |

Ein Dokument, welches heute mit einer gültigen, geregelten oder qualifizierten elektronischen Signatur versehen worden ist, werden Informationen fortlaufend so beigefügt, dass

- innerhalb der von den jeweiligen Bestimmungen geforderten Aufbewahrungsfrist verlässlich

festgestellt werden kann, dass zum Herstellungszeitpunkt der elektronischen Signatur das entsprechende Zertifikat gültig war.
- innerhalb der genannten Zeit und Frist die Verantwortlichkeit für das Leisten dieser elektronischen Signatur verlässlich zugeordnet werden kann.

Dies unter der Voraussetzung, dass die beigefügten Informationen, das Dokument und die elektronische Signatur dazu in der Zwischenzeit unverändert geblieben sind. Es soll hiermit die Beweis- oder Aussagekraft der elektronischen Signatur erhalten bleiben. Z.B. soll die Haftung nach Art. 59a OR nicht obsolet werden, weil die Gültigkeitsfrist des entsprechenden Zertifikats abgelaufen ist und somit die Beweiskraft der zur Diskussion stehenden elektronischen Signatur in Zweifel gezogen wird.

Die ETSI-Standards ETSI TS 119 102-1 und ETSI TS 102 778-2 bis 5, ETSI EN 319 142-1 und -2 definieren verschiedene Prüfschritte zur Verifikation einer elektronischen Signatur. Welche Prüfschritte erforderlich sind, damit die Signatur als gültig erachtet und folglich akzeptiert wird, hängt - wie in diesem Standard bereits erwähnt - von den Vorschriften zur Signatur ab (engl. signature policy).

Zusammenfassend: Man will mit der hier vorgeschlagenen Methode die Bewahrung der Gültigkeit elektronischer Signaturen erreichen, so dass die elektronische Signatur nach Erstellung, nach Empfang und nach deren Prüfung während der geforderten Aufbewahrungszeit allgemein akzeptiert werden wird. Dies (möglicherweise) auch bei einem strittigen Verwaltungs- oder Gerichtsverfahren.

In Analogie dazu: Gemäss Art. 14 GeoIV sollen Geobasisdaten so aufbewahrt werden, dass sie in *Bestand und Qualität* erhalten bleiben. Dabei werden die Geobasisdaten nach anerkannten Normen und nach dem Stand der Technik gesichert. Insbesondere werden die Daten periodisch in geeignete Datenformate ausgelagert und diese sicher aufbewahrt.

Das hier behandelte Profil basiert auf anerkannten Normen und entspricht dem Stand der Technik, weil die aktuellsten, verabschiedeten Normen von ETSI und ISO berücksichtigt worden sind.

**Anmerkung:** Die hier erwähnten Aufbewahrungs- und Verjährungsfristen überdauern meist die Gültigkeit des Zertifikats für die Verifikation der Dokument- oder Dateisignatur, gegebenenfalls auch die Gültigkeitsdauer eines oder mehrerer Zertifikate in der Zertifikatskette (engl. certification path).

### 1.3.2 Weg zum Ziel

Die Bewahrung der Gültigkeit von Signaturen in einem PDF-Dokument soll zuerst in Form eines Profils auf Basis der folgenden ETSI-Standards genormt werden:

- ETSI TS 102 778-1 bis 6

**Definition:** Ein Profil legt die Anwendung eines Standards oder eine Gruppe derer fest. (A profile specifies the use of a particular standard, or group of standards.)

Zur Bewahrung der Gültigkeit elektronisch signierter pdf-Dokumente sind bei ETSI und ISO folgende, aktuellere Standards verabschiedet worden:

- ETSI EN 319 142-1
- ETSI EN 319 134-2
- ISO 32000-2 (PDF 2.0)

Ausgangslage dieses Dokuments sind jedoch die Standard ETSI TS 102 778-1 bis 6 und ISO 32000-2, weil:

- sie eher selbsterklärend sind und zusätzliche Informationen zum Verständnis der Problematik enthalten.

- ETSI EN 319 142-1 und ETSI EN 319 142-2 für den Einstieg in die Problematik schwieriger sind und gewisse Themen/Problemfelder, wie das zu verwendende PDF-Format, nicht erläutert werden.

ETSI EN 319 142-1 und ETSI EN 319 142-2 werden deswegen anschliessend in diesem Dokument berücksichtigt. Doch ETSI-die Standards mit der Bezeichnung «EN» im Titel gehen solchen mit «TS» vor.

ETSI EN 319 142-1 und ETSI EN 319 142-2 werden von der Europäischen Union zur Bewahrung der Gültigkeit von elektronischen Signaturen in einem PDF empfohlen: https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/Standards+and+specifications

### 1.3.3 Abgrenzung

In diesem Zusammenhang ist es wichtig zu erwähnen: «Eine elektronische Signatur vermag die Integrität, d.h. die Unveränderheit, eines Dokumentes oder Objekts nicht zu schützen.» Das heisst, die Signatur stellt keine Massnahme dar, dass das Dokument nicht verändert wird. (Sie stellt also keine präventive Massnahme zum Schutz der Integrität eines Dokumentes dar.)

Sie vermag, verlässlich zu erkennen, ob das Dokument nach Erstellen der dazugehörigen Signatur verändert wurde und somit eine Integritätsverletzung vorliegt oder nicht. (Sie ist folglich ein Mittel der Detektion, ob eine Integritätsverletzung vorliegt.)

Folglich ist es unerlässlich, dass die Integrität (Unveränderheit) der elektronisch signierten Dokumente geschützt wird. Massnahmen zum Integritätsschutz von signierten PDF-Dokumenten bei der Archivierung/Aufbewahrung ist jedoch nicht primär Ziel dieses Standards.

## 1.4 Inhalt, Struktur des Dokuments

Dieses Dokument ist ein Profil der zugrundeliegenden ETSI und ISO Standard. Es wird hier lediglich erwähnt, was:

- fürs **eGovernment** nicht oder besonders relevant ist
- oder verbessert werden soll.

Im KAPITEL 4 werden zu den jeweiligen Kapiteln in den ETSI-Standard die entsprechenden Anmerkungen aufgeführt, wobei sich die Titel in den Unterkapiteln auf die Unterkapitel der jeweiligen ETSI-Standards beziehen.

## 1.5 Querverweise

Querverweise innerhalb dieses Dokuments beginnen mit «KAPITEL», d.h. in GROSSBUCHSTABEN. Querverweise mit «Kapitel», d.h. normal geschrieben, beziehen sich auf Kapitel externer Dokumente.

## 1.6 Anmerkung

Möglich wären andere als in den Standards vorgeschlagene Kompositionen von Attributen oder gar andere Verfahren für die Bewahrung der Gültigkeit elektronisch signierter Dokumente, so dass deren Signaturen auch während der Archivierungs-/Aufbewahrungszeit verlässlich geprüft werden können.

Der hier unterbreitete Vorschlag stützt sich auf international anerkannte ETSI-, ISO Standards und

EU-Richtlinien ab und bewahrt die Vertraulichkeit des Inhalts.

### 1.7 Terminologie der Empfehlung

Richtlinien in diesem Dokument werden gemäss der Terminologie aus RFC 2119 angegeben, dabei kommen die folgenden Ausdrücke zur Anwendung, die durch GROSSSCHREIBUNG als Wörter mit den folgenden Bedeutungen kenntlich gemacht werden (Zitat aus RFC 2119):

- **MUST**: This word, or the terms «REQUIRED» or «SHALL», mean that the definition is an absolute requirement of the specification.
- **MUST NOT**: This phrase, or the phrase «SHALL NOT», mean that that definition is an absolute prohibition of the specification.
- **SHOULD**: This word, or the adjective «RECOMMENDED», mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase «NOT RECOMMENDED» mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY**: This word, or the adjective «OPTIONAL», means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

## 2 Begriffe/Empfehlungen zu Signaturen in einem PDF

In diesem Dokument werden einige Begriffe im Kontext zu Signaturen in einem PDF erläutert und definiert, wie auch Normen zum PDF-Format festgelegt.

### 2.1 Signaturen in einem PDF

Ein PDF kann mittels einer CMS-Signatur signiert werden oder die darin gegebenenfalls enthaltenen XML-Objekte mit einer XML-Signatur. Also wird ein Profil für die Bewahrung der Gültigkeit von Signaturen im CMS- oder XML-Format hier erstellt.

ETSI normiert die Bewahrung der Gültigkeit von Signaturen in einem PDF (PAdES) jeweils für CMS-Signaturen und XML-Signaturen in folgenden Standards.

- ETSI EN 319 142-1 für im PDF enthaltenen CMS-Signaturen
- ETSI EN 319 142-2 nebst CMS-Signaturen noch für die im PDF enthaltenen XML-Signaturen

Während ISO dies für die CMS-Signatur in ISO 32000-2 vornimmt.

**Anmerkung:** Von ETSI standardisierte Signaturen in einem PDF sind im CMS- oder im XML-Format. Standards zur Bewahrung der Gültigkeit von Signaturen in einem PDF tragen bei ETSI-die Bezeichnung «PDF Advanced Electronic Signature», kurz «PAdES» im Titel.

### 2.1.1 PDF mit CMS-Signaturen

Eine CMS-Signatur kann das PDF-Dokument enthalten oder in einem PDF-Dokument eingebettet sein. Zur Bewahrung der Gültigkeit sei für Ersteres auf den eCH-0220 Standard verwiesen. In diesem Dokument und bei den erwähnten ETSI-Standards zu PAdES wird lediglich Letzteres betrachtet. Wenn zukünftig von CMS-Signaturen die Rede sein wird, so ist eine in einem PDF eingebettete CMS-Signatur gemeint, siehe ETSI TS 102 778-1 Kapitel 4.

Im Unterschied zu CMS-Signaturen nach RFC 5652 kann ein PDF nicht zwei CMS-Signaturen enthalten, welche dasselbe signiert haben. Die nächstfolgende CMS-Signatur in einem PDF umfasst den zu signierenden Inhalt inklusiv alle zuvor geleisteten Signaturen, siehe ETSI TS 102 778-1 Kapitel 4.4. Eine Gegensignatur (engl. countersignature, Deutsch Gegenzeichnung) im Sinne des Standards RFC 5652 ist folglich nicht möglich.

**Definition:** Als PDF-Signatur wird eine CMS-Signatur in einem PDF bezeichnet, welche zu Kapitel 12.8 in ISO 32000-1 (PDF 1.7) oder in ISO 32000-2 (PDF 2.0) konform ist.

**MUST NOT:** PDF-Signaturen mit einer Version älter als ISO 32000-1 (PDF 1.7) dürfen nicht verwendet werden. U.a. wird das Zertifikat zur Verifikation der PDF-Signatur bei PDF 1.6 anderswo im PDF abgelegt, als bei PDF 1.7 oder 2.0.

Zu den Ausprägungen von PDF-Signaturen siehe KAPITEL 2.4 «Typen von PDF-Signaturen».

### 2.1.2 PDF mit XML Signaturen

XML Forms Architecture (XFA) ist ein Set an proprietären XML-Spezifikationen. XFA ist ab PDF 1.5 in PDF Dokumenten integrierbar. Die Summe aller XML-Objekte in einem PDF wird als XFA-Form bezeichnet. Adobe hat die Integration von XFA in einem PDF in Adobe ® XFA: XML Forms Architecture (XFA) Specification version 2.5, (June 2007), spezifiziert. Sowohl die XFA-Form als Ganzes wie auch die einzelnen XML-Objekte in der XFA-Form können mit einer XML-Signatur versehen werden.

Anmerkung zur gemischten Anwendung von CMS- und XML-Signaturen in einem XFA-Dokument aus ETSI TS 102 778-1 hierzu:

> *Data encoded in XML may be carried within a PDF document. This may be used, for example, to carry PDF form data mapped into the PDF document using the XML Forms Architecture (XFA [i.2]). An XML signature, using the XAdES [3] format, may be applied to this data.*
>
> *The XML data, with or without an XML/XAdES signature, may be also signed along with the rest of the PDF document using a PDF signature as described above.* ***Once signed with a PDF signature further information cannot be added directly to any XAdES Signature that may be present.*** *Where a XAdES signature is applied using XFA the related validation data may be provided using PDF data structures to support long term validation (see clause 5.8). However, if raw XML structures are used (i.e. not using XFA) once a XAdES signature has been placed within a document signed with a PDF Signature* ***it cannot be extended to support long term validation*** *(see clause 5.6).*

Zu XAdES (XML Advanced Electronic Signature) siehe eCH-0230.

### 2.1.3 Ausprägungen von CMS-Signaturen in einem PDF

Siehe hierzu KAPITEL 4.2 «ETSI TS 102 778-1».

### 2.1.4 Typen von XML-Signaturen in einem PDF

Siehe hierzu KAPITEL 4.6 «ETSI TS 102 778-5».

## 2.2 PDF-Format

Es ist nicht zielführend, Vorkehrung zur über Jahre hinweg dauernden Bewahrung der Gültigkeit einer PDF-Signatur zu treffen, wenn das zugrundeliegende PDF-Format nicht archivtauglich ist. Für die Archivierung einer PDF-Datei wurde das PDF/A-Format in ISO 19005 spezifiziert.

Nachfolgend werden die diversen PDF/A-Versionen in Bezug auf die Bewahrung der Gültigkeit von PDF-Signaturen erläutert.

### 2.2.1 PDF/A-1

**MUST NOT:** PDF/A-1 Format (ISO 19005-1) basierend auf PDF 1.4 darf im Hinblick auf eine Archivierung elektronisch signierter Dokumente nicht mehr verwendet werden, wenn die Gültigkeit der Signatur nach den hier vorgeschlagenen Verfahren bewahrt werden soll. Aus ETSI TS 102 778-1 Kapitel 4.6 die Begründung hierfür:

> «As PDF/A-1 is based on Adobe PDF 1.4 and not on ISO 32000-1, it does not fully support all of its features available to digital signatures - specifically lacking are embedded revocation information and time-stamping. However, since such features are not explicitly forbidden there is nothing that prevents a PDF/A-1 conforming writer from putting these extended features into a file - but there should be no expectation that a PDF/A-1 conforming reader will process them accordingly. A PDF/A-1 conforming reader is, however, free to implement functionality beyond that specified in PDF/A-1.»

### 2.2.2 PDF/A-2

**SHOULD:** PDF/A-2 Format (ISO 19005-2) basierend auf ISO-32000-1 (PDF 1.7) soll im Hinblick auf eine Archivierung elektronisch signierter Dokumente verwendet werden.

Begründung, warum nur ein «SHOULD» und nicht ein «MUST» empfohlen wird:

> Die ETSI-Standards verweisen bei der Bildung der Signatur auf ISO 32000-1 (PDF 1.7). ISO 32000-1 (PDF 1.7) kann so verwendet werden, dass es zu ISO 19005-2 (PDF/A-2) kompatibel ist. In ISO 32000-1 (PDF 1.7) sind jedoch nicht alle Eigenschaften (engl. Features) enthalten/standardisiert, welche für die die Umsetzung der Standards ETSI TS 102 778-1 bis -4 und ETSI EN 319 142-1 bis -2 erforderlich sind. Es bedarf einer zu ISO 32000-1 nicht standardkonformen Erweiterung, um die Gültigkeit der PDF-Signatur zu bewahren, siehe ETSI EN 319 142-1 V1.1.1 (2016-04), Kapitel 5.4.1.

KOST empfiehlt für die Archivierung, falls möglich, PDF/A-2 im Konformitätslevel U zu verwenden (PDF/A-2u). Dazu drei Ergänzungen:

- Da PDF/A-2a strikter formuliert ist als PDF/A-2u, geht natürlich auch Konformitätslevel a. Doch dieser Konformitätslevel ist relativ schwierig zu erzeugen.
- Grundsätzlich werden alle Konformitätslevels der Version 2 als archivtauglich erachtet. Dies ist entsprechend im Katalog archivischer Dateiformate festgehalten. (https://kost-ceco.ch/cms/pdf-a-2.html ).
- Zum Zeitpunkt der Erstellung dieses Dokumentes ist in der Praxis nach wie vor ISO 32000-1 (PDF 1.7) respektive PDF/A-2 das aktuellste unterstützte Format.

### 2.2.3 PDF/A-3

**MUST NOT:** PDF/A-3 Format (ISO 19005-3) darf im Hinblick auf eine Archivierung des Dokuments nicht verwendet werden, weil es sich dafür nicht eignet, siehe: «Management Summary zur KOST-Studie: PDF/A-2 und PDF/A-3: Was ist neu?» [6].

### 2.2.4 PDF/A-4

**MAY:** PDF/A-4 Format (ISO 19005-4) basierend auf ISO-32000-2 (PDF 2.0) könnte im Hinblick auf eine Archivierung elektronisch signierter Dokuments zukünftig verwendet werden.

ISO 32000-2 (PDF 2.0) hat die notwendigen (ETSI)-Merkmale für die Bewahrung der Gültigkeit von PDF-Signaturen standardisiert und kann so verwendet werden, dass es zu ISO 19005-4 (PDF/A-4) kompatibel ist. Doch im Bereich PDF/A4 gibt es im Hinblick auf die Archivierung noch Unklarheiten, wie nun folgende Ausführungen zeigen.

Im November 2020 wurde PDF/A-4 (ISO 19005-4) veröffentlicht. Bei PDF/A-4 gibt es nur zwei Konformitätslevels:

- PDF/A-4f lässt auch Dateianhänge zu, die nicht PDF/A entsprechen.
- PDF/A-4e für den Engineering-Bereich erlaubt die Einbindung von 3D-Inhalten

Die KOST hat noch nicht die Archivtauglichkeit von PDF/A-4 untersucht. Mit dem Vergleich auf die vorangegangenen Versionen, lässt sich dennoch Folgendes festhalten:

- PDF/A-4f: Die Konformitätsstufe F (bzw. das subsidiary profile F) ist zu vermeiden, analog zu den Überlegungen zu PDF/A-3, siehe https://kost-ceco.ch/cms/PDF-A-3.html.
- PDF/A-4e: Zur Konformitätsstufe E, die PDF/E ablöst, kann von Seiten der KOST noch keine Aussage getroffen werden. Es gibt augenscheinlich nichts, was gegen eine Archivtauglichkeit von PDF/A-4e spricht.

Also ist nun abzuklären, inwiefern sich ISO 19005-4 (PDF/A-4e) für die Archivierung gemäss den Schweizerischen Bundesvorgaben eignet. Falls ISO 19005-4 (PDF/A-4) die Bundesvorgaben nicht in vollem Umfang zu erfüllen vermag, dann empfiehlt es sich, in einem Profil festzuhalten, wie die Vorgaben der KOST erfüllt werden können. D.h., welche Teile von ISO 19005-4 (PDF/A-4) den Anforderungen an die Archivierung gemäss den Schweizerischen Bundesvorgaben genügen.

Das Erstellen eines solchen Profils ist jedoch nicht Thema dieses Standards.

Falls sich herausstellt, dass sich PDF/A-4 (ISO 19005-4) für die Archivierung eignet, dann soll man dieses Format basierend auf ISO-32000-2 (PDF 2.0) gegenüber PDF/A-2 (ISO 19005-2) basierend auf ISO-32000-1 (PDF 1.7) für die Bewahrung der Gültigkeit der PDF-Signaturen vorziehen. Sobald

die Archivtauglichkeit von PDF/A-4 geklärt ist, wird dieser Standard entsprechend zeitnah angepasst werden. Zum Zeitpunkt der Erstellung dieses Standards ist PDF/A-4 jedoch noch nicht in der Praxis anzutreffen und erst ein theoretischer Standard.

**Anmerkung:** Die Europäische Union (EU) empfiehlt ETSI EN 319 142-1 und -2, d.h. einer zu ISO 32000-1 proprietären Erweiterung; dies betreffend Konformität mit eIDAS, siehe https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/Standards+and+specifications

Sie äussert sich jedoch zu ISO 32000-2 nicht, doch ihre Empfehlung wurde vor 2020 abgegeben. ISO 32000-2 wurde erst im Dezember 2020 publiziert.

## 2.3 XFA

**Definition:** XFA (XML Forms Architecture) ist ein Datei-/Objektformat, welches auf folgender Spezifikation basiert: XML Forms Architecture (XFA) Specification version 2.5, (June 2007), Adobe Systems Incorporated. XFA kann in ein PDF eingebettet sein oder als XML-Objekt vorliegen.

Im allgemeinen Sprachgebrauch wird u.a. eine Datei nach ISO 32000-1 als auch nach XFA, welches in ein PDF eingebettet ist, als PDF bezeichnet.

**Anmerkung:** XFA wird von Adobe nicht mehr unterstützt und gilt bei ISO 32000-2 (PDF 2.0) als überholt. Da es sich aber hier um einen Standard für die langfristige Gültigkeit von Signaturen handelt, werden trotzdem Empfehlungen im Kapitel 4.6 hierzu gemacht, welche aber nicht normativ sind.

## 2.4 Typen von PDF-Signaturen

Es wird zwischen folgenden PDF-Signaturen unterschieden:

a) usage right signature
b) certification signature und
c) approval signature

Wenn oben aufgeführte Signaturen erstellt werden, dann müssen sie zeitlich in der oben genannten Reihenfolge in einem PDF geleistet werden, wobei die ersten beiden Signaturen (usage rights, certification) nicht oder höchstens einmal im PDF enthalten sein dürfen.

a) usage right signature: Mit einer usage right (UR) signature kann festgelegt werden, welche Funktionalitäten in einem PDF-Reader genutzt werden können.

**MUST NOT:** usage rights signature (UR) dürfen nicht verwendet werden.

b) certification signature: Mit einer certification signature, auch author signature genannt, kann festgelegt werden, welche Änderungen im Dokument nach dem Leisten der certification signature vorgenommen werden können, ohne dass dabei die Signatur ungültig wird. Z.B. können Kommentare ins signierte PDF hinzugefügt werden, ohne dass dabei die Signatur ungültig wird.

Das Festlegen der Modifikationsmöglichkeiten an einem PDF nach einer PDF-Signatur darf bei beiden ISO Versionen 32000-1 und 32000-2 nur einmal im PDF auftreten.

c) approval signature: In einem PDF können beliebig viele approval signature vorhanden sein. Dabei

kann auch festgelegt werden, welche Felder im PDF genau nachträglich noch verändert werden können, ohne dass die Signatur ungültig wird.

**SHOULD:** Bevor eine approval signature angefertigt wird, soll geprüft werden, ob die Zertifikate zur Verifikation der zuvor geleisteten PDF-Signaturen noch gültig sind.

**SHOULD NOT:** Falls nicht alle gültig sind, soll keine PDF-Signatur mehr beigefügt werden.

**Anmerkung:** Ein Dokumentzeitstempel, welcher erst ab ISO 32000-2 standardmässig im PDF unterstützt wird, kann angefügt werden, unabhängig davon, wie die Restriktionen mittels der certification signature oder der approval signature zuvor im PDF definiert worden sind.

**SHOULD NOT:** Nach einem Dokumentzeitstempel soll keine approval signature mehr beigefügt werden. Entsprechende Vorkehrungen sollen beim Anfertigen des Dokumentzeitstempels getroffen werden.

## 2.5 Sicherheit von PDF und PDF-Signaturen

### 2.5.1 Beurkundung

**MUST:** Soll mit einer PDF-Signatur nicht nur dem Dokument Authentizität verliehen, sondern etwas beurkundet werden, dann muss die Signatur das ganze Dokument erfassen. Jegliche nachträgliche Änderung am Dokument muss zur Folge haben, dass die PDF-Signatur im Dokument ungültig wird. Mit Ausnahme, dass eine weitere approval signature zur Gegenzeichnung des bereits signierten Dokuments oder ein Dokumentzeitstempel beigefügt werden kann.

Es kann z.B. konfiguriert werden, dass die certification signature im Dokument nicht erscheint.

**MUST:** Bei einer Urkunde müssen alle (PDF)-Signaturen  für eine natürliche Person am Bildschirm erkennbar sein.

**Anmerkung:** Zum Begriff Urkunde, siehe Art. 110 Abs. 4 und 5 StGB und Art 177 ZPO. Erläuterungen hierzu betreffend Strafrecht siehe [5] Kommentar S. 1126, betreffend Zivilrecht siehe [7], S. 318.

### 2.5.2 Risiken durch PDF

Mittels eines PDF können Angriffe gestartet werden, siehe [3]. Ob diese erfolgreich sind, hängt davon ab, ob der PDF-Reader diese zu erkennen vermag. Nicht jeder Reader vermag gleich gut, solche Angriffe zu erkennen und abzuwehren. Dies geht aus dem erwähnten Paper [3] hervor. Welche Anforderungen der Reader zu erfüllen hat, hängt von den Sicherheitsanforderungen und den bestehenden Abwehrmassnahmen ab. Die Mindestanforderungen an einen Reader liegen ausserhalb des Themenbereichs dieses Standards und werden hier nicht behandelt.

**Anmerkung:** Die Untersuchung in [3] erfolgte auf Basis des PDF 1.7 Formats (ISO-32000-1).

### 2.5.3 Risiken in der Prüfung von PDF-Signaturen

Eine PDF-Signatur kann die Authentizität und die Integrität des gesamten Dokuments schützen oder nur eines Teils davon. Erforderlich ist jedoch, dass Veränderungen des von der Signatur geschützten Teils bei der Verifikation der Signatur erkannt und dem Anwender oder der Anwenderin angezeigt werden. Doch nicht jeder Reader erfüllt diese Anforderungen gleich gut, siehe [4].

**Anmerkung:** Die Untersuchung erfolgte auf Basis des PDF 1.7 Formats (ISO-32000-1).

**MUST:** Ein PDF-Reader muss Veränderungen des durch die Signatur geschützten Teils bei der Signaturprüfung erkennen und den Anwender/Innen entsprechend anzeigen können.

**SHOULD:** Es soll ein Profil erstellt werden, was im (signierten) PDF zu prüfen ist, bevor mit der Prüfung der Signatur begonnen wird. Dies ist jedoch nicht Thema dieses Standards.

### 2.5.4 Externe Referenzen

**MUST:** Alle Informationen, welche für die Zusammenstellung und Präsentation des PDF-Dokuments benötigt werden, müssen im PDF selber enthalten sein.

Folglich:

> **MUST NOT:** Es dürfen keine externen Referenzen eingebaut werden, welche für das Erscheinungsbild oder die Aussagekraft des PDF-Dokuments relevant sind.
>
> **MUST NOT:** Der dynamische Import externer Informationen darf nicht vorgenommen werden, siehe ISO 32000-1 Kapitel 7.11.4.1

Beispiel JavaScript:

> **MUST NOT:** Es dürfen keine externen JavaScript Programme dynamisch importiert werden, siehe Kapitel 3.6.1 in [2]. Dynamisch importiert heisst: Im Dokument besteht eine Referenz auf ein PDF-externes JavaScript Programm, welches beim Öffnen des PDF-Dokuments geladen und darin ausgeführt wird.
>
> Zudem:
>
> **MUST:** Alle JavaScript Aktionen müssen von der ersten PDF-Signatur erfasst werden, welche eine Beurkundung darstellt. Änderungen in den JavaScript Aktionen und deren Parameter müssen die PDF-Signatur ungültig werden lassen, siehe dazu auch KAPITEL 2.5.5 «Legal Content Attestation».

### 2.5.5 Legal Content Attestation

Mit der Legal Content Attestation Dictionary kann vor dem Leisten der certificate signature angegeben werden, wie viele Elemente eines Typs im PDF erhalten sind, welche das Erscheinungsbild (engl. appearance) beim Empfänger des (signierten) PDF verändern könnten. D.h. der Empfänger des signierten PDF-Dokuments mag etwas Anderes darin sehen als derjenige, welcher die certification signature geleistet/angefertigt hat.

**SHOULD:** Zu einer certification signature soll eine Legal Content Attestation beigefügt werden.

> Aus ISO-32000-1 Kapitel 12.8.5 und ISO-32000-2 Kapitel 12.8.2.2.1 «A certification signature should have a legal attestation dictionary.»

**MUST:** Falls eine Legal Content Attestation beigefügt wird, so müssen die darin enthaltenen Angaben zu einem Typ mit den tatsächlich vorhanden Anzahl Elemente dieses Typs im PDF übereinstimmen.

**MUST:** Der Signature Handler muss prüfen, ob ein entsprechender Widerspruch vorliegt und dies entsprechend melden.

Hier ein Profil für eine Legal Attestation, sofern eingefügt, wenn das Dokument archiviert werden soll oder eine Urkunde ist, wobei die folgende Tabelle aus ISO 32000-2 (Tabelle 264) stammt. In ISO 32000-1 ist es Tabelle 259.

**MUST:** U.a. gestützt auf die Ausführungen im KAPITEL 2.5.4 «Externe Referenzen» muss folgendes Profil für Legal Content Attestation angewandt werden.

| Entry | Value /Explanation | Recommendation |
|---|---|---|
| JavaScriptActions | The number of ECMAScript actions found in the document | E (Eintrag erforderlich) |
| LaunchActions | The number of launch actions found in the document. | E. Der Wert muss 0 sein. |
| URIActions | The number of URI actions found in the document | E. Der Wert muss 0 sein. |
| MovieActions | The number of movie actions found in the document | E. Der Wert muss 0 sein. |
| SoundActions | The number of sound actions found in the document | E. Der Wert muss 0 sein. |
| HideAnnotationActions | The number of hide actions found in the document | E. Der Wert muss 0 sein. |
| GoToRemoteActions | The number of remote go-to actions found in the document | E. Der Wert muss 0 sein. |
| AlternateImages | The number of alternate images found in the document | E. Der Wert muss 0 sein. |
| ExternalStreams | The number of external streams found in the document. | E. Der Wert muss 0 sein. |
| TrueTypeFonts | The number of TrueType fonts found in the document. | Keine Beschränkung |
| ExternalRefXobjects | The number of reference XObjects found in the document | E. Der Wert muss 0 sein. |
| ExternalOPIdicts | The number of OPI dictionaries found in the document | E. Der Wert muss 0 sein. |
| NonEmbeddedFonts | The number of non-embedded fonts found in the document | E. Der Wert muss 0 sein. |
| DevDepGS_OP | The number of references to the graphics state parameter OP found in the document | E. Der Wert muss 0 sein. |

| Entry | Value /Explanation | Recommendation |
|---|---|---|
| DevDepGS_HT | The number of references to the graphics state parameter HT found in the document | E. Der Wert muss 0 sein. |
| DevDepGS_TR | The number of references to the graphics state parameter TR found in the document | E. Der Wert muss 0 sein. |
| DevDepGS_UCR | The number of references to the graphics state parameter UCR found in the document | E. Der Wert muss 0 sein. |
| DevDepGS_BG | The number of references to the graphics state parameter BG found in the document | E. Der Wert muss 0 sein. |
| DevDepGS_FL | The number of references to the graphics state parameter FL found in the document | E. Der Wert muss 0 sein. |
| Annotations | The number of annotations found in the document | E. Der Wert muss 0 sein. |
| OptionalContent | *true* if optional content is found in the document | E. Der Wert muss 0 sein |
| Attestation | An attestation, created by the author of the document, explaining the presence of any of the other entries in this dictionary or the presence of any other content affecting the legal integrity of the document. | E: MAY |

Tabelle 1: Empfehlungen zu den jeweiligen Parametern bei «Legal Contest Attestation».

## 2.6 Andere relevante Signaturen

Für die hier behandelte Thematik werden noch andere Signaturen als die Signatur in einem pdf-Dokument verwendet, nämlich Signaturen bei

- Zeitstempeln
- OCSP (online Certificate Status Protocol)-Antworten (Statusinformationen zu Zertifikaten)
- Zertifikaten
- Zertifikatsrevokationslisten (engl. Certificate Revocation List, kurz CRL).

## 2.7 Begriff Prüfinformation

Prüfinformationen sind Angaben, welche es erlauben, die Signatur und die Gültigkeit des dazugehörigen Zertifikats zum Zeitpunkt der Herstellung der Signatur zu verifizieren. Dies sind:

- Signaturzertifikat, womit die PDF-Signatur geprüft werden kann, wie auch die Zertifikatskette zur Prüfung des Signaturzertifikats (siehe Art. 2 Abs. c ZertES)
- Status der Gültigkeit eines Signaturzertifikats wie in einer OCSP-Antwort oder in einer CRL, sowie die Zertifikate zur Prüfung dieser Angaben
- Verlässliche Zeitangaben in Form eines Zeitstempels, sowie die Zertifikate zur Prüfung der Signatur des Zeitstempels

## 2.8 Herausforderungen/Zusammenfassung

### 2.8.1 Prüfinformation

Die ETSI Standards zur Bewahrung der Gültigkeit von PDF-Signaturen und XFA-Signaturen basieren auf ISO-32000-1. Doch ISO 32000-1 (PDF 1.7) enthält nicht alle Merkmale für die Bewahrung der Gültigkeit der PDF-Signaturen. Deswegen wurden Erweiterungen in ISO 32000-2 (PDF 2.0) eingeführt, welche in ISO-32000-1 (PDF 1.7) nicht enthalten sind, wie

- Dokumentzeitstempel
- Document Security Store (DSS), in welchem die Informationen für Langzeitprüfung (engl. Long Time Validation, kurz LTV) eingepackt werden können.
- Zusätzliche Subfilter, u.a. zur Bestimmung der zu verwendenden Algorithmen

Die nun in ISO 32000-2 (PDF. 2.0) enthaltenen Funktionen/Merkmale wurden von ETSI übernommen.

Zudem werden die Prüfinformationen zum Status der CMS-Signatur gemäss ISO-32000-1 (PDF 1.7) als signiertes «PDF -proprietäres» ASN.1 Attribut beigefügt, wobei dieses Attribut nicht mit den CAdES-Standards von ETSI konform ist. Gemäss ISO 32000-1 (PDF 1.7) muss die Prüfinformation bei der Erstellung der Signatur eingebettet werden.

**Anmerkung:** Ein nachträgliches Beifügen weiterer Prüfinformationen bei der PDF-Signatur hätte die Ungültigkeit der Signatur zur Folge.

### 2.8.2 Archivierung

Mit der Bewahrung der Gültigkeit von PDF-Signaturen wird oft angestrebt, das Dokument auch zu archivieren. Hierzu sind Normen in ISO 19005-x festgehalten und gibt es Empfehlungen bei KOST.

### 2.8.3 Abstimmung der Standards untereinander

Die Standards sind untereinander nicht abgestimmt. Z.B. das Attribut «signature-policy-identifier» muss nach ISO-32000-2 (PDF 2.0) als signiertes Attribut der PDF-Signatur beigefügt werden, während es bei ETSI EN 319 142-1 als signiertes Attribut beigefügt werden kann.

### 2.8.4 Zeitnähe der Standards

ISO 32000-2 (PDF 2.0) und ISO 19005-4 (PDFA/4) wurden erst 2020 publiziert. Folglich ist mit Verzögerungen bei der Umsetzung in Reader und Writer zu rechnen.

### 2.8.5 Sicherheit von PDF als Solches

PDF galt als noch vor ein paar Jahren als «sicher». Doch kann ein Einfallstor für Angriffe auf die Sicherheit des IT-Systems in einem PDF eingebaut werden, siehe dazu KAPITEL 2.5.2, 2.5.3, 2.5.4.

### 2.8.6 Produkte

Was der PDF-Writer schreibt, soll der PDF-Reader auch verstehen und prüfen können. Vom PDF-Reader wird erwartet, dass er alle Ausprägungen der Standards unterstützt, hier die dazu passenden ETSI-Standards, ISO-32000-1 (PDF 1.7) und ISO-32000-2 (PDF 2.0). Dabei soll er auch irgendwelche Veränderungen an Feldern im PDF erkennen können, welche von der PDF-Signatur erfasst werden.

### 2.8.7 PDF-Signatur

Üblicherweise können der CMS-Signatur unsignierte Attribute wie eine OCSP-Antwort nach dem Leisten der Signatur problemlos beigefügt werden. Bei der PDF-Signatur ist dies nicht möglich, weil die PDF-Signatur ins PDF eingebettet ist. Werden nachträglich unsignierte CMS-Attribute der PDF-Signatur beigefügt, führt dies zur Ungültigkeit der PDF-Signatur.

# 3 Zu den Komponenten

In diesem Kapitel wird empfohlen, wie die Hauptkomponenten für die Bewahrung Gültigkeit elektronischer Signaturen grundsätzlich anzuwenden oder beschaffen zu sein haben.

## 3.1 Zertifikate

### 3.1.1 Herkunft

Mit der Bewahrung der Gültigkeit (elektronisch) signierter Dokumente wird hauptsächlich bezweckt, dass zu einem späteren Zeitpunkt die Rechtsverbindlichkeit und die Aussagekraft einer (elektronischen) Signatur erhalten bleiben. U.a. dass belegt werden kann, dass eine Partei den Inhalt des Dokuments signiert hat.

**SHOULD:** Die Signatur eines zu archivierenden Dokumentes soll mit einem nach ZertES definierten Zertifikat (Art. 2 Bst. g und h ZertES) verifiziert werden. Anderes würde die verlässliche und allgemein anerkannte «Konservierung» der elektronisch signierten Dokumente möglicherweise erheblich erschweren, wenn nicht gar verunmöglichen. Die Normierung dessen liegt (im Moment) ausserhalb der Zielsetzung (engl. scope) dieses Dokuments.

### 3.1.2 Zeitliche Gültigkeit

**MUST NOT:** Ein Zertifikat darf nicht länger und nicht früher gültig sein, als das nächst höher gelegenen CA-Zertifikat in der Zertifikatskette. Das X.509 v3 Gültigkeitsmodell zur Verifikation des Zertifikats ist hier relevant, siehe ITU-T X.509 Kapitel 7.7 Certification path. Dieses Gültigkeitsmodell wird als Schalenmodell bezeichnet, siehe auch [1].

Eine Vordatierung eines geregelten oder qualifizierten Zertifikats ist nicht erlaubt, d.h., dass das Zertifikat bereits vor dessen Ausstellungsdatum gültig ist. Es käme möglicherweise einer Falschbeurkundung gleich.

### 3.1.3 Format Zertifikate

**MUST:** Geregelte, resp. qualifizierte Zertifikate müssen die Bestimmung in der TAV, Kapitel 2.3.2, resp. 2.3.3 erfüllen.

## 3.2 Zeitstempel

### 3.2.1 Qualität der Zeitstempel

Zu der hier vorgeschlagenen Methode betreffend Erhalt der Gültigkeit elektronisch signierter Dokumente werden Zeitstempel verwendet.

**MUST:** Es müssen nach ZertES qualifizierte Zeitstempel verwendet werden, welche von einem nach ZertES anerkannten CSP (Zertifizierungsdienstanbieter) ausgestellt werden (Art. 2 Bst. j ZertES).

### 3.2.2 Format der Zeitstempel

**MUST:** Das Format der Zeitstempel muss die Bestimmung in der TAV, Kapitel 2.4 Abs. b erfüllen. Gemäss TAV müssen Zeitstempel erzeugt werden, welche dem Standard ETSI EN 319 422 entsprechen.

**MUST NOT:** Es besteht gemäss ETSI-Standard TS 101 903 V1.4.2 noch die Möglichkeit Zeitstempel im XML-Format beizufügen, siehe dort Kapitel 7.1.4.2. Diese dürfen folglich in diesem Kontext nicht verwendet werden, u.a. weil sie (rechtlich) nicht anerkannt sind.

## 3.3 Format der OSCP-Antworten

**MUST:** Das Format der OCSP-Antwort muss dem Standard RFC 6960 entsprechen.

**SHOULD:** Der OCSP-Antwort soll die Zertifikatskette zur Prüfung der OCSP-Signatur beigefügt werden.

Die Zertifikatskette zur Prüfung der OCSP-Antwort ist entweder der CMS-Signatur der OCSP-Antwort als unsigniertes Attribut in «certificate-values» und «revocation-values» beizufügen. Oder die OCSP-Antwort als solches oder ihre Zertifikatskette können in den Document Security Store (DSS) nachträglich abgelegt werden. Im DSS können die OCSP-Antwort und die dazu gehörige Zertifikatskette auch in einem separaten Feld abgelegt werden.

Bei einer XML-Signatur kann die Zertifikatskette zur OCSP-Antwort dem XML-Element «Revocation-Values» beigefügt werden.

## 3.4 Format der XML-Signatur

Aus eCH-0230, Kapitel 2.4:

> **MUST:** Eine XML-Signatur muss dem Standard XML Signature Syntax von W3C entsprechen. Was noch Bestandteil der Signatur sein kann/muss oder nicht sein soll/darf, siehe ETSI TS 101 903 V1.4.2 und eCH-0091. Zu Bewahrung der Gültigkeit von XML-Signaturen, siehe eCH-0230.

## 3.5 Format der CMS-Signatur

Zu den CMS-Formaten siehe eCH-0220.

## 3.6 Zeitstempel

### 3.6.1 Zeitstempel zu einer PDF-Signatur

PDF-Signaturen kennen im Unterschied zu CAdES (siehe eCH-0220) nur folgende 3 Arten von Zeitstempeln:

- Inhaltszeitstempel (engl. content timestamp). Hier wird Zeitstempel darüber angefertigt, was später zu signieren sein wird. Damit wird belegt, dass die Signatur zu einem späteren Zeitpunkt (als die Zeitangabe im Zeitstempel) angefertigt wurde.
- Signaturzeitstempel (signature timestamp), welcher die Signatur erfasst.) Damit wird belegt, dass die Signatur vor einem Zeitpunkt (Zeitangabe im Zeitstempel) angefertigt wurde.
- Dokumentzeitstempel, welcher das gesamte PDF-Dokument erfasst. Der Dokumentzeitstempel entspricht in etwa dem Archivzeitstempel bei CAdES und einer Dokument umfassenden PDF-Signatur, nur dass die Signatur nicht von dem User oder der Userin, sondern vom Zeitstempeldienst beigesteuert worden ist. Der Dokumentzeitstempel wird jedoch erst ab ISO-32000-2 (PDF 2.0) von ISO standardmässig unterstützt.

**Anmerkung:** Eine PDF-Signatur ist in einem PDF-Dokument eingebettet. Also können keine zusätzlichen Informationen der PDF-Signatur nachträglich beigefügt werden, ohne dass dabei die Signatur ungültig wird.

Illustration: Der CMS-Signatur können grundsätzlich weitere Informationen (unsignierte Attribute) beigefügt werden, ohne dass die CMS-Signatur ungültig wird. Bei der PDF-Signatur, eine besondere Ausprägung der CMS-Signatur, ist dies nicht möglich, ansonsten wird die PDF-Signatur ungültig. Der Grund dafür liegt darin, dass die PDF-Signatur im PDF eingebettet ist, siehe ETSI TS102 778 Kapitel 4.

### 3.6.2 Zeitstempel in XML-Objekten

Zu den möglichen Ausprägungen/Inhalten von Zeitstempeln, siehe eCH-0230, Tabelle 1. Zusätzlich besteht die Möglichkeit, ein Dokumentzeitstempel an ein in ein PDF eingebettetes XFA-Dokument beizufügen.

# 4 Profil

In diesem Kapitel wird für die jeweiligen ETSI Standards definiert, was davon zu nutzen und wie anzuwenden ist.

## 4.1 Grundsätzliches

### 4.1.1 Empfehlungen zur XML-Signatur

Siehe hierzu eCH-0230 und eCH-0091.

### 4.1.2 Empfehlungen zur PDF-Signatur

**SHOULD:** Siehe hierzu eCH-0220. Anders als in den ETSI-Standards zu PAdES soll bei der Anfertigung einer CMS-Signatur nur die Version in RFC 5652 unterstützt werden.

**MUST NOT:** Signaturen im PKCS#1 Format dürfen nicht verwendet werden.

Grund: PKCS#1 signatures are deprecated with 32000-2 (PDF 2.0).

### 4.1.3 Ablage der Prüfinformation

ISO 32000-2 (PDF 2.0) kennt folgende 4 verschiedene Orte, wo eine Prüfinformation zur Verifikation der PDF-Signaturen und zur Verifikation der Signaturen der Prüfinformation abgelegt werden kann:

1. In «Cert» im Signature Dictionary (für die Zertifikatskette) zur Prüfung der PDF-Signatur als solches.
2. Als unsigniertes Attribut bei der CMS-Signatur
3. ASN.1 Objekt «adbe-revocationInfoArchival», wo die OCSP Antwort und die CRL eingepackt werden können.
4. Im Document Security Store (DSS)

ISO 32000-1 (PDF 1.7) kennt 1, 2 und 3, ISO 32000-2 empfiehlt 2, 3, 4, während ETSI nur 2 und 4 unterstützt.

Anmerkung: «Cert» und «adbe-revocationInfoArchival» sind signierte Objekte, d.h. sie werden von der PDF-Signatur erfasst. Zu «adbe-revocationInfoArchival», siehe ISO 32000-1, Kapitel 12.8.3.3.1.

#### 4.1.3.1 Document Security Store

Inhalt und Eigenschaft des Document Security Store (DSS) wird in Kapitel 12.8.4.3 «Document Security Store (DSS)» in ISO 32000-2 beschrieben. Das Zusammenspiel zwischen DSS und DZT wird dort in Figur 86 und in Figur 2 und 3 in ETSI EN 319 142-1 illustriert.

#### 4.1.3.2 Empfehlungen

**MUST NOT:** «Cert» darf nicht verwendet werden.

**SHOULD NOT:** «adbe-revocationInfoArchival» soll nicht verwendet werden.

Begründung:

- In den ETSI-Standards ETSI EN 319 142-1 und ETSI EN 319 142-2 wird dieses Objekt nicht abgehandelt.
- Mit «adbe-revocationInfoArchival» wird nicht belegt, dass das Zertifikat gültig war, bevor die Signatur geleistet wurde. Ausser es wird unmittelbar danach ein Zeitstempel angefertigt, dessen Prüfinformation jedoch nicht in «adbe-revocationInfoArchival» enthalten ist.

**SHOULD:** Das Zertifikat zur Verifikation der PDF-Signatur soll beigelegt werden, wie auch die Zertifikatskette zur Verifikation dieses Zertifikats. Informationen zum Status des Zertifikats sollen ebenfalls beigefügt werden. Wenn möglich sollen die Informationen zwecks Kompatibilität mit ISO 32000-1 der CMS Signatur beigefügt werden, ansonsten im DSS.

**SHOULD:** Es sollen möglichst viele Informationen zur Prüfung der Signatur und zum Status des Signatur-Zertifikats wie Zertifikationsrevokationsliste (CRL) oder OCSP-Antworte beigefügt werden. Die Informationen sollen zum Zeitpunkt der Herstellung der PDF-Signatur geprüft und als gültig erachtet worden sein.

**SHOULD:** Der Status des Zertifikats soll priorisiert mittels OCSP-Antworten angegeben werden.

**Anmerkung:** Werden diese Antworten bei der Herstellung der PDF-Signatur nicht beigefügt, so können sie der PDF-Signatur später nicht mehr eingebunden werden. Werden der PDF-Signatur nachträglich unsignierte Attribute beigefügt, so wird die Signatur ungültig.

Falls die Prüfinformationen vor dem Signieren nicht beigefügt wurden, so können sie später im PDF über den Document Security Store Dictionary (DSS) noch ergänzt werden, siehe ETSI TS 102 778-4.

#### 4.1.4 Prüfung der PDF-Signatur

In ISO 32000-2 Kapitel 12.8.3.4.5 bis 12.8.3.4.8 sind Vorgaben zur Prüfung der PDF-Signatur enthalten.

**MUST:** Diese Mindestvorgaben an die Prüfung einer elektronischen Signatur müssen eingehalten werden.

### 4.2 ETSI TS 102 778-1

ETSI TS 102 778-1 gibt einen Überblick über die Thematik von PDF-Signaturen und XML-Signaturen in einem PDF. ETSI TS 102 778-2 bis 4 bespricht die Bewahrung der Gültigkeit von Signaturen im CMS-Format.

### 4.3 ETSI TS 102 778-2

In diesem Standard werden allgemeine Richtlinien zur Anfertigung einer PDF-Signatur definiert.

#### 4.3.1 Subfilter für PDF-Signaturen

Über «Subfilter» wird u.a. der mögliche Satz an Algorithmen definiert, welche für die Bildung der PDF-Signatur verwendet werden können. ISO 32000-2 (Tabelle 260) unterstützt mehr Klassen an Subfiltern und Algorithmen als ISO 32000-1 (Tabelle 257).

ISO 32000-2 kennt gegenüber ISO 32000-1 noch die Subfilter «ETSI.CAdES.detached» und «ETSI.RFC3161».

**MUST NOT:** «ETSI.RFC3161» darf bei der Bildung der PDF-Signatur nicht verwendet werden (gemäss ISO-32000-2), weil dieser Subfilter einzig für den Dokumentzeitstempel vorgesehen ist.

**SHOULD:** Die in ISO-32000-1 aufgeführten Subfilter sollen zwecks Kompatibilität verwendet werden. Wobei:

**MUST NOT:** Der Subfilter «adbe.x509.rsa_sha1» darf nicht verwendet werden.

**MUST:** Falls eine PDF-Signatur mit Elliptischen Kurven angefertigt werden soll, dann muss der Subfilter «ETSI.CAdES.detached» verwendet werden. Elliptische Kurven werden standardmässig erst bei

ISO-32000-2 (PDF 2.0) unterstützt. Dieser Subfilter ist u.a. dafür angedacht.

#### 4.3.2 seed value (signature field, certificate)

Aus ETSI EN 319 142-2 V1.1.1, Anhang A8:

> When preparing a document or form to be signed in the future, the author of the form can add to the signature field some additional entries (ISO 32000-1 [1], clause 12.7.4.5, table 232) including one called a seed value dictionary. A seed value dictionary (ISO 32000-1 [1], clause 12.7.4.5, table 234) contains information that conveys a set of rules (or policies) that the form's author wishes the signature handler to enforce at the time the signature is applied. These wishes can be specified either as requirements or recommendations.

Über das seed value Dictionary kann die Dokumentverarbeitung im Rahmen des Leistens einer elektronischen Signatur wie auch deren Ausprägung gesteuert werden. Z.B. kann über den seed value definiert werden, welcher Hash Algorithmus für die Signatur verwendet werden muss.

Im seed value wird auf im PDF enthaltene Informationen referenziert, siehe Tabelle 234 und 235 in ISO 32000-1 und in [2], Kapitel 6.1.2. Was mit welcher PDF-Version gesteuert werden kann, ist in ISO 32000-2 in Tabelle 237 und 238 beschrieben.

**MAY:** Der seed value kann eingefügt werden.

**MUST:** Falls der seed value eingefügt wird, dann müssen die darin enthaltenen Vorgaben mit den Empfehlungen in diesem Dokument übereinstimmen. D.h. u.a. der Signature Handler muss fähig sein, die im seed value enthaltenen Vorgaben zu befolgen, siehe auch Kapitel 4.2.6 ETSI EN 319 142-2.

Im KAPITEL 5.1.3 wird in Form einer Zusammenfassung dargelegt, welche Eigenschaften oder welche Konfiguration der seed value haben kann, damit er den in diesem Standard gemachten Empfehlungen entspricht.

### 4.4 ETSI TS 102 778-3

ETSI TS 102 778-2 definiert die Signaturbildung. ETSI TS 102 778-3 wird als Erweiterung zur Bewahrung der Gültigkeit von Signaturen in einem PDF erachtet. Doch die in ETSI TS 102 778-3 besprochenen Erweiterungen enthalten Attribute, welche von der CMS-Signatur erfasst werden müssen und nicht nachträglich hinzugefügt werden können.

#### 4.4.1 Zur Diskussion stehende (obligatorische) CMS-Attribute

##### 4.4.1.1 content-type Attribut

Im Unterschied zu ETSI EN 319 122-1 ist der Wert des content-type Attributes vorgeschrieben.

**MUST:** Der Wert «id-data» muss verwendet werden.

##### 4.4.1.2 message-digest Attribut

**MUST:** Message-digest Attribut muss beigefügt werden.

#### 4.4.1.3 signature-policy-identifier Attribute

Die Empfehlung in ETSI EN 319 142-1 widerspricht den Empfehlungen in ISO 32000-2 (PDF2.0) S. 582.

Gemäss ETSI EN 319 142-1 kann das zu signierende Attribut enthalten sein, während es bei ISO 32000-2 in der CMS-Signatur enthalten sein muss.

**SHOULD NOT:** Externe Referenzen auf Informationen zu einer Signatur sollen nicht enthalten sein.

#### 4.4.1.4 Referenz auf Signatur-Verifikationszertifikat

Siehe hierzu die Anmerkungen zu den Attributen ESS signing certificate und ESS signing-certificate – v2 in eCH-0220.

### 4.4.2 signature-time-stamp

**MUST:** Das Attribut signature-time-stamp mit einem darin enthaltenen Zeitstempel gemäss KAPITEL 3.2.1 «Qualität der Zeitstempel» muss enthalten sein.

**Anmerkung:** Eine qualifizierte Signatur nach Art. 12 Abs. 2$^{bis}$ OR erfordert einen Zeitstempel dieser Güteklasse.

### 4.4.3 Weitere Attribute

Es besteht die Möglichkeit, gleiche oder ähnliche Informationen an verschiedenen Stellen anzubringen.

1. im Text des Dokuments
2. zusätzlichen Angaben in der Signature Dictionary des PDF
3. wie auch in einem CMS-Attribut.

Z.B. kann der Ort angegeben werden, wo die Signatur geleistet wurde, oder der Grund dafür.

**SHOULD:** Diese Informationen sollen, wenn überhaupt, in der oben genannten Reihenfolge eingefügt werden. Dabei soll auf die darauf folgende Möglichkeit, die Information auch noch einzufügen, verzichtet werden. Grund für die empfohlene Priorisierung: Die Sichtbarkeit der Information ist für den Anwender oder die Anwenderin bei 1) grösser als bei 2), bei 2) wiederum grösser als bei 3)

Zu Erklärungen und Absichten des Unterzeichnenden, siehe Kapitel 3.1.2.8 in eCH-0220.

> **SHOULD NOT:** Die Erklärungen und Absichten, welche mit der Signatur abgegeben wurden, sollen aus dem zu signierenden Dokument zu entnehmen sein. Deswegen soll dieses Attribut nicht verwendet werden.

In ETSI EN 319 142-2, welcher eine höhere normative Bedeutung besitzt als ETSI TS 102 778-3, äussert sich auf S. 9 Abs. c wie folgt:

> «Some signature attributes found in CAdES [2] have the same or similar meaning as keys in the Signature Dictionary described in ISO 32000-1. For signature attributes and keys that have the same or similar meaning only one of them should be used according to the requirements set in table defined in clause 6.3 in the present document.»

Diese Aussage kann im Widerspruch zu den Empfehlungen in ETSI TS 102 778-3 stehen. Denn gemäss ETSI TS 102 778-3 dürfen die Attribute dort in Kapitel 4.5.3 bis 4.5.7 und 4.5.9, 4.5.10 nicht eingefügt werden.

Zu Attributen, welche vom Signierenden der Signatur beigegeben werden können, wird auf Folgendes im Kapitel 3.1.2.10 eCH-0220 verwiesen:

> **SHOULD NOT:** claimed attributes sollen nicht verwendet werden. Angaben, welche vom Unterzeichnenden in den «Raum gestellt werden», können zu einem späteren Zeitpunkt meist nicht verlässlich nachgewiesen und sollen folglich vermieden werden.

Zu Verweisen auf Policies, siehe Kapitel 3.1.2.4 in eCH-0220:

> **SHOULD NOT:** Policies sollen in der Signatur nicht referenziert werden. Folglich soll dieses Attribut nicht verwendet werden.

## 4.5 ETSI TS 102 778-4

Im Wesentlichen wird hier die Anfertigung des Dokumentzeitstempels an ein PDF genormt. Dieser Standard wurde durch ETSI EN 319 142-1 und -2 überholt.

## 4.6 ETSI TS 102 778-5

**Anmerkung:** Wie bereits im KAPITEL 2.3 «XFA» erwähnt, wird XFA von Adobe nicht mehr unterstützt und gilt bei ISO 32000-2 (PDF 2.0) als überholt. Deswegen hat dieses Unterkapitel keinen normativen Charakter.

ETSI TS 102 778-5 normt die Verwendung und die Bewahrung der Gültigkeit von XML-Signaturen von XML-Objekten in einem XFA-Objekt und die XML-Signatur über ein XFA-Objekt. Das XFA-Objekt ist dabei in ein PDF eingebettet.

### 4.6.1 Formen von XML-Signaturen in einem XFA Dokument

Es gibt grundsätzlich folgende 3 Formen, XML in einem PDF zu signieren:

1. XML-Signatur von XML-Objekten in einem XFA, eingebettet in einem PDF
2. XML-Signatur eines XFA-Objekts, eingebettet in einem PDF
3. PDF-Signatur eines PDF mit einem XFA-Objekt oder darin enthaltenen XML-Objekten

Die Bewahrung der Gültigkeit der Item 1 und 2 wird in dem hier zur Diskussion stehenden Standard genormt, während letzteres in ETSI TS 102 778-4, resp. in ETSI EN 319 142-1 und ETSI EN 319 142-2 standardisiert wird.

### 4.6.2 Grundsätzliches

Vereinfacht ausgedrückt ist XFA ein auf XML basierendes Objekt, welches in ein PDF eingebettet werden oder sich als XML-Dokument präsentieren kann.

**Anmerkung**: In ETSI TS 102 778-5, Kapitel 1, Note 3:

> «Readers should be aware that although PDF documents are addressed for human beings,

XFA forms, being them based on XML, may be consumed by software applications.»

**Hinweis, Anregung:** XFA bietet Anwender/innen (natürlichen Personen) eingeschränkt die Möglichkeit, zu sehen, was sie signieren, Deshalb könnte ein XFA zuerst in ein PDF/A-2 umgewandelt werden. Dies würde dann dem Anwender oder von der Anwenderin signiert. Damit die Möglichkeit der Datenverarbeitung nach der Umwandlung des XFA in ein PDF/A-2 oder gegebenenfalls in ein PDF/A-4 nicht allzu sehr eingeschränkt wird, können die Daten in einem Barcode oder QR-Code gespeichert und dieser ins PDF vor dem Leisten der Signatur integriert werden.

Hinweis in ETSI TS 102 778-5, Kapitel 1, Note 1:

> «Implementers should be aware that any subsequent approval signature (see ISO 32000-1 [4] clause 12.8.1) as specified in TS 102 778-2 [i.7], TS 102 778-3 [i.8] or TS 102 778-4 [i.9] also signs the embedded signed XML document. Any upgrade of the XAdES signature of the present document to support validation long after the expiration of the signing certificate or other extended features such a countersignatures (e.g. using XAdES-C or XAdES-X or XAdES-A) would invalidate the aforementioned approval signatures. Implementers should also be aware that certification signatures (see ISO 32000-1 [4] clause 12.8.1) as specified in TS 102 778-2 [i.7], TS 102 778-3 [i.8] or TS 102 778-4 [i.9] signing the embedded signed XML document, may be used in conjunction with the DocMDP dictionary, allowing changes in the embedded signed XML document (by upgrading the XAdES signatures, for example) without invalidating such signatures.»

Ziel und Zweck der Signatur ist es, Veränderungen im Dokument zu erkennen und das Dokument dem Signierenden zuzuordnen. Dies widerspricht aber nun der Möglichkeit, dass Veränderungen im Dokument vorgenommen werden können, ohne dass die Signatur dabei ungültig wird. Deswegen wird hier auf die Empfehlungen im KAPITEL 4.9 in diesem Dokument verwiesen.

In eCH-0091 ist u.a. aufgeführt, was bei der Erstellung einer XML-Signatur zu beachten ist. Weitere Empfehlungen zur XML-Signatur betreffend XFA im KAPITEL 4.9 dieses Dokuments.

### 4.6.3 Profil

Die hier erstellten Empfehlungen sind durch ETSI EN 319 142-2 überholt worden. (Wie bereits erwähnt, die Standards mit der Bezeichnung «EN» im Titel gehen solchen mit «TS» vor). Das Profil zu weiteren in ETSI TS 102 778-5 abgehandelten Themen wird im KAPITEL 4.9 «ETSI EN 319 142-2» vorgestellt.

## 4.7 ETSI TS 102 778-6

In diesem Standard wird festgelegt, was sich als Ergebnis einer Signaturprüfung dem Leser eines signierten PDF-Dokumentes zu präsentieren hat.

**MUST:** Alle in ETSI TS 102 778-6 beschriebener Anforderungen müssen erfüllt sein.

## 4.8 ETSI EN 319 142-1

ETSI EN 319 142-1 standardisiert die Attribute/Infos, welche dem PDF-Dokument mit ein oder mehreren PDF-Signaturen beigefügt werden kann/muss/soll/darf oder soll nicht. Dies mit dem Ziel, dass die

Gültigkeit der PDF-Signaturen nachweislich bewahrt werden kann. Die Bewahrung der Gültigkeit basiert darauf, dass beim Anfertigen des Dokumentzeitstempels alle Informationen, welche für die Prüfung der zuvor geleisteten PDF Signaturen und erhaltenen OCSP-Antworten und CRL gesammelt und im PDF abgespeichert werden. Zudem werden Ausprägungen zum Dokumentzeitstempel ETSI EN 319 142-1 normiert.

Im Folgenden werden Ergänzungen zum Standard aufgeführt und Empfehlungen im Standard anders gewertet.

### 4.8.1 Verwalten/Sammeln der Prüfinformationen als Solches

**MUST NOT:** Es dürfen keine Referenzen auf Prüfinformationen enthalten sein, die ausserhalb des PDF gespeichert sind und für die Prüfung relevant sind. Ausnahme bildet der zuletzt angefertigte Dokumentzeitstempel. Dessen Prüfinformationen müssen erst vor Anfertigen des nächst folgenden Zeitstempels beigefügt werden.

**MUST:** Die Prüfinformationen (CA-Zertifikate) zur Verifikation der OSCP- oder CRL-Signaturen sind ebenfalls beizulegen.

**MAY:** Die zur OCSP-Signatur gehörenden Prüfinformationen kann der OCSP-Signatur in einem PDF nach ISO-32000-1 (PDF 1.7) beigelegt werden.

**MAY:** Die zur CRL-Signatur gehörenden Prüfinformationen kann der Signatur in einem PDF nach ISO-32000-1 (PDF 1.7) beigelegt werden.

**SHOULD:** Gemäss ISO-32000-2 (PDF 2.0) sollen die Prüfinformationen für die OCSP-Signatur und für die CRL in den Document Security Store (DSS) abgelegt werden.

### 4.8.2 Dokumentzeitstempel

#### 4.8.2.1 SubFilter für Dokumentstempel (DZS)

**MUST:** Für Dokumentzeitstempel muss der Subfilter «ETSI.RFC3161» verwendet werden.

**Anmerkung:** Gemäss ISO 32000-2 und ETSI soll dieser Filter verwendet werden. ISO 32000-1 kennt den Dokumentzeitstempel wie auch diesen Subfilter nicht.

#### 4.8.2.2 Anfertigen des 1. Dokumentzeitstempels (DZS)

Sofern nicht bereits irgendwo anders enthalten:

> **MUST:** Unmittelbar vor dem Anfertigen des Dokumentzeitstempels sind die aktuellsten Prüfinformationen (OCSP, CRL) zum Status der Zertifikate zu den PDF Signaturen zu sammeln und im DSS des PDF abzuspeichern.
>
> Zudem muss die Zertifikatskette zu den PDF Signaturen abgelegt werden, wie auch die Zertifikatsketten zur Prüfung der OCSP-Antworten oder der CRL.
>
> **MUST:** Alle Signaturen müssen vor dem Erstellen des ersten Dokumentzeitstempels gültig sein. u.a. auch die certification signature.
>
> **MUST NOT:** Ansonsten darf kein Dokumentzeitstempel erstellt werden.

**SHOULD NOT:** Falls nicht mehr alle Signaturen vor dem ersten Dokumentzeitstempel gültig sind, dann soll die PDF-Signatur nicht mehr akzeptiert werden.

#### 4.8.2.3 Anfertigen des 2. und weiterer Dokumentzeitstempels

Vor Anfertigen des darauf folgenden Dokumentzeitstempels:

> **MUST:** Die Prüfinformationen (CRL, OCSP) zur Verifikation der Signatur des Dokumentzeitstempels sind abzuspeichern.
>
> **MUST:** Die Zertifikatskette zum Verifizieren der Signatur des Dokumentzeitstempels wie auch der Signatur der OSCP-Antworten und der CRL sind zu sammeln und abzulegen.
>
> **MUST:** Die Gültigkeit des vorangehenden Dokumentzeitstempel muss geprüft werden.

**SHOULD:** Wird der DZS als nicht mehr gültig erachtet, soll nicht ein weiterer DZS angefertigt und eingefügt werden.

### 4.8.3 Andere Bewertung der Empfehlungen

#### 4.8.3.1 Verschlüsselung

In Kapitel 5.5 EN 319 142-1 wird erwähnt, dass eine Verschlüsselung vor dem Leisten der Signatur vorgenommen werden muss. Hier gilt es zu unterscheiden.

**MUST:** Wird mit der Signatur etwas beurkundet, dann muss sie vor der Verschlüsselung angebracht werden. Grundsätzlich muss die Gültigkeit des Beurkundeten und nicht des Verschlüsselten bewahrt werden.

**SHOULD:** Dient die Signatur lediglich der Authentizität, dann soll sie nach der Verschlüsselung angefertigt werden. Damit reduziert sich das Risiko, dass der Empfänger etwas entschlüsselt, deren Ursprung er nicht zuzuordnen vermag.

#### 4.8.3.2 content-time-stamp

content-time-stamp ist ein signiertes Attribut. Darin ist eine verlässliche Zeitangabe t in Form eines Zeitstempels enthalten, Damit soll belegt, dass die PDF-Signatur nach diesem Zeitpunkt t erstellt wurde.

**SHOULD NOT:** Das content-time-stamp Attribut soll nicht verwendet werden. In ISO-32000-1 (PDF 1.7) und -2 (PDF 2.0) ist es nicht definiert und gemäss EN 319 142-1 (MAY) kann es enthalten sein.

**Anmerkung:** Hier liegt eine unterschiedliche Empfehlung zu eCH-0220 vor.

#### 4.8.3.3 signature-time-stamp

**MUST:** Das Attribut signature-time-stamp mit einem darin enthaltenen Zeitstempel gemäss Kapitel 3.2.1 «Qualität der Zeitstempel» muss enthalten sein.

**Anmerkung:** Eine qualifizierte Signatur nach Art. 12 Abs. $2^{bis}$ OR erfordert einen Zeitstempel dieser Güteklasse.

#### 4.8.3.4 Angaben zum Signierenden

**SHOULD NOT:** Angaben wie Ort, Grund des Leistens der Signatur oder die Kontaktadresse des Signierenden sollen nicht als Metadaten der PDF-Signatur aufgeführt werden, sondern aus dem Dokument zu entnehmen sein, siehe hierzu auch KAPITEL 4.4.3 «Weitere Attribute»

## 4.9 ETSI EN 319 142-2

Wie bereits im KAPITEL 2.3 «XFA» erwähnt, wird XFA von Adobe nicht mehr unterstützt und gilt bei ISO 32000-2 (PDF 2.0) als überholt. Deswegen hat dieses Unterkapitel keinen normativen Charakter.

### 4.9.1 Allgemeine Ergänzungen

**MUST:** Die Zertifikatskette zur Prüfung der XML-Signatur muss der XML-Signatur beigefügt werden.

**MUST:** Der Signaturzeitstempel (SignatureTimeStamp) muss der XML-Signatur beigefügt werden.

### 4.9.2 XML-Signatur über ein XFA- oder XML-Objekt in einem PDF

Grundsätzlich kann die Gültigkeit der XML-Signaturen von Objekten in einem XFA-Objekt oder über ein XFA-Objekt gemäss eCH-0230 bewahrt werden. Dies funktioniert dann aber nicht mehr, wenn zuvor oder danach eine PDF-Signatur angefertigt wurde. Zur Bewahrung der Gültigkeit einer PDF-Signatur bedarf es eines Dokumentzeitstempels. Nach einem Dokumentzeitstempel ist ein Update der XML-Signatur mit einem Zeitstempel gemäss eCH-0230 (XAdES) nicht mehr möglich. Dies hätte die Ungültigkeit des Dokumentzeitstempels oder der PDF-Signatur zur Folge.

### 4.9.3 LTV einer XML-Signatur mit einem (PDF-)DZS

Die Bewahrung der Gültigkeit einer XML-Signatur (eines XML-Dokuments oder eines XML-Objekts) in einem PDF kann über den Dokumentzeitstempel und Document Security Store (DSS) analog zu einer PDF-Signatur bewerkstelligt werden.

Wie das bewerkstelligt werden kann, siehe den informellen Annex A in ETSI TS 102 778-5 V1.1.2.

Anmerkung: Die LTV mit einem DZS zu errichten, ist z.B. nach einer PDF Signatur über ein PDF mit eingebettetem XFA oder XML-Objekten erforderlich.

# 5 Zusammenfassung

In den folgenden Tabellen ist eine Zusammenfassung über die hier behandelten und relevanten Attribute zusammengestellt.

## 5.1 PDF-Signatur

### 5.1.1 CMS-Attribute

In folgender Tabelle werden die Attribute bei einer CMS-Signatur in einem PDF aufgeführt. Es können sich dabei zu eCH-0220 unterschiedliche Empfehlungen ergeben.

| Nr | Attribut | Signiert | Emp. | Bem |
|---|---|---|---|---|
| 1. | content-type Attribut | J | M | Wert: «id-data» |
| 2. | countersignature | J | MN | |
| 3. | content-hints Attribute | J | MN | |
| 4. | signature-policy-identifier | J | SN | B, PDF-SIG |
| 5. | commitment-type-indication Attribute | J | SN | B, PDF-SIG |
| 6. | signer-location Attribute | J | SN | C, PDF-SIG |
| 7. | content-time-stamp Attribute | J | SN | |
| 8. | signature-time-stamp Attribute | N | M | |
| 9. | attribute-certificate-references Attribute | N | M, B | |
| 10. | attribute-revocation-references Attribute | N | M, B | |
| 11. | certificate-values Attribute | N | M, B | 2) |
| 12. | revocation-values Attribute | N | MAY, B | 1) über DZS |
| 13. | CAdES-C-time-stamp Attribute | N | MN | |
| 14. | time-stamped-certs-crls-references Attribute | N | MN | |
| 15. | archive-time-stamp Attribute | N | MN | |
| 16. | ats-hash-index Attribute | N | MN | |
| 17. | archive-time-stamp-v3 Attribute | N | MN | |
| 18. | long-term-validation Attribute | N | MN | |
| 19. | signer-attributes-v2 attribute | J | MAY | C |
| 20. | claimed-SAML-assertion | N | MN | |
| 21. | ats-hash-index-v2 attribute | N | MN | |
| 22. | signer-attributes Attribute | J | SN | C |
| 23. | ats-hash-index-v3 attribute | N | MN | |

Tabelle 2: Zusammenfassung der Empfehlungen zu den CMS-Attributen

Legende

A = Alternativ
B = Bedingt vorhanden
Bem = Bemerkung
C = Enthält ein «claimed attribute» des Signierenden. Diese vom Signierenden gemachte Angabe kann von einem Dritten nicht ohne weiteres verifiziert werden.
DZS = PDF-Dokumentzeitstempel
J = JA
M = MUST
MN = Must NOT
N = Nein

NE = Im Standard erwähnt, aber hier nicht behandelt, weil nicht anderer Meinung.

PDF-SIG die Information kann auch im PDF der Signatur beigegeben werden

S = SHOULD

Signiert = Bestandteil der zu archivierenden Dokument- oder Dateisignatur, d.h. der Inhalt des Attributs fliesst in Hashberechnung für die Signatur ein.

SN = SHOULD NOT

1) Die Revokationsinformationen können nachträglich auch über den DSS vor dem Anfertigen des DZS eingefügt werden.

2) Mindestens das Signaturzertifikat sollte der Signatur beigefügt werden. Weitere Prüfinformationen (Zertifikatskette) können später über den DSS eingefügt werden.

**SHOULD NOT:** Falls Attribute der PDF-Signatur beigegeben werden, soll die Information nicht auch noch als Attribut in der CMS-Signatur enthalten sein, und umgekehrt.

**Hinweis:** Falls CMS-Attribute nicht der CMS-Signatur beigegeben worden sind, dann können sie nicht nachträglich beigefügt werden, weil dann die PDF-Signatur ungültig wird.

### 5.1.2 Im PDF als Metadaten der PDF-Signatur mitgegeben

In folgender Tabelle sind PDF-Attribute aufgeführt, welche der PDF-Signatur als Metadaten beigegeben werden können:

| Nr | Attribut | Signiert | Emp. | Bem |
|---|---|---|---|---|
| 1 | Reason | J | SN | Er |
| 2 | Location | J | SN | Er, C |
| 3 | Legal Content Attestation | J | S | |
| 4 | Anforderung an das Zertifikat zur Verifikation der PDF-Signatur (OID im X.509 v3 Zertifikat) | J | MAY, B | 1) |
| 5 | Bestimmen des Herstellers des Zeitstempels | J | MAY | |
| 6 | Zeitpunkt der Signatur | J | SN | C, 2) |
| 7 | Kontakt | J | SN | Er |

Tabelle 3: Zusammenfassung der Empfehlungen zu den Attributen, welche der CMS Signatur beigegeben werden können.

Legende

A = Alternativ

B = Bedingt vorhanden

Bem = Bemerkung

C = Enthält ein «claimed attribute» des Signierenden. Diese vom Signierenden gemachte Angabe kann von einem Dritten nicht ohne weiteres verifiziert werden.

CMS = Info kann in der CMS-Signatur enthalten sein.

Er = Info sollte im PDF-Dokument enthalten sein.

J = JA

Signiert = Bestandteil der zu archivierenden Dokument- oder Dateisignatur, d.h. der Inhalt des Attributs fliesst in Hashberechnung für die Signatur ein.

SN = SHOULD NOT

1) Die Anforderung sollte aus dem rechtlichen Kontext hervorgehen.

2) Hier ist der Signaturzeitstempel relevant.

### 5.1.3 seed value

#### 5.1.3.1 signature field seed value

| Key | Value/Explanation/Begründung zur Empfehlung | Recommendation |
|---|---|---|
| Type | The type of PDF object that this dictionary describes; if present, shall be SV for a seed value dictionary. | MUST |
| Ff | A set of bit flags specifying the interpretation of specific entries in this dictionary. A value of 1 for the flag indicates that the associated entry is a required constraint.<br>Begründung: Es sind zwingende Vorgaben enthalten. | MUST |
| Filter | The signature handler that shall be used to sign the signature field, beginning with PDF 1.7 | SHOULD |
| SubFilter | An array of names indicating encodings to use when signing. The first name in the array that matches an encoding supported by the signature handler shall be the encoding that is actually used for signing.<br>Subfilter und das Encoding sollen, wenn möglich, festgelegt werden. | MUST |
| Digest-Method | An array of names indicating acceptable digest algorithms to use while signing. This property is only applicable if the digital credential signing contains RSA public/private keys. | SHOULD |
| V | The minimum required capability of the signature field seed value dictionary parser. A value of 1 specifies that the parser shall be able to recognise all seed value dictionary entries in a PDF 1.5 file. A value of 2 specifies that it shall be able to recognise all seed value dictionary entries specified. A value of 3 specifies that it shall be able to recognise all seed value dictionary entries specified in PDF 2.0 and earlier. | MAY |
| Cert | A certificate seed value dictionary containing information about the characteristics of the certificate that shall be used when signing. | SHOULD |
| Reasons | An array of text strings that specifying possible reasons for signing a document. If specified, the reasons supplied in this entry replace those used by interactive PDF processors. | MAY |

| Key | Value/Explanation/Begründung zur Empfehlung | Recommendation |
|---|---|---|
| MDP | A dictionary containing a single entry whose key is P and whose value is an integer between 0 and 3. A value of 0 defines the signature as an approval signature (see 12.8, "Digital signatures"). The values 1 through 3 shall be used for certification signatures and correspond to the value of P in a DocMDP transform parameters dictionary. | MUST |
| TimeStamp | (Optional; PDF 1.6) A timestamp dictionary containing two entries:<br>1. URL An ASCII string specifying the URL of a timestamping server, providing a timestamp that is compliant with Internet RFC 3161 as updated by Internet RFC 5816.<br>2. Ff An integer whose value is 1 (the signature shall have a timestamp) or 0 (the signature need not have a timestamp). Default value: 0.<br>Falls Angaben hierzu gemacht werden, dann muss der 2. Wert in diesem Kontext auf 1 gesetzt werden.<br>Die URL ist fakultativ. | MAY |
| LegalAttestation | An array of text strings specifying possible legal attestations (see 12.8.7, "Legal content attestations"). The value of the corresponding flag in the Ff entry indicates whether this is a required constraint | MAY |
| AddRevInfo | A flag indicating whether revocation checking shall be carried out. If AddRevInfo is true, the PDF processor shall perform the following additional tasks when signing the signature field:<br>• Perform revocation checking of the certificate (and the corresponding issuing certificates) used to sign.<br>• Include the revocation information within the signature value.<br>If AddRevInfo is true and the Ff entry indicates this is a required constraint, then the preceding tasks shall be performed. If they cannot be performed, then signing shall fail. | MUST |
| LockDocument | (Ab PDF 2.0) A name value supplying the author's intent for whether the signing dialogue should allow the user to lock the document at the time of signing.<br>Begründung: Wegen der Kompatibilität mit PDF 1.7 nicht. | SHOULD NOT |

| Key | Value/Explanation/Begründung zur Empfehlung | Recommendation |
|---|---|---|
| Appearance-Filter | (Optional ab PDF 2.0) A text string naming the appearance that shall be used when signing the signature field.<br>Wegen der Kompatibilität zur PDF 1.7 nicht. | SHOULD NOT |

Tabelle 4: Empfehlungen zum signature field seed value dictionary

#### 5.1.3.2 certificate seed value

| Key | Value/Explanation/Begründung zur Empfehlung | Recommendation |
|---|---|---|
| Type | The type of PDF object that this dictionary describes | MUST |
| Ff | A set of bit flags specifying the interpretation of specific entries in this dictionary. A value of 1 for the flag means that a signer shall be required to use only the specified values for the entry. Begründung: Es sind zwingende Vorgaben enthalten. | MUST |
| Subject | An array of byte strings containing DER-encoded X.509v3 certificates that are acceptable for the verification of the signature | MAY |
| SignaturePolicyOID | Feature in PDF 2.0: The string representation of the OID of the signature policy to use when signing.<br>Kompatibilität mit PDF 1.7 Signature Handler<br>Signature Policy sollte aus dem Kontext oder den Vorschriften zum Zeitpunkt des Leistens der Signatur ersichtlich sein. | SHOULD NOT |
| SignaturePolicyHash-Value | Feature in PDF 2.0: The computed hash value of the signature policy<br>Begründung: Kompatibilität mit PDF 1.7 Signature Handler<br>Signature Policy soll aus dem Kontext oder den Vorschriften zum Zeitpunkt des Leistens der Signatur ersichtlich sein. | SHOULD NOT |
| SignaturePolicyHashAlgorithm | Feature in PDF 2.0: The hash function used to compute the value of the SignaturePolicyHashValue entry. | MUST, falls die Signature Policy eingesetzt wird. |
| SignaturePolicyCommitmentType | Feature in PDF 2.0: If the SignaturePolicyOID is present, this array defines the commitment types that may be used within the signature policy.<br>Begründung: Kompatibilität mit PDF 1.7 Signature Handler<br>Signature Policy sollte aus dem Kontext oder den Vorschriften zum Zeitpunkt des Leistens der Signatur ersichtlich sein. | SHOULD NOT |

| Key | Value/Explanation/Begründung zur Empfehlung | Recommendation |
|---|---|---|
| SubjectDN | An array of dictionaries, each specifying a Subject Distinguished Name (DN) that shall be present within the certificate for it to be acceptable for signing. | MAY |
| KeyUsage | An array of ASCII strings, where each string specifies an acceptable key-usage extension in the certificate for the signature verification.<br>Falls verwendet, dann darf nur Folgendes im Zertifikat enthalten sein, welches für die Verifikation der Signatur verwendet wird:<br>1 digitalSignature<br>2 non-Repudiation | MAY |
| Issuer | An array of byte strings containing DER-encoded X.509v3 certificates of acceptable issuers. | MAY |
| OID | An array of byte strings that contain Object Identifiers (OIDs) of the certificate policies that shall be present in the signing certificate. | MAY |
| URL | A URL, the use for which shall be defined by the URLType entry.<br>Es dürfen keine relevanten Informationen referenziert werden. | MUST NOT |
| URLType | (Optional; PDF 1.7) A name indicating the usage of the URL entry.<br>Es dürfen keine für den Inhalt des Dokuments relevanten Informationen referenziert werden. | MUST NOT |

Tabelle 5: Empfehlungen zum certificate seed value dictionary

## 5.2 Bestandteil des Dokumentzeitstempels

In folgender Tabelle sind die Empfehlungen zum Dokumentzeitstempel zusammengefasst.

| Nr | Attribut | Signiert | Emp. | Bem |
|---|---|---|---|---|
| 1 | Certificate (Zertifikate der bisherigen PDF-Signaturen oder Zeitstempel) im DSS | J | M, B | 1) |
| 2 | CRL (Zertifikate der bisherigen PDF-Signaturen oder Zeitstempel) im DSS | J | M | |
| 3 | OCSP-Antwort (Gültigkeit der Zertifikate für die Verifikation der Signaturen) im DSS | J | M | |

| Nr | Attribut | Signiert | Emp. | Bem |
|---|---|---|---|---|
| 4 | Name (Angabe zum Zeitstempeldienst) im PDF signature dictionary | J | SN | |
| 5 | Location (Angabe zum Zeitstempeldienst) im PDF signature dictionary | J | SN | |
| 6 | Reason (Angabe zum Zeitstempeldienst) im PDF signature dictionary | J | SN | |
| 7 | Kontakt (Angabe zum Zeitstempeldienst) im PDF signature dictionary | J | SN | |
| 8 | Subfilter | J | M | Wert = «ETSI.RFC3161» |

Tabelle 6: Zusammenfassung der Empfehlungen zu den Attributen, welche der CMS Signatur beigegeben werden können.

Legende

A = Alternativ
B = Bedingt vorhanden
Bem = Bemerkung
M = MUST
N = Nein
SN = SHOULD NOT
1) Falls die Zertifikate für die Verifikation der Signaturen nicht bereits bei den jeweiligen Signaturen beigefügt wurden, dann müssen sie hier enthalten sein. Es soll darauf geachtet werden, dass Zertifikate nicht zweimal erscheinen. Das Zertifikat für die Verifikation der Signatur muss jedoch der Signatur über das Attribut «certificate-values» beigefügt werden, die CA-Zertifikatskette jedoch nicht.

## 5.3 Signatur mit XML

Dieses Unterkapitel ist nicht normativ.

### 5.3.1 Signatur von XML-Objekten in XFA eingebettet in ein PDF

Grundsätzlich können die Regeln in eCH-0230 angewandt werden. Zu beachten ist jedoch: Mit Beifügen der entsprechenden XML-Elementen können vorgängig geleisteten PDF-Signaturen ungültig werden. D.h. sobald eine PDF-Signatur oder ein DZS eingefügt wird, dann sollten die von der Signatur erfassten XML-Objekte unverändert bleiben.

### 5.3.2 PDF-Signatur über das im PDF eingebettete XFA

In folgender Tabelle werden diejenigen Attribute bei einer XML-Signatur aufgeführt, zu welchen es eine zu eCH-0230 unterschiedliche Empfehlung gibt. Grund dafür liegt darin, dass die LTV der XML-Signaturen im vorliegenden Fall mittels des DZS erreicht werden soll.

| Nr | Element | Signiert | Emp. | Bem |
|---|---|---|---|---|
| 1 | CompleteCertificateRefs | N | MN | |
| 2 | CompleteRevocationRefs | N | MN | |

| Nr | Element | Signiert | Emp. | Bem |
|---|---|---|---|---|
| 3 | SigAndRefsTimeStamp | N | MN | 1) |
| 4 | RefsOnlyTimeStamp element | N | MN | 1) |
| 5 | RevocationValues | N | B | 2) |
| 6 | ArchiveTimeStamp | N | MN | 1) |
| 7 | TimeStampValidationData | N | MN | 1) |

Tabelle 7: Zusammenfassung der Empfehlungen zu den Attributen, welche der XML-Signatur über ein XFA (eingebettet in ein PDF) beigegeben werden können.

Legende

B = Bedingt vorhanden
Bem = Bemerkung
M = MUST
MN = Must NOT
N = Nein
Signiert = Bestandteil der zu archivierenden Dokument- oder Dateisignatur, d.h. der Inhalt des Attributs fliesst in Hashberechnung für die Signatur ein.
1) Die Lösung des Problems erfolgt mittels des Dokumentzeitstempels.
2) Die Revokationsinformationen der Signaturen, deren Gültigkeit durch den anzufertigenden Zeitstempel bewahrt werden soll, müssen unmittelbar vor dem ersten Dokumentzeitstempel beigegeben werden.

# 6 Sicherheitsüberlegungen

Dieses Dokument behandelt die Bewahrung der Gültigkeit elektronisch signierter Dokumente, so dass zu einem viel späteren Zeitpunkt festgestellt werden kann, ob das Zertifikat für die Prüfung der Signatur zum Zeitpunkt des Leistens der elektronischen Signatur gültig war. Dies ist für sich selber ein Thema der IT-Sicherheit. Andere Themen zur IT-Sicherheit werden hier bewusst ausgeklammert; dies im Bewusstsein, dass sie zwar relevant sind, aber ansonsten die Abhandlungen hier ausufern würden.

# 7 Haftungsausschluss/Hinweise auf Rechte Dritter

**eCH**-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

# 8 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

**eCH**-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

# Anhang A – Referenzen & Bibliographie

### Fachliteratur/Paper


| | |
|---|---|
| [1] | Andreas Bertsch, Digitale Signaturen, Springer Verlag, 2001 |
| [2] | Digital Signatures Workflow Guide, A guide for workflow owners, 28.9.2012 |
| [3] | Jens Müller et al, Ruhr University, Dangerous Paths, on Security and Privacy of the Portable Document Format, 2021 |
| [4] | Karsten Meyer, Security of PDF Signatures, Master Thesis, Ruhr University, 2018 |
| [5] | Trechsel/Pieth, Schweizerisches Strafgesetzbuch, 2. Auflage, Dike Verlag, 2013 |
| [6] | Management Summary zur KOST-Studie: PDF/A-2 und PDF/A-3: Was ist neu?, https://kost-ceco.ch/cms/dl/9f3da1f53a75e54c2323a1bb6947fc2a/Summary_PDFA-2_PDFA-3_v1.0.pdf |
| [7] | Isaak Meier, Schweizerische Zivilprozessordnung, Schulthess Verlag, 2010 |


### Adobe (www.adobe.com)


Adobe ® XFA: XML Forms Architecture (XFA) Specification version 2.5, (June 2007), Adobe Systems Incorporated

ISO 32000-1: Document management - Portable document format - Part 1: PDF 1.7. Bemerkung: Kann im Internet kostenlos bezogen werden.


### eCH (www.ech.ch)


| | |
|---|---|
| eCH-0091 | Standard zu XML-Signatur und Verschlüsselung |
| eCH-0220 | Bewahrung der Gültigkeit elektronischer Signaturen im CMS Format |
| eCH-0230 | Bewahrung der Gültigkeit von XML-Signaturen |


### ETSI (www.etsi.org)


| | |
|---|---|
| ETSI EN 319 102-1 V1.1.1. | Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures |
| ETSI EN 319 122-1 V1.1.1 | Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures |
| ETSI EN 319 122-2 V1.1.1 | Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures |
| ETSI EN 319 132-1 V1.1.1 | Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures |
| ETSI EN 319 132-2 V1.1.1 | Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Building blocks and XAdES baseline signatures |
| ETSI EN 319 142-1 | Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures |
| ETSI EN 319 142-2 | Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles |
| ETSI EN 319 422 V1.1.1 | Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles |

| | |
|---|---|
| ETSI TS 101 903 V1.4.2 | Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES) |
| ETSI TS 102 778-1 bis -5 | Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1 to 5 |
| ETSI TS 119 102-1 V1.2.1 | Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation (2018-08) |

**ISO (www.iso.org)**

| | |
|---|---|
| ISO 19005-1 | ISO 19005-1 (2005): Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1). |
| ISO 19005-2 | ISO 19005-2 2011 Document management — Electronic document file format for long-term preservation — Part 2: Use of ISO 32000-1 (PDF/A-2) |
| ISO 19005-4 | ISO 19005-4 2020, Document management — Electronic document file format for long-term preservation — Part 4: Use of ISO 32000-2 (PDF/A-4) |
| ISO 32000-1 | Document management - Portable document format - Part 1: PDF 1.7. Bemerkung: Kann im Internet kostenlos bezogen werden. |
| ISO 32000-2 | Document management - Portable document format - Part 2: PDF 2.0 |

**ITU (www.itu.int)**

| | |
|---|---|
| ITU-T X.509 | Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, 10/2012 |

**IETF Standards (www.ietf.org)**

| | |
|---|---|
| RFC 3023 | XML Media Types |
| RFC 3076 | Canonical XML Version 1.0 |
| RFC 3161 | Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP) |
| RFC 3275 | XML Signature Syntax and Processing |
| RFC 3741 | Exclusive XML Canonicalization, Version 1.0 |
| RFC 3986 | Uniform Resource Identifier (URI): Generic Syntax |
| RFC 4452 | The «info» URI Scheme for Information Assets with Identifiers in Public Namespaces |
| RFC 5652 | Cryptographic Message Syntax (CMS) |
| RFC 6960 | Online Certificate Status Protocol – OCSP |

**W3C Standards (www.w3c.org)**

Canonical XML Version 1.0 und 1.1 Recommendation March 2001 and May 2008

Exclusive XML Canonicalization Version 1.0 Recommendation, July 2002

XML Path Language (XPath) Version 1.0

XML Schema Part 1: Structures Second Edition. 28 October 2004. W3C Recommendation

XML Schema Part 2: Datatypes Second Edition. 28 October 2004. W3C Recommendation

XML Signature Best Practices Working Group Note, April 2013

XML Signature Syntax and Processing Recommendation Version 1.1, 11 April 2013

Anmerkung: Die hier angegebenen Standards basieren wiederum auf eine Reihe anderer ETSI, ITU,

W3C oder RFC Standards. Diese werden aber dort aufgelistet.

**Erlasse**

StGB: Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0, in Kraft seit 1. Januar 1942

TAV: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032.1

UIDG: Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010, SR 431.03

VZertES; Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032

ZertES: Bundesgesetz vom 18. März 2016 Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.03)

ZPO: Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (SR 272)

# Anhang B – Mitarbeit & Überprüfung

| | |
|---|---|
| Amrhyn Peter | Swisscom AG |
| Röthlisberger Claire | KOST |

# Anhang C – Abkürzungen und Glossar

| Abs. | Absatz |
|---|---|
| Archivierung | Sichere und dauerhafte Aufbewahrung von Unterlagen in einem Archiv, welche rechtlich, administrativ, politisch, wirtschaftlich, historisch, kulturell, sozial oder wissenschaftlich wertvoll sind. |
| Art. | Artikel |
| ASN.1 | Abstract Syntax Notation One |
| Aufbewahrung | Organisierte und systematische Verwaltung von Geschäftsinformation für eine angemessene (endliche) Zeitperiode unter Berücksichtigung gesetzlicher, betrieblicher oder historischer Anforderungen. |
| Bst. | Buchstabe |
| CA | Certification Authority |
| CAdES | CMS Advanced Electronic Signature |
| CMS | Cryptographic Message Syntax, siehe RFC 5652 |
| CRL | Certificate Revocation List |
| CSP | Certification Service Provider |
| DSS | Document Security Store |
| DZS | Dokumentzeitstempel |
| eIDAS | electronic Identification, Authentication and trust Services, EU Regulation 910/2014 of 23 July 2014 |

| Abs. | Absatz |
|---|---|
| ETSI | European Telecommunications Standards Institute |
| GeBüV | Verordnung über die Führung und Aufbewahrung der Geschäftsbücher vom 24. April 2002 (Stand am 1. Januar 2013), SR 221.431 |
| GeoIV | Verordnung über Geoinformation vom 21. Mai 2008, 510.620 |
| IETF | Internet Engineering Task Force |
| ISO | International Standardisation Organisation |
| LTV | Long Term Validation |
| OCSP | Online Certificate Status Protocol, siehe RFC 6960 |
| OID | Object Identifier |
| OR | Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911. SR 220 |
| PAdES | PDF Advanced Electronic Signature |
| Pdf | Portable Document Format |
| POE | Proof of Existence |
| RFC | Request for Comments (IETF Standard) |
| SAML | Security Assertion Markup Language |
| SR | Systematische Rechtsetzungsnummer |
| SR | Systematische Rechtssammlung |
| StGB | Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0, in Kraft seit 1. Januar 1942 |
| TAV | Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032.1 |
| TSP | Trusted Service Provider |
| u.a. | unter anderem |
| UIDG | Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010, SR 431.03 |
| UR | usage rights signature |
| URL | Uniform Ressource Locator |
| VZertES | Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032 |
| XAdES | XML Advanced Electronic Signature. Näheres dazu siehe ETSI TS 101 904 V.1.4.2 |
| XAdES-T | XML advanced Electronic Signature with Timestamp. Näheres dazu siehe ETSI TS 101 904 V.1.4.2 |
| XFA | XML Forms Architecture |
| XML | Extended Markup Language |

| Abs. | Absatz |
|---|---|
| XML Signature Syntax | XML Signature Syntax and Processing Recommendation Version 1.1, 11 April 2013 |
| ZertES | Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate, vom 18. März 2016 (Stand am 1. Januar 2017), SR 943.03 |
| Ziff. | Ziffer |
| ZPO | Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (SR 272) |

# Anhang D – Änderungen gegenüber Vorversion

Dies ist die erste Version.

# Anhang E – Abbildungsverzeichnis

# Anhang F – Tabellenverzeichnis