eCH-0230 – Bewahrung der Gültigkeit elektronischer Signaturen im XML-Format

Name	Bewahrung der Gültigkeit elektronischer Signaturen im XML-Format
eCH-Nummer	eCH-0230
Kategorie	Standard
Reifegrad	Definiert
Version	1.0.0
Status	Genehmigt
Beschluss am	2021-03-02
Ausgabedatum	2021-03-10
Ersetzt Version	-
Voraussetzungen	ETSI TS 101 903 V1.4.2 ETSI EN 319 132-1 V1.1.1 ETSI EN 319 132-2 V1.1.1 ZertES (Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur) eCH-0091
Beilagen	-
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Fachgruppe Technologie Büchler Georg (KOST) Müller Adrian (SwissSign AG) Muster Daniel (it-rm IT-Riskmanagement GmbH) Niederberger Marcel (ESTV) von Niederhäuser Michael (BIT) Rötzer Hubert Schmid Josef 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 XML-Format, so dass die elektronische Signatur der aufzubewahrenden XML-Dokumente während dieser Zeit verlässlich geprüft werden kann. Langzeit meint, dass die Signatur z.B. auch noch nach Ablauf der Gültigkeitsdauer des zur Signatur korrespondierenden Zertifikats entsprechend verifiziert und bei erfolgreicher Prüfung allgemein anerkannt werden kann. Die Gültigkeit eines Zertifikats kann z.B. nach seiner Laufzeit oder nach beantragter Revokation des Eigentümers des Zertifikats verfallen.

Es gibt andere Signaturformate wie CMS- oder PDF-Signaturen. Das hier behandelte elektronische Signatur-Format basiert auf dem W3C-Standard «XML Signature and Processing» Version 1.1 und auf eCH-0091.

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

- ETSI TS 101 903 V1.4.2
- ETSI EN 319 132-1 V1.1.1
- ETSI EN 319 132-2 V1.1.1

Bei der hier vorgenommenen Auswahl an XML-Elementen wurde darauf geachtet, dass das ganze Konstrukt der «Konservierung» elektronisch signierter XML-Dokumente und XML-Objekte wenn möglich auf Elementen und -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.
- ETSI-Standards zu diesem Thema

Für die Prüfung elektronisch signierter Dokumente sei auch 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

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

1.2 Anwendungsgebiet

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

- ETSI TS 101 903 V1.4.2

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 XML-Dokumente und XML-Objekte 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.

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

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

Ausgangslage dieses Dokuments war aber der Standard ETSI TS 101 903 V1.4.2 in seiner letzten Version, weil:

- er selbsterklärend ist und zusätzliche Informationen zum Verständnis der Problematik enthält.
- ETSI EN 319 132-1 und V1.1.1 und ETSI EN 319 132-2 V1.1.1 für den Einstieg in die Problematik schwieriger sind.

ETSI EN 319 132-1 und V1.1.1 und ETSI EN 319 132-2 V1.1.1 werden anschliessend in diesem Dokument berücksichtigt.

1.3 Ausgangslage

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

- Das Zertifikat mit dem öffentlichen Schlüssel zur Verifikation der elektronischen Signatur, kurz das Prüfzertifikat, ist nicht mehr gültig.
- Das Root-Zertifikat zum Prüfzertifikat ist nicht mehr gültig.

- Der private Signaturschlüssel wurde kompromittiert und das Zertifikat wurde dann revoziert.
- Das Zertifikat ist aus anderen Gründen revoziert worden.

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

1.4 Ziel(e) und Abgrenzung

1.4.1 Ziel

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

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

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

- innerhalb der von den jeweiligen Bestimmungen geforderten 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 ETSI-Standards ETSI TS 119 102-1 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, 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).

1.4.2 Abgrenzung

In diesem Zusammenhang ist es wichtig zu erwähnen: Eine elektronische Signatur vermag die Integrität, d.h. die Unveränderheit, 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 (Unveränderheit) 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 einerseits um XML-Signaturen an XML-Dokumente oder XML-Objekte. Andererseits werden zur Prüfung weitere Informationen wie ein Zeitstempel, Zertifikate, eine Zertifikatsrevokationsliste (CRL) oder eine OCSP-Antwort. benötigt. Diese Angaben werden jedoch im CMS-Format signiert.

Nicht behandelt wird hier die Bewahrung der Gültigkeit für elektronische Signaturen im CMS-Format oder elektronische Signaturen an ein PDF-Dokument. 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 319 102-1 V1.1.1.
- ETSI EN 319 102-2 V1.1.1.

1.5 Inhalt, Struktur des Dokuments

Dieses Dokument ist ein Profil der zugrundeliegenden 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.

1.6 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.

1.7 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.)

1.8 Begriffliches

1.8.1 Signatur

Für die hier behandelte Thematik werden noch andere Signaturen als die Signatur an ein XML-Dokument oder an ein XML-Objekt thematisiert, nämlich Signaturen bei

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

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

1.8.2 XML-Element und XML-Objekt

Ein XML-Element, resp. XML-Objekt, wird hier lediglich als Element, resp. Objekt, bezeichnet.

1.9 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 oder beschaffen zu sein haben.

2.1 Zertifikate

2.1.1 Herkunft

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

SHOULD: Die Signatur eines zu archivierenden Dokumentes soll mit einem nach ZertES definierten Zertifikat (Art. 2 Bst. g und h ZertES) verifiziert werden. Anderes würde die verlässliche und allgemein anerkannte «Konservierung» der elektronisch signierten Dokumente 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.

2.1.3 Format Zertifikate

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

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: Es dürfen nur nach ZertES qualifizierte Zeitstempel verwendet werden, welche von eines 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 NOT: Es besteht gemäss ETSI-Standards TS 101 903 V1.4.2 noch die Möglichkeit Zeitstempel im XML-Format beizufügen, siehe dort Kapitel 7.1.4.2. Diese dürfen folglich in diesem Kontext

nicht verwendet werden, u.a. weil sie (rechtlich) nicht anerkannt sind.

2.2.3 Prüfinformationen 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.

Ausser wenn diese Information in einem dafür vorgesehenen XML-Element eingefügt wird.

In folgender Tabelle sind die hier behandelten Elemente aufgeführt, welche Zeitstempel enthalten (Kolonne 1). In Kolonne 2, wo die Zertifikate für die Prüfung des Zeitstempels **sonst noch** in *Elemente zur Dokument- oder Objektsignatur* abgelegt werden können. In Kolonne 3 wird noch aufgeführt, welche Informationen in die Erstellung des Hashwerts einfliessen, der an den Zeitstempeldienst gesandt wird.

Element mit Zeitstempel	**Zertifikatsinfo (Alternative)**	**Elemente für den Hashwert**
AllDataObjectsTimeStamp	CertificateValues, XAdESv141:TimeStampValidationData.	Alle Referenzen im Element ds:SignedInfo gemäss W3C-Sig, ausser die Referenz auf dieses Objekt selber. siehe Kapitel 7.2.9 in ETSI TS 101 903 V1.4.2
IndividualDataObjectsTimeStamp	CertificateValues, XAdESv141:TimeStampValidationData.	Wahlweise Bestandteile von den Referenzen im AllDataObjectsTimeStamp siehe Kapitel 7.2.10 in ETSI TS 101 903 V1.4.2
SignatureTimeStamp	CertificateValues XAdESv141:TimeStampValidationData	ds:SignatureValue Element, gemäss W3C-Sig siehe Kapitel 7.3 in ETSI TS 101 903 V1.4.2
RefsOnlyTimeStamp	CertificateValues, XAdESv141:TimeStampValidationData.	CompleteCertificateRefs, CompleteRevocationRefs, falls vorhanden, AttributeCertificateRefs and AttributeRevocationRefs, siehe Kapitel 7.5.2 in ETSI TS 101 903 V1.4.2

Element mit Zeitstempel	Zertifikatsinfo (Alternative)	Elemente für den Hashwert
SigAndRefsTimeStamp	CertificateValues, XAdESv141:TimeStampValidationData.	ds:SignatureValue, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, falls vorhanden AttributeCertificateRefs, AttributeRevocationRefs, siehe Kapitel 7.5.1 in ETSI TS 101 903 V1.4.2
XAdESv1.3.2:ArchiveTimeStamp		Das Format dieses Zeitstempels wurde in einer früheren Version (1.3.2) definiert. Doch dieses ist von xadesv141:ArchiveTimeStamp abgelöst worden. Siehe Kapitel 7.7 in ETSI TS 101 903 V1.4.2
xadesv141:ArchiveTimeStamp	XAdESv141:TimeStampValidationData	Alle zuvor erstellten Elemente, u.a. auch die referenzierten Objekte für die XML-Signatur. Siehe Kapitel 8.2.1 in ETSI TS 101 903 V1.4.2

Tabelle 1: Infos zu den Zeitstempeln

ds: Ist der Namensraum-Präfix gemäss W3C-Sig für die XML-Signatur.
xadesv141: ist ein Namensraum-Präfix gemäss ETSI TS 101 903 V1.4.2.

Aus der Tabelle ist ersichtlich, dass nur der Archivzeitstempel das signierte Dokument oder Objekt vor einer Schwächung derjenigen Hashwerte schützt, welche zur Signierung des Dokuments verwendet werden.

Anmerkung: Die folgenden Zeitstempel sind Bestandteil der XML-Signatur, deren Gültigkeit es zu bewahren gilt.

- AllDataObjectsTimeStamp
- IndividualDataObjectsTimeStamp

Die Prüfinformationen für die Verifikation des Zeitstempels in der Kolonne 2 werden jedoch von der Signatur nicht erfasst.

2.3 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, die OCSP-Signatur zu prüfen und festzustellen, ob das dazu korrespondierende Zertifikat zum Zeitpunkt der Erstellung OCSP-Antwort gültig war. Diese Informationen sind der CMS-Signatur der OCSP-Antwort als von der OCSP-Antwort unsignierte Information unter anderem in die Attribute certificate-values und revocation-values beizufügen.

Ausser wenn diese Information in einem dafür vorgesehenen XML-Elemente eingefügt wird.

2.4 Format der XML-Signatur

MUST: Eine XML-Signatur muss W3C-Sig entsprechen. Was noch Bestandteil der Signatur sein kann/muss oder nicht sein soll/darf, siehe ETSI TS 101 903 V1.4.2 und eCH-0091.

3 Profil

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

3.1 ETSI TS 101 903 V1.4.2

3.1.1 XAdES-Format

Ausgangslage des hier vorliegenden Profils zur Bewahrung der Gültigkeit elektronischer Signaturen sind die Prüfinformationen/Elemente, welche in der Figur G5 und G6 im Kapitel G.1.2 des Standard ETSI TS 101 903 V1.4.2. dargestellt sind. Die in den Figuren G1 bis G4 dargestellten Formate enthalten für die hier verfolgten Absichten noch nicht ausreichend Informationen.

Angestrebt wird, dass alle für die Prüfung einer elektronischen Signatur relevanten Informationen möglichst beieinander sind.

3.1.2 Einleitende Bemerkung

ETSI TS 101 903 V1.4.2 legt die Namen und Bedeutung weiterer Elementen fest, welche im W3C-Sig nicht erwähnt werden, aber für den vorliegenden Zweck relevant sind.

MUST: Diese Elemente müssen in der von ETSI TS 101 903 V1.4.2 definierten Struktur (Schema) eingebettet sein.

Weiter wird unterschieden zwischen Elementen,

- die von der zu bewahrenden Signatur geschützt/erfasst werden.
- die für die Bewahrung der Gültigkeit der Signatur relevant sind, aber von der Signatur nicht erfasst werden.

Betreffend den zu verwendenden Namensraum, siehe Kapitel 5, ETSI TS 101 903 V1.4.2.

3.1.3 Von der Signatur erfasste Elemente

3.1.3.1 Kapitel 7.2.2 SigningCertificate

Gemäss Standard besteht die Möglichkeit, das Element «SigningCertificate» zu verwenden, wenn der Benutzer verschiedene Zertifikate mit dem gleichen öffentlichen Schlüssel darin verwendet. In diesem Element sind Referenzen auf dasjenige Zertifikat enthalten, welches zur Prüfung der Signatur verwendet werden soll.

MUST NOT: Dieses Element darf nicht verwendet werden.

Begründung: Unterschiedliche Zertifikate mit gleichem öffentlichem Schlüssel darin dürfen nicht erstellt werden.

3.1.3.2 Kapitel 7.2.3 SignaturePolicyIdentifier

Mit dem Element «SignaturePolicyIdentifier» können Vorschriften referenziert werden, welche hierfür gelten sollen.

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

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

3.1.3.3 Von einer anerkannten Stelle nicht bestätigte Informationen

Folgende Elemente enthalten Informationen, welche der Signierende beigefügt hat, aber von einer anerkannten Stelle nicht bestätigt sind.

- SigningTime: Zeit, wann die Signatur erstellt wurde (Kapitel 7.2.1). Diese Zeitangabe ist vom Unterzeichnenden geleistet.
- SignatureProductionPlace: Ortsangabe, wo die Signatur erstellt wurde (Kapitel 7.2.7)
- SignerRole: Rolle des Signierenden bei der Signaturerstellung (Kapitel 7.2.8).

MAY: Diese Elemente können beigefügt werden.

Die Informationen, welche in den Elementen enthalten sind, können auch aus dem Zeitstempel, den Attributzertifikaten, den Zertifikaten oder aus dem zu signierenden Dokument ersichtlich sein.

Eine Zeitangabe durch den Unterzeichnenden ist nicht ausreichend, um die Verbindlichkeit der Zeitangabe anerkannt begründen oder darlegen zu können. Falls es rechtlich relevant ist, dass die Signatur nach einem bestimmten Zeitpunkt erstellt wurde, dann sind die Informationen in den oben genannten Elementen nicht mehr ausreichend. Folglich:

MUST: Es muss ein anerkannter Zeitstempel beigefügt werden.

3.1.3.4 Kapitel 7.2.6 CommitmentTypeIndication

Das Element «CommitmentTypeIndication» enthält Informationen, zu welchen sich der Signierende mit der Signatur bekennt.

MAY: Dieses Element kann verwendet werden.

Zu was sich der Signierende bekennt, soll jedoch grundsätzlich aus der von ihm signierenden XML-Information oder aus dem Kontext entnommen werden.

3.1.3.5 Kapitel 7.2.5 DataObjectFormat

Das Element «DataObjectFormat» enthält Angaben zu XML-Objekten oder Dateien, welche signiert werden sollen.

MAY: Dieses Element kann verwendet werden.

Wird das Element verwendet, dann soll Folgendes beachtet werden.

SHOULD: Zuerst sollen die Angaben im ds:Object mittels Attributen festgehalten werden. Erst, wenn dies für gewisse Anwendungen nicht ausreicht, kann dieses Element verwendet werden.

3.1.3.6 Kapitel 7.2.9 AllDataObjectsTimeStamp

Im Element «AllDataObjectsTimeStamp» ist ein anerkannter Zeitstempel über all die noch zu signierenden Objekte enthalten. Damit wird belegt, dass die Signatur nach einem bestimmten Zeitpunkt erstellt wurde.

MUST: Falls belegt werden muss, dass die Signatur nach einem bestimmten Zeitpunkt erstellt wurde, dann ist dieses Element in die Signatur einzubinden.

3.1.3.7 Kapitel 7.2.10 IndividualDataObjectsTimeStamp

Im Element «IndividualDataObjectsTimeStamp» ist ein anerkannter Zeitstempel über Teile der zu signierenden Objekte enthalten. Damit wird belegt, dass die Signatur über diese Objekte nach einem bestimmten Zeitpunkt erstellt wurde.

SHOULD NOT: Dieses Element soll nicht verwendet werden.

SHOULD: Anstelle dieses Elements soll das Element «AllDataObjectsTimeStamp» verwendet und eingefügt werden.

3.1.4 Von der Signatur nicht erfasste Elemente

3.1.4.1 Kapitel 7.2.4 CounterSignature

Wie aus der englischen Bezeichnung abzuleiten ist, enthält das Element «CounterSignature» eine Gegenzeichnung des signierten Dokuments.

Im Element CounterSignature/ds:Signature/ds:SignedInfo/ds:Reference kann ein Attribut eingefügt werden, um anzuzeigen, dass es sich hiermit um eine Gegensignatur handelt.

SHOULD: Das Attribut soll verwendet werden.

SHOULD: Die Prüfinformationen für die Gegensignatur wie Zertifikate sollen in CounterSignature/ds:Signature/ als von der Gegensignatur nicht erfasste Elemente beigefügt werden.

3.1.4.2 Kapitel 7.3 SignatureTimeStamp

Im Element «SignatureTimeStamp» ist ein Zeitstempel enthalten, welcher belegt, dass die Signatur nach einem bestimmten Zeitpunkt erstellt wurde. In den Zeitstempel fliesst das Element «ds:SignatureValue» ein.

MUST: Dieses Element muss eingebaut werden.

3.1.4.3 Kapitel 7.4.1 CompleteCertificateRefs

Im Element «CompleteCertificateRefs» sind alle Referenzen auf Zertifikate enthalten, welche für die Prüfung der Signatur zu einem bestimmten Zeitpunkt notwendig sind.

MAY: Dieses Element kann enthalten sein, darf aber nicht leer sein.

Im Unterschied zum CAeDS Standard ETSI EN 319 122-2 wird diese Information vom Standard für das XAdES-T Format nicht gefordert.

3.1.4.4 Kapitel 7.4.2 CompleteRevocationRefs

Im Element «CompleteRevocationRefs» sind alle Referenzen auf Revokationslisten (CRL) enthalten, welche für die Prüfung der Signatur zu einem bestimmten Zeitpunkt notwendig sind.

MAY: Dieses Element kann enthalten sein, darf aber nicht leer sein.

Im Unterschied zum CAeDS Standard ETSI EN 319 122-2 wird diese Information vom Standard für das XAdES-T Format nicht gefordert.

3.1.4.5 Kapitel 7.4.3 AttributeCertificateRefs

Im Element «AttributeCertificateRefs» sind alle Referenzen auf Attributzertifikate enthalten, welche für

die Prüfung der Attribute zu einem bestimmten Zeitpunkt notwendig sind.

SHOULD NOT Dieses Element soll nicht enthalten sein, darf aber nicht leer sein.

Im Unterschied zum CAeDS Standard ETSI EN 319 122-2 wird diese Information vom Standard für das XAdES-T Format nicht gefordert, falls Attributzertifikate beigefügt werden.

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

3.1.4.6 Kapitel 7.4.4 AttributeRevocationRefs

Im Element «AttributeRevocationRefs» sind alle Referenzen auf Attributrevokationslisten enthalten, welche für die Prüfung der Attribute zu einem bestimmten Zeitpunkt notwendig sind.

MAY: Dieses Element kann enthalten sein, darf aber nicht leer sein.

Im Unterschied zum CAeDS Standard ETSI EN 319 122-2 wird diese Information vom Standard für das XAdES-T Format nicht gefordert, falls Attributzertifikate beigefügt werden.

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

3.1.4.7 Kapitel 7.5.2 RefsOnlyTimeStamp

Im Element «RefsOnlyTimeStamp» ist ein Zeitstempel über die Elemente, welche die referenzierten Informationen enthalten (CompleteCertificateRefs, CertificateRevocationRefs, AttributeCertificateRefs, AttributeRevocationRefs).

SHOULD NOT: Der darin vorgesehene Zeitstempel soll nicht erstellt werden,

Die von diesem Zeitstempel erfassten Informationen werden bereits durch «SigAndRefsTimeStamp» abgedeckt.

3.1.4.8 Kapitel 7.5.1 SigAndRefsTimeStamp

Im Element «SigAndRefsTimeStamp» ist ein Zeitstempel über:

- die Signatur selber (ds:SignatureValue)
- SignatureTimeStamp und
- die Elemente, welche die referenzierten Informationen zur Prüfung der Signatur enthalten. Dies sind CompleteCertificateRefs, CertificateRevocationRefs und falls Attributzertifikate aufgeführt sind AttributeCertificateRefs, AttributeRevocationRefs)

MUST: Der im Element vorgesehene Zeitstempel muss erstellt und eingefügt werden.

3.1.4.9 Kapitel 7.6.1 CertificateValues

Im Element «CertificateValues» sind die Zertifikate zur Prüfung der vorhandenen Signaturen enthalten.

MUST: Die Zertifikate zur Prüfung der Signatur müssen in diesem Element eingefügt werden, falls sie nicht bereits an einem andern als dafür vorgesehenen Ort abgelegt sind.

3.1.4.10 Kapitel 7.6.2 RevocationValues

Im Element «RevocationValues» sind die Revokationslisten zur Prüfung der Zertifikate enthalten.

MUST: Die Revokationslisten zur Prüfung der Zertifikate müssen in diesem Element eingefügt werden, falls sie nicht bereits an einem andern als dafür vorgesehenen Ort abgelegt sind.

3.1.4.11 Kapitel 7.6.3 AttrAuthoritiesCertValues

Im Element «AttrAuthoritiesCertValues» sind die Zertifikate zur Prüfung der Attribute und Attributzertifikate enthalten.

MUST: Diese Zertifikate müssen im Element «AttrAuthoritiesCertValues» eingefügt werden, falls Attributzertifikate verwendet werden.

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

3.1.4.12 Kapitel 7.6.4 AttributeRevocationValues

Im Element «AttributeRevocationValues» sind die Revokationslisten zur Prüfung der Attribute und der Attributzertifikate enthalten.

MUST: Die Revokationslisten zur Prüfung der Attributzertifikate müssen im Element «AttributeRevocationValues» eingefügt werden, falls Attributzertifikate verwendet werden.

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

3.1.4.13 Kapitel 8.2 ArchiveTimeStamp

Im Element «ArchiveTimeStamp» ist ein Archivzeitstempel enthalten.

MUST: Dieser Archivzeitstempel muss integriert werden; dies im Format nach ETSI EN 319 122-1 V1.1.1.

3.1.4.14 Kapitel 8.1 TimeStampValidationData

Im Element «TimeStampValidationData» können Prüfinformationen zur Verifikation eines Zeitstempels eingefügt werden. Pro Zeitstempel ist ein separates Element anzufertigen und eine entsprechende Referenz auf diesen Zeitstempel beizufügen.

MUST: Im Element «TimeStampValidationData» mit entsprechendem Verweis auf das Element mit dem Archivzeitstempel müssen die Zertifikate für die Prüfung des entsprechenden Archivzeitstempels enthalten sein.

MUST: Falls Prüfinformationen zu einem Zeitstempel beigefügt werden müssen, welcher kein Archivzeitstempel ist, soll gelten: In diesem Element mit entsprechendem Verweis auf das Element mit dem jeweiligen Zeitstempel müssen die Zertifikate für die Prüfung dieses Zeitstempels enthalten sein. Sofern die entsprechenden Zertifikate nicht bereits in einem anderen Element aufgeführt sind.

3.2 ETSI EN 319 132-1 V1.1.1

3.2.1 Einleitende Bemerkung

Auch hier wird zwischen Elementen unterschieden, welche von der zu bewahrenden Signatur erfasst werden und den für die Bewahrung der Signatur beizufügenden Informationen. Letztere Information ist nicht Bestandteil dieser Signatur.

Die von der Signatur erfassten Elemente und Objekte sind dem Element «SignedProperties» untergeordnet. Zum zu verwendenden Namensraum, siehe Kapitel 4.2

In diesem Unterkapitel werden lediglich Ergänzungen und Anmerkungen zum zuvor behandelten ETSI-Standard TS 101 903 V1.4.2 aufgeführt.

3.2.2 Von der Signatur erfasste Elemente

3.2.2.1 Kapitel 5.2.2 SigningCertificateV2

Gemäss Standard besteht die Möglichkeit, das Element «SigningCertificateV2» zu verwenden, wenn der Benutzer verschiedene Zertifikate mit dem gleichen öffentlichen Schlüssel darin verwendet. In diesem Element sind Referenzen auf dasjenige Zertifikat enthalten, welches zur Prüfung der Signatur verwendet werden soll.

MUST NOT: Dieses Element darf nicht verwendet werden.

Begründung: Unterschiedliche Zertifikate mit gleichem öffentlichem Schlüssel darin dürfen nicht erstellt werden.

3.2.2.2 Kapitel 5.2.5 SignatureProductionPlaceV2

Sowohl das Element «SignatureProductionPlace» als auch das Element «SignatureProductionPlaceV2» können je wahlweise und miteinander hinzugefügt werden.

MAY: Das Element kann verwendet werden.

Die Information, welche darin eingepackt werden kann, kann auch aus dem zu signierenden Dokument ersichtlich sein.

3.2.2.3 Kapitel 5.2.6 SignerRoleV2

Sowohl das Element «SignerRole» als auch das Element «SignerRoleV2» können je wahlweise und miteinander aufgeführt werden. Beim Element «SignerRoleV2» können zusätzlich Bestätigungen (engl. Assertions) eingefügt werden.

MAY: Das Element kann z.B. für das Einbinden einer SAML Meldung verwendet werden.

MUST: Falls eine SAML Meldung für die Bewertung der Signatur relevant ist, dann muss sie vollständig, d.h. u.a. nicht referenziert, im Element «SignerRoleV2» untergebracht werden. Dabei soll beachtet werden:

SHOULD: Alle Informationen zur Rolle sollen in der SAML-Meldung nicht-referenziert enthalten sein.

SHOULD: Die Zertifikate für die Prüfung der SAML Signatur sollen der SAML-Signatur als unsigniertes Element beigefügt werden.

MUST NOT: Diese Zertifikate dürfen nach der Erstellung der Signatur nicht mehr einer darin enthaltenen Signatur beigefügt werden. Ansonsten ist die Signatur nicht mehr gültig.

3.2.3 Von der Signatur nicht erfasste Elemente

3.2.3.1 Kapitel 5.5.3 RenewedDigests

Das RenewedDigests Element enthält mit einer anderen Hashfunktion neu berechnete Hashwerte von Objekten, welche im ds:Manifest Element über das Element ds:Reference verwiesen sind. Die Bedeutung des ds:Reference Element ist in W3C-Sig beschrieben.

Das ds:Manifest Element darf gemäss eCH-0091 nicht verwendet werden.

MUST NOT: Folglich darf das Element nicht eingebaut werden.

3.2.3.2 Kapitel 5.2.10 SignaturePolicyStore

Im Element «SignaturePolicyStore» kann entweder eine Referenz auf die zugrundeliegende Policy

oder die Policy selber enthalten sein.

SHOULD: Wenn eine Policy sinnvoll ist, dann soll hier die gesamte Policy in einem Objekt in diesem Element enthalten sein.

Falls eine Policy eingefügt wird, dann:

MUST: Es müssen der Policy-Signatur sämtliche Informationen beigefügt werden, welche zur Prüfung der Policy-Signatur notwendig sind. Dies muss vor der Erstellung des ersten Archivzeitstempel erfolgen.

3.3 ETSI EN 319 132-2 V1.1.1

Im Standard ETSI EN 319 132-2 V1.1.1 wird tabellarisch festgelegt, welche Elemente für die entsprechenden XAeDS-Signaturformate enthalten sein können und beigefügt werden müssen. In dem hier vorliegenden Dokument wurde ein Konstrukt ausgewählt, welches lediglich so viele Informationen beigefügt, dass damit die in KAPITEL 1.4 definierte Zielsetzung erreicht wird.

Der Standard ist Grundlage für die Tabelle im KAPITEL 5 «Zusammenfassung der Empfehlungen».

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

Wie der Hashwert zu berechnen ist, welcher an den Archivzeitstempeldienst gesandt wird, ist im Kapitel 8 von ETSI TS 101 903 V1.4.2. beschrieben.

4.2 Behandlung der Prüfinformationen

Prüfinformationen sind Informationen, welche zur Prüfung der involvierten Signaturen verwendet werden, wie Zertifikate, Revokationslisten, OCSP-Antworten und die Zeitstempel nach Erstellung der elektronischen Signatur. (Davon ausgenommen können Zeitstempelinformationen sein, welche dem Dokument beigelegt werden und von der elektronischen Signatur erfasst werden, wie bei den Zeitstempeln in den Elementen «AllDataObjectsTimeStamp» und «IndividualDataObjectsTimeStamp».)

MUST: Das Aufbewahrungssystem muss alle Zertifikate zur Verifikation der Signatur(en) in den Elementen RevocationValues CertificateValues beifügen.

Davon ausgenommen sein kann, wenn die Zertifikate bereits anderswo enthalten sind. Z.B. bei der Gegensignatur, der OCSP-Antwort oder dem Zeitstempel. Es ist möglich, die Prüfinformationen für die erwähnten Signaturen in dieser Signatur bereits einzufügen.

Das Beifügen aller Prüfinformationen ist nicht Aufgabe der Signaturapplikation sein. (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.

- Falls der Zeitstempel in «RefsOnlyTimeStamp» beigefügt wird, dann müssen die entsprechenden Referenzen auf die Zertifikate, CRL vorgängig aktualisiert werden. Falls auch noch Referenzen auf die Attributzertifikate sowie deren Ungültigkeitsliste enthalten sind, sind diese ebenfalls zu aktualisieren. D.h. die Elemente CompleteCertificateRefs, CompleteRevocationRefs, falls vorhanden AttributeCertificateRefs and AttributeRevocationRefs sollen vervollständigt werden. Anmerkung: Dieser Zeitstempel soll nicht verwendet werden.
- Danach ist der Hashwert für die Zeitstempelanfrage herzustellen, der Zeitstempel zu beziehen, das RefsOnlyTimeStamp Element anzufertigen und als unsigniertes Element der Dokument- oder Dateisignatur beizufügen.
- Bevor der Hashwert für die Anfrage des Zeitstempels im SigAndRefsTimeStamp Element erstellt wird, müssen die entsprechenden Referenzen auf die Zertifikate, CRL zuerst aktualisiert werden. Falls auch noch Referenzen auf die Attributzertifikate sowie deren Ungültigkeitsliste enthalten sind, sind diese ebenfalls zu aktualisieren. D.h. die Elemente CompleteCertificateRefs, CompleteRevocationRefs, falls vorhanden AttributeCertificateRefs and AttributeRevocationRefs sollen vervollständigt werden. **Die Aktualisierung der aufgeführten Referenzen darf aber nur erfolgen, wenn zuvor kein «RefsOnlyTimeStamp»-Zeitstempel erstellt worden ist.**
- Danach ist der Hashwert für die Zeitstempelanfrage herzustellen, der Zeitstempel zu beziehen, das SigAndRefsTimeStamp Element anzufertigen und als unsigniertes Element der Dokument- oder Dateisignatur beizufügen.
- Die Elemente CertificateValues, RevocationValues mit den Prüfinformationen für Dokument- oder Dateisignaturen sind zu vervollständigen und als unsignierte Elemente der Dokument- oder Dateisignatur beizufügen.
- Falls die Attributzertifikate für die Dokument- oder Dateisignatur relevant sind, dann sind die AttrAuthoritiesCertValues, AttributeRevocationValues Elemente zu aktualisieren und als unsigniertes Element der Dokument- oder Objektsignatur beizufügen.
- *Bevor der erste Archivzeitstempel beigefügt wird, sollen die Prüfinformationen zur Verifikation der Zeitstempel gesammelt und der zuvor erstellten Zeitstempelsignatur als unsigniertes Element beim Zeitstempel selber oder in den Elementen* CertificateValues, RevocationValues *beigefügt werden.*
  Entsprechend solle dies auch für die zuvor erstellten OCSP-Signaturen der OCSP-Antworten vorgenommen werden.
- Der erste Archivzeitstempel ist zu erstellen.
- Beim zweiten Archivzeitstempel sind die Informationen, *welche zur Prüfung des vorherigen Archivzeitstempel benötigt werden,* zuerst zu aktualisieren. Dann ist daraus ein weiteres XAdESv141:TimeStampValidationData Element beizufügen. Eine Referenz auf den vorherigen Archivzeitstempel ist in diesem Element einzubinden.

MUST: Bevor das Zertifikat für die Verifikation des aktuellsten Archivzeitstempels abläuft, muss ein weiterer Archivzeitstempel erstellt und die dazu gehörigem Prüfzertifikate beigefügt 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, d.h. die CRL welche nach dem Signaturzeitstempel «SignatureTimeStamp» erstellt wurde. Danach soll gegebenenfalls das Zertifikat auf seine Gültigkeit 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 TS 101 903, Kapitel G.2 ist aufgelistet, wie die entsprechenden Elemente zu prüfen sind. In ETSI TS 119 102-1 sind Prozesse der Prüfung aufgezeigt

Hierzu folgende Ergänzung: 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	Element	Signiert	Emp.	Bem
1.	SigningCertificate	J	MN	
2.	SigningCertificateV2	J	MN	
3.	SigningTime	J	MAY	C
4.	SignatureProductionPlace	J	MAY	C
5.	SignatureProductionPlaceV2	J	MAY	C
6.	SignerRole	J	MAY	C
7.	SignerRoleV2	J	MAY	C
8.	CommitmentTypeIndication	J	MAY	C
9.	DataObjectFormat	J	MAY	C
10.	SignaturePolicyIdentifier	J	SN	
11.	AllDataObjectsTimeStamp	J	B	

12.	IndividualDataObjectsTimeStamp	J	SN	
13.	SignatureTimeStamp	N	M	
14.	CompleteCertificateRefs	N	B	
15.	CompleteRevocationRefs	N	B	
16.	AttributeRevocationRefs	N	B	
17.	AttributeRevocationRefs	N	B	
18.	CounterSignature	N	B	
19.	SigAndRefsTimeStamp	N	M	
20.	RefsOnlyTimeStamp element	N	SN	
21.	CertificateValues	N	M	
22.	RevocationValues	N	M	
23.	RenewedDigests	N	MN	
24.	AttrAuthoritiesCertValues	N	B	
25.	AttributeRevocationValues	N	B	
26.	SignaturePolicyStore	N	B	
27.	ArchiveTimeStamp	N	M	
28.	TimeStampValidationData	N	M	

Tabelle 2: Zusammenfassung der Empfehlungen der hier behandelten Elemente

Legende

B = Bedingt vorhanden

Bem. = Bemerkung

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

J = JA

M = MUST

MN = MUST NOT

N = Nein

S = SHOULD

Signiert = Bestandteil der zu archivierenden Dokument- oder Dateisignatur, d.h. der Inhalt des Elements 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

Es gilt 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 Elemente, welche mit dem Dokument oder Objekt zu signieren sind, sind Bestandteil des Signaturprozesses. Folglich sind entsprechende Funktionen in die Signaturapplikation einzubauen.

7 Sicherheitsüberlegungen

Dieses Dokument behandelt die Bewahrung der Gültigkeit elektronisch signierter XML-Dokumente und XML-Objekte, 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

Fachliteratur

BERTSCH	Andreas Bertsch, Digitale Signaturen, Springer Verlag, 2001

eCH (www.ech.ch)

eCH-0018	XML Best Practices
eCH-0036	Dokumentation für den XML-orientierten Datenaustausch
eCH-0091	eCH-0091: Standard zu XML-Signatur und Verschlüsselung

ETSI (www.etsi.org)

ETSI EN 319 102-1 V1.1.1.	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures
ETSI EN 319 122-1 V1.1.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
ETSI EN 319 122-2 V1.1.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures
ETSI EN 319 422 V1.1.1	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
ETSI EN 319 132-1 V1.1.1	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
ETSI EN 319 132-2 V1.1.1	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Building blocks and XAdES baseline signatures
ETSI TS 119 102-1 V1.2.1	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation (2018-08)
ETSI TS 101 903 V1.4.2	Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)

ITU (www.itu.int)

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

IETF Standards (www.ietf.org)

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

RFC 6960 Online Certificate Status Protocol – OCSP

W3C Standards (www.w3c.org)

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

Exclusive XML Canonicalization Version 1.0 Recommendation, July 2002

XML Path Language (XPath) Version 1.0

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

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

XML Signature Best Practices Working Group Note, April 2013

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

OASIS Standards (www.oasis-open.org)

Security Assertion Markup Language (SAML) v2.0

Anmerkung: Die hier angegebenen Standards basieren wiederum auf eine Reihe anderer ETSI, ITU, W3C oder RFC Standards. Diese werden aber dort aufgelistet.

Erlasse

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

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

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

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

Anhang B – Mitarbeit & Überprüfung

Siehe Titelblatt

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
ds:	Namensraum-Präfix gemäss W3C-Sig
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, siehe RFC 6960
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
W3C-Sig	XML Signature Syntax and Processing Recommendation Version 1.1, 11 April 2013
XAdES	XML Advanced Electronic Signature. Näheres dazu siehe ETSI TS 101 904 V.1.4.2
XAdES-T	XML advanced Electronic Signature with Timestamp. Näheres dazu siehe ETSI TS 101 904 V.1.4.2
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

Dies ist die erste Version.

Anhang E – Tabellenverzeichnis