

eCH-0092 Signatur und Verschlüsselung im digitalen Dokumentenverkehr

Name	Signatur und Verschlüsselung im digitalen Dokumentenverkehr
Standard-Nummer	eCH-0092
Kategorie	Standard
Reifegrad	Definiert
Version	1.00
Status	Entwurf
Genehmigt am	
Ausgabedatum	2008-07-07
Ersetzt Standard	
Sprachen	Deutsch
Autoren	Daniel Muster Fachgruppe Technologie Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich Tel: 044 / 388 74 64, Fax: 044 / 388 71 80 www.ech.ch / info@ech.ch
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

Dieses Dokument empfiehlt, wie Dokumente gesichert im eGovernment ausgetauscht werden. Bei den vorliegenden Empfehlungen wurde auf die bestehenden Schweizerischen Erlasse zur elektronischen Signatur abgestützt und darauf verwiesen. Weiter sind die eCH Empfehlungen aus SAGA.ch und zu XML Security, welches zurzeit auch in Bearbeitung ist, ebenfalls berücksichtigt worden. Dort wo die bestehenden Erlasse unseres Erachtens zu wenig ausführlich sind, sind hier weitere Empfehlungen dazu festgehalten worden, wie der gesicherte Dokumentenverkehr abgewickelt werden soll.

Inhaltsverzeichnis

1	Status des Dokuments	4
1.1	Anwendungs- und Einsatzgebiet.....	4
1.2	Terminologie der Empfehlungen	4
2	Zielsetzung	6
3	Empfehlungen	7
3.1	Transport (Versand) der Dokumente.....	7
3.2	Elektronische Signatur	7
3.2.1	Signatur	7
3.2.1.1	Signatortyp	7
3.2.1.2	Signaturen von natürlichen Personen	8
3.2.1.3	Signaturen von nicht natürlichen Personen	9
3.2.2	Prüfung der Signaturen.....	9
3.2.3	Digitale ID	9
3.2.4	Schlüsselgenerierung, Sicherung des Signaturschlüssels	10
3.2.5	Schlüsselhinterlegung.....	10
3.3	Verschlüsselung.....	11
3.3.1	Grundsätzliches	11
3.3.2	Verschlüsselungstyp.....	11
3.3.3	Zertifikate für die Verschlüsselung.....	12
3.3.4	Digitale ID	12
3.3.5	Sicherung des privaten Schlüssels.....	12
3.3.6	Schlüsselhinterlegung.....	12
3.3.7	Schlüsseltransport (Transport des Session Key).....	13
3.3.8	Symmetrische Verschlüsselungsverfahren.....	13
3.4	Dokumentenformat.....	13
3.4.1	Eingabe von Rechtsschriften	13
3.4.2	Sonstiger Dokumentenverkehr	13
3.5	Authentisierung von Server oder Dienste der Behörde oder von Privaten.....	14
3.5.1	Sicherheitstechnologien.....	14
3.5.2	Zertifikate	14

3.5.3	Digitale ID	14
3.5.4	Schlüsselaufbewahrung.....	14
3.5.5	Schlüssel hinterlegung.....	15
4	Haftungsausschluss/Hinweise auf Rechte Dritter	16
5	Urheberrechte.....	16
	Anhang A – Referenzen & Bibliographie	17
	Anhang B – Abkürzungen	19
	Anhang C – Glossar	20
	Anhang D – Mitwirkende	22

1 Status des Dokuments

Das vorliegende Dokument ist ein **Entwurf**. Es wurde von den zuständigen Referenten des Expertenausschusses zur öffentlichen Stellungnahme freigegeben, damit es von interessierten Kreisen begutachtet und bei Bedarf versuchsweise umgesetzt werden kann. Feedback ist erwünscht und sollte an die Geschäftsstelle von eCH gerichtet werden. Die Fachgruppe berücksichtigt die eingegangenen Antworten oder begründet Ablehnungen schriftlich. Der Inhalt ist vom Expertenausschuss noch nicht genehmigt, er kann auf der Basis des eingehenden Feedbacks noch ändern und hat daher keine normative Kraft.

Im Rahmen der Vernehmlassung sind nicht nur Stellungnahmen oder Verbesserungsvorschläge zum Inhalt erwünscht, sondern auch eine Rückmeldung, ob dieses Dokument als Standard oder Best Practice verabschiedet werden soll.

1.1 Anwendungs- und Einsatzgebiet

Dieses Dokument will Empfehlungen zur Signatur und Verschlüsselung für die Sicherung des elektronischen Austausches von Dokumenten oder Urkunden abgeben. Die hier gemachten Empfehlungen richten sich an den Dokumentenaustausch zwischen den Behörden und Privaten (G2B), zwischen den Privaten (B2B) und Behörden untereinander (G2G) und behördenintern.

Unter einem digitalen Dokument wird hier ein elektronisches Dokument verstanden, welches die an einem Verwaltungs- oder Geschäftsprozessprozess beteiligten Akteure einander zu senden, um einen bestimmten Geschäftsfall auszulösen, zu protokollieren, zu bearbeiten oder zu erledigen. Zur Gewährleistung der Nachvollziehbarkeit sind die Dokumente meist zu archivieren. Beispiele sind: Ausgefüllte Antragsformulare, Erlasse, Evaluationen, Berichte, Registerauszüge, Rechnungen etc.

Das Dokument gibt aber keine Empfehlungen dazu ab, wann ein Dokument zu verschlüsseln oder zu signieren ist.

Der Leserkreis richtet sich an Verantwortliche, welche Sicherheitsmassnahmen im digitalen Dokumentenverkehr, definieren, umsetzen oder kontrollieren.

1.2 Terminologie der Empfehlungen

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

- **MUST (Deutsch "Muss")**: This word, or the terms "**REQUIRED**" or "**SHALL**", mean that the definition is an absolute requirement of the specification.

- **MUST NOT (Deutsch "Darf Nicht!"):** This phrase, or the phrase "**SHALL NOT**", mean that that definition is an absolute prohibition of the specification.
- **SHOULD (Deutsch "Sollte"):** 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 (Deutsch "Sollte Nicht"):** 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 (Deutsch "Kann angewandt werden", "Optional"):** This word, or the adjective "**OPTIONAL**", mean 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.)

Die hier vorgestellte Terminologie wird neben IETF unter anderem auch noch von OASIS, W3C übernommen und verwendet, ist aber in keiner Weise rechtlich bindend. Es handelt sich hier um Empfehlungen.

2 Zielsetzung

Das hier vorliegende Dokument will Empfehlungen aussprechen, damit die Interoperabilität und Sicherheit im Dokumentenverkehr im eGovernment Umfeld verbessert werden kann, insbesondere dort, wo die bestehenden Vorschriften noch unpräzise oder noch nichts reglementiert haben.

Dieses Dokument stützt sich auf die folgenden, bestehenden Schweizerischen Erlasse für den elektronischen Dokumentenverkehr zwischen den Behörden und Privaten (G2B), zwischen den Privaten (B2B) und Behörden untereinander (G2G) und behördenintern:

- ZertES
- VZertES
- EIDI-V
- [Ver. z. VwVG]. Verordnung zum VwVG
- [TAV-Dig]
- [TAV-MWST]
- ReRBGer (Reglement für die Eingabe von Rechtsschriften ans Bundesgericht)

EIDI-V ist zwar eine Vorschrift für die MWST konforme Rechnungsstellung zwischen Privaten, doch die Vollzugsbehörde sollte die an die Privaten gestellten Anforderungen selber auch einhalten und befolgen, insbesondere bei der elektronischen Kommunikation zu den Privaten; selbstverständlich sofern nicht wirklich zwingende Gründe dagegen sprechen. Sinnvoll übertragbar sind die Vorschriften aus OR, ZertES, EIDI-V und [TAV-MWST] unter anderem bei:

- Der elektronischen Rechnungsstellung zwischen der Behörde und den Privaten
- Dem Versand von Massenverfügungen, wenn nicht an Fristen gebunden
- Dem Austausch von Dokumenten im nicht streitigen Bundesverwaltungsverfahren
- Elektronische Unterschrift unter Verträgen und Urkunden

Dort, wo aber der digitale Dokumentenverkehr an Fristen gekoppelt ist, sind zusätzliche (technische) Vorschriften zu beachten. Grundsätzlich sind aber einige der hier aufgeführten Empfehlungen auch dort anwendbar.

Bei den Empfehlungen zum digitalen Dokumentenverkehr wird in diesem Dokument der Aspekt der Archivierung aber nicht berücksichtigt. Zur Archivierung sind weitere Dokumente bei einer anderen Fachgruppe des Vereins eCH angedacht.

Hinweis: Zu juristischen Begriffen rund um die elektronische Signatur sei der Leser auf das Glossar im eCH Dokument [DigSig] verwiesen, für übrige Begriffe und technische Abhandlung auf die Fachliteratur und auf das Glossar in diesem Dokument.

Das Dokument XML Security ist während der Erstellung dieses Dokuments noch in Bearbeitung, doch die Ergebnisse daraus sind fortlaufend berücksichtigt worden.

3 Empfehlungen

3.1 Transport (Versand) der Dokumente

Grundsätzlich werden in diesem Dokument lediglich der Schutz und folglich die Sicherheit des im Behördenverkehr ausgetauschten, digitalen Dokuments und nicht der gesicherte Transport oder der sichere Versand des Dokuments betrachtet.

Deswegen können die in SAGA aufgeführten Technologien und dort vorgeschlagenen Transportprotokolle ohne etwelche Sicherheitstechnologien eingesetzt werden, wie z.B. HTTP, SMTP, POP oder MIME (E-Mail Verkehr) im Attachement. Selbstverständlich kann (**MAY**) auch der Versand der Dokumente mit Hilfe von SSL/TLS, IPSEC oder S/MIME geschützt werden.

MUST: Sind aber Fristen im Verwaltungsverfahren oder im Geschäftsprozess beim elektronischen Austausch von Dokumenten zu beachten und einzuhalten, muss ein Transaktionsprotokoll gewählt werden, welches den Eingang und den Empfang der Dokumente quittiert, wie das OSCI- oder Presto-Protokoll. (Presto ist wie OSCI ein IT Kommunikationsstandard zum Austausch von Dokumenten). Die Quittungen sind entsprechend elektronisch zu signieren und der betreffenden Partei zuzustellen. Zur elektronischen Signatur s. Kapitel 3.2. (Die Erlasse [Ver. z. VwVG] und ReRBGer verwenden hierzu den Begriff Zustellplattform.)

Begründung: Ohne elektronische Quittungen können die Prozesse nachträglich nicht belegt werden.

Rechtlicher Hinweis: Bei Eingabe von Rechtsschriften gilt es über die Zustellplattformen zu beachten:

- Im streitigen Bundesverwaltungsverfahren **ist** eine entsprechende Plattform nach Art. 2 [Ver. z. VwVG] zu verwenden.
- Bei Eingabe von Rechtsschriften ans Bundesgericht, s. Art. 2 ReRBGer

3.2 Elektronische Signatur

Hier werden Empfehlungen abgegeben, welche die Signatur unter dem Dokument zum Schutz dessen Authentizität und Integrität betreffen, nicht aber die Authentisierung des Transports der Daten. Beides ist losgelöst und folglich separat zu betrachten. Der Einsatz von Signaturen kann sich als notwendig erweisen, wenn gesetzliche Vorschriften dies verlangen oder wenn vertrauliche Dokumente ausgetauscht werden müssen. In folgendem wird lediglich über elektronische Signaturen unter Dokumenten abgehandelt.

Zur Sicherheit vom Transport der Daten, s. auch die Empfehlungen aus SAGA.ch.

3.2.1 Signatur

3.2.1.1 Signaturtyp

Die Signatur besteht nicht nur aus einem Hashwert, welcher mit dem Signaturschlüssel chiffriert worden ist, sondern auch aus weiteren notwendigen Zusatzinformationen. Welche Zu-

satzinformationen zu verwenden und wie diese zu gliedern sind, kann unterschiedlich sein und folglich zu technischen Inkompatibilitäten führen.

MUST: PKCS#7 Signaturen sind gemäss RFC 3852 einzusetzen. Ausnahme bilden XML Dokumente, weil es hierfür entsprechende Standards gibt.

Begründung: Es handelt sich beim RFC 3852 um einen weit eingesetzten und umgesetzten Standard, im Bereich der elektronischen Signatur:

SHOULD: Werden XML Dokumente ausgetauscht, dann sollen aber die Empfehlungen aus dem eCH Dokument zu XML Security beachtet werden. (Dieses Dokument befindet sich aber zurzeit noch in Bearbeitung)

3.2.1.2 Signaturen von natürlichen Personen

Hier wird empfohlen, welche Mindestanforderung an die Qualität resp. an die Sicherheit der elektronischen Signatur im Dokumentenverkehr gestellt wird.

Rechtlicher Hinweis: Bei **Eingabe von Rechtsschriften** sind im streitigen Bundesverwaltungsverfahren Signaturen gemäss Art. 6 Abs. 1 [Ver. z. VwVG] einzusetzen, für Rechtsschriften ans Bundesgericht, gemäss. Art. 4 Abs. 3 ReRBGer.

Rechtlicher Hinweis: Bei **Zustellung von Verfügungen oder Entscheidungen** (Art. 34 Abs. 1^{bis} VwVG) **sind** im streitigen Bundesverwaltungsverfahren Signaturen gemäss Art. 6 Abs. 1 [Ver. z. VwVG] einzusetzen.

SHOULD: Wird im streitigen (Bundes)Verwaltungsverfahren von der Option nach Art. 6 Abs. 1 [Ver. z. VwVG] Gebrauch gemacht, dann sollten Signaturen gemäss Art. 2 Abs. 2 lit. a EIDI-V angewandt werden.

Information: Die Urteile des Bundesgerichts, welche elektronisch den Parteien zugestellt werden, tragen gemäss Angaben des Bundesgerichts die anerkannt qualifizierte Signatur des Gerichtsschreibers. Die elektronische Zustellung der Gerichtsurkunden an die Zustellplattform erfolgt dann mit einer fortgeschrittenen Signatur der Gerichtskanzlei.

MUST: Die Signaturen unter Dokumente erfüllen die Anforderungen gemäss Art. 2 EIDI-V.

Begründung: Es ist nicht ohne weitere Begründung einsichtig, dass im geschützten Dokumentenverkehr zwischen Behörden und Privaten und behördenintern weniger Sicherheitsanforderungen (mit den damit verbundenen Kosten) an die elektronische Signatur gestellt werden als bei der Zustellung von MWST konformen Rechnungen, damit den Vorsteuerabzug geltend gemacht werden kann.

Im Sinne der Usability und Anwendungssicherheit sollten nicht x-verschiedene Zertifikats- und Signaturtypen eingesetzt werden, ansonsten dies den Anwender überfordert oder verunsichert.

Anmerkung: Die qualifizierten elektronischen Signaturen nach Art. 14 Abs. 2^{bis} OR sind aus der Warte Sicherheitstechnik mit den Fortgeschrittenen nach Art. 2 Abs. 2 EIDI-V praktisch gleich. Sie unterscheiden sich aber in den Haftungsbestimmungen bei der Verwendung der Signatur und bei der Herausgabe und Handhabung der Zertifikate.

SHOULD: Werden durch die Dokumente Rechtsgeschäfte beglaubigt, dann sollten qualifizierte elektronische Signatur nach Art. 14 Abs. 2^{bis} OR verwendet werden.

Begründung: Damit vorbehaltlos (d.h. ohne spezielle vorgängige Vereinbarung) eine der Handschrift gleichgestellte Signatur im privaten Geschäftsverkehr anerkannt wird, sind entsprechende Sicherheitsanforderungen daran gestellt worden. Entsprechende Sicherheitsmassnahmen sollten zwecks Verlässlichkeit auch im Geschäftsverkehr zwischen Behörden und den Privaten und zwischen den Behörden beim Einsatz der elektronischen Signatur eingehalten werden.

3.2.1.3 Signaturen von nicht natürlichen Personen

Unter einer elektronischen Signatur von nicht natürlichen Personen fallen unter anderem digitale Unterschriften von juristischen Personen oder von Informatiksystemen wie z.B. ein Server oder Dienste.

MUST: Für den Massenversand von Verfügungen und das Quittieren für den Erhalt oder die Zustellung von Rechtsschriften im streitigen Verwaltungsverfahren sind ebenfalls die Mindestvorschriften gemäss Art. 2 Abs. 2 lit. a EIDI-V einzuhalten.

Begründung: Es ist nicht ohne weitere Begründung einsichtig, dass bei der Zustellung von Dokumenten im Verwaltungsprozess weniger Sicherheitsanforderungen (mit den damit verbundenen Kosten) an die elektronische Signatur gestellt werden als bei der Zustellung der MWST konformen Rechnungen, damit der Vorsteuerabzug geltend gemacht werden kann.

3.2.2 Prüfung der Signaturen

Hier wird empfohlen, mit welcher Qualität die Signaturen zu prüfen sind.

MUST: Anforderung an die Signaturerstellung gemäss Art. 3 Abs. 1 lit. b, und die Erstellung eines Prüfprotokolls gemäss Art. 3 Abs. 1 lit. c EIDI-V.

Begründung: Es ist nicht ohne weitere Begründung einsichtig, dass im Dokumentenverkehr zwischen Behörden und Privaten und behördenintern weniger Sicherheitsanforderungen (mit den damit verbundenen Kosten) an die Prüfung der elektronischen Signatur gestellt werden als bei der Zustellung der MWST konformen Rechnungsstellung für den Vorsteuerabzug.

Hinweis: Zur Prüfung der elektronischen Signatur und der Erhaltung der Beweiskraft der elektronischen Signatur siehe auch Kapitel 7, insbesondere 7.3.2 und 7.3.3 [DigSig]. In [DigSig] wird auch auf die entsprechenden technischen Standards (RFC) zur Prüfung der elektronischen Signatur verwiesen.

3.2.3 Digitale ID

Als digitale Identitäten (ID) werden digitale Angaben zur Person (natürlich oder juristisch), zu einer Behörde, zu einer öffentlich-rechtlichen oder privaten Institution im Zertifikat bezeichnet. Um ein Durcheinander an ID und die daraus möglicherweise resultierenden Sicherheitslöcher zu vermeiden, werden Minimalanforderungen an die ID hier empfohlen.

SHOULD: Digitale ID sind gemäss Kapitel 4.1 [TAV-MWST] einzusetzen.

Grund: Aus ökonomischen Gründen sollen Zertifikate nicht nur gültig beim elektronischen Versand von Rechnungen eingesetzt werden, sondern auch beim Dokumentenverkehr. Deshalb sind die Anforderungen an die digitale ID übernommen worden, damit nicht gegebenenfalls pro eGovernment Anwendung ein separates Zertifikat zwecks Verifikation der Signatur ausgestellt werden muss.

3.2.4 Schlüsselgenerierung, Sicherung des Signaturschlüssels

Die Schlüsselgenerierung zur Erzeugung und Prüfung der elektronischen Signatur sind sicherheitsrelevant. Deswegen werden hierzu Empfehlungen abgegeben.

Rechtlicher Hinweis: Für qualifizierte Zertifikate s. die Bestimmungen zu [TAV-DigSig], VZertES und ZertES.

SHOULD: Die Schlüsselgenerierung für fortgeschrittene Signaturen sollte gemäss Art. 2 Abs. 2 lit. b EIDI-V erfolgen.

Begründung: Es ist nicht ohne weitere Begründung einsichtig, dass bei der Zustellung von Dokumenten im Verwaltungsprozess weniger Sicherheitsanforderungen (mit den damit verbundenen Kosten) an die elektronische Signatur gestellt werden als bei der Zustellung der MWST konformen Rechnungen, damit der Vorsteuerabzug geltend gemacht werden kann.

3.2.5 Schlüsselhinterlegung

Als Schlüsselhinterlegung wird in diesem Dokument die gesicherte Anfertigung einer oder mehrerer Kopien des privaten Schlüssels verstanden.

Rechtlicher Hinweis: Eine Kopie des Schlüssels für die Erstellung qualifizierter elektronischer Signaturen darf nicht angefertigt und darf folglich nicht hinterlegt werden, s. Art. 6 VZertES.

SHOULD NOT: Die Schlüssel der fortgeschrittenen elektronischen Signaturen sollten nicht hinterlegt werden.

Begründung: Kopien anzufertigen und zu hinterlegen enthalten meist Sicherheitsrisiken.

3.3 Verschlüsselung

Da im eGovernment auch bezüglich Vertraulichkeit sensitive Informationen ausgetauscht werden, **aber dazu keine detaillierten Bestimmungen erlassen worden sind**, werden hier entsprechende Empfehlungen zum Schutz der Dokumente abgegeben. Die Dokumente mit den sensitiven Informationen sollen grundsätzlich mittels Public Key Verfahren geschützt werden.

3.3.1 Grundsätzliches

Wird ein als vertraulich oder gar als geheim klassifiziertes Dokument verschlüsselt und dann versandt, so ist es wichtig, dass der Empfänger weiss, wer ihm das sensitive Dokument zugestellt hat und dass der Inhalt nicht verändert worden ist. Wenn der Absender für den Empfänger unbekannt ist, kann oder muss dieser mit Fug und Recht vermuten, dass es eine Sicherheitslücke besteht. Um solche Unklarheiten zu vermeiden, wird folgende Empfehlungen abgegeben:

MUST: Vertraulich oder geheim klassifizierte Dokumente müssen vor der Verschlüsselung signiert werden.

3.3.2 Verschlüsselungstyp

Die zu versendende Datei besteht nicht nur aus:

- dem verschlüsselten Dokument, welches mit einem zufälligen erzeugten Schlüssel (Session Key) verschlüsselt worden ist.
- und dem mit dem öffentlichen Schlüssel des Empfängers chiffrierten Verschlüsselungsschlüssel (verschlüsselter Session Key).

Es werden auch noch Zusatzinformationen beigefügt, wie die ID des Empfängers und die Angaben zum Verschlüsselungsverfahren. Wie diese Zusatzinformationen zu gliedern und anzufügen sind, kann unterschiedlich sein und folglich zu technischen Inkompatibilitäten führen.

MUST: PKCS#7 Verschlüsselung ist gemäss RFC 3852 einzusetzen.

Begründung: Es handelt sich beim RFC 3852 um einen weit eingesetzten und umgesetzten Standard, im Bereich der elektronischen Signatur:

Ausnahme: Werden vertrauliche XML Dokumente ausgetauscht, dann müssen die Empfehlungen aus dem eCH Dokument zu XML Security beachtet werden. (Dieses Dokument befindet sich aber zurzeit in Bearbeitung.)

3.3.3 Zertifikate für die Verschlüsselung

Es ist für die Sicherheit zentral und enorm wichtig, dass man die vertraulichen Informationen an den dafür vorgesehenen Adressaten zustellt, entsprechend die Information (besser Session Key) mit dessen Public Key verschlüsselt und die Information **nicht** an eine Person zustellt, welche für den Erhalt der Information nicht vorgesehen ist.

Deswegen werden hier entsprechende Empfehlungen zum Zertifikat und der darin enthaltenen ID des Empfängers des verschlüsselten Dokuments gemacht.

MUST: Gemäss Art. 2 Abs. 2 EIDI-V, ausser lit. a Ziff. 3. Zertifikatsinhalt sinngemäss Kapitel 3.4.2 Absatz b [TAV-MWST].

3.3.4 Digitale ID

Als digitale Identitäten (ID) werden digitale Angaben zur Person im Zertifikat bezeichnet.

MUST: Gemäss Kapitel 4.1 [TAV-MWST]

Grund: Aus ökonomischen Gründen sollen Zertifikate nicht nur gültig beim elektronischen Versand von Rechnungen eingesetzt werden, sondern auch beim Dokumentenverkehr. Deshalb sind die Anforderungen an die digitale ID übernommen worden, damit nicht gegebenenfalls pro eGovernment Anwendung ein separates Zertifikat zwecks Verifikation der Signatur ausgestellt werden muss.

3.3.5 Sicherung des privaten Schlüssels

MUST: Gemäss Art. 2 Abs2 lit. b EIDI-V

Anmerkung: Es macht keinen Sinn, den privaten Schlüssel zur Entschlüsselung des Dokuments in einem anderen Medium aufzubewahren, als die privaten Schlüssel für die Signaturerstellung. Eine getrennte Aufbewahrung würde die Handhabung erschweren und somit verkomplizieren.

3.3.6 Schlüsselhinterlegung

Als Schlüsselhinterlegung wird in diesem Dokument die gesicherte Anfertigung einer oder mehrerer Kopien des privaten Schlüssels verstanden.

Damit die verschlüsselt abgelegten Daten zuverlässig wieder entschlüsselt und zugänglich gemacht werden können, werden entsprechende Empfehlung für die Schlüsselhinterlegung (Backup des privaten Schlüssels) hier abgegeben.

MUST: Der private Schlüssel zur Entschlüsselung der Daten muss gemäss Art. 3 Abs. 1 lit. e EIDI-V aufbewahrt werden. Da u.a. bei einem Verlust oder bei einem Defekt des Aufbewahrungsmediums für den privaten Schlüssel der private Schlüssel nicht mehr verwendet werden kann, empfiehlt es sich, ein **gesichertes Backup** des privaten Schlüssels zur Entschlüsselung der Daten anfertigen zu lassen.

3.3.7 Schlüsseltransport (Transport des Session Key)

Hier wird festgelegt, wie der asymmetrische Schlüssel, welcher das Dokument verschlüsselt hat, gesichert an den Empfänger des Dokuments transportiert werden soll.

MUST: PKCS#7 Verschlüsselung gemäss RFC 3852 und SAGA.ch.

Begründung: Es handelt sich beim RFC 3852 um einen weit eingesetzten und umgesetzten Standard, im Bereich der elektronischen Signatur. SAGA ist ein vom IRB (Informatikrat des Bundes) verabschiedeter Standard.

3.3.8 Symmetrische Verschlüsselungsverfahren

Verschiedene Verschlüsselungsverfahren können eingesetzt werden. Deshalb wird Folgendes empfohlen.

MUST: Die in SAGA.ch empfohlenen Verfahren sind einzusetzen.

Begründung: Damit stützt man sich auf SAGA ab, einen vom IRB verabschiedeten Standard.

3.4 Dokumentenformat

3.4.1 Eingabe von Rechtsschriften

Rechtlicher Hinweis: Ans Bundesgericht: XML und PDF gemäss Art. 4 Abs. 3 ReRBGer, wobei hier die INCA Mail Plattform der Schweizerischen Post eingesetzt werden muss. Hierzu wird von der Schweizerischen Post die Client SW als Produkt ausgeliefert.

Im streitigen Bundesverwaltungsverfahren: PDF/A gemäss Art. 9 Abs. 2 der Verordnung zum Verwaltungsverfahren [Ver. z. VwVG].

3.4.2 Sonstiger Dokumentenverkehr

SHOULD: Verwendet werden sollten Dokumentenformate, welche es nicht ermöglichen, dass gewisse Informationen unterdrückt, zusätzlich angezeigt oder verändert werden können, ohne dass dabei die Signatur unter dem Dokument nicht an Gültigkeit verliert.

MUST: Dateiformate, welche in [BAR-Dateiformat] aufgeführt sind, wie auch ZIP, XML und PDF.

Anmerkung: Im Unterschied zu den anderen Datenformaten erlauben PDF und PDF/A die Verwendung von embedded Signaturen.

Werden XML Dokumente verwendet und ausgetauscht, dann **müssen** die Empfehlungen aus dem eCH Dokument zu XML Security beachtet werden.

Anmerkung: ZIP ist ein Kompressionsverfahren für Dateien, welches ein gleichnamiges Fileformat erzeugt. Wird eine Datei vor der Verschlüsselung komprimiert, so erhöht dies die Sicherheit der Verschlüsselung.

3.5 Authentisierung von Server oder Dienste der Behörde oder von Privaten

Es sind auch Anwendungen denkbar, bei denen Dokumente von einem Server heruntergeladen werden, wobei die Dokumente selber nicht authentisiert werden, aber die Verbindung zum Server.

3.5.1 Sicherheitstechnologien

MUST: s. SAGA.ch u.a. zu SSL/TLS und IPSEC

Begründung: Damit stützt man sich auf SAGA ab, einen vom IRB verabschiedeten Standard.

3.5.2 Zertifikate

MUST: Gemäss Art. 2 Abs. 2 EIDI-V, ausser lit. a Ziff. 3. Zertifikatsinhalt sinngemäss Kapitel 3.4.2 Absatz b [TAV-MWST].

Begründung: Es ist nicht ohne weitere Begründung einsichtig, dass im geschützten Dokumentenverkehr zwischen Behörden und Privaten und behördenintern weniger Sicherheitsanforderungen (mit den damit verbundenen Kosten) an die elektronische Signatur und somit an die Authentisierung gestellt werden als bei der Zustellung von MWST konformen Rechnungen, damit den Vorsteuerabzug geltend gemacht werden kann.

3.5.3 Digitale ID

Als digitale Identitäten (ID) werden digitale Angaben zum Dienst im Zertifikat bezeichnet.

SHOULD: Gemäss Kapitel 4.1 [TAV-MWST]

Begründung: Aus ökonomischen Gründen sollen Zertifikate nicht nur gültig beim elektronischen Versand von Rechnungen eingesetzt werden, sondern auch beim Dokumentenverkehr. Deshalb sind die Anforderungen an die digitale ID übernommen worden, damit nicht gegebenenfalls pro eGovernment Anwendung ein separates Zertifikat zwecks Verifikation der Signatur ausgestellt werden muss.

3.5.4 Schlüsselaufbewahrung

MUST: Gemäss Art. 2 Abs. b ELDI-V.

Begründung: Es ist nicht ohne weitere Begründung einsichtig, dass im geschützten Dokumentenverkehr zwischen Behörden und Privaten und behördenintern weniger Sicherheitsanforderungen (mit den damit verbundenen Kosten) an die elektronische Signatur und somit an die Authentisierung gestellt werden als bei der Zustellung von MWST konformen Rechnungen, damit den Vorsteuerabzug geltend gemacht werden kann.

3.5.5 Schlüsselhinterlegung

MUST NOT: Schlüssel dürfen nicht hinterlegt werden.

Begründung: Das Ersetzen der Schlüssel für die Authentisierung bereitet einen relativ kleinen Aufwand. Deswegen spricht kein Grund dafür, die Sicherheit mit der Hinterlegung des Schlüssels zu verkleinern.

4 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche **eCH** referenziert, 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.

5 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende mittels spezieller, schriftlicher Vereinbarung, 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

- [Bea] Bertsch Andreas, Digitale Signaturen, Springer Verlag, 2002, ISBN 3 540 42351 6
- [Mud] Muster Daniel, Digitale Unterschriften und PKI, 3. Auflage 2006, ISBN 3 9522387 3 2

Gesetzestexte (www.admin.ch Systematische Rechtssammlung)

- [TAV-DigSig] Technische und administrative Vorschriften des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)
- [TAV-MWST] Technische und administrative Vorschriften des EFD vom 12. Oktober 07 über Zertifizierungsdienste im Bereich EIDI-V im Zusammenhang mit der Ausstellung von Zertifikaten basierend auf fortgeschrittenen Zertifikaten (SR 641.201.11)
- [Ver. z. VwVG] Verordnung vom 17. Oktober 2007 über die elektronische Übermittlung im Verwaltungsverfahren (SR 172.021.2)
- BGG Bundesgesetz vom 17. Juni 2005 über das Bundesgericht (SR 173.110)
- EIDI-V Verordnung des EFD vom 30. Januar 2002 über die elektronisch übermittelten Daten und Informationen (SR 641.201.1)
- OR Schweizerisches Obligationenrecht vom 30. März 1911 (SR 220)
- ReRBGer Reglement des Bundesgerichts vom 5. Dezember 2006 über den elektronischen Rechtsverkehr mit Parteien und Vorinstanzen (SR 173.110.29)
- VGG Bundesgesetz vom 17. Juni 2005 über das Verwaltungsgericht (SR 173.32)
- VwVG Bundesgesetz vom 20. Dezember 1968 über das Verwaltungsverfahren (SR 172.021)
- VZertES Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032)
- ZertES Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)

Technische Standard des Bundes (www.admin.ch)

- [BAR-Dateiformat] Schweizerisches Bundesarchiv (www.bar.admin.ch), Archivtaugliche Dateiformate, Standards für die Archivierung digitaler Unterlagen, <http://www.bar.admin.ch/dienstleistungen/00516/00517/index.html?lang=de>

eCH (www.ech.ch)

- eCH-0014 SAGA.ch
- [DigSig] Wissenswertes zur Anwendung der elektronischen Signatur

IETF Standards (www.ietf.org)

RFC 1939	Post Office Protocol - Version 3
RFC 1945	Hypertext Transfer Protocol 1.0
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2046	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
RFC 2047	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
RFC 2048	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2251	LDAPv.3 Lightweight Directory Access Protocol
RFC 2311	S/MIME Version 2 Message Specification und zugehörige
RFC 2616	Hypertext Transfer Protocol 1.1
RFC 2634	Enhanced Security Services for S/MIME
RFC 2821	Simple Mail Transfer Protocol
RFC 2849	The LDAP Data Interchange Format
RFC 2965	HTTP State Management Mechanism
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3384	LDAP (version 3) Replication Requirements
RFC 3739	Qualified Certificates Profile
RFC 3850	S/MIME v.3.1 Certificate Handling
RFC 3851	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1
RFC 3852	Cryptographic Message Syntax (CMS)

ISO Standards (www.iso.org)

ISO 15929: 2002	Graphic technology -- Prepress digital data exchange -- Guidelines and principles for the development of PDF/X standards
ISO 15930 Series 1-6	Graphic technology -- Prepress digital data exchange
ISO 19005-1: 2005	Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)

ITU Standards (www.itu.org)

ITU-T Information Technology - Open Systems Inter-connections - Public Key
X.509v.3 and Attribute Certificate Framework

Online Service Computer Interface (www.osci.de)

OSCI-Transport v.1.2 Online Service Computer Interface

Ministère de France

Presto (Protocole D' Echange Standard et Ouvert),
https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/a131_b_protocole/public/view

Anhang B – Abkürzungen

Abs	Absatz
Art.	Artikel
bzw.	beziehungsweise
CA	Certification Authority, zu Deutsch Zertifizierungsstelle
CEN	Comité Européen de Normalisation
CRL	Certificate Revocation List
CSP	1) Cryptographic Service Provider 2) Certificate Service Provider
ETSI	European Telecommunications Standards Institute
FG	Fachgruppe
G2B	Government to Business
G2C	Government to Citizen
G2Con	Government to Consumer
G2G	Government to Government
G2O	Government to Organisation
G-I	Government internal
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ID	Identität
IRB	Informatikrat des Bundes
LDAP	Lightweight Directory Access Protocol
lit.	litera (Buchstabe)
OSCI	Online Services Computer Interface
PC	Personal Computer

PDF	Portable Document Format
PDF/X	PDF Exchange (Subset of PDF)
PK	Public Key
PKI	Public Key Infrastructure, Public Key Infrastruktur
s.	Siehe
S/MIME	Secure Multipurpose Internet Mail Extension
SAGA.ch	Standards und Architekturen für eGovernment Anwendungen Schweiz
SMTP	Simple Mail Transfer Protocol
TIFF	Tagged Image File Format
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
Ver.	Verordnung
XML	Extensible Markup Language
z.B.	zum Beispiel

Anhang C – Glossar

Das hier vorgestellte Glossar setzt sich aus Begriffen und den dazugehörigen Erklärungen zusammen, welche von der Web Page des Instituts für Wirtschaft und Verwaltung (www.iwv.ch) in Bern stammen und für den hier vorliegenden Zweck angepasst worden sind.

Administration	Im Zusammenhang mit eGovernment entspricht „Administration“ der Verwaltung im Sinne einer Abgrenzung zu Exekutive, Legislative, Judikative und dem Staat im umfassenden Sinne. Ausschliessend formuliert gilt als öffentliche Verwaltung alles, was nicht Gesetzgebung, Rechtsprechung ist. Grundsätzlich gilt die Administration als eine öffentliche Verwaltung oder als ein Vollzugsorgan, das durch die Regierung gesteuert und durch die Justiz kontrolliert wird.
Amtsgang, virtuel- ler	Der virtuelle Amtsgang beschreibt, wie Amtsgeschäfte mit Hilfe der Informations- und Kommunikationstechnologie (IKT) erledigt werden können.
Authentisierung	Vorgang zur Bestimmung der Authentizität.
Best Practice	„Best Practice“ ist eine allgemein anerkannte, in der Praxis umgesetzte und sehr bewährte Lösung. Dabei werden Produkte, Dienstleistungen, (IT) Realisierungen auf Grund von einheitlichen Qualitätskriterien miteinander verglichen.
Certificate Revo- cation List	Certificate Revocation List, kurz CRL, englischer Fachausdruck für die von der CA (s. Certification Authority) beglaubigte Liste der für ungültig erklärten Zertifikate. Die Beglaubigung erfolgt mittels digitaler Signatur.
Certification Authority	Certification Authority, kurz CA, zu Deutsch auch Zertifizierungsstelle oder Zertifikatsaussteller, ist eine Instanz, welche die Beglaubigung von Schlüsseln für PK Verfahren mittels Zertifikaten (s. Zertifikat) vornimmt.

Dienst	Ein Dienst, engl. Service, ist eine konkrete und genau definierte eGovernment Anwendung, welcher einen ganzen „Geschäftsfall“ abhandelt, wie z.B. die elektronische Eingabe von Dokumenten an ein Gericht.
Diffie Hellman	Ein von W. Diffie und W. Hellman entwickeltes Public Key Verfahren.
DMZ	Der Begriff „DMZ“ steht für Demilitarisierte Zone (engl. Demilitarised Zone) und wird in der IT Security im Bereich Firewall verwendet. DMZ sind vom internen Netz und vom Internet abgetrennte Netzbereiche. Sie sind nicht so sicher, wie das interne, aber auch nicht so unsicher wie das externe Netz. Im Netzbereich DMZ werden z.B. Server installiert, welche E-Mails vom internen Netz ans Internet weiterreichen und umgekehrt oder welche die HTTP Pakete vom internen ans externe Netz weiterreichen und umgekehrt. In die DMZ werden z.B. auch der Web-Server oder der Inhaltsprüfungsserver verlegt, welcher die Inhalte von HTTP oder E-Mail Paketen auf Viren prüft.
eAdministration	eAdministration bezeichnet den Einsatz der Informations- und Kommunikationstechnologien (IKT) zur Unterstützung des amtlichen Geschäftsverkehrs.
eBusiness	Unter eBusiness wird die Abwicklung von Geschäftsprozessen mit Hilfe von Informations- und Kommunikationstechnologie (IKT) verstanden.
eCommerce	eCommerce umfasst den Teil des eBusiness, welcher sich mit der Vereinbarung und Abwicklung rechtsverbindlicher Geschäftstransaktionen befasst. Es wird zwischen drei Beziehungstypen unterschieden: <ul style="list-style-type: none">- Business-to-Business (Unternehmen – Unternehmen)- Business-to-Consumer (Unternehmen – Endverbraucher)- Consumer-to-Consumer (Spezialfall, wo das Unternehmen nur als Vermittler auftritt, z.B. Online-Auktionen).
eGovernment	eGovernment umfasst die Unterstützung der Beziehungen, Prozesse und der politischen Partizipation innerhalb aller staatlichen Ebenen sowie gegenüber allen Anspruchsgruppen durch Bereitstellung von Interaktionsmöglichkeiten mittels elektronischer Medien.
electronic Public Services (ePS)	Abgabe von öffentlichen Leistungen an die Leistungsempfänger, Privatpersonen oder Unternehmungen über lokale, regionale oder nationale Portale.
elektronische Signatur	Die elektronische, auch digitale, Signatur schützt die Authentizität und Integrität einer Datei. Die elektronische Signatur basiert auf dem Hashwert (s. Hashwert) der zu schützenden Datei und einem PK Verfahren (s. PK Verfahren). Der Hashwert der Datei wird mit dem privaten Schlüssel verschlüsselt. Das Resultat davon wird als elektronische Signatur bezeichnet.
Elliptische Kurven	Ein von N. Koblitz und V.S. Miller unabhängig voneinander entwickeltes Public Key Verfahren.
S/MIME	Sicherheitstechnologie und -standard von der IETF für die Absicherung der E-Mail Kommunikation.
SAGA.ch	SAGA.ch steht für Standards und Architekturen für eGovernment Anwendungen Schweiz und ist ein vom Verein eCH hergestelltes Dokument, welches in verdichteter Form die technischen Richtlinien für die Umsetzung von eGovernment Anwendungen in der Schweiz darstellt.

Service Public	Unter Service Public wird meist die Sicherstellung einer flächendeckenden und Kosten günstigen Grundversorgung mit Infrastrukturleistungen verstanden. Diese Leistungen können sowohl materieller (Verkehr, Telekommunikation, Post, Energie usw.) als auch immaterieller Art sein (Gesundheit, Bildung, Kultur etc.). Unerheblich ist dabei, ob die Leistungserbringung durch die öffentliche Hand selbst oder durch private Dritte erfolgt (auf Basis Leistungsvereinbarung/-auftrag).
SSL/TLS	SSL steht für den englischen Ausdruck Secure Socket Layer und ist eine von Netscape entwickelte Sicherheitstechnologie, ursprünglich zur Sicherung des HTTP-Protokolls. SSL hat sich zum de facto Standard erhoben. TLS, Transport Layer Security, ist eine von der IETF standardisierte Sicherheitstechnologie und basiert etwa zu 95% auf SSL, doch die beiden Verfahren sind untereinander nicht kompatibel.
Transaktion	<p>1) Transaktionen umfassen die Auslösung von Prozessen der Güterbewegung oder der Erbringung von Dienstleistungen bzw. den gesamten Nachrichtenaustausch, welcher während der Durchführung eines solchen Prozesses notwendig ist.</p> <p>2) Von Transaktionen wird in der Technik gesprochen, wenn</p> <ul style="list-style-type: none"> - mehrere Instanzen eingebunden sind. - Datenänderungen bei unterschiedlichen Instanzen vorgenommen werden. - Datenkonsistenz nach der Aktion vorhanden sein muss, ansonsten die Aktion rückgängig gemacht werden muss.
Unterschrift, digitale	s. Signatur, digitale.
Use Case	Ein Use Case ist eine konkrete IT Anwendung oder ein konkreter Ablauf, welcher durch die IT abgewickelt wird.
WWW	World Wide Web. Ein Internetdienst zur plattformunabhängigen Bereitstellung von untereinander verbundenen Dokumenten.
XML	XML steht für eXtensible Markup Language und ist eine "vereinfachte" Version der Standard Generalized Markup Language (SGML). Die Entwicklung von XML begann 1996, und seit Februar 1998 ist XML ein W3C-Standard. XML soll es den Web-Site-Programmierern erleichtern, SGML-Anwendungen zu schreiben und dabei eigene Dokumententypen festzulegen. XML bietet viele Mechanismen, welche u.a. die Datenverwaltung im Netz erleichtern sollen.

Anhang D – Mitwirkende

Josef A. Schmid	Informatikstrategieorgan des Bundes ISB
Marc Holitscher	Microsoft Schweiz GmbH
Ernest Peter	Net Consult AG
Daniel Gabi	Schweizerische Bundeskanzlei
Erich Vogt	SignPool Group AG
Eric Dubuis	Berner Fachhochschule

André von Arx

Oracle Software (Schweiz) GmbH

Norbert Bollow

Schweizerische Internet Usergroup SIUG

Reto Gantenbein

Sun Microsystems Schweiz AG