eCH-0220 – Bewahrung der Gültigkeit elektronischer Signaturen im CMS-Format

Name	Bewahrung der Gültigkeit elektronischer Signaturen im CMS-Format
eCH-Nummer	eCH-0220
Kategorie	Standard
Reifegrad	Definiert
Version	2.0.0
Status	Genehmigt
Beschluss am	2021-03-02
Ausgabedatum	2021-03-10
Ersetzt Version	1.0 – Minor Change
Voraussetzungen	ETSI TS 101 733 V2.2.1 ETSI TS 119 122-1 V1.01 ETSI TS 119 122-2 V1.01 ETSI EN 319 192-1 V1.1.1 ETSI EN 319 192-2 V1.1.1 ZertES (Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur)
Beilagen	-
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Fachgruppe Technologie Böhlen Jörg bei der Version 2.0 nicht mehr dabei Büchler Georg (KOST) Bütler Christian (BJ) bei der Version 2.0 nicht mehr dabei Müller Adrian damals Cyber Identity, aktuell SwissSign AG, neu bei der Version 2.0 dabei Muster Daniel (it-rm IT-Riskmanagement GmbH) Niederberger Marcel (ESTV) Schmid Josef von Niederhäusern Michael (BIT) Waldegger Hans-Peter (Swisscom AG)
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Der hier vorliegende Standard gibt eine Anleitung zur Bewahrung der Gültigkeit elektronisch signierter Dokumente im CMS-Format, so dass die elektronische Signatur der aufzubewahrenden Dokumente während dieser Zeit verlässlich geprüft werden kann. Langzeit meint, dass die Signatur z.B. auch noch nach Ablauf der Gültigkeitsdauer des dazu korrespondierenden Zertifikats entsprechend verifiziert und bei erfolgreicher Prüfung allgemein anerkannt werden kann. Die Gültigkeit eines Zertifikats kann z.B. nach seiner Laufzeit oder nach beantragter Revokation des Eigentümers des Zertifikats verfallen.

Es gibt andere Signaturformate wie XML- oder PDF-Signaturen. Das hier behandelte elektronische Signatur-Format basiert auf dem RFC-Standard 5652.

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

- ETSI TS 101 733 V2.2.1
- ETSI TS 119 122-1 V1.0.1
- ETSI TS 119 122-2 V1.0.1
- ETSI EN 319 192-1 V1.1.1
- ETSI EN 319 192-2 V1.1.1

Bei der hier vorgenommenen Auswahl an Attributen wurde darauf geachtet, dass das ganze Konstrukt der «Konservierung» elektronisch signierter Dokumente, wenn möglich, auf Attributen von allgemein anerkannten Institutionen basiert und dabei möglichst einfach bleibt. Informationen von allgemein anerkannten Institutionen sind z.B. Angaben, welche in Bundesvorschriften geregelt sind, wie:

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

Für die Prüfung elektronisch signierter Dokumente sei auf den Standard ETSI EN 319 102-1 V1.1.1 verwiesen.

Inhaltsverzeichnis

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Einleitung

1.1 Status

Vorschlag: Das Dokument wird dem Expertenausschuss zur Genehmigung 02.03.2021 vorgelegt, ist aber normativ noch nicht gültig.

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt.

1.2 Unterschied zur Version 1.0

Hauptsächlich wurde der Titel dieses Standards angepasst, damit aufgrund des Titels zwischen eCH-0230 und dem hier vorliegenden Standard unterschieden werden kann. Zwecks Kompatibilität mit dem eCH-Standard sind wenige Anpassungen vorgenommen worden.

1.3 Anwendungsgebiet

Die Bewahrung der Gültigkeit elektronisch signierter Dokumente oder Objekte im XML-Format soll zuerst in Form eines Profils auf Basis der folgenden ETSI-Standards genormt werden:

- ETSI TS 101 733 V2.2.1
- ETSI TS 119 122-1 V1.01
- ETSI TS 119 122-2 V1.01

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

Überall dort, wo elektronisch signierte Dokumente noch über Tage, Wochen oder gar Jahre hinweg aufbewahrt werden sollen, so dass deren elektronische Signatur auch nach dieser Zeitspanne verlässlich geprüft und bei erfolgreicher Prüfung akzeptiert werden kann.

Anmerkung: ETSI TS 119 122-1 V1.01 und ETSI TS 119 122-2 V1.01 sind Erneuerungen und Ergänzungen (engl. Updates) des Standards ETSI TS 101 733 V2.2.1, sind jedoch für sich alleine nicht selbsterklärend.

Zur Bewahrung der Gültigkeit elektronisch signierter Dokumente sind bei ETSI noch folgende und aktuellere Standards verabschiedet worden:

- ETSI EN 319 122-1 V1.1.1
- ETSI EN 319 122-2 V1.1.1
- ETSI TS 119 122-3 V1.1.1

Ausgangslage dieses Dokuments war aber der Standard ETSI TS 101 733 V2.2.1 in seiner letzten Version, weil:

- er selbsterklärend ist und zusätzliche Informationen zum Verständnis der Problematik enthält.
- ETSI EN 319 122-1 V1.1.1 und ETSI EN 319 122-2 V1.1.1 für den Einstieg in die Problematik schwieriger sind.

ETSI TS 119 122-3 V1.1.1, ETSI EN 319 122-2 V1.1.1 und ETSI TS 119 122-3 V1.1.1 werden anschliessend in diesem Dokument berücksichtigt.

1.4 Ausgangslage

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

- Das Zertifikat mit dem öffentlichen Schlüssel zur Verifikation der elektronischen Signatur, kurz das Prüfzertifikat, ist nicht mehr gültig.
- Das Root-Zertifikat zum Prüfzertifikat ist nicht mehr gültig.
- Der private Signaturschlüssel wurde kompromittiert und das Zertifikat wurde dann revoziert.
- Das Zertifikat ist aus anderen Gründen revoziert worden.

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

1.5 Ziel(e) und Abgrenzung

1.5.1 Ziel

Mit dem hier vorliegenden Dokument und den zugrunde liegenden ETSI-Standards soll Folgendes ermöglicht werden.

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

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

- innerhalb der von den jeweiligen Bestimmungen geforderten Aufbewahrungszeit oder der rechtlich geforderten Aufbewahrungsfrist zuverlässig festgestellt werden kann, dass zum Herstellungszeitpunkt der elektronischen Signatur die Signatur wie auch das entsprechende Zertifikat gültig war.
- innerhalb der genannten Zeit und Frist die Verantwortlichkeit für das Leisten dieser elektronischen Signatur verlässlich einer juristischen oder natürlichen Person zugeordnet werden kann.

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

Die Standard EN 319 192-1 V1.1.1 und ETSI TS 101 903 V1.4.2 definieren verschiedene Prüfschritte zur Verifikation einer elektronischen Signatur. Welche Prüfschritte erforderlich sind, damit die Signatur als gültig erachtet und folglich akzeptiert wird, hängt - wie in diesem Standard bereits erwähnt - von den Vorschriften zur Signatur ab (engl. signature policy).

Letztlich will man mit der hier vorgeschlagenen Methode die Bewahrung der Gültigkeit elektronischer

Signaturen erreichen, so dass nach der Erstellung oder nach dem Empfang einer gültigen elektronischen Signatur deren Prüfung und somit die Signatur während der Aufbewahrungszeit weiterhin allgemein akzeptiert werden kann. Dies möglicherweise auch bei einem strittigen Verwaltungs- oder Gerichtsverfahren.

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

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

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

1.5.2 Abgrenzung

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

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

Folglich ist es unerlässlich, dass die Integrität (Unverändertheit) der elektronisch signierten Dokumente geschützt wird. Massnahmen zum Integritätsschutz von signierten Dokumenten bei der Archivierung/Aufbewahrung ist jedoch nicht Ziel dieses Dokuments, wie auch nicht die Dateiformate der zu signierenden Dokumente.

Bei den hier behandelten elektronischen Signaturen handelt sich um Signaturen an elektronische Dokumente oder Dateien und um Signaturen, welche ermöglichen sollen, die aufbewahrten, elektronisch signierten Dokumente über Jahre hinweg verlässlich zu prüfen, wie z.B. ein Zeitstempel, Zertifikate, eine Zertifikatsrevokationsliste (CRL) oder eine OCSP-Antwort. Es handelt sich hierbei um Signaturen nach dem CMS-Format.

Nicht behandelt wird hier die Bewahrung der Gültigkeit elektronischer Signaturen an ein PDF-Dokument oder an eine XML-Datei. Bei ETSI werden sie separat bei den folgenden Standards genormt:

- ETSI EN 319 142-1 V1.1.1
- ETSI EN 319 142-2 V1.1.1
- ETSI EN 319 132-1 V1.1.1
- ETSI EN 319 132-2 V1.1.1

1.6 Inhalt, Struktur des Dokuments

Dieses Dokument ist ein Profil der zugrunde liegenden ETSI Standard. Es wird hier lediglich erwähnt, was:

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

Im folgenden Kapitel 2 werden zu den jeweiligen Kapiteln in den ETSI-Standard die entsprechenden Anmerkungen aufgeführt, wobei sich die Titel der Unterkapitel hier auf die Unterkapitel der jeweiligen ETSI-Standards beziehen.

1.7 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.

1.8 Terminologie der Empfehlung

Richtlinien in diesem Dokument werden gemäss der Terminologie aus [RFC2119] 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.)

1.9 Weitere Signaturen

Für die hier behandelte Thematik werden noch andere Signaturen als die Signatur an einem Dokument oder an einer Datei thematisiert, nämlich Signaturen bei

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

Zur Unterscheidung werden die Signaturen an einem Dokument oder an einer Datei schlicht als Signatur bezeichnet, deren Gültigkeit bewahrt werden soll. Dies ist das Thema dieses Dokuments.

1.10 Anmerkung

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

Der hier unterbreitete Vorschlag stützt sich auf international anerkannte ETSI-Standards ab.

2 Zu den Komponenten

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

2.1 Zertifikate

2.1.1 Herkunft

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

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

2.1.2 Zeitliche Gültigkeit

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

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

2.2 Zeitstempel

2.2.1 Qualität der Zeitstempel

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

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

2.2.2 Format der Zeitstempel

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

MUST: Die Zeitstempel müssen im CMS-Format signiert sein. Zu CMS, siehe RFC 5652.

2.3 Signatur

2.3.1 Format

Mit Ausnahme der Zertifikate, werden hier nur elektronische Signaturen nach dem Cryptographic Message Syntax (CMS) Format behandelt. (Zu CMS siehe RFC 5652) Dies betrifft auch Zeitstempel und OCSP-Antworten.

2.3.2 Signaturtyp

SHOULD: Es sollen verschiedene Signaturtypen u.a. detached, embedded signature unterstützt werden, wie auch zusätzliche Signaturen ans Dokument oder an die Datei wie eine Counter Signature; siehe auch Kapitel C.5 «Multiple Signatures» in ETSI TS 101 733 V2.2.1.

Anmerkung: Bei detached Signaturen kann die Signatur losgelöst vom Dokument behandelt werden.

2.3.3 Dem Dokument beizufügende Informationen zum Zeitstempel

Die Signatur eines Zeitstempels wird ebenfalls mittels einer Zertifikatskette verifiziert. Diese Zertifikate, gegebenenfalls auch deren Statusangabe, sind zwecks späterer Prüfung des Zeitstempels ebenfalls aufzubewahren. Dies wie Zertifikate zur Prüfung der elektronischen Dokument- oder Dateisignatur. Eventuell soll/muss das Dokument länger archiviert oder aufbewahrt werden als die Gültigkeitsdauer der Zertifikate, welche zur Prüfung der Zeitstempelsignatur benötigt werden.

MUST: Dem Zeitstempel müssen diejenigen Informationen beigefügt werden, welche es ermöglichen, die Zeitstempelsignatur zu prüfen und festzustellen, ob das dazu korrespondierende Zertifikat zum Zeit der Erstellung des Zeitstempels gültig war. Diese Informationen sind der Signatur des Zeitstempels als vom Zeitstempel unsignierte Informationen unter anderem in die Attribute certificate-values und revocation-values beizufügen, siehe auch letzter Absatz ETSI TS 119 122-1 V1.0.1, Kapitel A.1.1.2, wie auch Seite 26 in der Mitte, 2. Aufzählungspunkt, sowie in ETSI EN 319 122-1 V1.1.1, Seite 28.In folgender Tabelle sind die hier behandelten Informationsobjekte aufgeführt, welche Zeitstempel enthalten (Kolonne 1). In Kolonne 2, wo die Zertifikate für die Prüfung des Zeitstempels **sonst noch** als *unsignierte Attribute zur Dokument- oder Dateisignatur* abgelegt oder eingepackt werden können, welche zur Verifikation benötigt werden. In Kolonne 3 wird noch aufgeführt, welche Informationen in die Erstellung des Hashwerts einfliessen, der an den Zeitstempeldienst gesandt wird.

Objekt mit Zeitstempel	Zertifikatsinfo (Alternative)	Information für den Hashwert
content-time-stamp	certificate-values, revocation-values bei der Dokument- oder Dateisignatur, complete-certificate-references, complete-revocation-references. Dies nur, wenn die Information nicht bereits als unsigniertes Attribut der Zeitstempelsignatur beigefügt worden ist.	Das zu signierende Dokument. Zum Wert von «messageImprint» an den Zeitstempel siehe ETSI EN 319 122-1 V1.1.1 Kapitel 5.2.8 letzte 2 Bullet Points.
signature-time-stamp		SignatureValue
CAdES-C-time-stamp		SignatureValue, signature-time-stamp, complete-certificate-references, complete-revocation-references
time-stamped-certs-crls-references		complete-certificate-references, complete-revocation-references
Archivzeitstempel		Alle Informationen zeitlich zuvor

Tabelle 1: Infos zu den Zeitstempeln

Aus der Tabelle geht hervor, dass nur der Archivzeitstempel das signierte Dokument vor einer Schwächung desjenigen Hashwerts schützt, welche zur Signierung des Dokuments verwendet wird. Dies aber auch nur, wenn eine andere Hashfunktion zur Bildung des an den Archivzeitstempeldienst zu sendenden Hashwert verwendet wird, als zur Bildung der Signatur. Über den Archivzeitstempel werden unter anderem auch die Attributzertifikate wie auch ihre Prüfinformationen erfasst. Die Hashwerte für die Anfrage an die Zeitstempeldienste sollen als ausreichend sicher anerkannt sein.

2.4 Format der OSCP-Antworten

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

Die OCSP Antworten sind in einem entsprechenden Unterelement des Elements RevocationValues enthalten.

MUST: Der OCSP-Antwort müssen diejenigen Informationen beigefügt werden, welche es ermöglichen, deren Signatur zu prüfen und festzustellen, ob das dazu korrespondierende Zertifikat zum Zeit der Erstellung OCSP-Antwort gültig war. Diese Informationen sind der Signatur der OCSP-Antwort als von OCSP-Antwort unsignierte Informationen unter anderem in die Attribute certificate-values und revocation-values beizufügen.

3 Profil der jeweiligen ETSI-Standards

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

3.1 ETSI TS 101 733 V2.2.1

3.1.1 Kapitel 4 Overview

3.1.1.1 Einleitende Bemerkung

Relevant für die Zwecke hier ist nur das CAdES-A Format in Kapitel 4.4.4.1, mit Ausprägung Type 1 in Kapitel 4.4.3.2.

Bei dem hier präsentierten Profil werden keine time-mark Dienste in Betracht gezogen. Zum Begriff time-mark siehe Kapitel 3.1.

3.1.1.2 Kapitel 4.2 Signature Policies

SHOULD NOT: Policies sollen in der Signatur nicht referenziert werden. Ansonsten müssten diese dann separat archiviert werden.

Weiter sind in diesem Zusammenhang die bestehenden Bundesbestimmungen massgebend (ZertES, VZertES, TAV).

3.1.1.3 Kapitel 4.4.3.3 EXtended Electronic Signature with Time Type 2

MUST NOT: Dieses Format (CAdES-X Type 2) darf nicht verwendet werden, sondern das Format Type 1 in Kapitel 4.4.3.2.

3.1.2 Kapitel 5 Electronic Signature Attributes

Anmerkung: Bei den in Kapitel 5 definierten ASN.1 Signaturobjekte handelt sich um Angaben, welche mehrheitlich von der elektronischen Signatur erfasst werden. ***Folglich sind die nun folgenden Angaben relevant für die Signaturapplikation.***

3.1.2.1 Kapitel 5.7.3 ESS signing-certificate Attribute

SHOULD NOT: Dieses Attribut solle nicht mehr verwendet werden. Statt dessen soll die neue Version v2 bevorzugt werden, weil damit noch andere Hashfunktionen als SHA-1 eingesetzt werden können, siehe auch in Kapitel 5.7.3.2.

3.1.2.2 Kapitel 5.7.3.2 ESS signing-certificate-v2 Attribute

SHOULD: Dieses Attribut soll verwendet werden.

MUST: Entweder das ESS signing-certificate oder ESS signing-certificate-v2 Attribut muss gemäss Standard verwendet werden.

3.1.2.3 Kapitel 5.7.3.3 signing-certificate Attribute

SHOULD NOT: Dieses Attribut soll nicht mehr verwendet werden. Siehe auch Kapitel A.2.2 in ETSI TS 119 122-1 V1.01.

3.1.2.4 Kapitel 5.8.1 signature-policy-identifier

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

3.1.2.5 Kapitel 5.9.1 signing-time

SHOULD NOT: Falls es rechtlich relevant sein soll, dass die Signatur später als zu einem bestimmten Zeitpunkt erstellt worden ist, und dies auch verlässlich belegt werden soll, so soll dieses Attribut nicht verwendet werden. Es ist ein vom Signierenden behauptetes Attribut, engl. claimed attribute.

SHOULD: Stattdessen soll das im Kapitel 5.11.4 content-time-stamp Attribut verwendet werden.

3.1.2.6 Kapitel 5.9.2 countersignature

MAY: Dieses Attribut wird zur elektronischen Gegenzeichnung eines bereits elektronisch signierten Dokuments verwendet.

3.1.2.7 Kapitel 5.10.1 content-reference Attribute

SHOULD NOT: Es sollen keine Referenzen auf andere Dokumente in der Signatur aufgeführt werden. Ansonsten müssten die referenzierten Dokumente auch entsprechend archiviert und dem signierten Dokument beigelegt werden.

3.1.2.8 Kapitel 5.11.1 commitment-type-indication Attribute

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

3.1.2.9 Kapitel 5.11.2 signer-location Attribute

SHOULD NOT: Angaben zum Aufenthaltshort beim Leisten einer Signatur sollen wegen rechtlicher Aspekte im elektronisch signierten Dokument ersichtlich sein. Zudem können die Angaben, welche vom Unterzeichnenden in den «Raum gestellt werden», leicht umgangen werden und sind folglich nicht verlässlich. Deswegen soll dieses Attribut nicht verwendet werden. Zu solchen Attributen, engl. claimed attributes genannt, siehe auch Kapitel C.3.4.

3.1.2.10 Kapitel 5.11.3 signer-attributes Attribute

SHOULD: Es soll stattdessen signer-attributes-v2 verwendet werden, siehe Kapitel 5.2.6.1 in ETSI TS 119 122-1 V1.01.

Falls es doch verwendet wird, dann ist Folgendes zu beachten.

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

MUST: certified Attributes müssen verwendet werden, falls die Angaben im Attributzertifikat für die Signatur relevant sind.

3.1.2.11 Kapitel 5.11.4 content-time-stamp Attribute

MUST: Falls es rechtlich relevant ist, dass die Signatur später als zu einem bestimmten Zeitpunkt erstellt worden ist, und dies gegebenenfalls auch verlässlich belegt werden muss, ist dieses Attribut zu verwenden.

SHOULD: *Falls der Zeitstempeldienst die Informationen zur Prüfung der Zeitstempelsignatur dem*

Zeitstempel nicht mitgeliefert hat, so soll diese noch beigefügt werden.

Anmerkung: Diese Information ist wichtig, weil das Zertifikat zum Zeitstempel zu den nun folgenden Zeitstempeln ein anderes Root-Zertifikat besitzen kann.

3.1.3 Kapitel 6

In diesem Kapitel werden die Angaben festgelegt, welche der Signatur als solches biegefügt wird, damit die Signatur noch nach dem Zeitpunkt verifiziert werden kann, nachdem das dazugehörige Zertifikat nicht mehr gültig ist.

3.1.3.1 Kapitel 6.1.1 signature-time-stamp Attribute

MUST: Dieses Attribut muss beigefügt werden.

3.1.3.2 Kapitel 6.2.1 complete-certificate-references Attribute

MUST: Dieses Attribut muss beigefügt werden.

3.1.3.3 Kapitel 6.2.2 complete-revocation-references Attribute

MUST: Dieses Attribut muss beigefügt werden.

3.1.3.4 Kapitel 6.2.3 attribute-certificate-references Attribute

MUST: Dieses Attribut muss beigefügt werden, wenn das Attributzertifikat für die Signatur rechtlich relevant ist.

Anmerkung: Attributzertifikate werden in der Schweiz kaum verwendet und werden von einer anerkannten Stelle (CSP) nicht angeboten. Das ZertES regelt Attributzertifikate nicht.

3.1.3.5 Kapitel 6.2.4 attribute-revocation-references Attribute

MUST: Dieses Attribut muss beigefügt werden, wenn das Attributzertifikat für die Signatur rechtlich relevant ist.

Anmerkung: Attributzertifikate werden in der Schweiz kaum verwendet und werden von einer anerkannten Stelle (CSP) nicht angeboten. Das ZertES regelt Attributzertifikate nicht.

3.1.3.6 Kapitel 6.3.3 certificate-values Attribute

MUST: Dieses Attribut muss beigefügt werden.

Anmerkung: Attributzertifikate werden in der Schweiz kaum verwendet und werden von einer anerkannten Stelle (CSP) nicht angeboten. Das ZertES regelt Attributzertifikate nicht.

3.1.3.7 Kapitel 6.3.4 revocation-values Attribute

MUST: Dieses Attribut muss beigefügt werden.

Anmerkung: Attributzertifikate werden in der Schweiz kaum verwendet und werden von einer anerkannten Stelle (CSP) nicht angeboten. Das ZertES regelt Attributzertifikate nicht.

3.1.3.8 Kapitel 6.3.5 CAdES-C-time-stamp Attribute

MUST: Dieses Attribut muss beigefügt werden.

Kapitel 6.3.6 time-stamped-certs-crls-references Attribute Definition
MUST NOT: Dieses Attribut darf nicht verwendet werden, weil es lediglich einen Zeitstempel über die Zertifikatsreferenzen und Referenzen zu den Revokationslisten erstellt. Besser ist es deshalb, dass

CAdES-C-time-stamp Attribut zu verwenden.

3.1.3.9 Kapitel 6.4.1 archive-time-stamp Attribute

SHOULD NOT: Dieses Attribut soll gemäss ETSI TS 119 122-1 Kapitel A.2.4 nicht mehr verwendet werden.

3.1.3.10 Kapitel 6.4.2 ats-hash-index Attribute

SHOULD NOT: Dieses Attribut soll gemäss ETSI TS 119 122-1 Kapitel A.2.6 nicht mehr verwendet werden.

3.1.3.11 Kapitel 6.4.3 archive-time-stamp-v3 Attribute

SHOULD: Dieses Attribut soll verwendet werden.

3.1.3.12 Kapitel 6.5.1 long-term-validation Attribute

SHOULD NOT: Dieses Attribut soll gemäss ETSI TS 119 122-1 Kapitel A.2.5 nicht mehr verwendet werden, siehe auch ETSI EN 319 122 V1.1.1 Kapitel A.2.5.

3.2 ETSI TS 119 122-1 V1.0.1

ETSI TS 101 733 referenziert noch den alten RFC Standard 3852 zu CMS. Jedoch soll der neuere Standard RFC 5652 im Zweifelsfall Anwendung finden, siehe ETSI TS 119 122-1.

3.2.1 Kapitel 5.2.6.1 signer-attributes-v2 attribute

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

MUST: certified attributes müssen verwendet werden, falls die Angaben im Attributzertifikat für die Signatur relevant sind.

MUST NOT: Zusätzliche durch Dritte signierte Bestätigungen dürfen nicht verwendet werden. Diese Bestätigungen müssten einerseits archiviert werden, andererseits ist die Struktur der Signatur möglicherweise nicht CMS-konform (RFC 5652), z.B. eine XML-Signatur

3.2.2 Kapitel 5.2.6.2 claimed-SAML-assertion

MUST NOT: Darin enthalten ist eine SAML-Bestätigung der vom Signierenden in den «Raum gestellten» Attribute. Damit diese Bestätigung eine gewisse Beweiskraft erhält, soll dies signiert werden. SAML weist jedoch eine XML-Struktur auf, somit deren Signatur eine XML-Signatur. Die Archivierung und langfristige Prüfung von XML-Signaturen liegt ausserhalb des Blickfelds und der Zielsetzung dieses Dokuments. Ein Profile zur Bewahrung der Gültigkeit von XML-Signaturen wird in eCH-0230 beschrieben.

3.2.3 Kapitel 5.5.2 The ats-hash-index-v2 Attribute

SHOULD NOT: Dieses Attribut soll für die Bewahrung der Gültigkeit elektronischer Signaturen nicht mehr verwendet werden.

SHOULD: Anstelle dessen soll das The ats-hash-index-v3 Attribute verwendet werden, siehe KAPITEL 3.4.1.

3.3 ETSI TS 119 122-2 V1.0.1

Die Tabelle A.1. auf Seite 13 und die dazugehörigen Anmerkungen auf Seite 14 folgende enthalten eine Zusammenfassung der behandelten Attribute. Am meisten, aber bedingt relevant für die Zwecke hier, ist die Kolonne mit dem Titel «Presence in E-X-L level». Hinzukommen soll noch zwingend die Attribute zum Archivzeitstempel.

3.4 ETSI EN 319 122-1 V1.1.1

3.4.1 Kapitel 5.5.2 The ats-hash-index-v3 Attribute

SHOULD: Dieses Attribut soll für die Langzeitgültigkeitswahrung verwendet werden.

Ansonsten hat sich gegenüber dem ETSI Standard TS 119 122-1 für die hier behandelten Themen nichts Wesentliches geändert.

3.5 ETSI EN 319 122-2 V1.1.1

Es hat sich gegenüber dem ETSI Standard TS 119 122-2 für die hier behandelten Themen nichts Wesentliches geändert.

3.6 ETSI TS 119 122-3 V1.1.1

Dieser Standard legt unter anderem fest, wie extern referenzierte Objekte durch einen Zeitstempel erfasst werden können. In diesem Profil soll aus Gründen der Einfachheit keine externen Referenzen zum Dokument behandelt werden.

4 Ergänzung

Es wird ergänzt, was ausser der korrekten Formatierung und Angaben noch für die Bewahrung der Gültigkeit relevant ist. Dies sind der Berechnung des Hashwerts, die Behandlung der Prüfinformationen, Informationen zum Zertifikatstatus und eine Anmerkung betreffend die Prüfung der Signatur.

4.1 Berechnung des Hashwerts für den Archivzeitstempel

SHOULD: Für den Archivzeitstempel soll das Attribut archive-time-stamp-v3 in Kombination mit dem ats-hash-index-v3 Attribut verwendet werden.

MUST: In diesem Fall muss zur Berechnung des Hashwertes für die Anfrage an den Zeitstempeldienst das Verfahren in ETSI EN 319-122 V1.1.1 Seite 28 herangezogen werden.

Anmerkung: Externe Dokumente dort in Figur 1 zum Hash-Herstellungsprozess sind lediglich die detached Dokumente. Andere externe Dokumente sollen nicht referenziert und bei der Hashherstellung nicht hinzugezogen werden.

MUST: Falls jedoch noch das long-term-validation Attribut für den Archivzeitstempel bereits verwendet worden ist, dann muss die Berechnung des Hashwertes an den Zeitstempeldienst gemäss ETSI TS 101 733 V2.2.1, Seite 49, erfolgen. Eine nochmalige Berechnung dieses Hashwertes ist bei der Prüfung des Attributs notwendig.

4.2 Behandlung der Prüfinformationen

Prüfinformationen sind Informationen, welche zur Prüfung der involvierten Signaturen verwendet werden, wie Zertifikate, Revokationslisten, die OCSP-Antworten und die Zeitstempel nach Erstellung der elektronischen Signatur. (Davon ausgenommen sind Zeitstempelinformationen, welche dem Dokument beigelegt werden und von der elektronischen Signatur erfasst werden, wie beim Attribut content-time-stamp.)

MUST: Das Aufbewahrungssystem muss alle Informationen zur Prüfung aller Signaturen beifügen.

Das Beifügen aller Prüfinformationen ist nicht Aufgabe der Signaturapplikation. (Es mag Signaturapplikationen wie z.B. bei der Adobe Signatur geben, die der Signatur noch eine OCSP-Antwort beifügen

Hier wird nun ein Verfahren empfohlen, wie und wo diese Informationen beizufügen sind.

- Bevor der Hashwert für die Anfrage des Zeitstempels im CAdES-C-time-stamp Attribut erstellt wird, sollen die entsprechenden Zertifikats- und CRL-Referenzen aktualisiert werden. D.h. die Attribute complete-certificate-references und complete-revocation-references sollen vervollständigt werden. Danach ist der Hashwert für die Zeitstempelanfrage herzustellen, ist der Zeitstempel zu beziehen, das CAdES-C-time-stamp Attribut anzufertigen und als unsigniertes Attribut der Dokument- oder Dateisignatur beizufügen.

  Anmerkung: In die Attribute complete-certificate-references und complete-revocation-references sind die Referenzen der Prüfinformationen für den Zeitstempel content-time-stamp aufzunehmen, falls der Zeitstempel vorhanden ist und diese Information der Zeitstempelsignatur nicht bereits als unsigniertes Attribut beigefügt wurde, siehe dazu auch ETSI EN 319 122-1 V1.1.1 Kapitel A.1.1.1, Note 4, Kapitel A.1.2.1, Note 6.

  Wichtig: Der Zeitstempel content-time-stamp darf nicht mehr verändert werden, wenn er bereits Bestandteil der Dokumentsignatur ist, da er Teil eines signierten Attributs ist.
- Die Attribute certificate-values, revocation-values mit den Prüfinformationen für Dokument- oder Dateisignaturen sind zu vervollständigen und als unsignierte Attribute der Dokument- oder Dateisignatur beizufügen.

  Anmerkung: In die Attribute certificate-values, revocation-values sind die Prüfinformationen für den Zeitstempel content-time-stamp aufzunehmen, falls der Zeitstempel vorhanden ist und diese Information der Zeitstempelsignatur nicht bereits als unsigniertes Attribut beigefügt wurde, siehe dazu auch ETSI EN 319 122-1 V1.1.1 Kapitel A.1.1.2, Note 2, Kapitel A.1.2.2, Note.
- Falls die Attributzertifikate für die Dokument- oder Dateisignatur relevant sind, dann sind die signer-attributes-v2, attribute-certificate-references und attribute-revocation-references Attribute zu aktualisieren und als unsigniertes Attribut der Dokument- oder Dateisignatur beizufügen.
- Bevor der erste Archivzeitstempel beigefügt wird, sollen die Prüfinformationen zur Verifikation der Zeitstempel gesammelt und der zuvor erstellten Zeitstempelsignatur als unsigniertes Attribut beigefügt werden. Betroffen sind dabei die Zeitstempel signature-time-stamp, CAeDS-C-time-stamp. D.h. für die Zeitstempelsignaturen sind die Attribute certificate-values, revocation-values herzustellen und als unsigniertes Attribut der Zeitstempelsignatur beizufügen, siehe

auch ETSI EN 319 122-1 V1.1.1 Seite 27 Absatz nach Note 4.
Sinngemäss soll dies auch für die OCSP-Signaturen der OCSP-Antworten vorgenommen werden.

- Der erste Archivzeitstempel ist zu erstellen.
- Beim zweiten Archivzeitstempel sind die Prüfinformationen des vorherigen Archivzeitstempel zu aktualisieren und als unsigniertes Attribut der vorherigen Zeitstempelsignatur beizufügen, siehe auch ETSI EN 319 122-1 V1.1.1, Seite 28 Bemerkungen nach dem ersten Bullet Point. Keine weiteren Informationen sind noch beizufügen. Ansonsten besteht die Gefahr, dass die Prüfung der Signatur nicht erfolgreich verläuft, weil die Berechnung der für die Prüfung relevanten Hashwerte ein anderes Ergebnis liefern könnte.

MUST: Spätestens, bevor das Zertifikat für die Verifikation des Archivzeitstempels abläuft, muss ein weiterer Archivzeitstempel mit neuem, dazu gehörigem Prüfzertifikat erstellt werden.

4.3 Informationen zum Zertifikatsstatus der Dokumentsignatur

SHOULD: Die OCSP Antworten liefert gemäss RFC 6960 den aktuellen Status eines Zertifikats und genügt den Anforderungen aus Art. 9 Abs. 2 VZertES. Deswegen soll diese Information gegenüber der CRL bei der Dokumentsignatur bevorzugt werden.

Beim Hinzufügen einer CRL soll darauf geachtet werden, dass die zeitlich nächstfolgende CRL verwendet wird. Danach soll gegebenenfalls das Zertifikat nochmals geprüft werden.

4.4 Prüfung der Signatur

Das ZertES und seine Ausführungsvorschriften regeln lediglich den Ausstellungsprozess der Zertifikate, das OR den Erstellungsprozess der Signatur, nicht aber deren Verifikation.

In ETSI EN 319 102-1 V1.1.1 sind Verfahren aufgezeigt, wie die aufbewahrten, elektronischen Signaturen zu prüfen sind. Für unsere Zwecke sind die unter «Signatures with Long-Term Validation Material» und «Signatures with Long-Term Availability and Integrity of Validation Material» relevant, siehe auch Anhang B dort.

Hierzu folgende Ergänzung:

- Für die Prüfung der Archivzeitstempel gilt es auch ETSI EN 319 122-1 V1.1.1., Kapitel 5.5.2 3. Absatz zu beachten.
- Ein Zeitstempel B stellt folgenden Beleg oder gar Beweis der Existenz (engl. Proof of Existence, kurz POE) dar: «Die Informationen A, deren Hashwert an den Zeitstempeldienst gesandt worden ist und für die Herstellung des Zeitstempels B zum Zeitpunkt T verwendet wurde, lag vor dem Zeitpunkt T vor.»

Wenn vor dem besagten Zeitpunkt T keine Ungültigkeitserklärung zu den Informationen A oder Teile davon publiziert worden sind, so kann berechtigterweise angenommen werden, dass die Information A als Gesamtes vor dem Zeitpunkt T gültig war. Dies, sofern der Zeitstempel B noch immer mit einem gültigen Zertifikat verifiziert werden kann. Ansonsten sind wiederum Vorkehrungen zu treffen, d.h. weitere Zeitstempel beizufügen, um die Akzeptanzdauer des Zeitstempels B zu verlängern.

5 Zusammenfassung der Empfehlungen

In folgender Tabelle ist eine Zusammenfassung über die hier behandelten und relevanten Attribute zusammengestellt.

Nr	Attribut	Signiert	Emp.	Bem
1.	ESS signing-certificate Attribute	J	SN	
2.	ESS signing-certificate-v2	J	S	
3.	message-digest attribute	N	M	NE
4.	Other signing-certificate Attribute	J	SN	
5.	signature-policy-identifier	J	SN	
6.	mime-type	J	MAY	
7.	signing-time	J	SN	C
8.	countersignature	J	MAY	
9.	content-reference Attribute	J	SN	NE
10.	content-hints Attribute	J	MAY	
11.	commitment-type-indication Attribute	J	SN	
12.	signer-location Attribute	J	SN	C
13.	signer-attributes Attribute	J	SN	CLA
14.	content-time-stamp	J	M, B	
15.	signature-time-stamp Attribute	N	M	
16.	complete-certificate-references Attribute	N	M	
17.	complete-revocation-references Attribute	N	M	
18.	attribute-certificate-references Attribute	N	M, B	
19.	attribute-revocation-references Attribute	N	M, B	
20.	certificate-values Attribute	N	M	
21.	revocation-values Attribute	N	M	
22.	CAdES-C-time-stamp Attribute	N	M	
23.	time-stamped-certs-crls-references Attribute	N	MN	
24.	archive-time-stamp Attribute	N	SN	
25.	ats-hash-index Attribute	N	SN	
26.	archive-time-stamp-v3 Attribute	N	S	
27.	long-term-validation Attribute	N	SN	
28.	signer-attributes-v2 attribute	J	S	CLA
29.	claimed-SAML-assertion	N	SN	CLA

Nr	Attribut	Signiert	Emp.	Bem
30.	ats-hash-index-v2 attribute	N	SN	
31.	ats-hash-index-v3 attribute	N	S	

Tabelle 2: Zusammenfassung der Empfehlungen der hier behandelten Attribute

Legende

B = Bedingt vorhanden

Bem. = Bemerkung

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

CLA = Kann «claimed attribute» des Signierenden enthalten, welche nicht eingefügt werden sollen.

J = JA

M = MUST

MN = Must NOT

N = Nein

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

S = SHOULD

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

SN = SHOULD NOT

6 Weitere Aspekte zur Bewahrung der Gültigkeit

In diesem Kapitel werden weitere Komponenten vorgestellt, welche einen Einfluss auf die Gültigkeit elektronischer Signaturen haben. Dies sind der CSP (Cerificate Service Provider) und die Signaturapplikation.

6.1 CSP

Die CSP haben zu beachten, dass die Signaturen im Zeitstempel und in der OCSP-Antwort nach dem CMS Format hergestellt werden.

Weiter sind die Restriktionen zur Gültigkeitsdauer eines Zertifikats zu beachten, siehe KAPITEL 2.1.2.

Anmerkungen: Bei dem hier präsentierten Konzept muss der CSP keine Aufbewahrungsfristen beachten, ausser dass er Informationen zur Verifikation der Gültigkeit der von ihr ausgestellten Zertifikate beizusteuern hat.

6.2 Signaturapplikation

All die hier erwähnten Attribute, welche mit dem Dokument zu signieren sind, sind Bestandteil des Signaturprozesses. Folglich sind entsprechende Merkmale in die Signaturapplikation einzubauen.

7 Sicherheitsüberlegungen

Dieses Dokument behandelt die Bewahrung der Gültigkeit elektronisch signierter Dokumente, so dass

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

8 Haftungsausschluss/Hinweise auf Rechte Dritter

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

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

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

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

9 Urheberrechte

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

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

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

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

Anhang A – Referenzen & Bibliographie

BERTSCH	Andreas Bertsch, Digitale Signaturen, Springer Verlag, 2001
ETSI EN 319 102-1 V1.1.1.	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures
ETSI EN 319 122-1 V1.1.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
ETSI EN 319 122-2 V1.1.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures
ETSI EN 319 422 V1.1.1	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
ETSI TS 101 733 V2.2.1	Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
ETSI TS 119 122-1 V1.0.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
ETSI TS 119 122-2 V 1.0.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures
ETSI TS 119 122-3 V1.1.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES
ITU-T X.509	Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, 10/2012
RFC 3161	Time-Stamp Protocol
RFC 5652	Cryptographic Message Syntax Format
RFC 6960	Online Certificate Status Protocol – OCSP

Anhang B – Mitarbeit & Überprüfung

Gabi Daniel Bundeskanzlei

Moretti Thomas damals QuoVadis

Anhang C – Abkürzungen und Glossar

Abs.	Absatz
Archivierung	Sichere und dauerhafte Aufbewahrung von Unterlagen in einem Archiv, welche rechtlich, administrativ, politisch, wirtschaftlich, historisch, kulturell, sozial oder wissenschaftlich wertvoll sind.
Aufbewahrung	Organisierte und systematische Verwaltung von Geschäftsinformation für eine angemessene (endliche) Zeitperiode unter Berücksichtigung gesetzlicher, betrieblicher oder historischer Anforderungen.
Bst.	Buchstabe

CMS	Cryptographic Message Syntax, siehe RFC 5652
CRL	Certificate Revocation List
CSP	Certification Service Provider
ETSI	European Telecommunications Standards Institute
GeBüV	Verordnung über die Führung und Aufbewahrung der Geschäftsbücher vom 24. April 2002 (Stand am 1. Januar 2013), SR 221.431
GeoIV	Verordnung über Geoinformation vom 21. Mai 2008, 510.620
OCSP	Online Certificate Status Protocol
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911. SR 220
POE	Proof of Existence
RFC	Request for Comments (IETF Standard)
SAML	Security Assertion Markup Language
SR	Systematische Rechtsetzungsnummer
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032.1
TSP	Trusted Service Provider
UIDG	Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010, SR 431.03
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032
XML	Extended Markup Language
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate, vom 18. März 2016 (Stand am 1. Januar 2017), SR 943.03
Ziff.	Ziffer

Anhang D – Änderungen gegenüber Vorversion

In dieser Version sind zur Version 1.0 keine Empfehlungen beigefügt oder geändert worden. Es wurde lediglich darauf geachtet, dass diese Version mit dem eCH-Standard 0230 kompatibel ist. Darunter fällt u.a. Titel des Standards, Kapitelnummerierung, Anmerkungen oder Erläuterungen.

Zudem sind Präzisierung/Verbesserung in der Sprache vorgenommen worden.

Request	Kapitel	Seite	Anpassung
	Titel	1	Änderung des Titels
	2.2.	10	Ergänzung
	4.2	18	Erweiterung
	4.4	19	Erweiterung

Anhang E– Tabellenverzeichnis