

## eCH-0282 – Prüfung einer elektronischen Signatur

<b>Name</b>	Prüfung einer elektronischen Signatur
<b>eCH-Nummer</b>	eCH-0282
<b>Kategorie</b>	Standard
<b>Reifegrad</b>	Definiert
<b>Version</b>	1.0.0
<b>Status</b>	Genehmigt
<b>Beschluss am</b>	2026-04-09
<b>Ausgabedatum</b>	2026-02-25
<b>Ersetzt Version</b>	Neu – Major Change
<b>Voraussetzungen</b>	ETSI EN 319 102-1 eCH-0250, eCH-0230, eCH-0220, eCH-0091 SAR_EC_BASELINE ZertES, VZertES, TAV
<b>Beilagen</b>	---
<b>Sprachen</b>	Deutsch (Original), Französisch (Übersetzung)
<b>Fachgruppe</b>	Technologie
<b>Herausgeber / Vertrieb</b>	Verein eCH, Affolternstrasse 52, 8050 Zürich T 044 388 74 64 / <a href="mailto:info@ech.ch">info@ech.ch</a> / <a href="http://www.ech.ch">www.ech.ch</a>

## Zusammenfassung

Der hier vorliegende Standard gibt eine Anleitung, wie elektronische Signaturen, hier kurz Signaturen, zu prüfen sind. U.a. auch Signaturen, welche mit Zusatzinformationen wie einem Zeitstempel versehen sind, so dass die Gültigkeit der Signatur und deren Beweiskraft bewahrt werden kann.

Bestimmungen aus Bundesgesetz (ZertES) und folglich deren Ausführungsvorschriften (Verordnung, technische administrative Vorschriften) bestehen jedoch zur Prüfung einer Signatur nicht. Weil Signaturen zu prüfen sind, bedarf es dieser Anleitung.

Die hier vorliegende Anleitung basiert auf:

- ETSI Standards (ETSI EN 319 102-1, ETSI TS 119 172-4)
- EU-Vorschriften, wie eine Signatur zu prüfen ist.
- Bundesvorschriften (ZertES, VZertES und TAV)
- eCH-Standards (eCH-0091, eCH-0220, eCH-0230, eCH-0250), wie eine Signatur herzustellen ist.

Vorschriften und Empfehlungen, wie eine elektronische Signatur herzustellen ist, legen implizit die Kriterien und das mögliche Resultat einer Prüfung fest.

In eCH-0220, eCH-0230, eCH-0250 sind mehr Anforderungen an die Herstellung einer elektronischen Signatur für die Bewahrung deren Gültigkeit festgelegt worden, als in den entsprechenden ETSI Standards, in den EU-Vorschriften SAR\_EC\_BASELINE und im DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 zu finden sind.

Folgende Aspekte werden hier zusätzlich mitberücksichtigt:

- Die Aufbewahrung des Signierten
- und die Nichtfälschbarkeit der Visualisierung des Signierten

Entsprechend ist der Prüfungsumfang grösser als in den einschlägigen ETSI Standards und in den EU-Vorschriften.

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	<b>8</b>
<b>1.1</b>	<b>Status</b> .....	<b>8</b>
<b>1.2</b>	<b>Anwendungsgebiet</b> .....	<b>8</b>
<b>1.3</b>	<b>Ziel(e) und Abgrenzung</b> .....	<b>9</b>
1.3.1	Ziel .....	9
1.3.2	Weg zum Ziel .....	10
1.3.3	Abgrenzung.....	10
1.3.3.1	Unverändertheit (Integrität) .....	10
1.3.3.2	Erstellung einer Signatur .....	11
1.3.3.3	Konsequenzen .....	11
1.3.3.4	Umfang der Prüfung.....	11
<b>1.4</b>	<b>Querverweise</b> .....	<b>11</b>
<b>1.5</b>	<b>Inhalt, Struktur des Dokuments</b> .....	<b>11</b>
<b>1.6</b>	<b>Angesprochener Leserkreis</b> .....	<b>12</b>
<b>1.7</b>	<b>Terminologie der Empfehlung</b> .....	<b>12</b>
<b>2</b>	<b>Grundsätzliches</b> .....	<b>13</b>
<b>2.1</b>	<b>Begriffe</b> .....	<b>13</b>
2.1.1	Zertifikat .....	13
2.1.2	Advanced Electronic Signature (AdES) .....	13
2.1.3	TSP .....	13
2.1.4	Potentiell schädlicher Link .....	13
<b>2.2</b>	<b>Zu den Vorgaben der EU</b> .....	<b>14</b>
2.2.1	Geltungsbereich .....	15
2.2.2	Überblick über die EU-Vorschriften zur Signatur .....	15
<b>2.3</b>	<b>Standards</b> .....	<b>17</b>
2.3.1	Standards.....	17
2.3.2	Version der Standards.....	17
<b>2.4</b>	<b>Grundsätze zur Gültigkeit</b> .....	<b>17</b>
2.4.1	Security Policy/Kontext.....	17

2.4.2	Gültigkeit eines Zertifikats .....	18
2.4.3	Gültigkeit einer Signatur .....	19
2.4.4	Geeignet für die Aufbewahrung .....	20
2.4.5	Verlässlichkeit der Anzeige des Signierten und dessen Bedeutung .....	21
<b>2.5</b>	<b>Erstellung einer advanced electronic signature (AdES) nach ETSI .....</b>	<b>22</b>
<b>2.6</b>	<b>Revokations-Prüfung vs. Short-term-Zertifikate .....</b>	<b>22</b>
<b>2.7</b>	<b>Eckpfeiler der Prüfung .....</b>	<b>23</b>
2.7.1	Resultat der Prüfung .....	23
2.7.2	Amtlich anerkannte Stelle .....	23
2.7.3	Zeitangaben .....	23
2.7.4	Best signature time .....	24
2.7.5	Signaturformat .....	24
<b>2.8</b>	<b>Prüfungsumfeld .....</b>	<b>25</b>
<b>2.9</b>	<b>Trusted List .....</b>	<b>25</b>
2.9.1	eIDAS .....	25
2.9.2	ZertES .....	25
2.9.3	Nicht gesetzlich geregelte Signaturen .....	26
<b>3</b>	<b>Kapitel 5 Signature Validation .....</b>	<b>27</b>
<b>3.1</b>	<b>Kapitel 5.1.1 General Requirements .....</b>	<b>27</b>
<b>3.2</b>	<b>Kapitel 5.1.2. Selecting Validation Process .....</b>	<b>27</b>
<b>3.3</b>	<b>Kapitel 5.1.3 Status indication of the signature validation process and signature validation report .....</b>	<b>28</b>
3.3.1	Grundsatz zur Bewertung .....	28
3.3.2	Zusätzliche Rückmeldungen .....	28
<b>3.4</b>	<b>Kapitel 5.2.2 Format Checking .....</b>	<b>30</b>
3.4.1	Zu unterstützende Signaturformate gemäss eCH .....	30
3.4.2	Zu unterstützende Signaturformate gemäss SAR_EC_BASELINE .....	30
<b>3.5</b>	<b>Kapitel 5.2.7.2 Inputs .....</b>	<b>30</b>
<b>3.6</b>	<b>Kapitel 5.2.9 Signature validation presentation building block .....</b>	<b>31</b>
<b>3.7</b>	<b>Format und Inhalte .....</b>	<b>31</b>
3.7.1	Verlässlichkeit der Anzeige .....	31
3.7.2	Aufbewahrungstauglichkeit der Datenformate .....	31

3.7.3	Zuordnung Signatur Dateiformat .....	31
<b>3.8</b>	<b>Commitment-type-indication .....</b>	<b>31</b>
<b>3.9</b>	<b>«Claimed Attribute» .....</b>	<b>32</b>
3.9.1	Anmerkung zu «Claimed Attribute» .....	32
3.9.2	Vom Benutzer zu prüfen.....	32
3.9.3	Kapitel 5.2.8.4.3.2 Processing claimed signing time .....	32
3.9.4	Kapitel 5.2.8.4.2.5 Processing indication of production place .....	32
3.9.5	Sichere Signaturerstellungseinheit .....	32
<b>3.10</b>	<b>Kapitel 5.2.3 Identification of the signature certificate.....</b>	<b>33</b>
<b>3.11</b>	<b>Kapitel 5.4 Time-stamp validation building block.....</b>	<b>33</b>
<b>4</b>	<b>Beurteilung/Anforderung an die Akzeptanz.....</b>	<b>34</b>
<b>4.1</b>	<b>Allgemeines.....</b>	<b>34</b>
4.1.1	Konvention .....	34
4.1.2	Unterschied zu ETSI EN 319 102-1.....	34
4.1.3	Prozess der Prüfung (Prüfungsablauf).....	35
4.1.4	Zu den Rückmeldungen .....	35
4.1.5	Zur Gesamtbewertung (summarisches Ergebnis).....	35
<b>4.2</b>	<b>Überblick über die Prüfschritte.....</b>	<b>36</b>
<b>4.3</b>	<b>Basis-Signatur .....</b>	<b>36</b>
4.3.1	Was zu prüfen ist .....	36
4.3.2	Rückmeldungen zur Prüfung .....	37
4.3.2.1	MUSS geprüft werden.....	37
4.3.2.1.1	A) Signatur.....	37
4.3.2.1.2	B) Zertifikat .....	38
4.3.2.2	SOLL geprüft werden .....	38
<b>4.4</b>	<b>Die der Handunterschrift gleichgestellte Signatur .....</b>	<b>39</b>
4.4.1	Was zu prüfen ist .....	39
4.4.2	Rückmeldungen zur Prüfung .....	40
4.4.2.1	MUSS geprüft werden.....	40
4.4.2.1.1	A) Signatur und dazugehöriges Zertifikat .....	40
4.4.2.1.2	B) Zeitstempel .....	41
4.4.2.2	SOLL geprüft werden .....	42

<b>4.5</b>	<b>Basis Signatur mit Zeitstempel</b>	<b>42</b>
<b>4.6</b>	<b>Austausch von Signaturen im Behördenumfeld der Schweiz</b>	<b>42</b>
<b>4.7</b>	<b>Qualifizierte Signatur gemäss EU</b>	<b>43</b>
4.7.1	Was zu prüfen ist	43
4.7.2	Rückmeldungen zur Prüfung	44
4.7.2.1	MUSS geprüft werden	44
4.7.2.2	SOLL geprüft werden	45
4.7.3	Ergänzung	45
<b>4.8</b>	<b>Signature with Long Term Validation Material</b>	<b>45</b>
4.8.1	Was zu prüfen ist	46
4.8.2	Rückmeldungen zur Prüfung	46
4.8.2.1	MUSS geprüft werden	46
4.8.2.2	SOLL geprüft werden	47
<b>4.9</b>	<b>Vor dem Überführen in die Institution für die Aufbewahrung</b>	<b>48</b>
4.9.1	Was zu prüfen ist	48
4.9.2	Rückmeldungen zur Prüfung	49
4.9.2.1	MUSS geprüft werden	49
4.9.2.2	SOLL geprüft werden	49
<b>4.10</b>	<b>Von der Institution für die Aufbewahrung</b>	<b>49</b>
4.10.1	Was zu prüfen ist	49
4.10.1.1	Rückmeldungen zur Prüfung	50
4.10.1.2	MUSS geprüft werden	50
<b>4.11</b>	<b>Konsequenz</b>	<b>50</b>
<b>5</b>	<b>Sicherheitsüberlegungen</b>	<b>51</b>
<b>6</b>	<b>Haftungsausschluss/Hinweise auf Rechte Dritter</b>	<b>51</b>
<b>7</b>	<b>Urheberrechte</b>	<b>52</b>
<b>Anhang A – Referenzen &amp; Bibliographie</b>		<b>53</b>
<b>Anhang B – Mitarbeit &amp; Überprüfung</b>		<b>54</b>
<b>Anhang C – Abkürzungen und Glossar</b>		<b>55</b>
<b>Anhang D – Vorschriften</b>		<b>58</b>
<b>Anhang E – Standardisierungsorganisationen</b>		<b>59</b>
<b>Anhang F – Änderungen gegenüber Vorversion</b>		<b>59</b>

<b>Anhang G – Abbildungsverzeichnis.....</b>	<b>59</b>
<b>Anhang H – Tabellenverzeichnis .....</b>	<b>60</b>

## Hinweis

Im vorliegenden Dokument wird bei der Bezeichnung von Personen eine geschlechtsneutrale Formulierung verwendet. Basis bildet der [Leitfaden](#) der Bundeskanzlei. Je nach Situation kommen Paarformen (Bürgerinnen und Bürger), geschlechtsabstrakte Formen (versicherte Person), geschlechtsneutrale Formen (Versicherte) oder Umschreibungen ohne Personenbezug zum Einsatz. Das generische Maskulin (Bürger) ist nicht zulässig. Vollformen werden in fortlaufenden Texten verwendet, also in Texten, die aus ausformulierten Sätzen bestehen. In verknappten Textpassagen, namentlich in Tabellen, können Kurzformen verwendet werden. Dabei wird die Kurzform mit Schrägstrich, aber ohne Auslassungsstrich verwendet (Referent/in). Genderstern und ähnliche Schreibweisen werden nicht verwendet.

# 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

**Konvention:** In diesem Dokument ist unter einer Signatur Folgendes zu verstehen:

- Im rechtlichen Sinne eine elektronische Signatur nach ZertES oder eIDAS.
- Im technischen Sinne eine digitale Signatur gemäss RFC 5652 oder 2315 (PKCS#7).

Das Anwendungsgebiet besteht dort, wo Signaturen oder deren Bestandteile geprüft werden sollen. Bei der Prüfung gilt es zu beachten, dass die Signatur bereits während Tagen, Wochen oder gar Jahren aufbewahrt wurde. Trotzdem soll die Signatur auch nach dieser Zeitspanne verlässlich geprüft und bei erfolgreicher Prüfung akzeptiert werden können. Dies, wenn aufgrund der geprüften Informationen festgestellt werden kann, dass die Signatur zu einem Zeitpunkt geleistet wurde, an dem das dazugehörige Zertifikat noch gültig war.

Als Massstab für die Verlässlichkeit soll gelten: Das von der Signatur Erfasste wird als Beleg beim Geschäfts-/Behördenverkehr anerkannt.

**Anmerkung:** Eine elektronische oder handschriftliche Signatur reicht normalerweise im Geschäftsverkehr und bei einem strittigen Verfahren als Beleg mit erhöhter Beweiskraft für einen Sachverhalt aus. Eine Signatur (handschriftlich oder elektronisch) zu einer öffentlichen Beurkundung erlangt volle Beweiskraft (Art. 9 ZGB).

**Konvention:** Grau hinterlegte Passagen enthalten Aussagen oder Grundsätze, welche für die Prüfung der Signatur zentral sind.

### 1.3 Ziel(e) und Abgrenzung

Bei der Bewahrung der Gültigkeit von elektronisch Signiertem 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 Signatur und der späteren (nochmaligen) Prüfung der Signatur können z.B. folgende Ereignisse eintreten, welche die verlässliche Prüfung und folglich die Akzeptanz der Signatur zu einem späteren Zeitpunkt erschweren:

- Das Zertifikat mit dem öffentlichen Schlüssel zur Prüfung einer Signatur ist nicht mehr gültig.
- Das Root-Zertifikat zu diesem Zertifikat ist nicht mehr gültig.
- Der private Signaturschlüssel wurde kompromittiert, und das dazugehörige Zertifikat wurde dann revoziert.
- Das Zertifikat wurde aus anderen Gründen revoziert.
- Die für die Signatur verwendeten kryptografischen Algorithmen können im Zuge der technischen Entwicklung als weniger sicher erklärt werden, was zur Revokation der bestehenden Schlüssel führen kann.

**Anmerkung:** In [1] und ETSI EN 319 102-1 Anhang A sind diese und weitere Fälle, sowie ihre Auswirkungen auf die nachträgliche Prüfung der Signatur erläutert.

Damit aus einer Signaturprüfung Verlässliches resultiert, müssen der Signatur Informationen beigefügt werden. Was, wird u.a. in den eCH-0220, eCH-0230 und eCH-0250 beschrieben. Doch auch diese Informationen gilt es zu prüfen, damit sich letztendlich Verlässliches daraus ergibt.

#### 1.3.1 Ziel

Mit einer Prüfung soll ersichtlich gemacht werden, ob die Zielvorgaben an die Erstellung der Signatur erfüllt sind. Mit dem hier vorliegenden Dokument und den zugrundeliegenden ETSI-Standards werden dadurch Ziele implizit vorgegeben, wie eine Signatur zu erstellen ist.

Die Vorgaben an die Herstellung, resp. Prüfung einer Signatur lassen sich wie folgt zusammenfassen:

- Bei einer (nach ZertES geregelten) Signatur oder bei einem (nach ZertES geregelten) Siegel soll verlässlich geprüft werden können, ob das dazu entsprechende Signaturzertifikat bei der Erstellung der Signatur gültig war, siehe u.a. auch Art. 2 Abs. c und d ZertES.
- Zudem soll auch Inhalt und Format verifiziert werden, um u.a. feststellen zu können, ob das Dokument oder die Datei archivtauglich ist, das Erscheinungsbild/die Aussagekraft des Signierten unter Wahrung des Hashwertes der Signatur nicht verändert werden kann.
- Der Anwender oder die Anwenderin muss verlässlich sehen können, was er/sie signieren wird, oder was signiert worden ist. U.a. darf/soll das Erscheinungsbild bei Beibehaltung der Gültigkeit der Signatur nicht verändert werden können.

### 1.3.2 Weg zum Ziel

Der hier vorliegende eCH Standard basiert hauptsächlich auf:

- ZertES und dessen Ausführungsvorschriften
- ETSI EN 319 102-1 und ETSI TS 119 172-4
- Vorgaben und Empfehlungen der EU, siehe KAPITEL 2.2
- eCH-0091, eCH-0220, eCH-0230, eCH-0250
- Empfehlungen der KOST zu archivtauglichen Dateiformaten

Davon ist der hier vorliegende eCH Standard 0282 für die Prüfung einer Signatur abgeleitet worden. Er unterscheidet sich von den ETSI-Standards und den Empfehlungen der EU u.a.:

- In der zusätzlichen Prüfung zur Aufbewahrungstauglichkeit der signierten Datei
- In den Empfehlungen betreffend die verlässliche Darstellung des zu Signierenden oder des Signierten
- In zusätzlichen Anforderungen, welche sich aus dem ZertES ergeben
- In Empfehlungen bei konkreten Anwendungen (s. KAPITEL 4)

### 1.3.3 Abgrenzung

#### 1.3.3.1 Unverändertheit (Integrität)

In diesem Zusammenhang ist es wichtig zu erwähnen:

Eine Signatur vermag die Integrität, d.h. die Unverändertheit des von der Signatur Erfassten nicht zu schützen.

Das heisst, die Signatur stellt keine Massnahme dar, dass das Signierte nicht verändert (werden) wird. Sie stellt also keine präventive Massnahme zum Schutz der Integrität dar.

Mit der Signatur vermag man verlässlich zu erkennen, ob das Signierte oder die Signatur verändert wurden und somit ob eine Integritätsverletzung vorliegt oder nicht. Die Signatur ist folglich ein Mittel der Detektion, ob eine Integritätsverletzung vorliegt. In der englischen Fachsprache heisst dies:

A digital signature is tamper-evident, but not tamper-resistant.

Folglich ist es unerlässlich, dass die Integrität (Unverändertheit) des Signierten präventiv geschützt wird. Massnahmen zum Integritätsschutz bei der Aufbewahrung sind jedoch nicht Bestandteil dieses Standards.

Nicht alle Dateiformate lassen sich gleich gut aufbewahren und archivieren.

**SHOULD:** Deshalb soll vor Erstellung der Signatur oder bei deren Empfang einer signierten Datei geprüft werden, ob sich deren Dateiformat fürs Aufbewahren eignet, falls die signierte Datei aufbewahrt werden muss.

### 1.3.3.2 Erstellung einer Signatur

Oft wird auf den ETSI Standard EN 319 102-1 «Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation» verwiesen. Dort wird auch der Prozess der Erstellung einer Signatur standardisiert. Doch wie eine Signatur anzufertigen ist, ist grundsätzlich nicht Thema dieses Standards. Zur Beschaffenheit einer Signatur sei auch auf die eCH-Standards eCH-0091, eCH-0220, eCH-0230, eCH-0250 und auf die einschlägigen ETSI Standards zu CAAdES, XAdES, PAdES, JAdES verwiesen.

### 1.3.3.3 Konsequenzen

Welche Folgen ein nicht befriedigendes Ergebnis einer Prüfung letztlich hat oder haben kann, wird hier im Prinzip nicht abgehandelt. Der Standard definiert die Prüfschritte einer Signatur und die möglichen Rückmeldungen für verschiedene Ausprägungen einer Signatur. Zudem empfiehlt er, ob das Ergebnis der Prüfung als befriedigend erachtet werden kann.

### 1.3.3.4 Umfang der Prüfung

Die Empfehlungen zur Prüfung beschränken sich auf die empfangene Signatur und sind Ausgangspunkt der Prüfung. Im ZertES, VZertES und in der TAV zum VZertES sind eine Reihe weiterer Vorschriften im Kontext zur elektronischen Signatur aufgeführt. Dies zu prüfen, ist nicht Thema dieses Dokuments.

## 1.4 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.

## 1.5 Inhalt, Struktur des Dokuments

Das Dokument ist wie folgt strukturiert:

- Ab KAPITEL 2 wird Grundsätzliches vermittelt und festgelegt, wie im KAPITEL 2.1 «Begriffe», im KAPITEL 2.2 «Zu den Vorgaben der EU» und im KAPITEL 2.4 «Grundsätze zur Gültigkeit».
- Im KAPITEL 3 liegt ein Profile (engl. für Profil) von ETSI EN 319 102-1 V.1.4.1.vor. D.h., dass Anmerkungen und zusätzliche Anforderungen an die Prüfung einer Signatur aufgeführt sind. Z.B. fordert die EU, dass auch geprüft werden kann, ob ein qualifiziertes Siegel oder eine qualifizierte Signatur vorliegt.
- Im KAPITEL 4 werden Prüfschritte bei einer Signatur unter verschiedenen Umständen (Use Cases) empfohlen und was dabei von der Prüfapplikation zurückgemeldet werden muss oder soll.

## 1.6 Angesprochener Leserkreis

Der Standard richtet sich u.a. an Mitarbeiter des Dokumentmanagement, welche sich u.a. mit elektronischen Signaturen, deren Akzeptanz, sowie der Aufbewahrung von elektronisch Signiertem befassen, z.B. mit elektronisch signierten (öffentlichen) Urkunden.

## 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 Grundsätzliches

Der hier vorliegende Standard basiert auf anerkannten Standards oder Vorgaben und entspricht dem Stand der Technik, weil die aktuellen, verabschiedeten Normen von ETSI und die Vorgaben und Empfehlungen der EU berücksichtigt worden sind. Zudem sollen die Empfehlungen der KOST betreffend archivtaugliche Dateiformate berücksichtigt werden.

### 2.1 Begriffe

#### 2.1.1 Zertifikat

Ein elektronisches Zertifikat nach ITU X.509 v.3 wird kurz als Zertifikat bezeichnet.

#### 2.1.2 Advanced Electronic Signature (AdES)

Der Ausdruck «Advanced Electronic Signature» (AdES) hat in diesem Kontext folgende zwei unterschiedliche Bedeutungen:

1. Im rechtlichen Sinne (Art.2 Abs. b ZertES und Art. 26 eIDAS) legt es die Anforderung an die Signatur und implizit an die Herstellung des Zertifikats fest, mit welchem die Signatur verifiziert wird.
2. Im technischen Umfeld (ETSI) drückt es eine Erweiterung von Informationen aus, welche der Signatur beigegeben werden, wie z.B. die OCSP Antwort, das Zertifikat für die Prüfung der Signatur. Diese Zusatzinformationen werden vom ZertES und von eIDAS nicht erfasst, resp. dort geregelt.

In diesem Dokument werden beide Bedeutungen des Begriffs verwendet, wobei jedoch erwähnt wird, welche Bedeutung zu verstehen ist.

#### 2.1.3 TSP

Als TSP (Trusted Service Provider) bezeichnet man in diesem Kontext einen amtlich anerkannten Dienstleister gemäss Art. 2 Bst. k und l und Art. 3-5 ZertES oder gemäss EU VERORDNUNG Nr. 910/2014. Im Kontext zur Herausgabe von Zertifikaten auf nationaler Ebene, siehe Homepage der SAS, <https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki1.html>. Dort sind die anerkannten Dienstleister aufgeführt.

#### 2.1.4 Potentiell schädlicher Link

Ein potentiell schädlicher Link in einer Datei oder in einem Objekt ist ein Link auf eine Informationsquelle, deren Inhalt beim Laden der Datei in der Anwendung heruntergeladen wird. Diese Links verleihen der Datei/dem Objekt in der Anwendung eine andere Bedeutung oder ein anderes Erscheinungsbild als die Informationen im Signierten selbst.

Potentiell schädliche Links sind z.B. Verweise auf Quellen eines JavaScript Objekts in einer HTML Datei, welche beim Laden der HTML Datei ausgeführt werden. Das Ausführen dieses JavaScript Objekts verleiht der HTML-Datei in der Anwendung (Browser) eine andere Bedeutung (Erscheinungsbild), als nur das Laden der signierten Datei selbst.

Signiert wird jedoch in vielen Fällen lediglich die Datei als solches (z.B. die HTML-Datei) und nicht all das, was in der Anwendung in diesem Kontext von Bedeutung ist, z.B. das PDF, welches aus der HTML Seite im Browser abgeleitet wurde.

Ändert sich nun der Inhalt der Quelle, z.B. hier das JavaScript Objekt, kann daraus folgen:

- Die Aussagekraft/Bedeutung in der Anwendung verändert sich (z.B. das Erscheinungsbild im Browser).
- Der Hashwert der Datei (z.B. der HTML-Datei) ändert sich jedoch nicht. Folglich bleibt die Signatur in kryptographischer Hinsicht weiterhin gültig.

Dies widerspricht jedoch Ziel und Zweck einer Signatur.

**SHOULD NOT:** Es soll kein potentiell schädlicher Link in dem von der Signatur Erfassten enthalten sein.

**SHOULD:** Folglich soll vor der Erstellung der Signatur und nach deren Empfang geprüft werden, ob ein solcher Link vorhanden ist.

## 2.2 Zu den Vorgaben der EU

Die Vorgaben der EU betreffend die elektronische Signatur und der damit verbundenen elektronischen Zertifikate sind enthalten in:

1. eIDAS: VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
2. DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 DER KOMMISSION vom 8. September 2015 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt anerkannt werden
3. DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1505 DER KOMMISSION vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
4. CEF: eSignature DSS, Version 1.03. Qualified electronic signature (QES) validation algorithm, 2019, hier kurz CEF: eSignature DSS.
5. SAR\_EC\_BASELINE: European Commission: Signature applicability rules for electronic signature and seals received by the European Commission, 19.12.2023

### 2.2.1 Geltungsbereich

Die Vorschriften 1, 2 und 3 gelten für den EWR, 4 ist für den EWR standardisiert worden, während die Vorschrift 5 nur für die Kommission der Europäischen Union und für die EUIBA verbindlich ist. EUIBA ist die Abkürzung für EU Institutions, Bodies and Agencies. Was darunter fällt, ist unter folgendem Link ersichtlich: [https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/types-institutions-and-bodies\\_en](https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/types-institutions-and-bodies_en).

Im Rahmen einer Initiative der EU Kommission zur Umsetzung der Digitalisierung im EWR wurden eine Reihe von Vorgaben betreffend die elektronische Signatur erstellt. Dies für die Kommunikation mit elektronischen Signaturen zwischen den EWR-Mitgliedstaaten. Dabei wurden auch Tools für die Verifikation einer elektronischen Signatur und die dazugehörige technische Vorgabe «CEF: eSignature DSS» für die Prüfung einer elektronischen Signatur publiziert.

Beispielsweise aus CEF: eSignature DSS, Seite 4, 1. Abs.:

The following algorithm has been implemented in the DSS open-source library in version 5.5, and represents the Connecting Europe Facility's (CEF) eSignature Building Block's interpretation of the eIDAS Regulation's and related standards' requirements for the validation of qualified and advanced electronic signatures (e-signatures) and electronic seals (e-seals).

CEF ist die Abkürzung von Connecting Europe Facility und ist eine Initiative der EU Kommission zur Umsetzung von Schlüsselprojekten im EWR.

### 2.2.2 Überblick über die EU-Vorschriften zur Signatur

Die EU hat die Vorschriften zur Prüfung einer Signatur im DURCHFÜHRUNGSBESCHLUSS 2015/1506 grob festgelegt. In SAR\_EC\_BASELINE und CEF: eSignature DSS und in ETSI TS 119 172-4 ist die Prüfung qualifizierter Siegel und Signaturen technisch konkretisiert worden. Dabei beschränken sich die Ausführungen auf qualifizierte Signaturen und qualifizierte Siegel.

Zudem wird im Anhang A dieses DURCHFÜHRUNGSBESCHLUSSES definiert, wie eine elektronische Signatur (für longterm validation) beschaffen sein muss. Dies erfolgt mittels Verweisen auf ETSI Standards. Damit wird auch festgelegt, welche Signaturformate zu unterstützen sind.

Die ETSI-Standards mit neuem Datum sind in SAR-EC\_BASELINE aufgeführt und unter folgendem Link publiziert worden: <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109093/Standards+and+specifications>.

Wie erwähnt, beschränken sich die Ausführungen in CEF: eSignature DSS auf die Prüfung der qualifizierten Signatur und der qualifizierten Siegel. Der Aspekt AdES nach ETSI wird dort nicht behandelt, siehe Kapitel 4, Seite 16 3. Aufzählung. Zudem werden dort die Signaturformate wie die Signatur in einem PDF oder die XML-Signatur nicht definiert.

Im Anhang II von eIDAS wird die Beschaffenheit des qualifizierten Zertifikats und im Anhang vom DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 die Beschaffenheit einer elektronischen Signatur geregelt. Die Anforderungen an die Herstellung einer EU-konformen Signatur lassen sich auch aus den geforderten Prüfschritten und aus den Prüfkriterien in SAR\_EC\_BASELINE und CEF: e-Signature DSS ableiten, welche bei der Prüfung erfüllt sein müssen. Die Anforderungen an das Leisten einer Signatur sind gemäss aktuellem Wissensstand nicht in einer technischen Spezifikation der EU festgehalten worden.

Hauptkriterium für die Gültigkeit einer Signatur ist gemäss Art. 2 Abs. 2 Bst. c Ziff.1 DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 Folgendes:

die Gültigkeit einer fortgeschrittenen elektronischen Signatur bestätigen, sofern:

1. das der fortgeschrittenen elektronischen Signatur zugrunde liegende Zertifikat zum Zeitpunkt des Signierens gültig war, und, wenn die fortgeschrittene elektronische Signatur auf einem qualifizierten Zertifikat beruht, es sich bei dem der fortgeschrittenen elektronischen Signatur zugrunde liegenden qualifizierten Zertifikat zum Zeitpunkt des Signierens um ein qualifiziertes Zertifikat für elektronische Signaturen handelte, das mit Anhang I der Verordnung (EU) Nr. 910/2014 im Einklang stand und von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde;

**MUST:** In Beziehung mit der Europäischen Kommission und der EUIBA muss die qualifizierte Signatur und das qualifizierte Siegel nach der Vorschrift SAR\_EC\_BASELINE (Kapitel 3.3.2, S. 26) geprüft werden können. CEF: eSignature DSS dient als Richtlinie für die Prüfung qualifizierter Signaturen und Siegel für die Kommunikation zwischen den Mitgliedstaaten des EWR.

Infos zur Digitalisierungsinitiative der EU im Bereich der elektronischen Signaturen befinden sich bei:

- <https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Standards+and+specifications>
- <https://ec.europa.eu/digital-building-blocks/sites/display/digital/eSignature+Overview>
- <https://eidas.ec.europa.eu/efda/validation-tool>
- <https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation>

Zusätzliche Anforderungen der EU an die Prüfung einer elektronischen Signatur werden hier bei den jeweiligen Themen erwähnt und lassen sich auch aus SAR\_EC\_BASELINE und in CEF: eSignature DSS entnehmen.

## 2.3 Standards

### 2.3.1 Standards

Was und wie geprüft wird, basiert hauptsächlich auf dem Standard ETSI EN 319 102-1. Dabei soll die Signatur nach Vorgabe einer Security Policy geprüft werden. Eine Security Policy widerspiegelt die Vorschriften/Anforderungen an den Umgang mit einer Signatur in einem speziellen Kontext. Dies können z.B. eIDAS oder das ZertES und die dazu gehörigen Ausführungsvorschriften sein.

**MUST:** Auf nationaler Ebene muss untersucht werden, ob die Signatur nach den folgenden Vorgaben erstellt wurde:

- eCH-0091 eCH (XML-Signatur)
- eCH 0220 (Bewahrung der Gültigkeit einer CMS-Signatur)
- eCH-0230 (Bewahrung der Gültigkeit einer XML-Signatur)
- eCH-0250 (Bewahrung der Gültigkeit einer PDF-Signatur)

### 2.3.2 Version der Standards

**SHOULD:** Zur Version der referenzierten Standards und Empfehlungen soll analog zu SAR\_EC\_BASELINE, S. 10, gelten:

«When the version is not indicated in the description, the latest version of the document applies».

**Anmerkung:** SAR\_EC\_BASELINE bezieht sich auf ETSI EN Standards, während sich der DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 DER KOMMISSION auf ältere TS-Standards von ETSI bezieht. Auch bei dem folgenden Link werden die ETSI EN Standards erwähnt.

<https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109093/Standards+and+specifications>

## 2.4 Grundsätze zur Gültigkeit

### 2.4.1 Security Policy/Kontext

Bei einer Prüfung geht es u.a. darum, festzustellen, ob ein Sollzustand vorliegt oder nicht. Die Konformität des zu Prüfenden wird dabei untersucht. Ob letztlich eine Signatur als konform/akzeptabel gilt, hängt vom Kontext der Prüfung ab, d.h. von den Regelungen (engl. Policy) zur Prüfung und dem konkreten Anwendungsfall. Folglich kann eine Signatur in einem Fall als gültig erachtet, in einem anderen Fall nicht akzeptiert werden, siehe hierzu ETSI EN 319 102-1 V1.4.1, Kapitel 5.1.1, 5.1.3 und 5.1.4.1.

**Begriff:** Eine Signatur wird als gültig erachtet, wenn sie unter den gegebenen Umständen als konform/akzeptabel gilt. D.h. das Resultat und der Umfang der Prüfung den Umständen entsprechend als befriedigend erachtet werden.

**Anmerkung:** ETSI EN 319 102-1 enthält einen Katalog an **Mindestanforderungen** und weiterer Optionen für die Prüfung einer AdES-Signatur (fortgeschrittene Signatur gemäss Begriffsdefinition von ETSI). «The signature creation and validation procedures specified in the present document provide several options and possibilities. The selection of these options is driven by a signature creation policy, a signature augmentation policy or a signature validation policy respectively.», Kapitel 1, Note 2 dort.

**SHOULD:** Beim Melden des Ergebnisses einer Signaturprüfung soll auch noch angezeigt/mitgeteilt werden, unter welchem Kontext (Security Policy) die Prüfung vorgenommen wurde, siehe ETSI EN 319 102-1 V1.4.1, Kapitel 5.1.3, erste Aufzählung.

**Anmerkung:** SAR\_EC\_BASELINE ist eine technische Vorschrift der EU, zusätzlich mit Empfehlungen. Darin wird auf ETSI TS 119 172-4 verwiesen und abgestützt. Beide Dokumente beschreiben, wie eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel von der EU Kommission und der EUIBA zu prüfen ist. Des Weiteren, was der Sollzustand bei einer qualifizierten elektronischen Signatur ist, damit ein qualifiziertes Siegel oder eine qualifizierte Signatur gemäss eIDAS von der Europäischen Kommission und der EUIBA akzeptiert wird. SAR\_EC\_BASELINE sind Vorschriften zur technischen Umsetzung des DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506.

**MUST:** Im Kontext zu den Signaturen, welche aus dem EWR, von der EUIBA, von der EU-Kommission stammen oder in den EWR/an die EUIBA oder an die EU Kommission gesandt werden, muss zuerst abgeklärt werden, welche technischen Vorschriften anzuwenden sind, wie z.B. SAR\_EC\_BASELINE.

**MUST:** Analog zu ETSI EN 319 102-1 ist hier eine Signatur nur dann gültig, wenn sie konform mit den Anforderungen im konkreten Fall ist.

Wie erwähnt, bestehen keine Bundesvorschriften zur Prüfung einer (nach ZertES geregelten) Signatur oder eines (nach ZertES geregelten) Siegels. U.a. deshalb wurde dieser Standard geschaffen.

Letztlich entscheidet der Empfänger/die Empfängerin einer Signatur, ob er/sie eine Signatur akzeptieren will oder zu akzeptieren hat. Im Falle eines Streits zwischen den Parteien kann zur Klärung der Rechtsverbindlichkeit einer Signatur ein Gericht angerufen werden, das über deren rechtliche Bindungskraft endgültig entscheidet.

## 2.4.2 Gültigkeit eines Zertifikats

Ein Zertifikat wird dann als gültig erachtet, wenn

1. die eingesetzten technischen Verfahren zur Herstellung einer Signatur als anerkannt ausreichend sicher gelten,
2. die Signaturen der Zertifikate kryptographisch korrekt sind,
3. es gemäss ITU X.509 hergestellt wurde,
4. die Zertifikatskette zur Verifikation des Zertifikats zu einem TSP führt,
5. es innerhalb der darin definierten Gültigkeitsdauer vorliegt,
6. nicht revoziert worden ist,
7. und die unter den Umständen geforderten Angaben enthält.

**Anmerkung:** Gemäss EU (Art. 28 Abs. 5 Bst. a und b eIDAS) kann ein Zertifikat auch vorübergehend als ungültig erklärt werden. Diese Erklärung muss innerhalb der im Zertifikat erwähnten Gültigkeitsdauer liegen.

**Definition:** Ein Zertifikat ist in der darin definierten Zeitspanne gültig, d.h. zeitlich gültig, sofern es nicht zuvor für ungültig erklärt worden ist.

### 2.4.3 Gültigkeit einer Signatur

**MUST:** Gültig darf eine Signatur nur dann sein, wenn das dazugehörige Zertifikat zum Zeitpunkt der Erstellung der Signatur gültig war, in Analogie zu Art. 2 Abs. c ZertES.

Der Beleg (Beweiskraft) hierfür soll u.a. mit kryptographischen Verfahren und amtlich anerkannten Belegen erbracht werden. U.a. dann, wenn das Zertifikat zum Zeitpunkt der Prüfung nicht mehr gültig ist.

Die EU folgt in ihren Anforderungen diesem Grundsatz, siehe DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 Art. 4 Abs. 2, Bst. c Ziff. 1.

**Anmerkung:** D.h., eine Signatur kann auch dann akzeptiert werden, wenn das dazugehörige Zertifikat zum Zeitpunkt der Prüfung nicht mehr gültig ist. Z.B., wenn verlässlich festgestellt werden kann, dass die Signatur zu einem Zeitpunkt geleistet wurde, als das dazu korrespondierende Zertifikat noch gültig war.

**Anmerkung:** Das Signaturformat AdES gemäss ETSI dient u.a. dazu, verlässlich festzustellen, ob das Zertifikat beim Leisten der Signatur gültig war. Dies mit den der Signaturen beigefügten technischen Informationen.

Mittels eines amtlich anerkannten Zeitstempels wird der Beleg, eventuell sogar der Beweis erbracht, dass das Zertifikat beim Leisten der Signatur gültig war.

**MUST:** Die Zeitangabe im Zeitstempel zur Signatur muss innerhalb der Gültigkeitsdauer des Zertifikats liegen, mit welchem die Signatur verifiziert werden kann.

**MUST:** Bei der Prüfung einer Signatur muss gelten: Sofern die Signatur nach der jeweils aktuellen Fassung eines Standards oder einer Bestimmung nicht anerkannt wird, ist zu überprüfen, ob die Signatur den Anforderungen entspricht, als die Signatur geleistet wurde.

**Beispiel:** Die Prüfung, ob die Schlüssellänge ausreichend oder das Verfahren «anerkannt ausreichend sicher» ist. Diese Anforderung kann sich im Laufe der Zeit ändern.

**Feststellen, ob das Zertifikat zum Zeitpunkt der Erstellung der dazu gehörigen Signatur gültig war.** Gemäss eCH-0220, eCH-0230, eCH-0250 und den zugrundeliegenden ETSI Standards soll dem Signierten fortlaufend Informationen so beigefügt werden, dass

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

Dies unter der Voraussetzung, dass die beigefügten Informationen, das von der Signatur Erfasste und dessen Signatur in der Zwischenzeit unverändert geblieben sind.

Es soll die Beweis- oder Aussagekraft der elektronischen Signatur erhalten bleiben. Z.B. soll die Haftung (nach Art. 59a OR) oder die Rechtskraft des Signierten 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.

Wie dies von statten geht, ist im Standard ETSI EN 319 102-1 festgehalten. In den Standards eCH-0220 (CMS-Signatur), eCH-0230 (XML-Signatur), eCH-0250 (Signatur in einem PDF) ist lediglich das empfohlene Ergebnis standardisiert und zudem konkretisiert.

Man will mit den in den erwähnten Standards vorgeschlagenen Methoden die Bewahrung der Gültigkeit elektronischer Signaturen erreichen, so dass die Signatur nach Erstellung, nach Empfang und nach deren Prüfung während der geforderten Aufbewahrungszeit allgemein akzeptiert werden wird. Dies gilt ebenso im Rahmen eines Gerichtsverfahrens.

**MUST:** Die kryptographische Prüfung (Hashwert, Resultat der Public Key Operation mit dem Schlüssel im Zertifikat) muss stimmen. Ansonsten wird die Signatur als «nicht akzeptabel» erachtet.

**SHOULD:** Die zur Signaturbildung verwendeten Verfahren sollen zum Zeitpunkt der Signaturprüfung «anerkannt ausreichend sicher» sein.

#### 2.4.4 Geeignet für die Aufbewahrung

Es nützt wenig, die Signatur während der geforderten oder gewünschten Aufbewahrungsfrist zu erhalten, ohne gleichzeitig darauf zu achten, dass auch das Signierte während dieser Zeit gelesen und dem Anwender oder der Anwenderin präsentiert werden kann. Muss eine Datei z.B. für die Lesbarkeit konvertiert werden, verliert die Signatur ihre Gültigkeit. Um solche Konvertierungen zu vermeiden, sollten auch für die gesetzliche Aufbewahrung archivtaugliche Dateiformate gewählt werden.

Deshalb empfiehlt es sich, lediglich Dateien zu signieren, deren Format von der KOST empfohlen wird. Zum Begriff Archivierung siehe Glossar.

**SHOULD:** Falls die signierte Datei (im Rahmen der gesetzlich geforderten Frist) aufbewahrt werden muss, dann soll deren Format den Empfehlungen der KOST entsprechen.

**Anmerkung:** In SAR\_EC\_BASELINE und CEF: eSignature DSS wird keine Prüfung dazu erwähnt.

## 2.4.5 Verlässlichkeit der Anzeige des Signierten und dessen Bedeutung

Mit der Verlässlichkeit der Anzeige will man erreichen, dass eine Person verlässlich sieht, was sie unterschreiben wird, und verlässlich erkennt, was unterschrieben wurde. Zudem soll verhindert werden, dass sich das Erscheinungsbild (Visualisierung) des Signierten und dessen Bedeutung ändern kann, während die Signatur weiterhin gültig bleibt.

In ETSI EN 319 102-1 V.1.4.1, S. 18 oben wird aufgelistet, was den Signatur Prozess oder was die Verlässlichkeit der Anzeige dessen beeinflussen kann, was der Anwender oder die Anwenderin zu signieren gedenkt oder signiert worden ist:

The SD potentially has a number of important variants and components that impact the signing process and the status of the signature:

- 1) It can be in revisable format such as a word processor document or a message or file that can be edited, and where its presentation is dependent on the current configuration of the viewing device, and where the signer can potentially be presented a representation of the SD having an appearance different from that presented to the verifier.
- 2) It can be in an unambiguous form (e.g. txt, Postscript, ODA final form, etc.). These formats contain complete presentation rules that guarantee that the signer and verifier can be presented the SD in the same way if the same presentation rules are followed.
- 3) Hidden encoded information can be present (e.g. macros, hidden text, active or calculated components, viruses, etc.). These can be invisible to the signer during the preview and verification processes, and the signer can be unaware of their presence. These represent potential ambiguities in the SD.
- 4) It can be in a form that is not normally presented to the signer or verifier directly, or it can be in a form that is inherently presented to the signer and verifier in different ways (whilst representing the same semantics). Examples of these formats are Electronic Data Interchange formats, Web Pages (HTML), XML, SGML, and computer files.
- 5) It can be in a form representing multiple individual documents, either referenced or packed together using some data format. Each of these individual documents can be anything, from random data to business documents. Examples for such forms are ASIC or XMLDSig.

In ETSI EN 319 102-1 V.1.4.1, Kapitel 5.2.9 wird das Problem bei der Prüfung der Signatur wieder aufgegriffen, doch zu beiden Fällen werden keine konkreten Anforderungen gestellt oder Angaben gemacht, wie dies bewerkstelligt werden kann.

Die EU hat das Problem nur marginal erwähnt, in dem sie in SAR\_EC\_BASELINE, Kapitel 3.2.4 und auf S. 29 letzte Spalte folgende Empfehlungen stellt:

«A "what you see is what has been signed" environment is recommended.»

In eCH-0091 Kapitel 2.1 wird anhand eines Beispiels das Problem erläutert. In eCH-0091 für XML, Kapitel 4.1.3, und eCH-0250 für PDF, Kapitel 2.5, sind entsprechende Anforderungen konkretisiert worden.

**Hinweis:** Potentiell schädliche Links können im PDF vermieden werden, wenn anstelle von PDF das Dateiformat PDF/A verwendet wird. Die empfohlenen PDF/A-Versionen sind in eCH-0250 ersichtlich. Dies weil gemäss PDF/A-2 und PDF/A-1 solche Links verboten sind und entsprechend einfach mit einem den Prüfungsanforderungen entsprechenden «PDF/A-Validator» kontrolliert werden können. Ein «PDF/A-Validator» prüft in diesem Kontext die Konformität des PDF/A-Standards und darf nicht verwechselt werden mit dem «Validator» des Bundes. Dieser prüft zurzeit lediglich die Signatur ohne Long Term Validation-Material.

## Zusammenfassend

**SHOULD NOT:** Das, was signiert werden wird und was signiert wurde, soll in seiner Bedeutung oder in seinem Erscheinungsbild nicht verändert werden können, dies bei Wahrung der kryptographischen Gültigkeit der Signatur.

**SHOULD:** Wenn dem Anwender oder der Anwenderin das von der Signatur Erfasste präsentiert wird, soll die Signature Validation Application (SVA) prüfen, ob er oder sie verlässlich zu sehen vermag, was signiert worden ist, und ob diesbezüglich ein Missbrauchspotential besteht. U.a. soll geprüft werden, ob potentiell schädliche Links vorhanden sind.

**SHOULD:** Falls ein potentiell schädlicher Link vorhanden ist, soll eine entsprechende Meldung dem Anwender oder der Anwenderin gut sichtbar und verständlich angezeigt werden.

Sinnvoll ist, diesen Empfehlungen unabhängig von der Signatur vor der Aufbewahrung Folge zu leisten.

**Wichtig:** Bestimmungen aus Bundesgesetz und aus Ausführungsvorschriften (Verordnung, technische administrative Vorschriften) bestehen jedoch hierzu nicht.

## 2.5 Erstellung einer advanced electronic signature (AdES) nach ETSI

In ETSI EN 319 102-1 wird auch standardisiert, wie eine Signatur zu bilden ist, so dass deren Gültigkeit bewahrt wird. Dies ist jedoch grundsätzlich nicht Thema dieses Standards. In eCH-0091, eCH-0220, eCH-0230 und eCH-0250 wird standardisiert, wie eine solche Signatur mit ihren Zusatzinformationen beschaffen sein soll, damit die Gültigkeit der Signatur bewahrt werden kann, nicht aber der Weg dazu. Ein Vorschlag hierzu ist wie erwähnt in ETSI EN 319 102-1 beschrieben.

## 2.6 Revokations-Prüfung vs. Short-term-Zertifikate

Ein Zertifikat kann revoziert worden sein. Es muss daher bei der Gültigkeitsprüfung auf seinen Revokations-Status hin überprüft werden.

Eine Ausnahme bilden Short-term-Zertifikate. Diese werden mit einer Laufzeit ausgestellt, welche kürzer als die maximal zulässige Bearbeitungszeit eines Revokations-Antrags ist (z.B. 10 Minuten Laufzeit). Die Zertifikate laufen also bereits vor der genannten Bearbeitungszeit ab, womit die Revokation hinfällig wird. Die Anbieterin muss somit keine Revokations-Dienste zur Verfügung stellen und auch nicht zwingend den Revokations-Status per CRL oder OCSP angeben.

Short-term-Zertifikate werden oft mit Fernsignatur-Diensten verwendet. Wenn eine Fernsignatur erstellt wird, wird üblicherweise ein Schlüsselpaar nur einmal verwendet, das Zertifikat ad-hoc vor der Signaturerstellung ausgestellt und der private Schlüssel direkt nach dem Signaturvorgang gelöscht.

Zur Markierung von Short-term-Zertifikaten hat ETSI die Zertifikats-Erweiterung *ext-etsi-validated-ST-certs* in ETSI EN 319 412-1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures" definiert und spezifiziert.

In ETSI EN 319 411-1 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements" wird die richtige Verwendung der Zertifikats-Erweiterung *ext-etsi-valassured-ST-certs* seitens Anbieterin beschrieben.

Als Konsequenz kann bei markierten Short-term-Zertifikaten eine Revokations-Prüfung entfallen. Sämtliche weiteren Schritte einer Signaturprüfung müssen aber durchgeführt werden.

**MUST:** Es muss auch hier ein qualifizierter Zeitstempel bei Signaturen, welche mit einem Short-Term Zertifikat verifiziert werden, beigefügt werden, resp. vorhanden sein.

## 2.7 Eckpfeiler der Prüfung

### 2.7.1 Resultat der Prüfung

**MUST:** Was geprüft wird und was daraus resultiert, muss angezeigt oder einfach verfügbar gemacht werden.

### 2.7.2 Amtlich anerkannte Stelle

**MUST:** Die Angaben einer amtlich anerkannten Stelle im Kontext der Signatur sind anzuerkennen, solange von einer Partei kein Argument/Indiz für dessen Gegenteil vorgebracht wird.

Solche Angaben sind z.B. eine OCSP-Antwort, eine CRL, ein Zeitstempel eines (amtlich) anerkannten TSP. Als anerkannt gelten die TSP, welche von der SAS anerkannt wurden, oder der TSP, der von der EU anerkannt wurde und in einer Trusted List der EU geführt wird.

**MUST:** Falls sich Angaben widersprechen, dann muss man sich gemäss folgender Priorität an die Angaben orientieren:

- i. Angabe einer amtlich anerkannten Stelle
- ii. Angabe im dem von der Signatur Erfassten
- iii. Angabe in der Signatur

### 2.7.3 Zeitangaben

Aus ETSI TS 119 172-4:

the signature applicability rules checking report shall indicate, whenever applicable, the following timing information:

- claimed signing time in dem von der Signatur Erfassten
- time of the document time-stamp/time assertion
- time of the signature time-stamp/time assertion
- time of revocation (or suspension) of the signer's certificate
- time of OCSP response/time of CRL issuance & next update, at least for the signer's certificate
- Zeitangabe in der Signatur
- «best signature time». Zum Begriff, siehe KAPITEL 2.7.4.

**Ergänzung:** Falls vorhanden, kann auch noch die Zeitangabe in dem von der Signatur Erfassten (time indication in the file/object) relevant sein.

Wie bereits erwähnt, sollen Zeitstempel, Revokationslisten (CRL), CA Zertifikate oder OCSP Antworten, welche von einer amtlich anerkannten Stelle gemäss Art. 1 und 2 ZertES hergestellt werden, verwendet werden. Ohne einen Grund sind die dort enthaltenen Angaben nicht in Zweifel zu ziehen, siehe KAPITEL 2.7.2.

Folglich:

**MUST:** Falls vorhanden, muss geprüft werden, ob diese Zeitangaben bis auf die «claimed signing time» von einer amtlich anerkannten Stelle stammen.

**MUST:** Falls sich die genannten Zeitangaben widersprechen, dann muss man sich mit folgender Priorität in Bezug auf die Zeitangabe orientieren:

- i. Zeitangabe einer amtlich anerkannten Stelle
- ii. Zeitangabe in dem von der Signatur Erfassten
- iii. Zeitangabe in der Signatur

**Hinweis:** Im Anhang A von ETSI EN 319 102-1 ist summarisch aufgeführt, was sich im Laufe der Zeit betreffend die Signatur ereignen kann und was dann unter den gegebenen Umständen zu prüfen ist.

#### 2.7.4 Best signature time

**Begriff:** Als «best signature time» wird der späteste Zeitpunkt erachtet, an welchem die Signatur angefertigt wurde. Zudem stellt dieser Zeitpunkt den frühestmöglichen Nachweis (Proof of Existence, kurz POE) dar, an dem belegt werden kann, dass die Signatur erstellt wurde. Hierzu aus ETSI EN 319 102-1 V.1.4.1, Kapitel 5.5.4, Note 1:

Best-signature-time is an internal variable for the algorithm denoting the earliest time when it can be trusted by the SVA (either because proven by some POE present in the signature or passed by the DA and for this reason assumed to be trusted) that a signature has existed.

**MUST:** Die «best signature time» muss in einem Zeitraum liegen, der auf amtlich anerkannten Angaben basiert und aus dem sich ableiten lässt, dass das zur Verifikation verwendete Zertifikat zum Zeitpunkt der Signaturerstellung gültig war. Dieses Ergebnis muss aus der Prüfung hervorgehen.

#### 2.7.5 Signaturformat

**SHOULD:** Zu Signierendes, welches nicht über ein eigenes Signaturformat verfügt, sollt mit einer CMS-Signatur versehen werden.

**Beispiel:** XML, PDF, JSON verfügen über ein eigenes Signaturformat sind.

**SHOULD:** Die Richtigkeit der soeben genannten Zuordnung soll geprüft werden.

## 2.8 Prüfungsumfeld

Es werden Prüfungen betreffend die Signatur vorgeschlagen, welche auf den Bereich des eGovernment zugeschnitten sind, d.h. in einem Bereich, wo es sich um eine ausservertragliche Situation handelt.

Private Organisationen und Personen können formfrei untereinander vereinbaren, was sie als gültige Signaturen erachten, siehe Art. 14 Abs. 2<sup>bis</sup> OR. Es empfiehlt sich in diesem Fall, eine entsprechende technische Policy auszuarbeiten und unter den beiden Parteien als verbindlich zu erklären.

**Anmerkung:** Die hier vorgestellten Prüfschritte können auch in anderen Bereichen als im eGovernment- Bereich angewandt werden.

## 2.9 Trusted List

### 2.9.1 eIDAS

Gemäss eIDAS sind sämtliche Mitgliedsstaaten der Europäischen Union (EU) und des gesamten Europäischen Wirtschaftsraums (EWR) verpflichtet, jeweils eine eigene nationale "Trusted List" (auch "Trust List") der gemäss eIDAS amtlich anerkannten TSP zu führen. Diese nationalen Listen werden wiederum in einer einheitlichen, EU/EWR-weiten Liste referenziert. Ein Dienst zur Ausgabe von qualifizierten Signaturen, Siegeln oder Zeitstempeln muss in einer nationalen Trusted List aufgeführt sein, um als amtlich anerkannt zu gelten. Ein solcher Dienst ist in jedem EU/EWR-Mitgliedsstaat eIDAS-konform. (Information: Neben Signatur-spezifischen Diensten enthalten diese Listen auch weitere Vertrauensdienste/Trust Services.)

Jede Dienste-Anbieterin, welche als konform mit den eIDAS-Anforderungen anerkannt ist, und jeder eIDAS-konforme Dienst werden in der entsprechenden nationalen Liste mit seinen Attributen aufgeführt wie z.B. Name, Art des Dienstes, CA-Zertifikat etc. Auch der Gültigkeitsanfang und ein etwaiges Gültigkeitsende (sofern nicht mehr aktiv) wird für jeden Dienst aufgeführt. Die Listen enthalten also auch eine Historie sowohl bezüglich aktiver Dienste als auch hinsichtlich der Dienste, welche in der Vergangenheit gültig waren.

Eine lesbare Darstellung der im XML-Format geführten Listen ist unter folgendem Link einsehbar/erkennbar: <https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls>

### 2.9.2 ZertES

Auch die Schweiz führt eine solche Trusted List für ZertES-konforme Dienste. Da zum Zeitpunkt der Erstellung dieses Dokuments diesbezüglich kein internationales Abkommen mit der EU besteht, ist die schweizerische Trusted List nicht in der EU/EWR-weiten Liste aufgeführt und es besteht keine gegenseitige gesetzliche Anerkennung von Anbieterinnen. Es gibt also keine Abhängigkeit oder Beziehung.

Gemäss ZertES anerkannte Anbieterinnen und die Zertifizierungsdienste zur Ausstellung geregelter und qualifizierter Zertifikate werden in einer Trusted List im Namen der Schweizerischen Akkreditierungsstelle (SAS) geführt. Das heisst, eine Certification Authority (CA) zur Ausstellung von qualifizierten oder geregelten Zertifikaten muss auf ihr Vorhandensein in der schweizerischen Trusted List geprüft werden. Die aktuelle Version der schweizerischen Trusted List kann unter der folgenden Adresse heruntergeladen werden:

<https://trustedlist.tsl-switzerland.ch/tsl-ch.xml>

Der Aufbau und das technische Format werden durch die ETSI-Spezifikation ETSI TS 119 612 "Electronic Signatures and Infrastructures (ESI); Trusted Lists" geregelt.

Die Vorgaben zur Prüfung regelt die Spezifikation ETSI TS 119 615 "Electronic Signatures and Infra- structures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists".

Technische Parameter zur Dienstbeschreibung spezifisch für die Schweiz werden unter <https://uri.tsl-switzerland.ch/TrstSvc/TrustedList/schemerules/CH> (Swiss-TL) aufgeführt.

**Zu beachten ist:** Nur gemäss ZertES anerkannte und betriebene Dienste sind in der schweizerischen Trusted List aufgeführt. Z.B. gibt es für **nicht nach ZertES geregelte** Signaturen und für **nicht nach ZertES geregelte** Siegel in der Schweiz **keine Anerkennung** gemäss ZertES. Die entsprechenden Dienste sind darum nicht in der Trusted List für ZertES enthalten, auch wenn diese von einer anerkannten Anbieterin von Zertifizierungsdiensten angeboten werden.

Weitere Informationen zur schweizerischen Trusted List werden vom Bakom unter <https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki1.html> zur Verfügung gestellt.

### 2.9.3 Nicht gesetzlich geregelte Signaturen

Für Anwendungsfälle, welche nicht einer ZertES- oder eIDAS-konformen Signatur bedürfen, können auch gesonderte Trusted Lists erstellt werden. Für solche Dienste können eigene Trusted Lists erstellt werden.

**MAY:** Das technische Format der Trusted List für nicht gesetzlich geregelte Signaturen kann auch von demjenigen in ETSI TS 119 615 Beschriebenen abweichen.

**MUST:** Auch wenn die aktuell gültigen Trusted Lists und die dazugehörige Historie aufbewahrt und publiziert werden, müssen die entsprechenden CA-Zertifikate bei den LTV-Informationen beigefügt werden: Es sind die entsprechenden Empfehlungen in eCH-0220, eCH-0230 und eCH-0250 sowie die entsprechenden Standards zu AdES von ETSI zu PDF, XML und CMS zu beachten.

### 3 Kapitel 5 Signature Validation

Wie bereits erwähnt, bildet Kapitel 5 aus ETSI EN 319 102-1 V1.4.1 die Basis der Signaturprüfung. Es beschreibt u.a. die Mindestanforderungen an das, was unter den gegebenen Umständen geprüft werden muss und wie die Ergebnisse der Prüfung zu bewerten sind. Dabei wird noch ein summarisches Ergebnis der Prüfung vorgeschlagen, siehe KAPITEL 3.1.

Der Inhalt der Prüfung hängt von den gegebenen Umständen ab. Dem trägt ETSI EN 319 102-1 Rechnung, indem nicht jeder Prüfschritt bei gewissen Konstellationen durchgeführt werden muss.

Es wird ein «Profile» des Kapitels 5 dieses Standards vorgenommen. D.h. es wird ergänzt, wo dies als notwendig erachtet wird. Folgende Anmerkungen und Empfehlungen beziehen sich auf die jeweiligen Kapitel in diesem Standard.

#### 3.1 Kapitel 5.1.1 General Requirements

In diesem KAPITEL wird u.a. standardisiert, welche Rückmeldungen eine Applikation für die Signatur-Prüfung (engl. Signatur Validation Application, kurz SVA) nach einer Signaturprüfung generieren kann. Dabei werden auch folgende 3 Statusmeldungen standardisiert, welche ein Gesamtergebnis der Prüfung verkörpern:

**TOTAL-PASSED:** when the cryptographic checks of the signature (including checks of hashes of individual data objects that have been signed indirectly) succeeded as well as all checks prescribed by the signature validation policy have been passed.

**TOTAL-FAILED:** the cryptographic checks of the signature failed (including checks of hashes of individual data objects that have been signed indirectly), or it is proven that the signing certificate was invalid at the time of generation of the signature, or because the signature is not conformant to one of the base standards to the extent that the cryptographic verification building block is unable to process it.

**INDETERMINATE:** the results of the performed checks do not allow to ascertain the signature to be TOTAL-PASSED or TOTAL-FAILED.

**Anmerkung:** Der Empfänger einer Signatur entscheidet, ob er eine Signatur akzeptieren will oder zu akzeptieren hat, wenn das Prüfungsergebnis INDETERMINATE lautet. Kurzum: Die Bewertung der Prüfungsergebnisse liegt in der Verantwortung des Empfängers oder der Empfängerin.

#### 3.2 Kapitel 5.1.2. Selecting Validation Process

**Anmerkung:** Welcher Prüfprozess initiiert werden muss, hängt von der Security Policy ab.

**MUST:** Die Security Policy muss mit den bestehenden Vorschriften verträglich/kompatibel sein.

### 3.3 Kapitel 5.1.3 Status indication of the signature validation process and signature validation report

#### 3.3.1 Grundsatz zur Bewertung

In den Tabellen 5 und 6 des ETSI- Standards wird definiert, welches Prüfungsergebnis welche Form der summarischen Meldung (TOTAL-PASSED, TOTAL-FAILED, INDETERMINATE) zur Folge hat.

**MUST NOT:** Die Anforderungen an das, was als TOTAL-PASSED akzeptiert wird, dürfen im eGovernment-Bereich nicht geringer sein, als sie im ETSI-Standard beschrieben werden.

Folglich können mehrere Prüfungsergebnisse, wie sie in Tabelle 6 des Standards aufgeführt sind, im eGovernment -Bereich das summarische Ergebnis TOTAL-FAILED haben.

#### 3.3.2 Zusätzliche Rückmeldungen

Weil gemäss dem hier vorliegenden eCH-Standard und gemäss den Vorgaben der EU-Kommission (SAR\_EC\_BASELINE) unter gewissen Umständen weitere Schritte zu prüfen sind, werden hier weitere Rückmeldungen der Signaturapplikation aufgeführt.

**Wichtig:** Im Folgenden werden die möglichen Rückmeldungen zu den jeweiligen Prüfungen in Kürzel aufgeführt. Die hier aufgeführten Kürzel unterscheiden sich in der Schreibweise von denjenigen von ETSI, indem sie im Allgemeinen nur Kleinbuchstaben enthalten.

Kürzel	Bedeutung
no_qualified_signature	Keine qualifizierte Signatur oder kein qualifiziertes Siegel
no_qualified_timestamp	Nicht qualifizierte(r) Zeitstempel enthalten
not_appropriate_for_longterm_storage	Format des Signierten ist nicht geeignet für die dauerhafte Aufbewahrung.
pdf_content_constraints_failure	Inhalt des PDF entspricht nicht den Vorgaben von eCH-0250
integrity_constraints_failure	Teile des Signierten können verändert werden, so dass inhaltlich Relevantes oder das Erscheinungsbild des Signierten verändert werden kann, wobei die Gültigkeit der Signatur nicht verändert wird.
no_timestamp	Kein Zeitstempel
no-Swiss-gov_accepted_certificate	Zertifikat wurde nicht von einem von der Schweiz anerkannten TSP ausgestellt.
no-EU-gov_accepted_certificate	Zertifikat wurde nicht von einem von der EU anerkannten TSP ausgestellt.
detached_signature	Detached Signature enthalten <sup>1)</sup>
format_content_mismatch	Das Signierte stimmt nicht mit dem dazu vorgegebenen Signaturformat überein.

Kürzel	Bedeutung
signature_format_unknown	Das Signaturformat ist unbekannt oder wird nicht unterstützt.
commitment_type_indication	Keine «Commitment Type Indication» vorhanden, siehe dazu KAPITEL 3.6
no_sscd_indication	Keine Angabe darüber, ob die Signatur in einer sicheren Signaturerstellungseinheit gebildet wurde.
tsp_in_no_accepted_trustlist	Der TSP ist nicht in einer amtlich anerkannten Trustlist aufgeführt.
OverlappingProhibited <sup>2)</sup>	Im PDF befinden sich zwei oder mehr vom Benutzer erkennbare Signaturen (Signaturfelder), die sich überlagern (overlapping of visible signatures)
no_Swiss_qualified_certificate	Das (qualifizierte) Zertifikat entspricht nicht den Anforderungen der TAV
no_EU_qualified_certificate	Das (qualifizierte) Zertifikat entspricht nicht den Anforderungen der SAR_EC_BASELINE oder der CEF: eSignature DSS

Tabelle 1: Weitere Rückmeldungen zu den Prüfungsergebnissen

<sup>1)</sup> **Anmerkung:** Detached Signaturen sind z.B. bei CMS- und XML-Signaturen möglich. Folgende Vorschrift in SAR\_EC\_BASELINE dazu:

Signed data may only be detached from the signatures when both the detached signatures and the signed data are within an ASiC container.

Die Thematik der detached Signaturen wird in CEF: eSignature DSS nicht erwähnt.

<sup>2)</sup> **Anmerkung:** Das Kürzel stammt aus SAR\_EC\_BASELINE, S. 33 Zeile c. Dazu in SAR\_EC\_BASELINE, S. 21 unten: When electronic documents contain more than one visible signature, there shall not be any overlapping of such signatures.

**Anmerkung:** Weder SAR\_EC\_BASELINE noch ETSI TS 119 172-4 enthalten Kürzel für Rückmeldungen, welche aus den zusätzlichen, hier empfohlenen Prüfungen einer qualifizierten Signatur, eines qualifizierten Siegels oder eines qualifizierten Zeitstempels stammen. Zusätzlich heisst, mehr Prüfungen als in ETSI EN 319 102-1 V.1.4.1 oder SAR\_EC\_BASELINE aufgeführt sind.

### 3.4 Kapitel 5.2.2 Format Checking

#### 3.4.1 Zu unterstützende Signaturformate gemäss eCH

**MUST:** Folgende Signaturformate müssen in der Schweiz bei der Prüfung unterstützt werden:

- XAdES (ETSI EN 319 132-1), eCH-0230
- PAdES (ETSI EN 319 142-1) mit ISO 32000-1 und -2, eCH-0250
- CAdES (ETSI EN 319 122-1), eCH-0220

**MAY:** JSON Signature (JAdES). JSON Signaturen sind bei Verifiable Credentials (VC) im SSI Umfeld angedacht.

#### 3.4.2 Zu unterstützende Signaturformate gemäss SAR\_EC\_BASELINE

DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 2015/1506 legt fest, welche Formate einer Signatur unterstützt werden müssen. Die Formate beschränken sich gemäss Anhang DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 2015/1506 auf:

- XAdES (ETSI EN 319 132-1)
- PAdES (ETSI EN 319 142-1) und PDF- Signaturen nach ISO 32000-1
- CAdES (ETSI EN 319 122-1)
- ASiC (ETSI EN 319 162-1)

**MUST:** Eine Signaturprüfung muss die soeben genannten Signaturformate bei Signaturen aus der EU unterstützen.

**SHOULD:** Die Prüfapplikation soll in diesem Kontext bei einer Signatur in einem PDF auch das Format ISO 32000-2 unterstützen.

**Anmerkung:** Zu ASiC gibt es kein eCH-Profil.

**Anmerkung:** eCH-0220, eCH-0230 und eCH-0250 stützen sich ebenfalls auf diese Standards ab. Im Unterschied zur SAR\_EC\_BASELINE soll die Prüfapplikation noch das PDF-Format ISO 32000-2 unterstützen. ISO 32000-2 (PDF 2.0) hat im Unterschied zu 32000-1 die notwendigen (ETSI)-Merkmale für die Bewahrung der Gültigkeit von PDF-Signaturen standardisiert. ETSI führt in ihrem Standard ETSI EN 319 142-1 zu ISO-32000-1 proprietäre Erweiterungen ein.

### 3.5 Kapitel 5.2.7.2 Inputs

Note 2 dort:

When validating signatures like detached signatures, where only the hashes, of objects are signed but the objects themselves are not part of the signature, it is unspecified whether it is the task of the DA to validate these hashes or whether an implementation uses the present clause for having the hash(es) of such objects validated by the SVA. Both variants are possible.

**MUST:** Die SVA muss prüfen, ob das Signierte mit dem Hashwert übereinstimmt oder nicht. D.h. das von der Signatur Erfasste muss dem Prüfenden vorliegen.

**MUST:** Wenn diese nicht übereinstimmen, dann muss das Resultat der Prüfung «FAILED» lauten.

### 3.6 Kapitel 5.2.9 Signature validation presentation building block

**SHOULD:** Zusätzlich soll angezeigt werden, ob es in dem von der Signatur Erfassten Informationen hat, welche die Verlässlichkeit der Anzeige und die Bedeutung des Signierten beeinträchtigen können, siehe KAPITEL 2.4.5.

### 3.7 Format und Inhalte

#### 3.7.1 Verlässlichkeit der Anzeige

**SHOULD:** Die Verlässlichkeit der Anzeige soll entsprechend dem KAPITEL 2.4.5 geprüft werden können.

#### 3.7.2 Aufbewahrungstauglichkeit der Datenformate

**SHOULD:** Die Aufbewahrungstauglichkeit der Datei soll entsprechend dem KAPITEL 2.4.4 geprüft werden können.

#### 3.7.3 Zuordnung Signatur Dateiformat

**SHOULD:** Zu Signierendes, welches nicht über ein eigenes Signaturformat verfügt, soll eine CMS-Signatur haben.

**SHOULD:** Dies soll verifiziert werden.

**Beispiel:** XML (XAdES), PDF (PAdES), JSON (JAdES) haben eigenes Signaturformat.

### 3.8 Commitment-type-indication

Gemäss Vorgaben von SAR\_EC\_BASELINE, S. 24, Kapitel 3.2.2 soll gelten:

An indication of that commitment should be present in the electronic signatures, using standard attributes and values intended for that purpose.

In PAdES signatures, the commitment-type-indication attribute defined in ETSI EN 319 122-1 clause 5.2.3 (whose presence is conditioned according to ETSI EN 319 142-1 clause 6.3) should be present, and should indicate either the commitment type “Proof of Origin” or “Proof of approval” identified by the OIDs 1.2.840.113549.1.9.16.6.1 and 1.2.840.113549.1.9.16.6.5 respectively, as defined in ETSI TS 119 172-1 Annex B.

Anders die Empfehlungen der eCH-Standards, z.B. in eCH-0220:

Die Erklärungen und Absichten, welche mit der Signatur abgegeben wurden, sollen aus dem Signierten zu entnehmen sein. Deswegen soll dieses Attribut nicht verwendet werden.

Dies basierend auf der Vermutung, dass bei einem Rechtsverfahren jener Inhalt geltend gemacht wird, welcher im Signierten steht, und nicht, was der Signatur beigefügt wurde.

**MUST:** Falls es im Austausch von Signaturen im EU-Raum notwendig ist, muss geprüft werden können, ob diese Angaben der Signatur beigefügt wurden.

**MAY:** Man kann man eine solche Prüfung vorsehen.

### 3.9 «Claimed Attribute»

#### 3.9.1 Anmerkung zu «Claimed Attribute»

Bei «Claimed Attribute» handelt es sich um Informationen, welche der Empfänger oder die Empfängerin der Signatur nicht oder sehr eingeschränkt prüfen und somit vermutlich nicht als Beleg verwenden kann. Es fehlt ein POE (PROOF OF EXISTENCE).

Davon unterscheiden sich die von amtlich anerkannten Dritten bestätigten Informationen, z.B. ein Zeitstempel eines nach ZertES anerkannten TSP oder eines TSP aus der EU und dem EWR, welcher in deren Trustlist dort aufgeführt ist.

#### 3.9.2 Vom Benutzer zu prüfen

«Claimed» Informationen, wie die Zeit- oder Ortsangabe in dem von der Signatur Erfassten oder in der Signatur selbst können im Widerspruch zu anderen Angaben stehen.

**MUST:** Der Benutzer/die Benutzerin oder die Anwendung muss prüfen können, ob diesbezüglich ein solcher Widerspruch besteht.

#### 3.9.3 Kapitel 5.2.8.4.3.2 Processing claimed signing time

Siehe KAPITEL 2.7.3.

#### 3.9.4 Kapitel 5.2.8.4.2.5 Processing indication of production place

Siehe KAPITEL 2.7.2.

#### 3.9.5 Sichere Signaturerstellungseinheit

Das ZertES (Art. 2 Bst. c und d) fordert, dass eine geregelte Signatur oder eine geregeltes Siegel in einer sicheren Signaturerstellungseinheit kreiert wird. Die Anforderungen an eine sichere Signaturerstellungseinheit gemäss ZertES sind in der TAV Kapitel 2.2.3 geregelt.

eIDAS fordert bei einer qualifizierten elektronischen Signatur (Art. 3 Ziff. 12) und bei einem qualifizierten Siegel (Art. 3 Ziff. 27), dass die Signatur in einer gemäss eIDAS qualifizierten Signaturerstellungseinheit kreiert wird. Die Anforderungen an eine sichere Signaturerstellungseinheit sind im Anhang II eIDAS beschrieben.

Der Empfänger einer Signatur kann jedoch nicht prüfen, ob die Signatur entsprechend hergestellt wurde. Er hat sich auf die Angaben in der Signatur, resp. Zertifikat zu verlassen. Folglich handelt es sich hiermit um ein «Claimed Attribute».

### 3.10 Kapitel 5.2.3 Identification of the signature certificate

**MUST:** Es muss geprüft werden können, ob die Signatur zu einem geregelten Zertifikat oder qualifizierten Zertifikat gemäss ZertES passt oder den Vorgaben von SAR\_EC\_BASELINE oder von CEF: eSignature DSS entspricht.

**Anmerkung:** Zur geforderten Beschaffenheit eines nach ZertES hergestellten qualifizierten Zertifikats, siehe TAV Kapitel 2.3.3. Zu den Vorgaben der EU, siehe CEF: eSignature DSS und SAR\_EC\_BASELINE, S. 30 Zeile (m) mit Verweis auf ETSI TS 119 615 v.1.2., Kapitel 4.4.

### 3.11 Kapitel 5.4 Time-stamp validation building block

**MUST:** Es muss geprüft werden können, ob es sich um einen qualifizierten Zeitstempel gemäss ZertES oder eIDAS handelt.

**Anmerkung:** Zur geforderten Beschaffenheit eines nach ZertES hergestellten geregelten oder qualifizierten Zertifikats, siehe TAV Kapitel 2.4. Zu den Vorgaben gemäss SAR\_EC\_BASELINE, siehe S. 30 Zeile h mit Verweis auf ETSI TS 119 615.

## 4 Beurteilung/Anforderung an die Akzeptanz

In diesem KAPITEL werden eine Reihe von Konstellationen (Use Cases) beim Empfang einer Signatur vorgestellt. Dabei wird standardisiert, was zu prüfen ist und welche Rückmeldungen aus einer nicht erfolgreichen Prüfung zu erfolgen haben. Das jeweilige Ergebnis einer nicht erfolgreichen Prüfung wird dabei klassifiziert (FAILED, INDETERMINATE).

Wie bereits erwähnt, hängt das, was zu prüfen ist und wie die Prüfungsergebnisse zu beurteilen sind, von der Security Policy ab.

**MUST:** Diese muss mit den rechtlichen Rahmenbedingungen verträglich/kompatibel sein.

### 4.1 Allgemeines

#### 4.1.1 Konvention

Die jeweils geforderten Prüfschritte werden hier unter «MUST» aufgeführt.

#### 4.1.2 Unterschied zu ETSI EN 319 102-1

ETSI EN 319 102-1 V.1.4.1 lässt bei einigen Prüfschritten offen, ob ausreichend Informationen für die gesamte Prüfung vorhanden sind, siehe z.B. Tabelle 9,10,11,12 dort.

Im Unterschied zu ETSI wird hier jedoch angenommen, dass die für die Prüfung geforderten Informationen der SVA verfügbar sind.

**MUST:** Ansonsten muss das summarische Ergebnis der Prüfung lauten: «Nicht akzeptiert», nach ETSI «TOTAL-FAILED». Ausnahme hiervon ist, wenn das Ergebnis einer Prüfung zeitabhängig ist, wie :

- die zeitliche Gültigkeit des Zertifikats
- die eingesetzten Verfahren gelten als «anerkannt ausreichend sicher».

**MAY:** Dann kann das summarische Ergebnis der Prüfung auch «INDETERMINATE» sein.

**MUST:** Falls möglich, muss geprüft werden, ob die Prüfung mit den Parametern erfolgreich ist, welche zum Zeitpunkt der Erstellung der Signatur als gültig erachtet wurden.

#### Beispiele:

- Beim Zertifikat muss geprüft werden, ob das Zertifikat zum Zeitpunkt des Leistens der Signatur gültig war.
- Eine der Handunterschrift gleichgestellte Signatur nach Art. 14 OR Abs. 2<sup>bis</sup> wird heute geprüft. Die Signatur wurde vor dem 18. März 2016 erstellt. In diesem Fall darf nicht beanstandet werden, dass sie nicht der Handunterschrift gleichgestellt ist, wenn der qualifizierte Zeitstempel fehlt. Vor dem 18. März 2016 wurde noch nicht verlangt, dass eine der Handunterschrift gleichgestellte Signatur mit einem (qualifizierten) Zeitstempel versehen werden muss.

**Anmerkung:** Wie die Prüfung eines Zertifikats erfolgt und was dazu benötigt wird, kann unterschiedlich sein. Hier wird auf ETSI-Standards abgestützt, worauf auch das technische Konzept der EU basiert.

### 4.1.3 Prozess der Prüfung (Prüfungsablauf)

In ETSI EN 319 102-1 V.1.4.1 wird ein Vorschlag dargelegt, wie der Prozess der Prüfung abgewickelt werden kann. Er ist jedoch nicht normativ. In diesem Dokument wird lediglich aufgeführt, was zu prüfen ist, jedoch keine Angaben darüber gemacht, in welcher Reihenfolge zu prüfen ist.

### 4.1.4 Zu den Rückmeldungen

Im KAPITEL 3.3 sind mehr Rückmeldungen als bei ETSI EN 319 102-1 aufgeführt. Dies im Bewusstsein, dass diese Rückmeldungen nicht ETSI konform sind. Dort, wo die Prüfschritte mit ETSI übereinstimmen, werden die Rückmeldungen von ETSI 319 102-1 übernommen.

Die Rückmeldungen in ETSI EN 319 102-1 sind technischer Natur und nicht allgemein verständlich. Deswegen bedürfen sie einer weiteren Überarbeitung, falls diese als allgemein verständliche Informationen dienen sollen.

**MUST:** Falls ein Prüfungsergebnis dem Anwender oder Anwenderin präsentiert werden soll, dann muss es allgemein verständlich sein, siehe Kapitel 5.1.3. ETSI EN 319 102-1 V1.4.1. und SAR\_EC\_BASELINE, S. 17.

**Visible signature:** visual representation of the human act of signing placed within an electronic in a human understandable way as part of the human readable and printable content of the document.

Was angezeigt werden muss/soll, ist im KAPITEL 3.6 aufgeführt.

### 4.1.5 Zur Gesamtbewertung (summarisches Ergebnis)

#### Konvention:

- Wird eine der Prüfungen, welche unter «MUST» aufgeführt wird, als nicht befriedigend erachtet (FAILED), dann lautet auch das summarische Ergebnis in der Regel «FAILED».
- Sind alle Prüfungen, welche unter «MUST» aufgeführt werden, erfolgreich, dann lautet das summarische Ergebnis «TOTAL-PASSED», ansonsten «INDETERMINATE».
- Wird eine der Prüfungen, welche unter «SOLL» aufgeführt wird, als nicht befriedigend erachtet (FAILED), dann ist es am Empfänger/an der Empfängerin der Signatur darüber zu entscheiden, was er unternehmen möchte. Z.B. kann er/sie den Absender oder die Absenderin bitten, eine dem Kriterium entsprechende Signatur/Datei zu senden.
- Wird eine Prüfung als «TOTAL-FAILED» eingestuft, dann wird sie nicht akzeptiert und vice-versa.

**MUST NOT:** Eine Signatur mit einer fehlgeschlagenen Prüfung, d.h. mit der Gesamtbewertung «TOTAL-FAILED», darf nicht akzeptiert werden.

## 4.2 Überblick über die Prüfschritte

Die Schritte zur Prüfung einer elektronischen Signatur lassen sich wie folgt unterteilen:

1. Prüfen, ob die Signatur kryptographisch korrekt hergestellt wurde und dem Signaturschema entspricht. Dies ist bei allen für die Prüfung relevanten Signaturen vorzunehmen, z.B. bei X.509 Zertifikaten oder bei OCSP-Antworten.
2. Prüfen der Zertifikate und der dazu gehörigen Zertifikatsketten.
3. Prüfen, ob die Signatur zum Zeitpunkt hergestellt wurde, als das dazu gehörige Zertifikat noch gültig war. Dies bedingt das Feststellen der «best signature time». Diese Zeit muss mit der Zeitangabe im Zeitstempel übereinstimmen, welcher als erstes nach der Signatur angefertigt wurde.
4. Prüfen des Inhalts. Enthält das von der Signatur Erfasste Bestandteile, welche das Erscheinungsbild in der Applikation verändern lassen könnten, wobei die Signatur jedoch gültig bliebe, siehe dazu KAPITEL 2.4.5.
5. Prüfen der Aufbewahrungstauglichkeit des Signierten

## 4.3 Basis-Signatur

Die Basis Signatur bildet das Grundgerüst der Prüfung einer Signatur. Dabei kann es sich z.B. um eine Signatur in einem PDF, um eine JSON Signatur, um eine OCSP Antwort, um einen Zeitstempel oder um eine Signatur handeln, welche mit einem nach ZertES geregelten Zertifikat verifiziert werden kann. Das Grundgerüst der Basis-Signatur entspricht der Figur 6 in ETSI EN 319 102.1 V.1.3.1.

### 4.3.1 Was zu prüfen ist

**MUST:** Die Prüfung muss folgende Schritte umfassen:

- Signaturformat bekannt und wird unterstützt
- Korrektheit des Signaturformats
- Kryptographische Richtigkeit der Signatur
- Eingesetzte Verfahren zur Bildung einer elektronischen Signatur sind vorschriftsgemäss
- Gültigkeit des dazu gehörigen Zertifikats
- Das Zertifikat ist von einem TSP herausgegeben worden, welcher in der Trusted List aufgeführt ist.
- Prüfen, ob eine «detached signature» und das von der Signatur Erfasste vorliegen.

**SHOULD:** Die Prüfung soll folgende Schritte umfassen:

- Die Verlässlichkeit der Anzeige, siehe KAPITEL 2.4.5
- Die signierte Datei ist für die Aufbewahrung geeignet, siehe KAPITEL 2.4.4
- Zugehörigkeit Signatur und Dateiformat, siehe KAPITEL 2.1.3
- Beim PDF: Überlagerung der Signaturfenster. Bei einem PDF dürfen sich nach einer Gegenzeichnung die Signaturfenster nicht überlagern; dies gemäss SAR\_EC\_BASELINE, S.33 Zeile c.

**Anmerkung zur E-Mail- Signatur:** Die unter «MUST» aufgeführten Prüfschritte entsprechen in etwa dem, was normalerweise bei der Prüfung einer E-Mail-Signatur vorgenommen wird. Eine grosse Gefahr bei der E-Mail-Signatur besteht in der Verlässlichkeit der Anzeige. Z.B., wenn die E-Mail HTML-Objekte mit Links enthält.

### 4.3.2 Rückmeldungen zur Prüfung

#### 4.3.2.1 MUSS geprüft werden

##### 4.3.2.1.1 A) Signatur

Prüfschritt	Mögliche Rückmeldung bei Fehler	Bewertung bei Fehler
Signaturformat bekannt, unterstützt	signature_format_unknown	FAILED
Korrektheit des Signaturformats	<i>FORMAT_FAILURE</i>	TOTAL-FAILED
Vorhandensein des Zertifikats	<i>NO_SIGNING_CERTIFICATE_FOUND</i>	FAILED
Der öffentliche Schlüssel im Zertifikat kann nicht dazu verwendet werden, die Signatur zu prüfen.	<i>SIG_CRYPTO_FAILURE</i>	TOTAL-FAILED
Kryptographische Richtigkeit der Signatur	<i>HASH_FAILURE</i>	TOTAL FAILED
Die eingesetzten Verfahren gelten als «anerkannt ausreichend sicher».	<i>CRYPTO_CONSTRAINTS_FAILURE</i> ,	INDETERMINATE
TSP in einer Trusted List	tsp_in_no_accepted_trustlist, no-Swiss-gov_accepted_certificate, no-EU-gov_accepted_certificate	INDETERMINATE oder FAILED <sup>1)</sup>
Prüfen, ob eine detached signature vorliegt und wenn ja, ob das dazugehörige Signierte vorliegt.	detached_signature <i>SIGNED_DATA_NOT_FOUND</i>	INDETERMINATE TOTAL-FAILED oder INDETERMINATE <sup>2)</sup>

Tabelle 2: Rückmeldungen der Prüfungsergebnisse zur Basis Signatur (MUST)

<sup>1)</sup> **Anmerkung:** Falls ein qualifiziertes oder geregeltes Zertifikat bei der Prüfung der Signatur gefordert wird, dann muss das Ergebnis FAILED lauten.

<sup>2)</sup> **Anmerkung:** In einem Fall von selective disclosure muss nicht alles von der Signatur Erfasste vorhanden sein oder dem Prüfer im Klartext präsentiert werden. Deswegen kann das Prüfungsergebnis auch als INDETERMINATE eingestuft werden.

**Begriff:** Bei selective disclosure wird nur ein Teil des von der Signatur Erfassten bei der Prüfung der Signatur offengelegt.

#### 4.3.2.1.2 B) Zertifikat

Prüfschritt	Mögliche Rückmeldung bei Fehler	Bewertung bei Fehler
Prüfschritte in Tabelle 2 angewandt auf die Signatur des Zertifikats	Siehe Tabelle 2	Siehe Tabelle 2
Prüfen der Zertifikatskette, siehe dazu Item 3 im KAPITEL 2.4.2	<i>CERTIFICATE_CHAIN_GENERAL_FAILURE, CHAIN_CONSTRAINTS_FAILURE</i>	FAILED
Zeitliche Gültigkeit des Zertifikats <sup>2)</sup> . Anforderung an die Gültigkeit eines Zertifikats, siehe KAPITEL 2.4.2 Item 4 und 5.	<i>NO_POE, REVOKED_NO_POE, REVOKED_CA_NO_POE, OUT_OF_BOUNDS_NOT_REVOKED, OUT_OF_BOUNDS_NO_POE, CHAIN_CONSTRAINTS_FAILURE, CERTIFICATE_GENERAL_FAILURE</i>	INDETERMINATE

Tabelle 3: Rückmeldungen der Prüfungsergebnisse zur Basis Signatur (MUST) betreffend das dazugehörige Zertifikat

<sup>1)</sup> **Anmerkung:** Die Prüfung ist für sämtliche relevanten Zertifikate vorzunehmen, d.h. z.B. für das dazugehörige Zertifikat einer OCSP-Antwort, eines Zeitstempels oder einer CRL.

<sup>2)</sup> **Anmerkung:** Die zeitliche Gültigkeit eines Zertifikats wird mittels einer OCSP-Antwort oder einer CRL Liste belegt.

#### 4.3.2.2 SOLL geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Verlässlichkeit der Anzeige/Bedeutung Bei einem PDF	<i>integrity_constraints_failure</i> <i>pdf_content_constraints_failure</i>	INDETERMINATE
geeignet für die Aufbewahrung	<i>not_appropriate_for_longterm_storage</i>	INDETERMINATE
Zugehörigkeit Dateiformat, Signaturformat	<i>format_content_mismatch</i>	INDETERMINATE
Beim PDF: Sich überlagernde signature icon	<i>OverlappingProhibited</i>	INDETERMINATE

Tabelle 4: Rückmeldungen der Prüfungsergebnisse zur Basis Signatur (SHOULD)

## 4.4 Die der Handunterschrift gleichgestellte Signatur

Die Anforderungen an eine der Handunterschrift gleichgestellte Signatur sind in Art 14 Abs. 2<sup>bis</sup> OR festgehalten:

Der eigenhändigen Unterschrift gleichgestellt ist die mit einem qualifizierten Zeitstempel verbundene qualifizierte elektronische Signatur gemäss Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES). Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten.

Falls nichts anderes geregelt wurde, wird davon ausgegangen, dass keine abweichende gesetzliche oder vertragliche Regelung vorliegt.

**Anmerkung:** Die Struktur der Signatur entspricht der Figur 7 in ETSI EN 319 102-1 V.1.4.1.

### 4.4.1 Was zu prüfen ist

**MUST:** Die Prüfung muss folgende Schritte umfassen:

- Alle Bestandteile aus KAPITEL 4.3 Basis-Signatur.
- Prüfen, ob das Zertifikat zur Verifikation der qualifizierten Signatur den Anforderungen in der TAV an ein qualifiziertes Zertifikat entspricht.
- Prüfen, ob es sich um eine nach ZertES qualifizierte Signatur handelt.
- Prüfen, ob ein Zeitstempel vorliegt und ob es sich dabei um einen nach ZertES qualifizierten Zeitstempel handelt.
- Prüfen, ob eine «detached signature» und das dazugehörige Signierte vorliegt.
- Prüfen des Zeitstempels, u.a. die Prüfschritte aus KAPITEL 4.3 Basis-Signatur für die Signatur des Zeitstempels und dessen Zertifikat.
- Prüfen, ob das Zertifikat vor und nach der Zeit gültig war, welche im Zeitstempel aufgeführt ist.

**SHOULD:** Die Prüfung soll folgende Schritte umfassen:

- Die Verlässlichkeit der Anzeige, siehe KAPITEL 2.4.5.
- Die signierte Datei ist geeignet für die Aufbewahrung siehe KAPITEL 2.4.4.
- Zugehörigkeit Signatur und Dateiformat, siehe KAPITEL 2.7.5.
- Beim PDF: Überlagerung der Signaturfenster. Bei einem PDF dürfen sich nach einer Gegenzeichnung die Signaturfenster nicht überlagern, dies gemäss SAR\_EC\_BASELINE, S.33 Zeile c.

Aufgrund von Art. 2 Abs. c und d ZertES muss das qualifizierte Zertifikat zum Zeitpunkt der Erstellung der Signatur gültig sein. Das Beifügen eines qualifizierten Zeitstempels ermöglicht, nachträglich zu eruieren, ob das qualifizierte Zertifikat zur Verifikation der qualifizierten Signatur zum Zeitpunkt der Erstellung des Zeitstempels gültig war.

#### 4.4.2 Rückmeldungen zur Prüfung

##### 4.4.2.1 MUSS geprüft werden

##### 4.4.2.1.1 A) Signatur und dazugehöriges Zertifikat

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Alle obligatorischen Prüfschritte im KAPITEL 4.3	siehe KAPITEL 4.3	siehe KAPITEL 4.3
Qualifiziertes Zertifikat	no_Swiss_qualified_certificate	FAILED
Signatur passend zu einem qualifizierten Zertifikat eines von der Schweiz amtlich anerkannten TSP	<i>CERTIFICATE_CHAIN_GENERAL_FAILURE, CHAIN_CONSTRAINTS_FAILURE, tsp_in_no_accepted_trustlist, no-Swiss-gov_accepted_certificate</i>	FAILED
Prüfen, ob es sich um eine detached signature handelt. Falls ja, ob das von dieser Signatur Erfasste ebenfalls vorliegt und geprüft werden kann.	detached_signature <i>SIGNED_DATA_NOT_FOUND</i>	INDETERMINATE FAILED oder INDETERMINATE <sup>1)</sup>

Tabelle 5: Rückmeldungen der Prüfungsergebnisse zur Basis Signatur (MUST)

<sup>1)</sup> **Anmerkung:** Im Fall von selective disclosure muss nicht alles von der Signatur Erfasste vorhanden sein oder dem Prüfer im Klartext präsentiert werden. Deswegen kann das Prüfungsergebnis auch als INDETERMINATE eingestuft werden.

4.4.2.1.2 B) Zeitstempel

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Zeitstempel	no_timestamp	INDETERMINATE <sup>2</sup>
Prüfung des Zertifikats eines Zeitstempels	Siehe KAPITEL 4.3.2.1.2 angewandt auf das Zertifikat des Zeitstempels.	Siehe KAPITEL 4.3.2.1.2
Das Zertifikat des Zeitstempels ist von einem amtlich anerkannten TSP herausgegeben worden	tsp_in_no_accepted_trustlist	FAILED
Qualifizierter Zeitstempel	no_qualified_timestamp	FAILED
Zeitstempel nicht in der richtigen Reihenfolge erstellt.	<i>TIMESTAMP_ORDER_FAILURE</i>	INDETERMINATE
Prüfen, ob das Zertifikat für die Signaturverifikation vor und nach der Zeit gültig war, welche im Zeitstempel aufgeführt ist.	<i>REVOKED<sup>1</sup>, EXPIRED<sup>1</sup></i>	TOTAL-FAILED

Tabelle 6: Rückmeldungen der Prüfungsergebnisse zum Zeitstempel (MUST)

<sup>1)</sup>**Anmerkung:** Die Rückmeldung *REVOKED* bei ETSI EN 319 102-1 V.1.4.1 Tabelle 6 bedeutet:

The signature validation process results into *TOTAL-FAILED* because:

- the signing certificate has been revoked; and
- there is proof that the signature has been created after the revocation time.

Ähnliches gilt hier für die Rückmeldung *EXPIRED*.

<sup>2)</sup>**Anmerkung:** Für eine vor dem 18. März 2016 hergestellte, der Handunterschrift gleichgestellte Signatur war kein Zeitstempel erforderlich.

**MUST:** Hier muss verifiziert werden, ob die Signatur nachweislich vor dem 18. März 2016 hergestellt wurde und folglich damals kein Zeitstempel erforderlich war.

#### 4.4.2.2 SOLL geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Verlässlichkeit der Anzeige/Bedeutung Bei einem PDF	integrity_constraints_failure  pdf_content_constraints_failure	INDETERMINATE
geeignet für die Aufbewahrung	not_appropriate_for_longterm_storage	INDETERMINATE
Zugehörigkeit Dateiformat, Signaturformat	format_content_mismatch	INDETERMINATE
Beim PDF: Sich überlagernde signature icon	OverlappingProhibited	INDETERMINATE

Tabelle 7: Rückmeldungen der Prüfungsergebnisse zur qualifizierten Signatur (SHOULD)

### 4.5 Basis Signatur mit Zeitstempel

**Anwendung:** Die Basis-Signatur mit Zeitstempel kann für Informationen relevant sein, welche nicht der Handunterschrift gleichgestellt signiert sein müssen.

Im Unterschied zu den Prüfungen bei der Basis Signatur sind die Prüfschritte entsprechend den Vorgaben im KAPITEL 4.4.2.1.2 und 4.4.2.2 vorzunehmen.

### 4.6 Austausch von Signaturen im Behördenumfeld der Schweiz

Wo eine elektronische Signatur auf Bundesebene im Behördenumfeld erforderlich ist, bedarf es einer qualifizierten elektronischen Signatur gemäss Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES). Z.B. Art. 21a VwVG, Art. 42 Abs. 4 BGG.

Im Unterschied zur Handunterschrift gleichgestellten Signatur nach Art. 14 Abs. 2<sup>bis</sup> OR ist hier kein qualifizierter Zeitstempel erforderlich. Entsprechend müsste auch nicht geprüft werden, ob ein solcher vorliegt. Ausserhalb der gesetzlichen Formvorschriften sind andere Signaturtypen möglich. Deren Prüfung ist jedoch nicht Thema in diesem Unterkapitel.

**Anmerkung:** Mit der Einführung des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) ist festgelegt, dass ein Zeitstempel für die Eingabe von Rechtsschriften erforderlich sein wird (Art. 22 Abs. 2 BEKJ).

## 4.7 Qualifizierte Signatur gemäss EU

In diesem Unterkapitel wird aufgeführt, was bei einer qualifizierten Signatur der EU zu prüfen ist, welche nicht mit AdES Informationen versehen sind. (AdES im Sinne von ETSI).

Im Unterschied zu der Handunterschrift gleichgestellten Signatur nach Art. 14 Abs. 2<sup>bis</sup> OR ist bei der qualifizierten Signatur der EU kein Zeitstempel erforderlich. Entsprechend muss auch nicht geprüft werden, ob ein solcher vorliegt, wenn das Zertifikat zur Prüfung der Signatur noch gültig ist. Doch falls ein Zeitstempel beigefügt wurde, dann muss es ein qualifizierter sein, SAR\_EC\_BASELINE, Kapitel 3.2.3 sein.

Die Prüfung, welche aufgrund zusätzlicher AdES-Informationen nach ETSI vorzunehmen ist, wird in den KAPITELN 4.8, 4.9 und 4.10 beschrieben. Dies entspricht dem, was auch zur CH-Signatur mit AdES Informationen hier empfohlen wird.

### 4.7.1 Was zu prüfen ist

In SAR\_EC\_BASELINE (Kapitel 3.2.1) und in CEF: eSignature DSS wird lediglich die Prüfung einer qualifizierten elektronischen Signatur/Siegel/Zeitstempel in Betracht gezogen.

**MUST:** Die Prüfung muss folgende Schritte umfassen:

- Alle Bestandteile aus KAPITEL 4.3 Basis-Signatur.
- Prüfen ob eine «detached signature» vorhanden ist. Falls ja, dann muss die Signatur im ASiC Format vorliegen, SAR\_EC\_BASELINE, S. 21, zweitletzter Absatz.
- Signaturformat passend zu den Vorgaben aus SAR\_EC\_BASELINE, siehe Kapitel 3.1.3.
- Prüfen, ob das Zertifikat zur Verifikation der qualifizierten Signatur den Anforderungen in SAR\_EC\_BASELINE an ein qualifiziertes Zertifikat oder in CEF: eSignature DSS entspricht.
- Prüfen, ob es sich bei der Signatur um eine qualifizierte gemäss eIDAS handelt.
- Prüfen, ob ein «Commitment Type Indication» vorliegt.
- Prüfen, ob im Zertifikat angegeben ist, dass die Signatur vermeintlich in einer sicheren Signaturerstellungseinheit erzeugt wurde.
- Beim PDF: Überlagerung der Signaturfenster. Bei einem PDF dürfen sich nach einer Gegenzeichnung die Signaturfenster nicht überlagern, SAR\_EC\_BASELINE, S. 33 Zeile c.

**SHOULD:** Die Prüfung soll folgende Schritte umfassen:

- Das Vorliegen eines Zeitstempels. Falls ein Zeitstempel vorliegt, dann sind die Prüfschritte im KAPITEL 4.4.2.1.2 vorzunehmen.
- Die Verlässlichkeit der Anzeige, siehe KAPITEL 2.4.5.
- Die signierte Datei ist für die Aufbewahrung geeignet, siehe KAPITEL 2.4.4
- Zugehörigkeit Signatur und Dateiformat, siehe KAPITEL 2.7.5.

## 4.7.2 Rückmeldungen zur Prüfung

### 4.7.2.1 MUSS geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Alle obligatorischen Prüfungsschritte im KAPITEL 4.3	siehe KAPITEL 4.3	siehe KAPITEL 4.3
Detached Signature	Detached Signature <i>SIGNED_DATA_NOT_FOUND</i> , <i>format_content_mismatch</i> <sup>1)</sup>	INDETERMINATE FAILED
Signatur gemäss SAR_EC_BASELINE, Kapitel 3.1.3 oder gemäss ISO 32000-2	<i>FORMAT_FAILURE</i>	FAILED
Qualifiziertes Zertifikat	<i>no_EU_qualified_certificate</i>	FAILED
Qualifizierte Signatur	<i>no_qualified_signature</i>	FAILED
Prüfen, ob ein «Commitment Type Indication» vorliegt	<i>commitment_type_indication</i>	INDETERMINATE
Angabe über die Erstellung der Signatur in einer sicheren Einheit	<i>no_sscd_indication</i>	INDETERMINATE
Beim PDF: Sich überlagernde signature icon	<i>OverlappingProhibited</i>	INDETERMINATE

Tabelle 8: Rückmeldungen der Prüfungsergebnisse zur qualifizierten Signatur (MUST)

<sup>1)</sup> **Anmerkung:** SAR\_EC\_BASELINE Seite 21 zweitletzter Absatz fordert, dass für «detached signature» das ASiC Format verwendet wird. Gemäss dieser Vorschrift:

Signed data may only be detached from the signatures when both the detached signatures and the signed data are within an ASiC container.

Auf <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109093/Standards+and+specifications> und in SAR\_EC\_BASELINE werden die aktuelleren ETSI Standards als diejenigen aufgeführt, welche im DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 erwähnt werden.

#### 4.7.2.2 SOLL geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Zeitstempel	no_timestamp	INDETERMINATE
Prüfen des Zeitstempels, falls vorhanden	Siehe KAPITEL 4.4.2.1.2	Siehe KAPITEL 4.4.2.1.2
Verlässlichkeit der Anzeige/Bedeutung Bei einem PDF	integrity_constraints_failure pdf_content_constraints_failure	INDETERMINATE
geeignet für die Aufbewahrung	not_appropriate_for_longterm_storage	INDETERMINATE
Zugehörigkeit Dateiformat, Signaturformat	format_content_mismatch <sup>1)</sup>	INDETERMINATE

Tabelle 9: Rückmeldungen der Prüfungsergebnisse zur qualifizierten Signatur (SHOULD)

<sup>1)</sup> **Anmerkung:** Diese Fehlermeldung kann sich auch ergeben, wenn die detached signature nicht in einem gemäss SAR\_EC\_BASELINE vorgegebenen Format vorliegt.

#### 4.7.3 Ergänzung

**SHOULD:** Folgende Bestimmungen der EU sollen bei der anschliessenden Beurteilung betreffend die Akzeptanz oder die Nichtakzeptanz in Betracht gezogen werden:

- Art. 25 Abs. 1 eIDAS: Einer elektronischen Signatur darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt.
- Art. 35 Abs. 1 eIDAS: Einem elektronischen Siegel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt.
- Art. 41 Abs.1 eIDAS: Einem elektronischen Zeitstempel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil er in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Zeitstempel erfüllt.

### 4.8 Signature with Long Term Validation Material

Der Begriff «Signature with Long Term Validation Material» bezieht sich auf das gleichnamige Kapitel 4.3.4 in ETSI EN 319 102-1 V.1.4.1. Im Wesentlichen wird die Signatur um Angaben zum Gültigkeitsstatus der jeweiligen Zertifikate mittels einer CRL oder OCSP-Antwort erweitert.

**Anmerkung:** Die Beschaffenheit der Signatur entspricht Figur 8 in ETSI EN 319 102.1 V.1.4.1.

#### 4.8.1 Was zu prüfen ist

**MUST:** Die Prüfung muss folgende Schritte umfassen:

- Alle Bestandteile aus KAPITEL 4.5 Basis Signatur mit Zeitstempel.
- Falls es sich bei der Signatur um eine qualifizierte handelt, dann sind die obligatorischen Prüfschritte im KAPITEL 4.4 oder KAPITEL 4.7 durchzuführen.
- Die signierte Datei ist geeignet für die Aufbewahrung, siehe KAPITEL 2.4.4.
- Das Vorliegen der Informationen zur Revokation der Zertifikate
- Falls ja, prüfen der CRL oder OCSP Antwort gemäss KAPITEL 4.3.1
- Prüfen, ob das Zertifikat zur Verifikation der Signatur beim Leisten der Signatur noch gültig war. (Feststellen der «best signature time»)

**Anmerkung:** U.a. muss geprüft werden, ob das Zertifikat zur Verifikation der Signatur beim Leisten der Signatur noch gültig war. Deswegen sind u.a. die Information zur Revokation dieses Zertifikats notwendig, wie auch die Informationen zur Revokation des Zertifikats zur Prüfung des Zeitstempels.

Bei einer qualifizierten Signatur der EU muss noch geprüft werden, ob ein Zeitstempel vorliegt, da ein Zeitstempel im Unterschied zur Handunterschrift gleichgestellten Signatur nach Art. 14 Abs. 2<sup>bis</sup> OR nicht erforderlich ist:

- Prüfen, ob ein Zeitstempel vorhanden ist. Falls vorhanden, Prüfen des Zeitstempels gemäss den Anforderungen aus KAPITEL 4.4.2.1.2.

**SHOULD:** Die Prüfung soll folgende Schritte umfassen:

- Die Verlässlichkeit der Anzeige, siehe KAPITEL 2.4.5.
- Zugehörigkeit Signatur und Dateiformat, siehe KAPITEL 2.7.5

#### 4.8.2 Rückmeldungen zur Prüfung

##### 4.8.2.1 MUSS geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Alle obligatorischen Prüfschritte im KAPITEL 4.5	siehe KAPITEL 4.5	siehe KAPITEL 4.5
Falls eine qualifizierte Signatur vorliegt, dann die Prüfschritte im KAPITEL 4.4 oder 4.7.	siehe KAPITEL 4.4 oder 4.7	siehe KAPITEL 4.4 oder 4.7
geeignet für die Aufbewahrung	not_appropriate_for_longterm_storage	FAILED
Das Vorliegen der Informationen zur Revokation/Gültigkeit der Zertifikate	Hier müssen alle Angaben zur Gültigkeit oder zur Revokation der Zertifikate (Signatur und Zeitstempel) vorliegen.	FAILED

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Prüfen der Signatur bei der CRL oder OCSP Antwort gemäss KAPITEL 4.3.1	siehe KAPITEL 4.3.1	siehe KAPITEL 4.3.1
Prüfen, ob das Zertifikat zur Verifikation der Signatur vor und nach der Zeit gültig war, welche im Zeitstempel aufgeführt ist.	<i>REVOKED<sup>1</sup>, EXPIRED<sup>1</sup></i>	TOTAL-FAILED

Tabelle 10: Rückmeldungen der Prüfungsergebnisse «Signature with Long Term Validation Material» (MUST)

1) **Anmerkung:** Die Rückmeldung *REVOKED* bei ETSI EN 319 102-1 V.1.4.1 Tabelle 6 bedeutet:

The signature validation process results into *TOTAL-FAILED* because:

- the signing certificate has been revoked; and
- there is proof that the signature has been created after the revocation time.

Ähnliches gilt hier für die Rückmeldung *EXPIRED*.

#### Bei einer nach EU qualifizierten Signatur

Die Basis-Signatur nach EU fordert keinen Zeitstempel, wie dies bei der Handunterschrift gleichgestellten Signatur nach Art. 14 Abs. 2<sup>bis</sup> OR der Fall ist. Doch hier ist der Zeitstempel erforderlich.

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Zeitstempel	no_timestamp	FAILED
Prüfen des Zeitstempels, falls vorhanden	Siehe KAPITEL 4.4.2.1.2	Siehe KAPITEL 4.4.2.1.2

Tabelle 11: Rückmeldungen der Prüfungsergebnisse «Signature with Long Term Validation Material» (MUST) bei einer nach EU qualifizierten Signatur

#### 4.8.2.2 SOLL geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Verlässlichkeit der Anzeige/Bedeutung Bei einem PDF	integrity_constraints_failure pdf_content_constraints_failure	INDETERMINATE
Zugehörigkeit Dateiformat, Signaturformat	format_content_mismatch	INDETERMINATE

Tabelle 12: Rückmeldungen der Prüfungsergebnisse «Signature with Long Term Validation Material» (SHOULD)

## 4.9 Vor dem Überführen in die Institution für die Aufbewahrung

**MUST:** Vor dem Überführen der Signatur muss sie in der Form vorliegen, wie sie in der Figur 9 bei ETSI EN 312 102-1 V.1.3.1 Kapitel 4.3.5.1 dargestellt ist.

### 4.9.1 Was zu prüfen ist

**MUST:** Die Prüfung muss folgende Schritte umfassen:

- Das Vorliegen einer «Signature with Long Term Validation Material», siehe KAPITEL 4.8.
- Die Signatur entspricht den Vorgaben aus eCH-0220, eCH-0230, eCH-0250 oder aus SAR\_EC\_BASELINE.
- Die Verlässlichkeit der Anzeige, siehe KAPITEL 2.4.5.
- Aufbewahrungstauglichkeit der signierten Datei siehe KAPITEL 2.4.4
- Die Informationen zur Gültigkeit oder Revokation müssen vorhanden sein.
- Vorhandensein und Gültigkeit eines qualifizierten archive timestamp. Die Gültigkeit muss nach den Prüfschritten zum Zeitstempel im KAPITEL 4.4.2.1.2 erfolgen.

**Begriff:** Der «archive timestamp» ist ein periodisch angefertigter Zeitstempel, welcher alle Informationen zur Signatur abdecken/erfassen muss. Ein weiterer archive timestamp muss vor Ablauf der Gültigkeit des Zertifikats des vorangehenden archive timestamp angefertigt werden.

**MUST:** Liegt kein oder kein gültiger qualifizierter archive timestamp vor, dann muss ein solcher angefertigt werden, sofern die Prüfungen gemäss KAPITEL 4.8 erfolgreich waren.

**SHOULD:** Die Prüfung soll folgende Schritte umfassen:

- Zugehörigkeit Signatur und Dateiformat, siehe KAPITEL 2.7.5.
- Beim PDF: Überlagerung der Signaturfenster. Bei einem PDF dürfen sich nach einer Gegenzeichnung die Signaturfenster nicht überlagern, dies gemäss SAR\_EC\_BASELINE, S.33 Zeile c.

## 4.9.2 Rückmeldungen zur Prüfung

### 4.9.2.1 MUSS geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Alle obligatorischen Prüfschritte im KAPITEL 4.8	siehe KAPITEL 4.8	KAPITEL 4.8
Verlässlichkeit der Anzeige/Bedeutung Bei einem PDF	integrity_constraints_failure pdf_content_constraints_failure	FAILED
geeignet für die Aufbewahrung	not_appropriate_for_longterm_storage	FAILED
Vorhandensein eines gültigen archive timestamp	no_timestamp	INDETERMINATE
Gültigkeit des zuletzt angefertigten archive timestamp	Siehe KAPITEL 4.4	FAILED

Tabelle 13: Rückmeldungen der Prüfungsergebnisse vor dem Überführen an die Institution für die Aufbewahrung (MUST)

### 4.9.2.2 SOLL geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Zugehörigkeit Dateiformat, Signaturformat	format_content_mismatch	INDETERMINATE

Tabelle 14: Rückmeldungen der Prüfungsergebnisse zu einer signierten Datei von der Institution für die Aufbewahrung (SHOULD)

## 4.10 Von der Institution für die Aufbewahrung

**MUST:** Vor dem Bezug der signierten Datei muss die Signatur in der Form vorliegen, wie sie in der Figur 10 bei ETSI EN 312 102-1 V.1.3.1 Kapitel 4.3.5.1 dargestellt ist.

### 4.10.1 Was zu prüfen ist

**MUST:** Folgendes muss geprüft werden:

- Alle Prüfschritte im KAPITEL 4.9
- Gültigkeit des zuletzt beigesteuerten «archive timestamp».

#### 4.10.1.1 Rückmeldungen zur Prüfung

#### 4.10.1.2 MUSS geprüft werden

Prüfschritt	Rückmeldung bei Fehler	Bewertung bei Fehler
Alle obligatorischen Prüfungsschritte im KAPITEL 4.9	Siehe KAPITEL 4.9	Siehe KAPITEL 4.9
Vorhandensein eines archive timestamp	no_timestamp	FAILED
Gültigkeit des Zertifikats des zuletzt beigesteuerten archive timestamp	Siehe KAPITEL 4.4	FAILED

Tabelle 15: Rückmeldungen der Prüfungsergebnisse zu einer signierten Datei von der Institution für die Aufbewahrung (MUST)

### 4.11 Konsequenz

In Erinnerung rufend (KAPITEL 1.3.3.3). Welche Folgen ein nicht befriedigendes Ergebnis einer Prüfung letztlich hat oder haben kann, wird hier im Prinzip nicht abgehandelt. Der Standard definiert die Prüfungsschritte einer Signatur und die möglichen Rückmeldungen für verschiedene Ausprägungen einer Signatur. Zudem empfiehlt er, ob das Ergebnis der Prüfung als befriedigend erachtet werden kann.

Doch folgende Empfehlung hierzu:

**SHOULD:** Falls das Prüfungsergebnis nicht befriedigend ist und es die Umstände erlauben, soll der oder die Signierende vom oder von der Prüfenden aufgefordert/gebeten werden, eine den Anforderungen genügende Signatur nochmals zuzustellen. Hierzu aus eIDAS:

Art. 25 (Rechtswirkung elektronischer Signaturen) Abs. 1, eIDAS: Einer elektronischen Signatur darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt.

Im BEKJ wird nicht geregelt, welche rechtlichen Konsequenzen eine nicht formgerechte Signatur bei einer an die Behörde eingereichte elektronisch signierte Schrift hat. Ebenso wird nicht geregelt, wie elektronisch signierte Belege einzureichen sind, damit sie ihre Beweiskraft haben, oder was zu unternehmen ist, damit die Aussage- oder Beweiskraft der signierten Belege erhalten bleibt.

Beispielsweise: Grundsätzlich hat derjenige, welcher aus dem Beleg eine Rechtswirkung erzielen will, darzulegen oder zu beweisen, dass der Beleg konform ist, d.h. akzeptiert wird. «Steuermindernde und steuerausschliessende Tatsachen sind hingegen durch die steuerpflichtige Person zu beweisen (BGE 140 II 248 E. 3.5 S. 252 mit Hinweisen)» aus BGE 2C\_118/2021, 2.4.1. Steuer-mindernde Tatsachen sind z.B. eingegangene Rechnungen. D.h. der Steuerpflichtige hat folglich darum besorgt zu sein, dass der Beleg für die Steuer-minderung von der Behörde anerkannt wird.

## 5 Sicherheitsüberlegungen

Dieses Dokument behandelt die Prüfung einer Signatur, wobei die Signatur zu einem viel früheren Zeitpunkt erstellt worden sein kann. Dabei gilt es u.a. zu prüfen, ob das Zertifikat für die Prüfung der Signatur zum Zeitpunkt des Leistens der Signatur gültig war. Dies ist 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.

## 6 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein eCH den Benutzenden 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 den Benutzenden auf Grund dieser Dokumente trifft und / oder ergreift. Die Benutzenden sind 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 der Benutzenden, 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 den Benutzenden aus dem Gebrauch der eCH-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

## 7 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichten sich die Erarbeitenden, ihr betreffendes geistiges Eigentum oder ihre 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 urhebenden Person 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

- [1] Andreas Bertsch, Digitale Signaturen, Springer Verlag, 2001
- CEF: eSignature DSS CEF: eSignature DSS, Version 1.03. Qualified electronic signature (QES) validation algorithm der EU, 2019
- eCH-0091 Standard zu XML-Signatur und -Verschlüsselung, V.2.0
- eCH-0164 Lebenszyklusmodell für Geschäfte (Prozesse, Dossiers und Dokumente), V.1.0
- eCH-0220 Bewahrung der Gültigkeit elektronischer Signaturen im CMS-Format, V.1.0
- eCH-0230 Bewahrung der Gültigkeit elektronischer Signaturen im XML-Format, V.1.0
- eCH-0250 Die Bewahrung der Gültigkeit von Signaturen in einem PDF, V. 1.0
- ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, V.1.4.1
- ETSI EN 319 122-1 Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures, V1.2.1
- ETSI EN 319 122-2 Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures, V1.1.1
- ETSI EN 319 162-1 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Additional ASiC containers, V.1.0
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates, V.1.0
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures, V.1.5.1
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, V1.1.1
- ETSI TS 119 172-4 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists, V1.1.1
- ETSI TS 119 615 Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists, V.1.2.1
- ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists, V.1.2.1
- ISO 32000-1 Document management – Portable document format – Part 1: PDF 1.7 : 2008  
Bemerkung: Kann im Internet kostenlos bezogen werden.
- ISO 32000-2 Document management – Portable document format – Part 2: PDF 2.0: 2020

---

ITU-T X.509	Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, 10/2012
RFC 2315	PKCS #7: Cryptographic Message Syntax, Version 1.5, (March 1998), Internet Engineering Task Force (IETF).
RFC 3161	Time-Stamp Protocol
RFC 5652	Cryptographic Message Syntax Format
RFC 8954	Online Certificate Status Protocol – OCSP

## Anhang B – Mitarbeit & Überprüfung

Adrian M. Müller

Claire Röthlisberger-Jourdan KOST (Koordinationsstelle für die dauerhafte Archivierung elektronischer Unterlagen)

Daniel Muster it-rm IT-Riskmanagement GmbH

Michael von Niederhäusern

Orlando Paganini Glaux Group

Stephanie Schäfer Kanton Zürich

## Anhang C – Abkürzungen und Glossar

Abs.	Absatz
AdES	Advanced Electronic Signature
Advanced Electronic Signature	Zu Deutsch «fortgeschrittene elektronische Signatur». Dieser Begriff hat im technischen und juristischen Bereich jeweils eine andere Bedeutung. Im juristischen Bereich legt es die Anforderung an das Zertifikat fest, mit welchem eine Signatur zu prüfen ist. Im technischen (ETSI) drückt es einer Erweiterung von Informationen aus, welche der Signatur beigegeben wird, wie z.B. die OCSP Antwort, das Zertifikat für die Prüfung der Signatur.
anerkannt ausreichend sicher	Anerkannte Stellen glauben, dass das kryptographische Verfahren zur Bildung der Signatur während der Gültigkeitsdauer des dazugehörigen Zertifikats nicht gebrochen werden kann.
Archiv	1) Der Begriff «Archiv» (engl. Archive) wird in den uns bekannten ETSI Standards nicht definiert. Gemäss SAR_EC_BASELINE und EN 319 102-1 V.1.4.1 sind im Begriff zwei Institutionen enthalten, nämlich für die Aufbewahrung und für die Archivierung. 2) gemäss eCH-0164: Das Archiv bezeichnet in einem allgemeinen Sinn jene Institution oder Organisationseinheit, die für die dauerhafte Archivierung von Dossiers verantwortlich ist.
archive timestamp	Zeitstempel, welcher zum Zweck der Aufbewahrung erzeugt und beige-steuert wurde. Der Begriff «archive» wird hier gemäss ETSI verwendet, siehe «Archiv».
Archivierung	Sichere und dauerhafte Aufbewahrung von Unterlagen in einem Archiv, welche rechtlich, administrativ, politisch, wirtschaftlich, historisch, kultu-rell, sozial oder wissenschaftlich relevant sind.
Art.	Artikel
Aufbewahrung	Organisierte und systematische Verwaltung von Geschäftsinformation für eine angemessene (endliche) Zeitperiode unter Berücksichtigung gesetzlicher, betrieblicher oder historischer Anforderungen.
best signature time	Als «best signature time» wird der späteste Zeitpunkt erachtet, an welchem die Signatur angefertigt wurde. Zudem ist es der früheste Zeitpunkt, zu welchem man den Beweis/Beleg hat (proof of existence, kurz POE), dass die Signatur hergestellt wurde, siehe ETSI EN 319 102-1 V.1.4.1, Kapitel 5.5.4, Note 1.
BGE	Bundesgerichtsentscheid
Bst.	Buchstabe
CEF	Connecting European Facility's

Claimed Attribute	Bei «Claimed Attribute» handelt es sich um Informationen, welche der Empfänger oder die Empfängerin der Signatur nicht oder sehr eingeschränkt prüfen und somit vermutlich nicht als Beleg verwenden kann. Es fehlt ein POE (PROOF OF EXISTENCE).
CMS	Cryptographic Message Syntax, siehe RFC 5652
counter signature	Zu Deutsch «Gegenzeichnung». Es ist in der Technik möglich, genau dasselbe oder dasselbe plus die bereits bestehende(n) Unterschrift(en) gegenzuzeichnen. Im ersten Fall sind die beiden Signaturen unabhängig voneinander. Im zweiten Fall ist die Folge des Leistens einer Signatur relevant, s. dazu ETSI EN 319 102 Kapitel 4.2.5.7.
CRL	Certificate Revocation List
detached signature	Zu Deutsch «abgehängte/losgelöste Signatur». Die Signatur ist von dem von der Signatur Erfassten losgelöst.
ETSI	European Telecommunications Standards Institute
EU	European Union
EUIBA	EU Institutions, Bodies and Agencies
EWR	Europäischer Wirtschaftsraum
FOITT	Federal Office of Information Technology, Systems and Telecommunication FOITT, November 2023, Discreet Validator Service 3.0, Interface Specification (Version 1.2.4)
JSON	JavaScript Object Notation
KOST	Koordinationsstelle für die dauerhafte Archivierung elektronischer Unterlagen, <a href="https://kost-ceco.ch/cms/willkommen.html">https://kost-ceco.ch/cms/willkommen.html</a> . Zu den archivtauglichen Dateiformaten: <a href="https://kost-ceco.ch/cms/dateiformate.html">https://kost-ceco.ch/cms/dateiformate.html</a>
OCSP	Online Certificate Status Protocol
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911. SR 220
PDF	Portable Document Format
POE	Proof of Existence
Potentiell schädlicher Link	Ein potentiell schädlicher Link in einer Datei ist ein Link auf eine Informationsquelle, welche beim Laden der Datei in der Anwendung heruntergeladen wird. Diese Links verleihen der Datei in der Anwendung eine andere Bedeutung als die Informationen in der signierten Datei selbst.
resp.	Respektiv
RFC	Request for Comments (IETF Standard)
SAS	Schweizerische Akkreditierungsstelle

---

selective disclosure	Bei selective disclosure wird nur ein Teil des Dokuments, welches von der Signatur erfasst wird, bei der Prüfung der Signatur offengelegt.
SR	Systematische Rechtsetzungsnummer
SSCD	Secure Signature Creation Device
SSI	Self Sovereign Identity
SVA	Signature Validation Application
TL	Trusted List
Trusted Service Provider	Als Trusted Service Provider (TSP) bezeichnet man in diesem Kontext einen amtlich anerkannten Dienstleister gemäss Art. 2 Bst. k und l und Art. 3-5 ZertES oder gemäss EU VERORDNUNG Nr. 910/2014. Im Kontext zur Herausgabe von Zertifikaten, siehe Homepage der SAS, <a href="https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellen-suchesas/pki1.html">https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellen-suchesas/pki1.html</a> .
TSP	Trusted Service Provider
VC	Verifiable Credential
XML	Extended Markup Language
Ziff.	Ziffer

## Anhang D – Vorschriften

BEKJ	Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz vom 20. Dezember 2024, SR 220
BGG	Bundesgesetz über das Bundesgericht (Bundesgerichtsgesetz, BGG) vom 17. Juni 2005, SR 173.110
DURCHFÜHRUNGS- BESCHLUSS (EU) 2015/1506	DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 DER KOMMISSION vom 8. September 2015 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt anerkannt werden
DURCHFÜHRUNGS- BESCHLUSS (EU) 2015/1505	DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1505 DER KOMMISSION vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
eIDAS	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
SAR_EC_BASELINE	European Commission: Signature applicability rules for electronic signature and seals received by the European Commission, 19.12.2023
Swiss TL	<a href="https://uri.tsl-switzerland.ch/TrstSvc/TrustedList/schemerules/CH">https://uri.tsl-switzerland.ch/TrstSvc/TrustedList/schemerules/CH</a>
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate Ausgabe 2: 17. Februar 2022, Inkrafttreten: 15. März 2022
VwVG	Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG) vom 20. Dezember 1968, SR 172.021
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032
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
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210

## Anhang E – Standardisierungsorganisationen

eCH	E-Government Standards, <a href="http://www.ech.ch">www.ech.ch</a>
ETSI	European Telecommunications Standards Institute, <a href="https://www.etsi.org/">https://www.etsi.org/</a>
IETF	Internet Engineering Task Force, <a href="https://www.ietf.org/">https://www.ietf.org/</a>
ISO	International Organization for Standardization <a href="https://www.iso.org/home.html">https://www.iso.org/home.html</a>

## Anhang F – Änderungen gegenüber Vorversion

Dies ist die erste Version.

## Anhang G – Abbildungsverzeichnis

Im Dokument sind keine Abbildungen enthalten.

## Anhang H – Tabellenverzeichnis

Tabelle 1: Weitere Rückmeldungen zu den Prüfungsergebnissen .....	29
Tabelle 2: Rückmeldungen der Prüfungsergebnisse zur Basis Signatur (MUST) .....	37
Tabelle 3: Rückmeldungen der Prüfungsergebnisse zur Basis Signatur (MUST) betreffend das dazugehörige Zertifikat .....	38
Tabelle 4: Rückmeldungen der Prüfungsergebnisse zur Basis Signatur (SHOULD) .....	38
Tabelle 5: Rückmeldungen der Prüfungsergebnisse zur Basis Signatur (MUST) .....	40
Tabelle 6: Rückmeldungen der Prüfungsergebnisse zum Zeitstempel (MUST).....	41
Tabelle 7: Rückmeldungen der Prüfungsergebnisse zur qualifizierten Signatur (SHOULD) .	42
Tabelle 8: Rückmeldungen der Prüfungsergebnisse zur qualifizierten Signatur (MUST).....	44
Tabelle 9: Rückmeldungen der Prüfungsergebnisse zur qualifizierten Signatur (SHOULD) .	45
Tabelle 10: Rückmeldungen der Prüfungsergebnisse «Signature with Long Term Validation Material» (MUST).....	47
Tabelle 11: Rückmeldungen der Prüfungsergebnisse «Signature with Long Term Validation Material» (MUST) bei einer nach EU qualifizierten Signatur.....	47
Tabelle 12: Rückmeldungen der Prüfungsergebnisse «Signature with Long Term Validation Material» (SHOULD).....	47
Tabelle 13: Rückmeldungen der Prüfungsergebnisse vor dem Überführen an die Institution für die Aufbewahrung (MUST) .....	49
Tabelle 14: Rückmeldungen der Prüfungsergebnisse zu einer signierten Datei von der Institution für die Aufbewahrung (SHOULD).....	49
Tabelle 15: Rückmeldungen der Prüfungsergebnisse zu einer signierten Datei von der Institution für die Aufbewahrung (MUST).....	50