

Relevantes und Wissenswertes zur Anwendung der elektronischen Signatur (im eGovernment)

Name	Relevantes und Wissenswertes zur Anwendung der elektronischen Signatur (im eGovernment), ein Dossier
Version	1.3 (20. Dezember 2005)
Status	Revidiertes Arbeitsergebnis der eCH Fachgruppe Digitale Signatur („White Paper“) Das vorliegende Dokument enthält den endgültigen Text, welcher die Fachgruppe Digitale Signatur erarbeitet hat. Es handelt sich um ein Dokument der Fachgruppe, welches dem Expertenausschuss von <i>eCH</i> nicht unterbreitet wird.
Basiert auf	u.a. auf dem Gutachten des Bundesamtes für Justiz VPB 63.46
Sprache	Deutsch
Herausgeber	Verein <i>eCH</i> , Laupenstrasse 18a, 3008 Bern T 031 560 00 20, F 031 560 00 25 www.ech.ch / info@ech.ch
Autoren	Daniel Muster (Bit Pattern Security) Jean-Maurice Geiser (BAKOM) Maria Winkler (IT & Law Consulting GmbH)
Weitere Mitwirkende	Attila Laczko (EVD) Christian Jenny (BAKOM) Eduard Mumprecht (FH Zürich Winterthur) Esther Peterhans (DMZ des Kantons Zürich) Joseph Doekbrijder (SwissSign AG) Michael R. Vetterli (SignPool GmbH), Leiter der Fachgruppe Lorenz Neher (Swisscom Solutions AG)
Redaktionelle Hoheit	Fachgruppe Digitale Signatur Verein <i>eCH</i>
Ansprechpartner	Michael Vetterli, SignPool GmbH, 8307 Effretikon, michael.vetterli@signpool.com Daniel Muster, 8048 Zürich, daniel.s.muster@bluewin.ch Verein <i>eCH</i> , Laupenstrasse 18a, 3008 Bern, T 031 560 00 20, F 031 560 00 25 www.ech.ch / info@ech.ch

Zielsetzung des Dokumentes

Das Dokument soll Antwort auf verschiedenste (rechtliche) Fragen geben, welche sich bei der Implementation der elektronischen Signatur stellen. Insbesondere sollen die im Fachgruppenantrag gestellten Fragen abgehandelt werden. In diesem Sinne soll das Dokument **eine Hilfe in der Gestaltung der IT-Prozesse sein.**

Doch viele praktische Fragen lassen sich meistens (noch) nicht über die bestehenden Erlasse und Vorschriften beantworten. Deswegen sind dort als Antwort auf diese Fragen **Empfehlungen** im Sinne von Ratschlägen abgegeben worden. **Ratschläge** sind in **folgenden Bereichen** abgegeben worden:

- Mindestvorschriften in der Nutzung von Zertifikaten für die Verschlüsselung (s. Kapitel 4.3.3)
- Notwendigkeit (s. Kapitel 5.3) und Mindestvorschriften beim Einsatz von Funktionszertifikaten (s. Kapitel 5.4)
- Sicherheitsanforderungen beim Leisten (s. Kapitel 6.4) und Verifizieren elektronischer Signaturen (s. Kapitel 7.2)
- Archivierung von elektronisch signierten Dokumenten (s. Kapitel 7.3 „Lösungsansätze“)
- Tipps bei der Namensgebung im Zertifikat (s. Kapitel 6.6)
- Tipps bei der Nutzung von vertraulichen E-Mails in Zusammenhang mit Spam (s. Kapitel 6.5)

Eine Ablehnung ist im Bereich der Nutzung verschiedener **Zertifikatsklassen** (im Sinne von verschiedenen Vertrauens- oder Güteklassen, engl. Trustlevel) im **eGovernment** Umfeld abgegeben worden (s. Kapitel 3.4.4).

Es kann durchaus sein, dass ein Mitglied dieser Fachgruppe, dessen Behörde oder dessen Unternehmen nicht die gleiche Meinung oder Ansicht zu bestimmten Aussagen in diesem Dokument vertreten.

Themenüberblick

Im Antrag der Fachgruppe (FG) „Digitale Signatur“, kurz DigSig, sind eine Reihe von Fragen aufgelistet, welche im Rahmen der Fachgruppensitzung besprochen worden sind. Die Antworten auf die betreffenden Fragen sind in diesem Dokument in den folgenden Themenblöcken zusammengefasst worden:

- Rechtswirksamkeit elektronischer Signaturen
- Serverzertifikate (Funktionszertifikate)
- (Langfristige) Prüfung elektronischer Signaturen und Archivierung elektronisch signierter Dokumente
- Verhinderung von Spam beim Austausch von vertraulichen Nachrichten
- Anforderungen an die Identitätskennungen im eGovernment Umfeld

Im Kapitel 9 sind die Antworten der im FG Antrag aufgeworfenen Fragen aufgeführt.

Redaktion: **eCH** Fachgruppe DigSig

Ansprechpartner:

eCH Geschäftsstelle

E-Mail: info@eCH.ch

Homepage und Download der digitalen Version: www.eCH.ch

Inhaltsverzeichnis

1	BEGRIFFE (GLOSSAR)	6
2	EGOVERNMENT ANWENDUNGEN	9
2.1	Akteure und Beziehungen	9
2.2	Der elektronische Zugang zu Behörden	9
2.3	Das hoheitliche Handeln der öffentlichen Verwaltung	9
2.4	Eingaben an Gerichte und Behörden	10
2.5	Die Zustellung	11
3	WIRKSAMKEIT ELEKTRONISCHER SIGNATUREN	12
3.1	Einleitung	12
3.2	Elektronische Signatur und Privatrecht	12
3.3	Die Verwendung der elektronischen Signatur im Bereich eGovernment	14
3.3.1	Gleichstellung der elektronischen Unterschrift mit der Handunterschrift im Bereich eGovernment	14
3.3.2	Die Ausgabe von Zertifikaten nach ZertES	14
3.3.3	Zusammenfassung.....	15
3.4	Absicherung (Haftung)	15
3.4.1	Haftungsbestimmungen im OR.....	15
3.4.2	Haftungsbestimmungen im ZertES.....	16
3.4.3	Haftungsbestimmungen im VG	17
3.4.4	Schlussfolgerung.....	18
3.5	Anmerkung zu qualifizierten elektronischen Zertifikaten	19
3.6	Zusammenfassung	20
4	ZUGANG ZU SENSITIVEN INFORMATIONEN	21
4.1	Einleitung	21
4.2	Authentisierung mit elektronischer Signatur	21
4.3	Authentisierung mit Entschlüsselung	22
4.3.1	Wie funktioniert es?	22
4.3.2	Rechtliche Probleme	23
4.3.3	Mindestvorschriften	24
4.4	Anmerkung	25
5	FUNKTIONSZERTIFIKATE	26
5.1	Einleitung	26

5.2	Angst vor funktionellen Signaturen	26
5.3	Einsatzgebiete für Funktionszertifikate.....	27
5.3.1	Besonders wichtige Einsatzgebiete.....	28
5.4	Lösungsansätze.....	28
5.5	Anmerkung.....	29
5.6	Beispiel	30
6	SICHERHEITSANFORDERUNGEN.....	32
6.1	Einleitung.....	32
6.2	Überblick	32
6.3	Zusammenstellung der bestehenden Vorschriften	33
6.4	Weiterführende Sicherheitsmassnahmen	34
6.5	Spam und Vertraulichkeit.....	34
6.6	Namensgebung	35
6.6.1	Einleitung.....	35
6.6.2	Massnahmen	35
7	ARCHIVIERUNG ELEKTRONISCH SIGNIERTER DOKUMENTE	37
7.1	Grundsätzliches.....	37
7.2	Prüfung elektronischer Signatur	38
7.3	Lösungsansätze.....	39
8	PRODUKTZERTIFIZIERUNG	40
9	BEANTWORTUNG DER FRAGEN IM ANTRAG	41
	ANHANG A – REFERENZEN	43
	ANHANG B – MITARBEIT & ÜBERPRÜFUNG.....	44
	ANHANG C – ABKÜRZUNGEN UND GESETZESTEXTE.....	44
	ANHANG D – HAFTUNG GEMÄSS OR 59A	46
	ANHANG E – MAC.....	48
	ANHANG F – URHEBERRECHTE	49

1 Begriffe (Glossar)

Anerkannt qualifizierte elektronische Signatur	Eine qualifizierte elektronische Signatur, welche mit einem öffentlichen Schlüssel aus einem qualifizierten Zertifikat eines anerkannten CSP verifiziert werden kann
Anerkannt qualifiziertes Zertifikat	Qualifiziertes Zertifikat, welches von einem nach ZertES anerkannten CSP ausgestellt worden ist.
Anerkannte CA	Synonym für eine nach ZertES anerkannte Anbieterin von Zertifizierungsdiensten
Anerkannte elektronische Signatur	Sinngemäss eine anerkannt qualifizierte elektronische Signatur
Anerkannter CSP	Synonym für eine nach ZertES anerkannte Anbieterin von Zertifizierungsdiensten
Anerkanntes Zertifikat	Zertifikat, welches von einem nach ZertES anerkannten CSP ausgestellt worden ist.
Anerkennungsstelle	s. Art. 2 Bst. h ZertES. Stelle, welche nach dem Akkreditierungsrecht für die Anerkennung und Überwachung der Anbieterinnen von Zertifizierungsdiensten akkreditiert ist.
Beweisen	Beweisen bedeutet, einen Sachverhalt zu belegen. Nach menschlichem Ermessen besteht dann kein Zweifel, dass sich der Sachverhalt wie dargelegt abgespielt hat.
CA	Certificate Authority. Institution, welche Zertifikate ausstellt.
CSP	Anbieterin von Zertifizierungsdiensten, engl Certificate Service Provider, gemäss [TAV]. So wird die Abkürzung in diesem Dokument verwendet. Crypto Service Provider. Bedeutung im Umfeld von Microsoft Betriebssystemen
Distinguished Name	Distinguished Name ist ein Name, welcher in Form und Inhalt konform zum X.500 Standard ist. Dieser Name ist gemäss dem Standard X.509 unbedingt ins Zertifikat einzufügen.
Elektronische Signatur	Gemäss Art. 2 Bst. a ZertES Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen.
Funktionelle elektronische Signatur	Eine elektronische Signatur, welche mittels eines Funktionszertifikats verifiziert werden kann.
Funktionszertifikate	Zertifikate, welche nicht einer natürlichen, aber einer juristischen Person, einem Server oder Dienst zugeordnet werden können.
Glaubhaft machen	Einen Sachverhalt ist glaubhaft dargelegt, wenn nichts dagegen spricht, dass der Sachverhalt sich wie geschildert abgespielt hat.

Provisorische Rechtsöffnung	<p>Eine provisorische Rechtsöffnung ist im Rahmen eines Schuldbetreibungs- und Konkursverfahrens ein gerichtlicher Entscheid, der auf Grund einer schriftlichen Schuldanerkennung die Wirkung des Rechtsvorschlags in einem Betreibungsverfahren aufhebt, die Nachprüfung der Forderung durch den Richter aber vorbehält (s. [AkGd], Seite 127 N65 ff.).</p> <p>Der Schuldner kann mittels Aberkennungsklage die gerichtliche Feststellung (Art. 83 Abs. 2 SchKG) des Nichtbestehens der Schuld verlangen und den Gegenbeweis antreten (s. [AkGd], Seite 134 ff.).</p>
Qualifizierte elektronische Signatur	<p>s. Art. 2 Bst. c ZertES: eine fortgeschrittene elektronische Signatur, die auf einer sicheren Signaturerstellungseinheit und auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat beruht.</p>
Qualifiziertes Zertifikat	<p>s. Art. 2 Bst. f ZertES: ein digitales Zertifikat, das die Anforderungen des Artikels 7 ZertES erfüllt.</p>
Qualifiziertes Zertifikat einer anerkannten CA	<p>Ein qualifiziertes Zertifikat, welches von einer nach ZertES anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt worden ist.</p>
Schriftlichkeit	<p>Schriftlichkeit im Sinne des Privatrechts bedeutet die Erklärung in Schriftform und die Unterzeichnung des Schriftstücks durch den Erklärenden (s. [GSSR], S. 93 ff.). Dabei wird grundsätzlich die eigenhändige Unterschrift verlangt.</p> <p>Es wird zwischen einfacher Schriftlichkeit, kurz Schriftlichkeit, und qualifizierter Schriftlichkeit unterschieden. Qualifizierte Schriftlichkeit besteht aus einfacher Schriftlichkeit, qualifiziert durch zusätzliche Elemente, wie eine öffentliche Beurkundung durch einen Notar oder gewisse Teile des Vertrags müssen handschriftlich abgefasst werden, s. [GSSR] Rz 522 und [Sci], Rz 31.15.</p> <p>Schriftlichkeit im Rahmen von Verwaltungs- und Gerichtsverfahren bedeutet, dass die Information in Schriftform abgefasst und zugestellt und nicht mündlich mitgeteilt wird.</p> <p>Die Behörden eröffnen im Allgemeinen die Verfügungen schriftlich (Art. 34 Abs. 1 VwVG), s. [KaHi], Seite 126 Rz 348 und Seite 131 Rz 365). Eine Verfügung muss in der Regel unterschrieben werden. Ob eine Handunterschrift Formerfordernis ist, wird in der Praxis unterschiedlich beurteilt. Massenverfügungen müssen hingegen nicht unterschrieben werden (so z.B. im Bereich der Steuertaxierung).</p>
Server	<p>Server ist ein Computer, ein Programm oder Applikation, welche eine bestimmte Dienstleistung bietet. Das englische Verb „to serve“ hat die Bedeutung „Dienen“.</p> <p>In gewissen nicht technischen Kreisen wird Server auch lediglich mit einem Web Server assoziiert, welcher über das http Protokoll angesprochen werden kann.</p>

Spam	Spam ist über das Internet verschickte (Werbe) E-Mail, welche der Empfänger nicht angefordert hat. Meist wird diese in Form von Massensendungen verteilt.
Zeitstempel	<p>Dienst der Anbieterin von Zertifizierungsdiensten, der eine mit dem Datum, der Uhrzeit und der qualifizierten Signatur des CSP versehene Bescheinigung abgibt, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt existiert haben [TAV].</p> <p>Ein gemäss ZertES anerkannter CSP hat Zeitstempeldienste anzubieten (Art. 12 ZertES).</p>

2 eGovernment Anwendungen

2.1 Akteure und Beziehungen

eGovernment wird traditionell in die folgenden Bereiche eingeteilt (s. [ISB 1], Regieren in der Informationsgesellschaft, Die eGovernment-Strategie des Bundes, 14. Februar 2002, Seite 9 ff.):

- **Government to Government (G2G)**

Beziehungen zwischen Bund, Kantonen und Gemeinden untereinander sowie Beziehungen zu ausländischen Regierungen und internationalen, überstaatlichen Organisationen (UNO etc.)

- **Government to Organisation (G2O)**

Beziehungen zwischen Bund, Kantonen und Gemeinden einerseits und den privatwirtschaftlichen Partnern (Unternehmen) und öffentlich-rechtlichen Organisationen (Verbänden, etc.) andererseits

- **Government to Citizen (G2C)**

Beziehungen zwischen dem Staat und den Einwohnerinnen und Einwohnern

Im vorliegenden Dokument werden vorwiegend die Aspekte des **hoheitlichen Staatshandelns** betrachtet und die Tätigkeit des Staates im **Privatrechtsbereich** nur bei der Haftung erwähnt.

2.2 Der elektronische Zugang zu Behörden

Der **elektronische Zugang** zu den Behörden ist heute noch nicht generell möglich. Der Bundesrat spricht sich jedoch in der Botschaft zur Totalrevision der Bundesrechtspflege vom 28. Februar 2001 für die Einführung eines „Grundsatzes des Zugangs zu Behörden auf elektronischem Weg“ aus, wobei der Bundesrat befristete Ausnahmen vorbehalten kann.

2.3 Das hoheitliche Handeln der öffentlichen Verwaltung

Der Staat kann wie eine Privatperson am Rechtsverkehr teilnehmen, indem er z.B. Software Lizenzen erwirbt, Büroeinrichtungen kauft, etc. Hier werden die Vorschriften des **Privatrechts** auch auf das Handeln des Staates analog angewandt. Wenn der Staat aber mit Hoheitsgewalt tätig wird, dann kommt **öffentliches Recht** zur Anwendung.

Als Verwaltungshandlungen sind alle Handlungen – d.h. jedes Tun, Dulden oder Unterlassen – zu betrachten, die ein Träger öffentlicher Gewalt bei der Erfüllung von Verwaltungsauf-

gaben vornimmt [siehe HUGM, Seite 177, Rz 694]. Dies betrifft also sowohl den Bereich G2G als auch G2O und G2C.

Grundsätzlich erfolgt das Verwaltungshandeln entweder in einem **streitigen oder im nicht-streitigen Verwaltungsverfahren**.

Die Normen des **streitigen Verwaltungsverfahrens** regeln die Anfechtung einer Verfügung vor einer Verwaltungsbehörde.

Das **nichtstreitige Verwaltungsverfahren** ist jedes erstinstanzliche Verfahren, das in der Regel zum Erlass einer Verfügung durch die zuständige Verwaltungsbehörde führt [siehe KaHi, Seite 3, Rz 3]. Für den Erlass von Verfügungen bestehen in der Regel **gesetzliche Formvorschriften**. Die Form, in der eine Verfügung erlassen und gegenüber dem Betroffenen eröffnet wird, bestimmt sich nach dem massgeblichen Verfahrensgesetz (z.B. Art. 34 f. VwVG).

Umstritten ist, ob sich aus den allgemeinen Lehren des Verwaltungsrechts ableiten lasse, dass bei schriftlicher Eröffnung die Verpflichtung zur Unterzeichnung der Verfügung bestehe. Enthält das massgebliche Gesetz keine Regelung, dann gilt der **Grundsatz der freien Wahl der Form**. Die Verfügung kann mündlich, schriftlich oder auf elektronischem Weg eröffnet werden. In diesen Fällen obliegt es somit den jeweiligen Behörden, zu entscheiden, ob sie sich bei grundsätzlicher Schriftlichkeit als Ersatz für die Handunterschrift auf eine anerkannt qualifizierte elektronische Signatur verlassen oder den Austausch der Dokumente, gezeichnet mit einer „normalen“ elektronischen Signatur, vornehmen wollen.

Eine Vielzahl der nichtstreitigen Verwaltungshandlungen führen aber lediglich einen tatsächlichen Erfolg herbei, ohne dass eine Verfügung erlassen wird. In diesem Bereich des **informellen Verwaltungshandelns** geht es um formlose Beziehungen zwischen dem Staat und den Bürgern oder zwischen zwei oder mehreren Behörden. Es ist gemäss Gesetz keinen formellen Schranken unterworfen. Dazu gehören z.B. die innerdienstliche Anordnung, amtliche Berichte und Vernehmlassungen, Auskünfte, Belehrungen, Empfehlungen, Rechnungsstellungen und Ermahnungen gegenüber Privaten.

2.4 Eingaben an Gerichte und Behörden

Bei Eingaben an ein Gericht wird in vielen Fällen die Unterschrift verlangt, so z.B. bei sämtlichen Rechtsschriften ans Bundesgericht (Art. 30 Abs. 1 OG) oder bei Beschwerden in einem Verwaltungsverfahren (Art. 52 Abs. 1 und 3 VwVG). Es sind bereits Gesetze in Vorbereitung, welche den Austausch von elektronisch signierten Dokumenten klar regeln. Gemäss Art. 39 Abs. 4 des Entwurfs zum BGG müssen z.B. die Rechtsschriften, welche elektronisch an das Bundesgericht eingereicht werden, mit einer „anerkannten, elektronischen“ Signatur versehen werden.

2.5 Die Zustellung

Die **Eröffnung der Verfügung** oder die Zustellung eines Gerichtsentscheids sind grundsätzlich empfangsbedürftige einseitige Rechtshandlungen. Die Verfügung bzw. der Entscheid gelten in der Regel als zugestellt, wenn sie vom Adressaten oder einer anderen dazu berechtigten Person entgegengenommen oder in den Briefkasten des Adressaten geworfen wird. Kann der Zeitpunkt der Zustellung nicht nachgewiesen werden, dann kann nichts Verbindliches über den Beginn und die Einhaltung von Beschwerdefristen gesagt werden. Die Folgen der Beweislosigkeit trägt dann die zuständige Behörde.

Wird eine Verfügung elektronisch eröffnet, dann muss sichergestellt werden, dass die Tatsache und der Zeitpunkt der Zustellung nachweisbar sind. Möglich wäre dies im elektronischen Behördenverkehr dadurch, dass die Frist auslösende Mitteilung dem Abholenden nur gegen eine elektronische Unterschrift zur Verfügung gestellt wird, wobei eine anerkannte elektronische Signatur vorausgesetzt werden muss (s. [Tsp]). Zur Zustellung von Verfügungen auf elektronischem Weg siehe auch Kapitel 5.3.1 „Besonders wichtige Einsatzgebiete“.

3 Wirksamkeit elektronischer Signaturen

3.1 Einleitung

In diesem Kapitel wird die Rechtswirksamkeit elektronischer Signaturen besprochen, welche mit qualifizierten Zertifikaten (eines anerkannten CSP) verifiziert werden können. Vielfach wird der Einsatz von qualifizierten Zertifikaten eines anerkannten CSP in Frage und deren Nutzen in Abrede gestellt, weil der Abschluss vieler Verträge formlos, d.h. nicht schriftlich, erfolgen kann und die Verträge somit auch ohne Unterschrift Gültigkeit haben. Weiter wird argumentiert, dass für die Verifikation elektronischer Signaturen keine qualifizierten Zertifikate eines anerkannten CSP benötigt werden, weil herkömmliche Zertifikate, d.h. nicht qualifizierte, den gleichen Dienst leisten und sich deshalb die Mehrkosten für die Herstellung von qualifizierten Zertifikaten eines anerkannten CSP nicht rechtfertigen lassen.

Dieses Kapitel soll u.a. die Vorteile und den Nutzen von qualifizierten Zertifikaten eines anerkannten CSP im eGovernment Umfeld und im privaten Geschäftsverkehr aufzeigen. Dabei wird u.a. auf das Gutachten des Bundesamts für Justiz VPB 63.46 abgestützt.

3.2 Elektronische Signatur und Privatrecht

Das Schweizerische Vertragsrecht baut auf dem Grundsatz der Vertragsfreiheit auf. Teil der Vertragsfreiheit ist die **Formfreiheit** (Art. 11 Abs. 1 OR). Neu können Verträge, für welche das Gesetz oder die Parteien selbst die einfache Schriftform vorgesehen haben, auch gültig elektronisch abgeschlossen werden (Art. 14 Abs. 2^{bis} OR). Grundsätzlich bedürfen Verträge nur dann einer bestimmten Form, wenn das Gesetz oder die Parteien dies ausdrücklich vorsehen. Nur wenige im OR aufgeführte Verträge bedürfen der Schriftlichkeit, wie z.B.:

- Im Entwurf zur Vernehmlassung geplant für Teilnutzung an Immobilien (Art. 40g ff. OR)
- Forderungsabtretung (Art. 165 Abs. 1 OR)
- Grundstückkauf (Vorkaufsverträge, die den Kaufpreis nicht zum Voraus bestimmen, Art. 216 Abs. 3 OR)
- Schenkungsversprechen (Art. 243 Abs. 1 OR)
- Handelsreisendenvertrag (Art. 347a Abs. 1 OR)
- Bürgschaft (Art. 493 OR)
- Leibrentenvertrag (Art. 517 OR)
- Konsumkreditverträge (Art. 9 ff. KKG)

Deshalb können auch nach dem Inkrafttreten des ZertES die meisten Verträge, welche keine Schriftlichkeit erfordern, weiterhin elektronisch gültig abgeschlossen werden. Schriftliche Verträge (s. VPB 63.46, S.1) geniessen wegen der freien Beweiswürdigung im (kantonalen) Prozessrecht keine privilegierte Behandlung.

Anmerkung: Obwohl viele Verträge auch ohne Unterschrift zustande kommen und Gültigkeit haben, werden in der Praxis die wesentlichen Punkte des Vertrages schriftlich festgehalten und unterschrieben, damit die getroffenen Abmachungen später bewiesen werden können.

Provisorische Rechtsöffnung erhält aber nur jener Gläubiger, welcher seine Forderung auf eine durch Unterschrift belegte Schuldanerkennung stützen kann (Art. 82 SchKG). Eine Schuldanerkennung kann in einer öffentlichen Urkunde (s. [AkGd], Seite 129 N71 ff.) oder einer Privaturkunde enthalten sein. Privaturkunden sind z.B. Briefe, Verträge in Formularen oder in einfacher Schriftform, Schuldscheine, Wechsel, Checks, usw. (s. [AkGd], Seite 130 N74 ff.). Bedingung für eine provisorische Rechtsöffnung ist, dass die Schuldanerkennung die Unterschrift des Schuldners oder seines Vertreters enthält. Die bisherige Praxis hat die Vorlage von Fotokopien nur dann akzeptiert, wenn dahinter ein vom Schuldner unterzeichnetes Original steht.

Die elektronische Signatur ist aber einer Unterschrift von Hand nur dann gleichgestellt, wenn sie qualifiziert ist und auf Basis eines qualifizierten Zertifikats eines anerkannten CSP verifiziert werden kann (Art. 14 Abs. 2^{bis} OR). Daher dürften elektronische Signaturen, welche nicht mit einem qualifizierten Zertifikat eines anerkannten CSP verifiziert werden können, nicht die gleiche Rechtswirkung gemäss SchKG entfalten.

Voraussetzung ist aber, dass die Gerichte über die technische Infrastruktur verfügen, um die elektronischen Signaturen auf Gültigkeit zu prüfen und darauf zu verifizieren, ob sie den gesetzlichen Anforderungen genügen. Eine Alternative dazu wäre auch, die Signaturen von einem fachkundigen, unbefangenen und vertrauenswürdigen Dritten prüfen zu lassen. Die Möglichkeit oder Gefahr besteht aber, dass die technischen und organisatorischen Massnahmen an den Gerichten noch nicht soweit umgesetzt sind, dass die elektronisch signierten Dokumente bei den Gerichten eingereicht werden können.

3.3 Die Verwendung der elektronischen Signatur im Bereich eGovernment

3.3.1 Gleichstellung der elektronischen Unterschrift mit der Handunterschrift im Bereich eGovernment

Der Bundesrat vertritt in der Botschaft zur Totalrevision der Bundesrechtspflege vom 28. Februar 2001 sinngemäss die Auffassung, dass es im Bereich des elektronischen Verkehrs des Einzelnen mit den Bundesbehörden möglich ist, die elektronische Unterschrift gleich zu werten wie die handschriftliche Signatur. Wo das Gesetz eine Unterschrift ausdrücklich vorschreibt (Art. 39 Abs. 1 BGG¹; Art. 52 Abs. 1 VwVG; Art. 23 Bst. g und 29 Bst. g BZP), kann diese handschriftlicher oder elektronischer Art sein (Art. 21a Abs. 2 VGG²; Art. 39 Abs. 4 BGG³). Bei Verwendung der elektronischen Signatur sei vor allem wichtig, dass die Unterschrift **durch die schweizerische Rechtsordnung anerkannt** ist. Eine elektronische Nachricht ohne anerkannte elektronische Signatur sei keine zulässige Alternative, soweit das Recht die **Schriftform** verlangt [siehe Botschaft zur Totalrevision der Bundesrechtspflege, Seite 4264].

3.3.2 Die Ausgabe von Zertifikaten nach ZertES

Im ZertES werden die Begriffe rund um die elektronische Signatur erläutert. Zudem definiert es die Pflichten des anerkannten CSP und der Anerkennungsstelle und regelt die Herausgabe qualifizierter elektronischer Zertifikate. Der elektronische Behördenverkehr sowie der Verkehr mit den Registern (Grundbuch, Handelsregister) werden von diesem Gesetz nicht berührt. Immerhin ermöglichen die durch die Übergangsbestimmungen geänderten ZGB- und OR-Bestimmungen (Art. 949a Abs. 2 Ziff. 3 ZGB und Art. 929a OR) dem Bundesrat, entsprechende Vorschriften aufzustellen (sinngemäss ZGBR online, Elektronische Signatur, Änderung von ZGB und OR).

Wird im öffentlich-rechtlichen Bereich die Handunterschrift verlangt, dann kann somit die elektronische Signatur nach ZertES nicht ohne weiteres angewandt werden. Dazu bedarf es zuerst der Schaffung der entsprechenden gesetzlichen Grundlage durch den Gesetzgeber. Aus dem oben Gesagten folgt zudem, dass der Gesetzgeber dabei nur eine von der Rechtsnorm anerkannte Signatur verwenden und deshalb sinngemäss die anerkannt qualifizierte elektroni-

¹ Noch nicht in Kraft

² Noch nicht in Kraft

³ Noch nicht in Kraft

sche Signatur vorsehen sollte, wie dies in der Botschaft zur Totalrevision der Bundesrechtspflege vorgeschlagen und im Art. 39 Abs. 4 BGG verlangt wird.

3.3.3 Zusammenfassung

Wenn der Staat hoheitlich tätig ist, kommt **öffentliches Recht** zu Anwendung.

Das Verwaltungsverfahren ist von zahlreichen Formvorschriften geprägt. Grundsätzlich kann davon ausgegangen werden, dass der Einsatz der elektronischen Signatur im Bereich des hoheitlichen Staatshandelns einer **gesetzlichen Grundlage** bedarf. Der Gesetzgeber sollte dabei aber nur die von der Rechtsordnung **anerkannte elektronische Signatur** vorsehen.

Nur dort, wo keine Formvorschriften existieren und die Behörde somit selbst bestimmen kann, wie sie mit den Bürgern kommuniziert, kann sie selbst frei wählen, ob sie die elektronische Signatur verwenden will und wenn ja, in welcher Form. In diesem Fall bedarf es keiner expliziten gesetzlichen Grundlage. Ideal wäre es aber, wenn ein standardisiertes Vorgehen in der Ausgestaltung, Umsetzung und Durchführung der IT-Prozesse angewandt würde.

3.4 Absicherung (Haftung)

Aus Sicht eines Praktikers hängt die Verlässlichkeit oder Sicherheit einer elektronischen Signatur davon ab, wie die Risiken bei deren (missbräuchlichem) Einsatz abgedeckt und überwältigt werden können, sprich wie die Haftung im Gesetz geregelt ist. Die Haftungsbestimmungen betreffend die qualifizierten Zertifikate sind einerseits im ZertES für den CSP und die Anerkennungsstelle, andererseits im OR für den Inhaber des privaten Schlüssels geregelt, welcher zu einem öffentlichen Schlüssel in einem qualifizierten Zertifikat eines anerkannten CSP passt.

3.4.1 Haftungsbestimmungen im OR

Übt der Staat eine gewerbliche Tätigkeit aus, die grundsätzlich auch Privaten offen steht und bei welcher die Erzielung von Gewinn eine Rolle spielt und bedient er sich dabei keiner hoheitlichen Mittel, sondern tritt den Privaten gleichgeordnet gegenüber auf, sind die **privatrechtlichen Haftungsbestimmungen** massgebend (HUMG, N 1770).

Die privatrechtliche Haftung nach Art. 59a OR bezieht sich auf ein zum Zeitpunkt der Signatur gültiges, qualifiziertes Zertifikat von eines anerkannten CSP. Gemäss Art. 59a OR haftet der Inhaber des privaten Schlüssels Drittpersonen für Schäden, welche diese erleiden, weil sie sich auf ein qualifiziertes Zertifikat eines anerkannten CSP verlassen haben. Die Haftung entfällt nur, wenn der Inhaber des privaten Schlüssels **glaubhaft machen** kann, dass er die not-

wendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch seines Signaturschlüssels zu verhindern

Die Haftung erstreckt sich sinngemäss nicht nur auf Vertragsabschlüsse, sondern auf jeglichen Schaden, der entstanden ist, weil sich jemand auf ein gültiges qualifiziertes Zertifikat eines anerkannten CSP verlassen hat. Die Haftung für elektronische Signaturen, welche nicht auf einem qualifizierten Zertifikat basieren, ist im OR nicht speziell geregelt, sondern richtet sich nach dem allgemeinen Haftpflichtrecht gemäss Art. 41 ff. bzw. 97 ff. OR. (Weitere Informationen zur Haftungsart von Art. 59a OR siehe dazu auch Anhang D.)

Beispiel: Herr MV vergisst seinen Geldbeutel mit der Smart Crypto Card (eine mögliche Form der sicheren Signaturerstellungseinheit) und dem Zettel mit der zugehörigen PIN in der Kantine. Herr DM will sich mit Herrn MV einen Scherz erlauben und bestellt übers Internet beim Elektroshop FAST einen PC, Drucker, einen Kühlschrank, einen Bildschirm, einen Fernseher und einen Mikrowellenherd im Namen von Herrn MV. Dabei unterzeichnet Herr DM die elektronische Bestellung mit dem privaten Schlüssel (Signaturschlüssel) von Herrn MV. Der Elektroshop FAST prüft die vermeintliche elektronische Signatur von MV mit dessen qualifizierten Zertifikat des anerkannten CSP CH-Signature. Die Prüfung verläuft erfolgreich, und das Unternehmen FAST liefert die Ware bei Herrn MV aus. Dieser bestreitet die Bestellung vehement und weigert sich, die Ware in Empfang zu nehmen.

Da nicht vermutet wird, dass eine elektronisch signierte Erklärung vom Inhaber des Signaturschlüssels stammt, ist mangels gegenseitiger Willenserklärung kein Vertrag zwischen Herr MV und dem Elektroshop FAST zustande gekommen. Herr MV haftet folglich zwar nicht aus Vertrag, aber aus Gesetz gemäss Art. 59a OR. Er muss den aus der Auslieferung entstandenen Schaden dem Elektroshop FAST vergüten, weil er nicht die notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat. Insbesondere hat er gegen Art. 11 Abs. 4 VZertES verstossen, indem er PIN und Karte zusammen aufbewahrt und in der Kantine liegengelassen hat.

3.4.2 Haftungsbestimmungen im ZertES

Die Anbieterin von Zertifizierungsdiensten haftet gemäss Art. 16 Abs. 1 ZertES gegenüber dem Inhaber des Signaturschlüssels und Drittpersonen, welche sich auf ein gültiges qualifiziertes Zertifikat verlassen haben, für Schäden, welche diese erleiden, weil die Anbieterin von Zertifizierungsdiensten den Pflichten aus ZertES und den dazugehörigen Ausführungsbestimmungen nicht nachgekommen ist. Die Haftung entfällt, sofern der CSP *beweisen* kann, dass sie den Pflichten aus ZertES und den dazugehörigen Ausführungsbestimmungen nachgekommen ist.

Sinngemäss gelten gemäss Art. 17 ZertES die gleichen Haftungsbestimmungen für die Anerkennungsstelle, sofern diese ihren Pflichten aus dem ZertES und dessen Ausführungsbestim-

mungen nicht nachkommt. Ebenso entfällt die Haftung, wenn die Anerkennungsstelle *beweisen* kann, dass sie ihre Pflichten erfüllt hat.

Diese (milde) Kausalhaftung beschränkt sich gemäss Wortlaut nicht nur auf Vertragsabschlüsse, sondern auf jeglichen Schaden, der entstanden ist, weil sich jemand auf ein gültiges qualifiziertes Zertifikat verlassen hat. Dies kann insbesondere beim ganzen Prozess- und Registrierungsablauf für die Authentisierung vorteilhaft sein, wenn Zugang zu sensiblen Daten gewährt werden soll.

Bemerkung: Die qualifizierten Zertifikate eines anerkannten CSP bieten gegenüber einem gewöhnlichen qualifizierten Zertifikat den Vorteil, dass der Geschädigte zusätzlich die Anerkennungsstelle belangen kann, sofern eine Sorgfaltspflichtverletzung durch die Anerkennungsstelle gemäss Art. 17 ZertES vorliegt.

3.4.3 Haftungsbestimmungen im VG

Ist der Staat hoheitlich aufgetreten und verwendet seinen Signaturschlüssel missbräuchlich, haftet er gemäss Verantwortlichkeitsgesetz (VG) gegenüber den Drittpersonen für Schäden, welche diese erleiden, weil sie sich auf das gültige qualifizierte Zertifikat verlassen haben.

Welche Haftungsgesetze (VG oder Haftungsgesetze der Kantone) in Frage kommen, hängt davon ab, ob der Bund, der Kanton oder die Gemeinde den elektronischen Schlüssel verwendet hat. Im Vordergrund steht vorliegend das VG, demnach für den Fall, dass der Bund gehandelt hat.

Damit der Staat gemäss VG haften kann, müssen folgende Voraussetzungen erfüllt sein:

- *Personen, für deren Verhalten der Staat haftbar werden kann:* Darunter fällt jede Person, die unmittelbar mit öffentlich rechtlichen Aufgaben des Bundes betraut ist (Art. 1 VG). Ein Dienstverhältnis zum Bund ist nicht notwendig.
- *Öffentlichrechtlicher Tätigkeitsbereich:* Der Staat haftet für schädigende Handlungen oder Unterlassungen im Bereich vom öffentlichen Recht geregelten amtlichen Tätigkeiten (vgl. Art. 3 VG).
- *Handlungen oder Unterlassungen in Ausübung einer amtlichen Tätigkeit:* Der Staat kann haftbar gemacht werden, wenn ein funktioneller Zusammenhang zwischen dem schädigenden Verhalten und einer amtlichen Tätigkeit besteht (vgl. Art. 3 VG).
- *Widerrechtlichkeit:* Die schädigende Handlung muss rechtswidrig sein. Die Verletzung absolut geschützter Rechtsgüter ist nicht widerrechtlich, wenn die schädigende Handlung durch einen Rechtfertigungsgrund gedeckt wird.
- *Schaden:* Die Haftung des Staates setzt den Eintritt eines Schadens voraus.

- *Adäquater Kausalzusammenhang:* Bei der Staatshaftung muss zwischen dem schädigenden Ereignis und dem Schaden ein Kausalzusammenhang bestehen, d.h. die Schadenursache muss nach dem gewöhnlichen Lauf der Dinge und nach den Erfahrungen des Lebens geeignet sein, einen Erfolg von der Art des eingetretenen herbeizuführen oder zu begünstigen.
- *Verschulden:* Die allgemeine Staatshaftung ist in der Regel als Kausalhaftung ausgestaltet, setzt demnach nur Widerrechtlichkeit, aber kein Verschulden voraus (Art. 3 Abs. 1 VG). In einigen Kantonen wird die Haftung des Staates jedoch vom Verschulden der handelnden Person abhängig gemacht.
- *Einschränkungen der Staatshaftung:* Die Ersatzpflicht kann ermässigt oder der Ersatzpflichtige gänzlich von ihr entbunden werden, wenn die geschädigte Person in die schädigende Handlung eingewilligt hat oder wenn Umstände, für die sie eintreten muss, auf die Entstehung oder Verschlimmerung des Schadens eingewirkt hat (Art. 4 VG; HUGM, N 1748 ff.).

3.4.4 Schlussfolgerung

Der Einsatz von Zertifikaten mit unterschiedlichen Vertrauens- oder Güteklassen für die Verifikation von elektronischen Unterschriften im eGovernment Umfeld birgt folgende Nachteile in sich:

- Nicht geklärt ist, welche Zertifikatsklassen (im Sinne von unterschiedlichen Vertrauens- oder Güteklassen) und welche entsprechenden elektronischen Signaturen in welcher eGovernment Anwendung eingesetzt werden müssen, damit die Rechtskonformität eingehalten werden kann. Dies kann zu langwierigen Diskussionen führen, was einer schnellen Realisierung von eGovernment Projekten abträglich ist. Zudem fördert es die (Recht)Sicherheit im Umgang mit der Behörde **nicht**. Im Privatbereich (Business 2 Business Umfeld) können jedoch vertragliche Vereinbarungen getroffen werden (Art.14 Abs. 2^{bis} OR), doch das **eGovernment Umfeld** ist im Allgemeinen **nicht von Verträgen, sondern von Verfügungen und rechtlich verbindlicher Kommunikation** (z.B. Austausch von Formularen) geprägt.
- Der (juristisch und technisch nicht versierte) Otto-Normalverbraucher will, muss und darf sich auf die von Bund und Kantonen gelieferten Informationen verlassen. Somit hat er gefühlsmässig nur eine Stufe von Vertrauensklasse gegenüber den Behörden.

- Insbesondere wegen der strengen Bundes⁴- und Staatsbeamtenhaftung⁵ sollten besondere Sicherheitsmassnahmen im Umgang mit elektronischen Signaturen erforderlich sein.
- Die Handhabung verschiedener Zertifikatsklassen und die Auswertung der Signatur werden dadurch beim Otto-Normalverbraucher (der natürlichen Person) erschwert, was die Akzeptanz für den Einsatz elektronischer Signaturen beeinträchtigt.

3.5 Anmerkung zu qualifizierten elektronischen Zertifikaten

Gemäss wörtlicher Interpretation Art. 2 Bst. c ZertES besteht die Möglichkeit, dass qualifizierte Zertifikate herausgegeben werden können, auch wenn der private Schlüssel (Signierschlüssel) sich nicht in einer sicheren Signaturerstellungseinheit befindet. Doch dann haftet der Schlüsselinhaber bei Missbrauch einer elektronischen Signatur nach Art. 59a Abs. 1 OR. Ohne sichere Signaturerstellungseinheit kann der Inhaber sicherlich nicht glaubhaft machen, dass er die notwendigen Sicherheitsmassnahmen getroffen hat.

Möglich wäre auch, dass der anerkannte CSP nach Art. 16 ZertES haftet, weil sie ihren Aufklärungspflichten nach Art. 9 Abs. 2 ZertES nicht nachgekommen ist. Infolgedessen hätte der Inhaber es versäumt, die Schlüssel in einer sicheren Signaturerstellungseinheit aufzubewahren.

In der Praxis wird der oben genannte Fall kaum anzutreffen sein, denn gemäss Kapitel 3.4.2 c) [TAV] ist im qualifizierten Zertifikat anzugeben, dass der Benutzer eine sichere Signaturerstellungseinheit verwendet. Dabei wird der Zertifikatsaussteller darauf achten, dass bei der Herausgabe des Zertifikats der dazu korrespondierende private Schlüssel sich in einer entsprechend sicheren Signaturerstellungseinheit befindet. Ansonsten haftet er dafür.

Anmerkung: Grundsätzlich kann der CSP nicht Gewähr dafür leisten, dass der Bezüger des Zertifikats die Schlüssel immer in einer sicheren Signaturerstellungseinheit aufbewahrt. Theoretisch möglich wäre es, dass der Schlüssel vom Bezüger generiert wird, die Kopie des privaten Schlüssels in eine Signaturerstellungseinheit eingefügt wird und damit dann ein qualifiziertes Zertifikat eines anerkannten CA bezogen wird.

⁴ Gemäss Art. 3 Abs. 1 VG liegt eine verschuldensunabhängige Haftung für die Beamten im Rahmen ihrer amtlichen Tätigkeit vor.

⁵ Viele Kantone haben eine verschuldensunabhängige Haftung für ihre Beamten im Rahmen ihrer amtlichen Tätigkeit.

Der Empfänger einer elektronischen Signatur kann nicht feststellen, ob die Signatur mit einer sicheren Einheit erzeugt worden ist oder nicht. Er kann lediglich anhand des qualifizierten Zertifikats, welches zur Verifikation der Signatur hinzugezogen wird, erkennen, dass bei der Herausgabe des Zertifikats sich der Schlüssel in einer sicheren Einheit befunden hat.

3.6 Zusammenfassung

Der Vorzug von qualifizierten elektronischen Signaturen, verifizierbar mit einem qualifizierten Zertifikat eines anerkannten Zertifizierungsdienstanbieters, gegenüber den „übrigen“ elektronischen Signaturen lässt sich u.a. wie folgt begründen:

- Qualifizierte elektronische Signaturen, verifizierbar mit einem Zertifikat eines anerkannten Zertifizierungsdienstanbieters, ermöglichen eine provisorische Rechtsöffnung nach SchKG.
- Qualifizierte elektronische Signaturen, verifizierbar mit einem qualifizierten Zertifikat eines anerkannten Zertifizierungsdienstanbieters, können unter Umständen vielfältiger eingesetzt werden. (Z.B. ist eine Formvorschrift für die elektronische Eingabe von Rechtsschriften an das Bundesgericht geplant.)
- Ab dem Inkrafttreten des VGG und BGG wird man mit anerkannten elektronischen Signaturen Rechtsschriften elektronisch ans Bundesgericht eingeben können.
- Qualifizierte elektronische Signaturen, verifizierbar mit einem qualifizierten Zertifikat oder einem qualifizierten Zertifikat eines anerkannten Zertifizierungsdienstanbieters, bieten mehr (Rechts)Sicherheit, weil die Haftung per Gesetz strenger geregelt ist⁶.

⁶ Wenn keine speziellen Bestimmungen vorgesehen sind, gelten die allgemeinen Regeln nach Art. 41 ff OR. Die nicht anerkannten Zertifizierungsdienstanbieter, welche qualifizierte Zertifikate ausstellen, haften aber aufgrund von Art. 16 ZertES genau gleich wie die Anerkannten.

4 Zugang zu sensiblen Informationen

4.1 Einleitung

Gemäss [TAV] darf das qualifizierte Zertifikat ausschliesslich für die Verifikation einer verbindlichen Signatur (engl. Non Repudiation) verwendet werden, s. [TAV] S. 16. Folglich kann die (anerkannt) qualifizierte elektronische Signatur ausschliesslich für die (rechtlich) verbindliche elektronische Signatur eingesetzt und nur für die der Handschrift gleichgestellten Unterzeichnung (von Verträgen) genutzt werden.

Will man die elektronische Signatur nicht zur Unterzeichnung eines Rechtsgeschäfts aber lediglich zur Prüfung der Authentizität von Dokumenten oder abgelegten Daten verwenden, dann müssen andere Zertifikate mit entsprechendem Verwendungszweck ausgestellt und zur Prüfung von Signaturen eingesetzt werden. Soll eine elektronische Signatur auch für Authentisierungen im Rahmen der online Kommunikation (z.B. für die Authentisierung, den Aufbau und später für die Verschlüsselung von SSL oder IPSEC⁷ Verbindungen) eingesetzt werden, dann darf diese elektronische Unterschrift nicht mit einem qualifizierten Zertifikat verifiziert werden. Doch werden Zertifikate mit einem anderen Verwendungszweck als der Verifikation einer verbindlichen elektronischen Signatur (auch im eGovernment Umfeld) benötigt.

Die Authentisierung mittels Zertifikaten läuft *sehr vereinfacht ausgedrückt* wie folgt ab:

Die zu authentisierende Person veranlasst eine Operation mit ihrem privaten Schlüssel. Mittels einer Operation des öffentlichen Schlüssels wird auf der Gegenseite verifiziert, ob diese Person im Besitz des zum Zertifikat passenden, privaten Schlüssels ist. Über die Verbindung Identität und öffentlicher Schlüssel im Zertifikat ist nun die Person authentisiert.

Eine Operation mit dem privaten Schlüssel kann beinhalten:

- Entweder eine elektronische Signatur (s. Kapitel 4.2)
- oder eine Entschlüsselung (s. Kapitel 4.3)

4.2 Authentisierung mit elektronischer Signatur

Die Authentisierung mit einer elektronischer Signatur, welche mit einem Zertifikat einer nach ZertES anerkannten CA verifiziert werden kann, eignet sich auch für den geschützten Zugang zu sehr sensiblen Informationen.

⁷ Zu den Begriffen SSL oder IPSEC s. SAGA.ch

Dies ist insbesondere dann empfehlenswert, wenn:

1. Die Bekanntgabe von Daten, welche gemäss Art. 3 Bst. c DSG besonders schützenswert sind⁸; die Bekanntgabe der Information selbst bei Fahrlässigkeit strafbar ist; oder die Bekanntgabe oder das Zugänglichmachen der Information als Vergehen oder Verbrechen eingestuft wird.
2. Auf die Daten über ein öffentliches Netz zugegriffen wird.

Beispiele für die unter Punkt 1 erwähnten Strafbestimmungen: Verletzung des Fabrikations- oder Geschäftsgeheimnisses Art. 162 StGB, Diplomatischer Landesverrat Art. 267 Ziff. 2 StGB, Wirtschaftlicher Nachrichtendienst Art. 273 StGB, Verletzung des Amtsgeheimnisses Art. 320 Ziff. 1 StGB, Verletzung des Berufsgeheimnisses Art. 321 Ziff. 1 StGB, Verletzung des Bankgeheimnisses Art. 47 BankG.

Anmerkung: Da bei der Übermittlung der vertraulichen Daten die Daten auch noch verschlüsselt werden müssen (sollten), muss der Verschlüsselungsschlüssel beim Verbindungsaufbau ausgehandelt werden. Mit einer elektronischen Signatur funktioniert dies nur bei der online Kommunikation (z.B. Client Server), nicht aber bei E-Mail. Hier kommt das im folgenden Kapitel 4.3 beschriebene Verfahren zum Einsatz.

4.3 Authentisierung mit Entschlüsselung

4.3.1 Wie funktioniert es?

Die Verfahren für die online Kommunikation und für E-Mail (Transport verschlüsselter Daten) sind unterschiedlich.

4.3.1.1 E-Mail

Das Verfahren ist ausführlich in [Mud] Kapitel 1 beschrieben. Die E-Mail wird mit einem zufällig erzeugten Schlüssel mit einem symmetrischen Verschlüsselungsverfahren wie AES verschlüsselt. Dieser zufällig erzeugte Schlüssel wird dann mit dem öffentlichen Schlüssel aus dem Zertifikat des Empfängers verschlüsselt. Dieses Chiffre wird der verschlüsselten E-Mail beigelegt. Beides zusammen wird dann an den Empfänger versandt.

Die Authentisierung erfolgt im Grunde genommen versteckt (nicht explizit) ab. Der Absender glaubt zu wissen, dass nur der Empfänger die E-Mail entschlüsseln kann, weil nur er den privaten Schlüssel besitzen sollte.

⁸ Zur Strafbarkeit der Bekanntgabe besonders schützenswerter Daten, siehe auch Art. 35 DSG

4.3.1.2 Online Kommunikation

Sehr vereinfacht ausgedrückt authentisiert sich Alice bei Bob wie folgt:

- Alice sendet Bob ihr Zertifikat
- Bob überprüft das Zertifikat auf Gültigkeit. Bei erfolgreicher Prüfung generiert Bob eine Zufallszahl R und verschlüsselt diese mit dem öffentlichen Schlüssel aus dem Zertifikat von Alice. Das Resultat davon $E_{\text{Alice}}(R)$ wird nun Alice zugestellt.
- Alice entschlüsselt $E_{\text{Alice}}(R)$ mit ihrem privaten Schlüssel. Ein Teil von R wird für die Authentisierung, der andere für die Verschlüsselung der an Bob zu versendenden Pakete benutzt.
- Die Authentisierung der an Bob versandten Pakete erfolgt mit dem restlichen Teil des Schlüssels und dem MAC Verfahren. Das MAC Verfahren ist bei [Mud] oder [Sch] beschrieben. Eine Kurzbeschreibung dazu befindet sich im Anhang D dieses Dokuments.

Anmerkung: Bei der online Kommunikation authentisiert sich meistens auch Bob bei Alice.

Anwendungsfälle: Das hier vorgestellte Verfahren in abgeänderter Form wird u.a. in folgenden Fällen angewandt:

- Authentisierung des Servers beim Internetbanking
- Authentisierung des Kommunikationsteilnehmers bei der Eingabe der Dokumente beim Server ans Bundesgericht
- Sicherung der Kommunikation zwischen den Heimarbeitsplätzen und dem Unternehmensnetz

Die im Kapitel 4.2 „Authentisierung mit elektronischer Signatur“ abgegebenen Empfehlungen gelten unseres Erachtens sinngemäss hier auch.

Qualifizierte Zertifikate und deren Schlüssel dürfen für den hier beschriebenen Fall nicht eingesetzt werden, weil der Schlüssel im Zertifikat lediglich zur Verifikation der verbindlichen elektronischen Signatur, nicht aber für die Verschlüsselung und die online Authentisierung verwendet werden darf, s. auch [TAV] Kapitel 3.4.2, Abschnitt c.

4.3.2 Rechtliche Probleme

Im Gesetz sind nur die qualifizierten Zertifikate geregelt. Qualifizierte Zertifikate dienen aber ausschliesslich der Verifikation elektronischer Signaturen und nicht der Verschlüsselung von Daten oder der online Authentisierung mittels elektronischer Signatur. Doch die Verschlüsselung von Daten ist u.a. beim Austausch von vertraulichen E-Mail wichtig.

Folgende Lösungsansätze gibt es grundsätzlich für dieses Problem:

- Das Gesetz würde zusätzlich die Herausgabe und Verwendung der Zertifikate für die Verschlüsselung und online Authentisierung regeln, was aber bisher nicht geplant ist. Es würden dann, im Unterschied zur bestehenden Regelung nach ZertES, auch „höherwertige“ Zertifikate für die Verschlüsselung herausgegeben werden. Der Inhalt dieser Zertifikate wäre per Verordnung definiert. Höherwertig im Sinne, dass das betreffende Zertifikate von eines anerkannten CSP ausgestellt wird und die Haftung analog zur Ausstellung von qualifizierten Zertifikaten geregelt ist.
- Man einigt sich darauf, die Mindestvorschriften aus folgendem Unterkapitel zu erfüllen.

4.3.3 Mindestvorschriften

Wir schlagen folgende Mindestvorschriften vor:

- Die Zertifikate werden mit dem öffentlichen Schlüssel eines anerkannten CSP verifiziert.
- Die Operation mit dem privaten Schlüssel findet in einer Einheit statt, welche die gleichen Sicherheitsanforderungen einer sicheren Signaturerstellungseinheit gemäss ZertES erfüllt (s. Art. 2 Bst. c ZertES).
- Für die Identifikation bei der Ausstellung eines Zertifikats für die Verschlüsselung und online Authentisierung mittels Signatur sind die gleichen Bestimmungen wie für die Ausstellung eines qualifizierten Zertifikats einzuhalten. Es muss u.a. die Identität des Antragstellers und die im Zertifikat verwendeten Attribute geprüft und zudem verifiziert werden, ob der Antragsteller im Namen der Organisation dazu ermächtigt ist. Art. 5 VZertES ist sinngemäss anzuwenden.

Hat ein Benutzer bereits ein qualifiziertes Zertifikat eines anerkannten CSP, so könnte der Antrag auf ein entsprechendes Zertifikat auch elektronisch signiert werden. Damit wäre der Anforderung an die Identifikation auch Genüge geleistet.

- Im Zertifikat ist zu kennzeichnen, dass der öffentliche Schlüssel im Zertifikat zur Verschlüsselung und nicht zur Verifikation von elektronischen Signaturen verwendet werden soll.

Aus praktischen Gründen drängt es sich auf, sämtliche privaten Schlüssel in der gleichen sicheren Signaturerstellungseinheit aufzubewahren.

4.4 Anmerkung

Die Ausstellung eines Zertifikats und die Prüfung der Authentisierung auf Basis eines Zertifikats stellen nur eine Komponente bei der Authentisierung dar. Weitere notwendige Komponenten, siehe SAGA.ch. Wie mittels Public Key Verfahren authentisiert wird, ist u.a. in [Sch] und [Mud] beschrieben.

Anerkannt qualifizierte Signaturen können auch im Rahmen von elektronischen Registrierungsprozesse behilflich sein und als Ausgangspunkt für die online Authentisierung dienen. Z.B. Zeichnungsberechtigter A meldet sich und zwei seiner Mitarbeiter mittels einer verbindlich signierten E-Mail bei der Stelle C an, damit er und seine Mitarbeiter dann online Dienste bei C beziehen dürfen. Dabei liefert er die Zertifikate für die online Authentisierung mit.

5 Funktionszertifikate

5.1 Einleitung

Qualifizierte Zertifikate dürfen mit einer Ausnahme (Art. 4 Abs. 2 VZertES) nur an natürliche Personen herausgegeben werden (Art. 7 Abs. 1 Bst. c ZertES). Deshalb können nur natürliche Personen mittels qualifizierter elektronischer Signatur auf elektronischem Weg der Handunterschrift gleichgestellt unterschreiben. Nichtsdestotrotz werden funktionelle Signaturen (u.a. elektronische Signaturen von Server) benötigt, folglich erstellt und eingesetzt. Zwecks Rechtssicherheit bedürften die funktionellen Signaturen eigentlich einer klareren gesetzlichen Regelung.

Dieses Kapitel soll:

- Die Angst vor funktionellen Signaturen, insbesondere vor elektronischen Signaturen von Server und deren möglichen Rechtswirkung verkleinern.
- Bestehende und mögliche Einsatzgebiete von Zertifikaten für Server und elektronischen Signaturen von Servern aufzeigen.
- Empfehlungen für den Einsatz von Serverzertifikaten und elektronischen Signaturen abgeben, welche von Server hergestellt worden sind.

Anmerkung: In der revidierten Fassung von ELDI-V sollen die elektronischen Signaturen von Server und deren Zertifikate geregelt werden.

5.2 Angst vor funktionellen Signaturen

Die Angst oder Bedenken nur gegenüber funktionellen Signaturen, insbesondere elektronischen Signaturen von Server, nicht aber gegenüber elektronischen Signaturen von natürlichen Personen, sind eher irrational und folglich wenig begründet. Qualifizierte elektronische Signaturen werden eigentlich nicht direkt von der natürlichen Person geleistet, sondern vom Mikroprozessor in der sicheren Signaturerstellungseinheit, welche im Besitz dieser natürlichen Person ist (sein sollte).

Folglich sollte auch keine Angst oder Bedenken vor elektronischen Signaturen bestehen, erstellt von einem Prozessor in einem Server, welcher im Besitz einer natürlichen oder juristischen Person ist.

Zudem werden versteckt und deshalb von vielen unbemerkt die elektronischen Signaturen bereits in einem speziellen Fall oder in einem speziellen Kontext im Gesetz erwähnt und dort geregelt. Ein (qualifiziertes) Zertifikat ist nämlich eine in Syntax und Form definierte Datei, welche vom Server des (anerkannten) CSP elektronisch unterschrieben worden ist. Bei der

Prüfung einer elektronischen Signatur einer natürlichen Person verlässt man sich unter anderem auf die Richtigkeit und Gültigkeit einer von einem Server elektronisch signierten Datei.

Für die erfolgreiche Verifikation eines Zertifikats sind wiederum beim heutigen Stand der Technik so genannte CA Zertifikate unabdingbar, welche den öffentlichen Schlüssel eines CSP in Form eines Zertifikats beglaubigen. Ein CA Zertifikate ist in der Regel ein für eine juristische Person ausgestelltes Zertifikat.

Die Haftung des CSP für eine elektronische Signatur in einem qualifizierten Zertifikat⁹, sprich für die elektronische Signatur eines Server, ist sogar strenger als für die anerkannt qualifizierte elektronische Signatur einer natürlichen Person. Die natürliche Person muss bei einer Klage lediglich *glaubhaft machen*, dass sie die notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, damit die Haftung entfällt. Im Gegensatz dazu muss gemäss Art. 16 Abs. 1 ZertES die CSP (im Normalfall eine juristische Person) *beweisen*, dass sie den Pflichten aus ZertES und den dazugehörigen Ausführungsbestimmungen nachgekommen ist, damit die Haftung entfällt.

Nota bene: Bei der soeben geschilderten Haftung handelt es sich um eine **Ausnahme** und **nicht** um den **Regelfall**. Es dürfen nur in einem Fall qualifizierte Zertifikate an eine juristische Person ausgehändigt werden, nämlich für den CSP selber. Deshalb darf von dem hier beschriebenen Fall bezüglich Haftung nicht eine allgemeine Gültigkeit abgeleitet werden.

5.3 Einsatzgebiete für Funktionszertifikate

Neben dem bereits geschilderten Einsatzgebiet für elektronische Signaturen von Server sind noch folgende Anwendungsfälle von funktionellen Signaturen möglich:

- Digitale Belege oder Quittungen für die elektronische Geschäftsführung
- Digitale Belege für die Eingabe von (Rechts)Schriften an das Bundesgericht
- Digitale Belege für den elektronischen Geschäftsverkehr zwischen Privaten und den Institutionen der öffentlichen Hand.
- Zeitstempeldienste (u.a. für die Archivierung)
- Halbautomatisch abgewickelte Geschäfte mit Staatsbetrieben (z.B. der Bezug von Fahrkarten bei der SBB, die Bestellung von Formularen oder Drucksachen)
- Massensignaturen (im Rahmen einer Rezertifizierung oder Neusignatur)

⁹ Aus Sicht der Technik ist ein Zertifikat unter anderem ein in Syntax und Format definierte Datei, welche von der CA signiert worden ist. Die Signatur wird von einem Server oder einer sicheren Signaturerstellungseinheit beim Server geleistet.

- Authentisierter und bezüglich Vertraulichkeit geschützter Zugang zu sensitiven Daten
- Transaktionen zwischen Server
- Backup von einem Server zum anderen

5.3.1 Besonders wichtige Einsatzgebiete

U.a. die Eingabe von Rechtsschriften, der Versand und die Zustellung von Verfügungen und die Zustellung von eingeschriebenen Briefen sind wichtige Abläufe im täglichen Berufs- und Privatleben. Will man die entsprechenden Abläufe auf elektronischem Weg schnell abwickeln, so werden Server benötigt.

Diese Server nehmen die Dokumente in Empfang und bestätigen dies dem Absender des Dokuments mittels eines elektronisch signierten Beleges. Somit kann der Absender zu einem späteren Zeitpunkt beweisen, dass er die Dokumente (fristgerecht) und in entsprechender Form versandt hat.

Gleichzeitig müssen sich die möglichen Empfänger dazu verpflichten, die Dokumente bei dem Server innerhalb einer gewissen Frist abzuholen, nachdem sie vom Server benachrichtigt worden sind, dass für sie ein Dokument zum Abholen bereitsteht. Die Verpflichtung kann auf Vertrag oder auf einer Einverständniserklärung und den entsprechenden Bestimmungen beruhen. Werden die Dokumente aber nicht fristgerecht vom Empfänger abgeholt, dann sollte der Absender benachrichtigt werden.

Voraussetzung: Der vom Server elektronisch signierte Beleg muss aber allgemein von den entsprechenden amtlichen Stellen anerkannt werden.

Ein weiteres wichtiges Einsatzgebiet sind die Zeitstempeldienste, welche u.a. bei der Archivierung elektronischer Dokumente eingesetzt werden, so dass die Erhaltung der Beweiskraft elektronisch signierter Dokumente nicht verloren geht; zur Wichtigkeit von Zeitstempeldiensten siehe auch CWA 14171.

5.4 Lösungsansätze

Ein Zertifikat besteht u.a. aus der Unterschrift des CSP. In den meisten Fällen handelt es sich hier um eine funktionelle Signatur. Einzig dieser Anwendungsfall von funktionellen Signaturen (Beurkundung eines Zertifikats) ist bisher im Gesetz klar geregelt worden.

Geplant ist aber, dass im Rahmen der Mehrwertsteuer eine revidierte Verordnung EIDI-V entsteht, welche die funktionellen Signaturen regelt. Sofern erforderlich, wird dann dieses Dokument entsprechend dieser Verordnung noch angepasst werden.

Wir schlagen im eGovernment Umfeld vorläufig folgende Mindestvorschriften für den weiteren Einsatz von elektronischen Signaturen von Server vor:

- Die Zertifikate für die Server werden mit dem gleichen öffentlichen Schlüssel aus dem CA Zertifikat verifiziert wie die qualifizierten Zertifikate.
- Die Operation mit dem privaten Schlüssel eines Server findet in einer Einheit statt, welche die gleichen Sicherheitsanforderungen einer sicheren Signaturerstellungseinheit nach ZertES erfüllt (s. Art. 2 Bst. c ZertES).
- Im Zertifikat ist zu kennzeichnen, dass das Zertifikat nicht für eine natürliche Person ausgestellt worden ist. Es muss erkennbar sein, welche Organisation das Zertifikat bezogen hat.
- Für die Identifikation bei der Ausstellung eines Serverzertifikats gelten die gleichen Bestimmungen wie für die Ausstellung eines qualifizierten Zertifikats. Es muss u.a. die Identität des Antragstellers und die im Zertifikat verwendeten Attribute geprüft und zudem verifiziert werden, ob der Antragsteller im Namen der Organisation dazu ermächtigt ist. Art. 5 VZertES ist sinngemäss anzuwenden.
- Wird nur der Zugang zu sensitiven Daten geschützt und werden mit der Authentisierung keine Rechtsgeschäfte begründet, dann kann die Authentisierung und die Schlüsselvereinbarung auf Basis eines Zertifikats für die Verschlüsselung vorgenommen werden.

Es muss eine klare Zuordnung des Zertifikats zu der (juristischen) Person ersichtlich sein (dies analog der Definition der fortgeschrittenen elektronischen Signatur Art. 2 Bst. b Ziff. 1 bis 4 ZertES). Dies muss über den Inhalt des Zertifikats erfolgen, z.B. durch Einfügen der in der Schweiz eindeutigen Identitätskennung eines Unternehmens in den Distinguished Name des Zertifikats. Der Distinguished Name kann trotz dieser Identitätskennung weiter verfeinert (unterteilt) werden und dadurch eine genauere Zuordnung enthalten. Der Nutzen und somit auch die Beschränkung des Einsatzes der entsprechenden funktionellen Signatur können über einen Verzeichnisdienst definiert werden; analog zum Hinweis im Zertifikat über den Verteilpunkt der Revokationsliste oder zum Hinweis im Zertifikat auf eine Policy, welche eingehalten werden sollte.

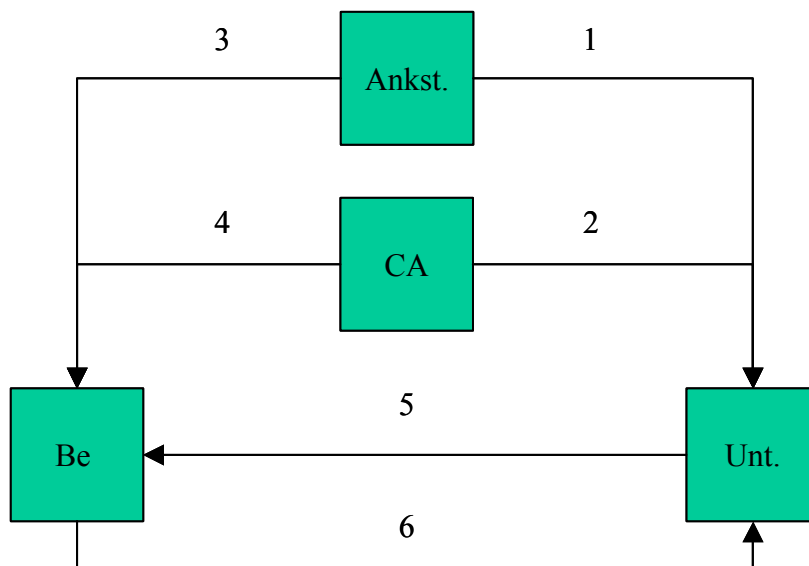
5.5 Anmerkung

Während der Bearbeitung und Behandlung des Themas „Serverzertifikate“ wurde der Entwurf der EIDI-V an interessierte Kreise verteilt. Die definitive Fassung der Verordnung konnte aber für dieses Dokument nicht mehr berücksichtigt werden.

5.6 Beispiel

Anhand des folgenden fiktiven Beispiels sollen die Haftungsbestimmungen in aller Kürze und in sehr vereinfachter Art und Weise aufgeführt werden. Dabei sind folgende Parteien involviert, s. auch Abbildung 1:

- Anerkennungsstelle (Ankst.)
- Anerkannte CSP
- Benutzer oder Bezüger eines qualifizierten Zertifikats (Be)
- Unternehmen (Unt.), welches ein Serverzertifikat eines anerkannten CSP bezogen hat.



Zeichenerklärung: A \longrightarrow B bedeutet, A haftet B

Abbildung 1 Haftungsszenario

1. Art. 17 ZertES, weil sich das Unternehmen auf die Gültigkeit des qualifizierten Zertifikats des Benutzers verlassen hat.
2. Art. 16 ZertES, weil sich das Unternehmen auf die Gültigkeit des qualifizierten Zertifikats des Benutzers verlassen hat.
3. Art. 41 OR aus unerlaubter Handlung, weil der Benutzer sich auf die Gültigkeit des Serverzertifikats verlassen hat.
4. Art. 41 OR aus unerlaubter Handlung, weil der Benutzer sich auf die Gültigkeit des Serverzertifikats verlassen hat.

5. Art. 41 OR aus unerlaubter Handlung, eventuell Art. 97 ff OR wegen Verletzung des Vertrags zwischen dem Unternehmen und dem Benutzer
6. Art. 59a OR, weil sich das Unternehmen auf die Gültigkeit des qualifizierten Zertifikats des Benutzers verlassen hat; eventuell Art. 97 ff OR wegen Verletzung des Vertrags zwischen dem Unternehmen und dem Benutzer.

Anmerkung: Wenn einer der Parteien, z.B. der CSP, der Bezüger des Zertifikats oder der Betreiber des Server Teil einer Behörde sind, kann unter Umständen auch das Verantwortlichkeitsgesetz VG oder die Staatshaftung angewandt werden.

6 Sicherheitsanforderungen

6.1 Einleitung

In diesem Kapitel werden die Sicherheitsanforderungen beim Leisten einer elektronischen Signatur zusammengestellt. Die Sicherheitsanforderungen und die getroffenen Sicherheitsmassnahmen beim Leisten einer (anerkannt qualifizierten) elektronischen Signatur sind aus folgenden Gründen wichtig:

- Unter Umständen entbindet es die natürliche Person beim Missbrauch eines privaten Schlüssels oder einer (anerkannt qualifizierten) elektronischen Signatur durch einen Dritten von der Haftung, siehe auch Anmerkung unten.
- Das Vertrauen in die neue Technologie und deren allgemeine Akzeptanz hängen davon ab, wie sicher die Technologie eingesetzt wird und wie klein die Anzahl der missbräuchlichen Anwendungen ausfällt.

Dieses Dokument stellt einerseits Hinweise auf die Artikel und Passagen in den Schweizerischen Vorschriften zusammen, welche die Sicherheitsanforderungen und die zu treffenden Massnahmen definieren. Weiter empfiehlt es darüber hinausgehende Massnahmen beim Leisten einer elektronischen Signatur. Diese erfolgen in Abstimmung zu SAGA.ch V.2.1.

Anmerkung: Der Missbrauch eines elektronischen Signaturschlüssels beinhaltet einen Missbrauch einer elektronischen Signatur. Doch gibt es Missbrauchsfälle der elektronischen Signatur, welche nicht auf den Missbrauch eines Signaturschlüssels zurückzuführen sind, z.B.:

- Falsche Verifikation der Signatur und der dazu gehörigen Zertifikate
- Missbräuchliche Unterbreitung der Dokumente
- Ausnutzen der Schwachstellen in der Namensgebung, siehe [Mus]

Hinweis: Weil es zum Schlüsselmissbrauch zusätzliche Missbrauchsfälle im Bereich der elektronischen Signatur gibt, sind die Standards wie CWA 14170 und 14171 von CEN entwickelt worden. In CWA 14170 sind eine Reihe von Empfehlungen enthalten, welche Sicherheitsanforderungen beim Leisten einer elektronischen Signatur zu beachten sind.

6.2 Überblick

Die bestehenden Gesetze und Verordnungen in der Schweiz, welche die Sicherheitsanforderungen beim Leisten einer qualifizierten elektronischen Signatur regeln, beschreiben im Wesentlichen den Umgang mit der sicheren Signaturerstellungseinheit und deren technischer Beschaffenheit. Doch sollten beim Leisten einer elektronischen Unterschrift zusätzliche Sicherheitsvorkehrungen beachtet werden.

6.3 Zusammenstellung der bestehenden Vorschriften

Die bestehenden Vorschriften in der Schweiz bezüglich sichere Signaturerstellungseinheit lassen sich grob wie folgt kategorisieren:

- Anforderung an die Generierung der Schlüssel
- Sicherheitsanforderung an die sichere Signaturerstellungseinheit
- Umgang mit der sicheren Signaturerstellungseinheit und deren Aktivierung für das Leisten der elektronischen Signatur
- Massnahmen beim Verlust der Signaturerstellungseinheit oder bei Kompromittierung der Schlüssel

Anforderung an die Generierung der Schlüssel sind in den folgenden Vorschriften enthalten:

- Art. 6 Abs. 2 ZertES
- Art. 3 VZertES Abs. 1 (Generierung der Schlüssel)
- Art. 6 VZertES (Kopier- und Aufbewahrungsverbot, falls der CSP die Schlüssel generiert)
- Kapitel 3.3.8 [TAV] mit Hinweis unter anderem auf folgende technische Standards: ETSI TS 101 456, ETSI SR 002 176, ISO/IEC 15408:1999, CWA 14167-3

Sicherheitsanforderung an die sichere Signaturerstellungseinheit sind in der folgenden Vorschrift enthalten:

- Kapitel 3.3.9 [TAV] Hinweis unter anderem auf folgende technische Standards: CWA 14169. Insbesondere muss die Signaturerstellungseinheit nach ISO/IEC 15408:1999 auf Prüfstufe EAL 4 erhöht um die Versicherungselemente AVA_MSU.3, AVA_VLA.4 oder auf Prüfstufe E3 nach ITSEC zertifiziert sein.

Anforderung an den Umgang mit der sicheren Signaturerstellungseinheit sind in den folgenden Vorschriften enthalten:

- Art. 11 Abs. 1 VZertES (Verbot der Weitergabe der Signaturerstellungseinheit)
- Art. 11 Abs. 3 bis 5 VZertES (Aktivierung der Signaturerstellungseinheit und Umgang mit den Aktivierungsdaten, beziehungsweise mit der PIN)
- Kapitel 3.3.9 [TAV] (Eingabe der PIN, Sperrung und Freischaltung der Signaturerstellungseinheit)

Massnahmen beim Verlust der Signaturerstellungseinheit sind in der folgenden Vorschrift enthalten:

- Art. 11 Abs. 2 VZertES (Massnahmen bei Verlust oder Diebstahl)

6.4 Weiterführende Sicherheitsmassnahmen

In SAGA.ch V.2.1 Kapitel 8.12 sind folgende Sicherheitsmassnahmen empfohlen worden, welche beim Leisten einer elektronischen Unterschrift eines Benutzers (natürlichen Person) beachtet werden sollte.

Falls eine Operation mit dem privaten Schlüssel (des Benutzers) vorgenommen werden muss/soll, sei dies nur für die Authentisierung, für das Eingehen eines Rechtsgeschäfts oder für die Entschlüsselung¹⁰ einer E-Mail, dann muss Folgendes beachtet werden:

- *Der ganze Vorgang vom Start bis zur Beendigung muss so gestaltet sein, dass keine versteckten Programme wie Java, JavaScript, ActiveX heruntergeladen werden müssen/dürfen.*
- *Die Applikation beim Endgerät, welche für die eGovernment Dienstleistung benötigt wird, muss so konfiguriert werden können, dass das Herunterladen der genannten Programme nicht erlaubt ist und somit nicht stattfinden darf.*
- *Der eGovernment Vorgang muss trotz der genannten Einstellung abgewickelt werden können.*

Zusätzlich wird hier noch Folgendes beim Leisten einer anerkannt qualifizierten elektronischen Signatur empfohlen, wenn damit ein Rechtsgeschäft beurkundet wird:

- Das zu signierende Dokument muss nicht nur die Daten, sondern auch die Informationen über das Layout (Darstellung) des Dokuments enthalten. Sowohl Inhalt wie auch die Darstellungsinformation für das Dokument müssen dabei signiert werden, s. dazu CWA 14170, Kapitel 8, und CWA 14171, Kapitel 6.3.2.
- Die CA Zertifikate, welche Ausgangspunkt für die Verifikation der Zertifikate sind, sollten so gespeichert werden, dass sie nicht ungewollt ausgetauscht und ersetzt werden können.

6.5 Spam und Vertraulichkeit

Werden E-Mails oder Dokumente verschlüsselt übertragen, dann besteht keine Möglichkeit mehr, die E-Mails auf Spam oder die Dokumente und E-Mails auf Viren zu prüfen. Infolgedessen, sollten die E-Mails zuerst signiert, dann verschlüsselt und zuletzt wieder signiert werden. Zuerst sollte grundsätzlich signiert und dann verschlüsselt werden, ansonsten kann das Dokument nicht unverschlüsselt und authentisch gelagert werden, denn die Signatur schützt

¹⁰ Für die Entschlüsselung und die Signatur sollten unterschiedliche private Schlüssel verwendet werden. Folglich sind auch unterschiedliche Zertifikate mit entsprechender Deklaration des Verwendungszwecks auszustellen.

die Authentizität nur für das verschlüsselte, aber nicht für das unverschlüsselte Dokument. Dies würde die Archivierung ungemein erschweren. Damit nicht alle verschlüsselten E-Mails und Dokumente geöffnet werden, sollte doch zuerst vom Empfänger bestimmt werden können, wer diese E-Mails oder Dokumente versandt hat.

In Folgendem ist eine der Möglichkeiten beschrieben, das vorher beschriebene Problem zu lösen:

- Das zu bearbeitende Dokument wird zuerst signiert und dann verschlüsselt.
- Das verschlüsselte Dokument wird mit einer signierten E-Mail zugestellt.

6.6 Namensgebung

6.6.1 Einleitung

Die Namensgebung hat einen wesentlichen Einfluss darauf, wie zuverlässig die Prüfung der elektronischen Signatur erfolgt. Ein Benutzer hat bekanntlich in der IT meistens verschiedene Namen, wie

- Namen bei der Anmeldung an den verschiedenen Betriebssystemen
- Namen im Zertifikat
- E-Mail Adresse

Die in [Mus] beschriebene Attacke nutzt eine Schwäche aus, dass der Benutzer im Zertifikat einen anderen Namen als in der zu schützenden Applikation hat. Mit Hilfe dieser Schwäche kann dem Empfänger vorgetäuscht werden, dass die Botschaft von jemand anderem stammt, als von dem, welcher die Botschaft elektronisch signiert hat.

6.6.2 Massnahmen

Um der im letzten Unterkapitel beschriebenen Attacke vorzubeugen, werden folgende drei Massnahmen empfohlen:

1. Die Sicherheitsapplikation beschränkt sich bei der Authentisierung nicht lediglich auf die reine Prüfung der Signatur und der dazu passenden Zertifikate, sondern beachtet u.a. folgende Mindestanforderungen aus SAGA v2.1:

Die Auflistung der Kriterien basiert auf RFC 3850. Wenn nur eines der folgenden Kriterien erfüllt ist, dann muss die Sicherheitsapplikation eine Fehlermeldung herausgeben und je nach Policy die Verbindung abbrechen.

- *Die in der Applikation angezeigte oder zugängliche Absenderadresse oder Name des Absenders stimmt nicht mit der Adresse im Zertifikat überein oder ist nicht im Zertifikat enthalten.*

2. Die entsprechenden Namen des Benutzers bei der zu schützenden Applikation sind folglich ins Zertifikats aufzunehmen. Die im eGovernment verwendeten Namen sollten deshalb aber so gestaltet sein, dass die entsprechenden Namen ins Zertifikat auch aufgenommen werden können. Die entsprechenden Namen sollte ins Feld *Subject* oder *Subject Alternative Name* des Zertifikats eingetragen werden können.

3. Wie bereits erwähnt, besitzt der Benutzer in der IT verschiedenste Namen, welche dann jeweils bei der Ausstellung eines Zertifikats zu prüfen sind. Zusätzlich müssen dann die Zertifikate angepasst, d.h. neu ausgestellt werden, falls sich ein entsprechender Name ändert. Um diesen Aufwand möglichst gering zu halten, empfehlen wir:

- So wenige Namen wie absolut notwendig ins (qualifizierte) Zertifikat einfügen. Eine E-Mail Adresse im Zertifikat oder einer URL im Funktionszertifikat neben dem Distinguished Name werden aber weiterhin erforderlich sein.
- Die Applikationshersteller dazu zu bewegen, den Distinguished Name oder die E-Mail Adresse als Namen für die Anmeldung der Benutzer zu verwenden.

7 Archivierung elektronisch signierter Dokumente

Eine Archivierung elektronischer Signaturen und deren Dokumente oder Dateien drängt sich u.a. dann auf, wenn mit der Signatur ein rechtlich relevanter Sachverhalt zu einem späteren Zeitpunkt weiterhin beweisbar dargelegt werden soll. Die Archivierung elektronisch signierter Dokumente sollte u.a. so gestaltet werden, dass die Beweiskraft der elektronischen Signatur im Laufe der Zeit nicht verloren geht. Gleichzeitig muss aber auch definiert werden, wie die Verifikation elektronisch signierter Dokumente erfolgen soll. Ansonsten können keine Massnahmen zur Archivierung getroffen und umgesetzt werden.

7.1 Grundsätzliches

Auf folgenden Punkt soll hier hingewiesen werden:

Obwohl in Art. 9. Abs. 1 Bst. b Ziff. 1 GeBüV erwähnt, ist eine elektronische Signatur für den Schutz der *Unversehrtheit* der archivierten Daten unzureichend. Mittels einer elektronischen Signatur kann man höchstens feststellen, dass eine Integritätsverletzung der Daten eingetreten ist. Man kann damit aber nicht den Ursprungszustand der Daten vor der Veränderung oder vor dem Integritätsverlust herstellen. Dies ist für den Schutz der gelagerten Dateien ungenügend. Mittels einer elektronischen Signatur kann einzig eine sorgfältige Archivierung beglaubigt werden. Doch sollten die Daten trotzdem vor Veränderung zusätzlich geschützt werden.

Man sollte grundsätzlich unterscheiden, ob zum Schutz der archivierten Daten elektronische Signaturen eingesetzt werden oder elektronische Signaturen archiviert werden. Ersteres ist als alleinige Massnahme gemäss oben genannter Ausführung wenig sinnvoll.

Bei zweitem sind Vorkehrungen zu treffen, dass die Beweiskraft der elektronischen Unterschrift im Laufe der Zeit nicht verloren geht und die elektronische Signatur über eine lange Zeit verifiziert werden kann. Zur Problematik der Archivierung von elektronischen Signaturen, siehe auch www.archisig.de. Eine Einführung in die Problematik der Nachhaltigkeit elektronischer Signaturen, siehe [Mud] Kapitel 10. Eine umfassende Erläuterung dazu ist in [Bea] erhältlich.

Die Massnahmen zum Schutz der Beweiskraft elektronischer Signaturen sollten unter anderem Schutz gegen folgende Ereignisse bieten:

- Kompromittierung des Schlüssels
- Revokation des Zertifikats für die Prüfung der elektronischen Unterschrift
- Verfall des CA Zertifikats
- Verfall des Benutzer- oder Funktionszertifikats
- Schwächung der eingesetzten Verfahren, wie Hashfunktion (z.B. SHA-1), Public Key Verfahren (z.B. RSA)

Aus den oben genannten Ereignissen lässt sich erahnen, dass die zu treffenden Massnahmen nicht einfacher Natur sind.

7.2 Prüfung elektronischer Signatur

Grundsätzlich gilt es zu unterscheiden, ob eine elektronische Signatur für die online Authentisierung (s. Kapitel 4.2 Authentisierung mit elektronischer Signatur⁴) verwendet wird oder für die Unterzeichnung eines Rechtsgeschäfts.

Bei Ersterem liegen das Leisten der Signatur und deren Prüfung zeitlich nahe beieinander. In diesem Fall können die Anforderungen aus CWA 14171 oder die aus RFC 3850 sinngemäss angewandt werden. Hierzu die Empfehlungen aus SAGAv.2.1:

Wenn nur einer der folgenden Kriterien erfüllt ist, dann muss die Sicherheitsapplikation eine Fehlermeldung herausgeben und je nach Policy die Verbindung abbrechen.

- *Die Signatur kann mit dem Public Key im entsprechenden Zertifikat nicht erfolgreich geprüft werden.*
- *Die in der Applikation angezeigte oder zugängliche Absenderadresse stimmt nicht mit der Adresse im Zertifikat überein oder ist nicht im Zertifikat enthalten.*
- *Die Zertifikatskette führt nicht zu einem CSP, welcher man vertraut.*
- *Die CRL und Revokationsinformationen (z.B. nach OCSP) können nicht überprüft werden.*
- *Eine ungültige CRL wurde empfangen oder deren Gültigkeit ist abgelaufen.*
- *Das Zertifikat ist bereits abgelaufen oder revoziert worden.*

In zweitem Fall (Unterzeichnung eines Rechtsgeschäfts) kann die Prüfung der elektronischen Unterschrift zu einem viel späteren Zeitpunkt als das Leisten der Unterschrift erfolgen. Zu jenem Zeitpunkt können ein oder mehrere der im Kapitel 7.1 aufgeführten Ereignisse in der Zwischenzeit eingetreten sein.

Um diesen Ereignissen vorzubeugen und die Beweiskraft der elektronischen Unterschrift zu erhalten, sind unter anderem Zeitstempeldienste notwendig. In CWA 14171 sind Empfehlungen enthalten, welche Vorkehrungen dazu zu treffen sind.

7.3 Lösungsansätze

In CWA 14171 sind grundsätzliche Empfehlungen dazu enthalten, was bei der Archivierung von elektronisch signierten Dokumenten zu beachten gilt.

8 Produktzertifizierung

In [TAV] werden technische Anforderungen an Produkte festgehalten, wie die

- Schlüsselgenerierung (Kapitel 3.3.8)
- Sicherheitsanforderung an die Signaturerstellungseinheit (Kapitel 3.3.9)

Der Otto-Normalverbraucher kann aber nicht verifizieren, ob z.B. eine ihm ausgehändigte Signaturerstellungseinheit den Anforderungen aus [TAV] genügt oder den im Kapitel 6 oder 7.2 beschriebenen Sicherheitsanforderungen genügt. Deswegen ist z.B. im Kapitel 3.3.9 b) [TAV] auch vorgeschrieben, dass die verwendete Signaturerstellungseinheit entsprechend zertifiziert, im Sinne von beglaubigt, worden sein muss.

In der Schweiz wurde bisher noch keine Produktzertifizierung im Zusammenhang der in [TAV] referenzierten Normen durchgeführt. Es bestehen aber internationale Abkommen, wonach die Beglaubigungen (Zertifizierungen) anderer Produkte von Prüfstellen in der Schweiz anerkannt sind. Eine ausländische Zertifizierung eines IT-Sicherheitsprodukts ist in der Schweiz gültig, wenn

- das entsprechende Land bzw. die entsprechende ausländische Akkreditierungsstelle ein "Multilateral Agreement" (MLA) der EA (European Agreement) für den Bereich der Produktzertifizierung unterzeichnet hat. Länderliste und Informationen über MLA findet man unter <http://www.sas.ch/de/akkreditierung/zusammenarbeit.html> und <http://www.european-accreditation.org/> unter der Rubrik „Products“.
- die entsprechende ausländische Zertifizierungsstelle (im Sinne von Beglaubigungsstelle) gemäss der Norm EN 45011 akkreditiert wurde.
- das entsprechende Produkt gemäss der Norm ISO/IEC 15408:1999 / CC (Common Criteria) oder ITSEC zertifiziert wurde und die Sicherheitsanforderungen der in den [TAV] referenzierten Dokumente erfüllt sind.

Die Vorschriften zur Akkreditierung einer Prüfstelle sind in der Verordnung AkkBV enthalten.

Anmerkung: Bei der Anerkennung eines CSP überprüft die Anerkennungsstelle, ob die oben erwähnten Konditionen für die beim CSP eingesetzten Produkte erfüllt sind.

9 Beantwortung der Fragen im Antrag

1. Wie hat die elektronische Eingabe von Dokumenten an die Behörden zu erfolgen, signiert, qualifiziert signiert? Bedarf es der qualifizierten Signatur für die notwendige Beweiskraft der erhaltenen Quittungen oder Bestätigungen? Welche Beweiskraft hat die nicht qualifizierte, die fortgeschrittene digitale Signatur?

Diese Fragen sind im Kapitel 3 „Wirksamkeit elektronischer Signaturen“ beantwortet worden.

2. Welche Zertifikate braucht es für Server und welche Beweiskraft hat deren Signatur? Anwendungsfall: Elektronische Eingabe von Dokumenten an die Behörde, Herunterladen von Informationen, automatische Ausstellung von Quittungen und Belegen.

Diese Frage ist im Kapitel 5 „Funktionszertifikate“ beantwortet worden. Im übrigen ist mit der revidierten EIDI-V geplant, die Server- oder Funktionszertifikate einzuführen und die Anforderungen an diese zu definieren.

3. Welche Identitätskennungen (z. Bsp. Personennamen, E-Mail Adressen) sollen im e-Government Umfeld erlaubt sein, insbesondere bei Dokumenten mit qualifizierter digitaler Signatur oder bei der Authentisierung mittels digitaler Signatur? Gibt es Unterschiede bei der Identitätskennung in den Anwendungen per se? Gibt es Unterschiede bei der Identitätskennung im Verkehr zu den Gemeinden, zu den Kantonen bzw. zum Bund?

Grundsätzlich sollten Identitätskennungen so gewählt werden, dass sie ins Zertifikat eingefügt werden können, ansonsten kann dies zu Sicherheitsproblemen bei auf Public Key basierten Sicherheitstechnologien führen, s. [Mus]. Selbstverständlich gibt es Unterschiede in der Identitätskennung bei der Behörde, doch diese sollten absolut minimal gehalten werden, s. dazu Kapitel 6.6 „Namensgebung“.

4. Welchen Einfluss hat Punkt 3 auf den Zertifikatsinhalt und auf die zu prüfende Identitätskennung in den Zertifikaten?

Sämtliche ins Zertifikat aufgenommenen Identitätskennungen oder Attribute sollten geprüft werden, bevor sie ins Zertifikat aufgenommen werden, ansonsten kann dies zu Sicherheitsproblemen führen, s. [Mus].

5. Welchen Gültigkeitsstatus haben elektronische Signaturen nach Ablauf oder nach Ungültigkeitserklärung des Zertifikats?

s. Kapitel 7.1 „Grundsätzliches“ 7.2 „Prüfung elektronischer Signatur“

6. Welche Konsequenzen ergeben sich daraus für die Aufbewahrungspflicht und für die Archivierung elektronisch signierter Dokumente?

s. Standard CWA 14 171

7. Wie sind die Zertifikatsformate für vertrauliche E-Mail Korrespondenz, bzw. wie lauten die Anforderungen an die vertrauliche, signierte Aufbewahrung von Dokumenten?
 - s. Kapitel 4.3.3 „Mindestvorschriften“

8. Wie muss ein vertrauliches Dokument versendet werden:
 - a) signiert und verschlüsselt?
 - b) signiert und verschlüsselt und signiert?
 - s. Kapitel 6.5 „Spam und Vertraulichkeit“

9. Bedarf es der Produktzertifizierung im Bereich qualifizierter Signatur. Welche Akzeptanz sollen Produkte haben, welche von einer ausländischen Behörde zertifiziert worden sind?
 - s. Kapitel 8 „Produktzertifizierung“

10. Wie lauten die minimalen Anforderungen an die Sicherheit der PC und Smart Cards bei der Herstellung qualifizierter, elektronischer Signaturen?
 - s. Kapitel 6 „Sicherheitsanforderungen“.

Anhang A – Referenzen

- [01.023] Botschaft zur Totalrevision der Bundesrechtspflege vom 28. Februar 2001
- [01.044] Botschaft des Bundesrates vom 3. Juli 2001 zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur
- [AkGd] Kurt Amonn, Dominik Glauser, Grundriss des Schuldbetreibungs- und Konkursrechts, Stämpfli Verlag, Bern 1997
- [Bea] Bertsch Andreas, Digitale Signaturen, Springer Verlag, 2002
- [GSSR] Gauch, Schluop, Schmid, Rey, Schweizerisches Obligationenrecht Band I und II, 7. Auflage, Schulthess Verlag 1998
- [HUMG] Häfelin Ulrich, Müller Georg, Grundriss des allgemeinen Verwaltungsrechts, 3. Auflage, Schulthess Verlag 1998
- [ISB 1] ISB, Regieren in der Informationsgesellschaft, Die eGovernment-Strategie des Bundes, 14. Februar 2002, Seite 9 ff, herunterladbar bei www.isb.admin.ch unter der Rubrik eGovernment.
- [KaHi] Alfred Kölz, Isabelle Häner, Verwaltungsverfahren und Verwaltungsrechtspflege des Bundes, 2. Auflage, Schulthess Verlag 1998
- [KeA] Keller Alfred, Haftpflicht im Privatrecht, Band I, 5. Auflage 1993, Stampfli Verlag
- [Mud] Muster Daniel, Digitale Unterschriften und PKI, 2. Auflage 2002
- [Mus] Muster Daniel, Attacke auf die Authentifizierung, Version 1.3, Juni 2004, als pdf bei www.sgrp.ch „public“ und beim Bakom unter der Rubrik eingegangene Stellungnahmen zu VZertES
- [Sch] Schneier Bruce, Angewandte Kryptographie, Addison Wesley Verlag, 1. Auflage 1996
- [Sci] Ingeborg Schwenzer, Schweizerisches Obligationenrecht Allgemeiner Teil, Stämpfli Verlag, Bern 2000
- [Tsp] Paul Tschümperlin, XIV. Treffen der obersten Verwaltungsgerichtshöfe Österreichs, Deutschlands, des Fürstentums Liechtenstein und der Schweiz, Landesbericht der Schweiz, Graz 2004, zu finden unter www.bger.ch/publication-federal-bedeutung-e-government-download.pdf
- CWA 14167-3 Security Requirements for Trustworthy System Managing Certificates for Electronic Signatures – Part 3: Cryptographic Module for CSP Key Generation Services – Protection Profile – CMCSO PP, May 2004
- CWA 14170 CEN (European Committee for Standardization), Security Requirements for Signature Creation Applications, May 2004
- CWA 14171 CEN (European Committee for Standardization), General Guidelines for electronic signature verification, May 2004
- ETSI SR 002 Electronic Signatures and Infrastructures (ESI) – Algorithms and Parameters for Secure Electronic Signatures
0176 v1.1.1

ETSI TS 101 456 v.1.2.1	Policy Requirements for Certification Authorities Issuing Qualified Certificates
ISO/IEC 15408: 1999	Information Technology – Security Techniques. Evaluation Criteria for IT Security
RFC 3850	S/MIME v.3.1 Certificate Handling
SAGA.ch	Standards und Architekturen für eGovernment Anwendungen in der Schweiz, V1.0, Standard des Vereins <i>eCH</i>
VPB 63.46	Gutachten des Bundesamts für Justiz vom 24. November 1998, Digitale Signatur und Privatrecht (Vertragsrecht), http://www.vpb.admin.ch/deutsch/doc/63/63.46.html
X.509	ITU-T Recommendation X.509v3 (2000), Information Technology –Open System Interconnection – The Directory: Public Key and Attribute Certificate framework

Anhang B – Mitarbeit & Überprüfung

Anhang C – Abkürzungen und Gesetzestexte

[TAV]	Technische und administrative Vorschriften des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)
Abs.	Absatz
AES	Advanced Encryption Standard
AkkBV	Verordnung vom 17. Juni 1996 über das Schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (SR 946.512)
Art.	Artikel
BankG	Bundesgesetz vom 8. November 1934 über Banken und Sparkassen (SR 952.0)
BBl	Bundesblatt
BGG	Bundesgesetz vom 17. Juni 2005 über das Bundesgericht (s. BBl 2005 4045)
Bst.	Buchstabe
BZP	Bundesgesetz vom 4. Dezember 1947 über den Zivilprozess (SR 273)
CA	Certification Authority (Ausstellerin von Zertifikaten)
CEN	Comité Européen de Normalisation
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (SR 235.1)
EA	European Agreement

EFD	Eidgenössische Finanzdirektion
EIDI-V	Verordnung des EFD vom 30. Januar 2002 über die elektronisch übermittelten Daten und Informationen (SR 641.201.1)
EMPA	Eidgenössische Materialprüfungs- und Forschungsanstalt
ff.	Folgende
G2C	Government to Citizen
G2G	Government to Government
GeBüV	Verordnung vom 24. April 2002 über die Führung und Aufbewahrung der Geschäftsbücher (SR 221.431)
GOG	Government to Organisation
KKG	Bundesgesetz vom 23. März 2001 über den Konsumkredit (SR 221.224.1)
MAC	Message Authentication Code
MLA	Multilateral Agreement
OG	Bundesgesetz vom 16. Dezember 1943 über die Organisation der Bundesrechtspflege (SR 173.110)
OR	Schweizerisches Obligationenrecht vom 30. März 1911 (SR 220)
Rz	Randziffer
s.	siehe
SchKG	Bundesgesetz vom 11. April 1889 über Schuldbetreibung und Konkurs (SR 281.1)
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0), in Kraft seit 1. Januar 1942
u.a.	unter anderem
VDSG	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (SR 235.11)
VG	Bundesgesetz vom 14. März 1958 über die Verantwortlichkeit des Bundes sowie seiner Behördemitglieder und Beamten (Verantwortlichkeitsgesetz) (SR170.32)
VGG	Bundesgesetz vom 17. Juni 2005 über das Verwaltungsgericht (BBl 2005 4093)
VVG	Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (SR 221.229.1)
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)
z.B.	zum Beispiel
ZertES	Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)

Anhang D – Haftung gemäss OR 59a

Die gewöhnliche Haftung nach Art. 41 ff. OR, auch Verschuldenshaftung genannt, verlangt 4 Voraussetzungen, welche vom Kläger (Geschädigten) **zu beweisen** sind, siehe [KeA], Seite 114 ff.):

- Ein Schaden muss entstanden sein.
- Der Schaden selber muss widerrechtlich¹¹ sein.
- Der Beklagte muss den Schaden verursacht haben (Adäquater Kausalzusammenhang¹² zwischen der Widerrechtlichkeit und dem Schaden).
- Ein Verschulden von Seiten des Beklagten, sei es Fahrlässigkeit oder Absicht, muss vorliegen.

Bemerkung zur Widerrechtlichkeit: "Widerrechtlichkeit liegt im objektiven Verstoss einer Norm und entfällt bei Vorliegen eines Rechtfertigungsgrund" (BGE 115 II 18, BGE 118 Ib 476). Gemäss [KeA], S. 90 und 91, kann der Schaden als solcher bereits eine Widerrechtlichkeit beinhalten, wenn ein absolutes Rechtsgut verletzt wird (Leib und Leben, Eigentum), siehe auch BGE 118 Ib 476. Rechtfertigungsgründe sind z.B. Notwehr (Art. 52 OR), das Handeln auf gesetzlicher Grundlage, Amtspflicht oder Einwilligung des Geschädigten (u.a. Patient beim Arzt).

Die Beweislast für die Widerrechtlichkeit obliegt dem Geschädigten (Kläger). Die Darlegung der Rechtfertigungsgründe obliegen dagegen dem Beklagten.

Bemerkung zur Fahrlässigkeit: „Fahrlässig verhält sich, wer die Sorgfalt nicht beachtet, ...“, [KeA] S. 101. Fahrlässiges Verhalten kann z.B. in der Herbeiführung eines gefährlichen Zustands, einer Fehlreaktion oder in **der Missachtung von Vorschriften oder Gesetzen** liegen (s. [KeA], S. 101 ff.). Die Missachtung von Vorschriften oder Gesetzen birgt ein widerrechtliches Verhalten des Schädigenden in sich, welches zum widerrechtlichen Schaden führt.

¹¹ Zum Begriff Widerrechtlichkeit, siehe [KeA], Seite 89 ff

¹² Zum Begriff Kausalzusammenhang, siehe [KeA], Seite 65 ff.

Dazu ein fiktives Beispiel:

Ein gross gewachsener, schwer gewichtiger Mann überquert die Strasse bei roter Ampel und kollidiert dabei mit einem (ausnahmsweise) korrekt fahrenden Velofahrer mit schwächlichem Körperbau. Der Velofahrer stützt und erleidet dabei Schürfwunden und eine leichte Hirnerschütterung. Das defekte Vorderrad des Velos muss ersetzt werden. Der widerrechtliche Schaden (Schürfwunden, Hirnerschütterung, defektes Vorderrad) beruht auf fahrlässigem Verhalten (Verletzung der Sorgfaltspflicht). Der Passant hat sich widerrechtlich verhalten, indem er bei roter Ampel die Strasse überqueren wollte.

Art. 59a OR ist eine **besondere Art der Verschuldenshaftung**. Im Unterschied zur gewöhnlichen Verschuldenshaftung nach Art. 41 OR verlangt Art. 59a OR für einen möglichen Ausschluss der Haftung, dass der Inhaber des Signaturschlüssels *glaubhaft* machen oder davon überzeugen muss, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern. Er muss also glaubhaft darlegen, dass er die Sicherheitsvorkehrungen gemäss Art. 11 VZertES eingehalten und eine sichere Signaturerstellungseinheit gemäss [TAV] eingesetzt hat, also nicht gegen diese Normen fahrlässig oder absichtlich verstossen hat.

Im Unterschied zu Art. 59a OR muss der Zertifizierungsdiensteanbieter gemäss Art. 16 ZertES *beweisen*, dass er die Pflichten aus ZertES und dessen Ausführungsbestimmungen eingehalten hat, d.h. nicht gegen diese Normen verstossen und sich also diesbezüglich nicht widerrechtlich verhalten hat.

Hierzu auch ein Auszug aus einer Stellungnahme von Herrn Dr. Felix Schöbi EJPD zur Haftung nach Art. 59a OR.

„Ich vertrete tatsächlich die Meinung (diese wurde in der Rechtskommission des Nationalrats, die sich mit der Frage kurz befasste, bestätigt), dass es sich bei Artikel 59a OR um eine Verschuldenshaftung handelt (*responsabilité pour faute*). Sie kommt nur dann zum Zug, wenn der Inhaber des Signaturschlüssels gesetzliche Sorgfaltspflichten missachtet hat und ihm die Missachtung dieser Sorgfaltspflichten auch subjektiv zum Vorwurf gemacht werden kann. Der Urteilsunfähige kann nicht zur Verantwortung gezogen werden. Dem Geschädigten kommt Artikel 59a OR nur insoweit entgegen, als der Inhaber des Signaturschlüssels die Beweislast dafür trägt, mit dem Signaturschlüssel sorgfältig umgegangen zu sein. Im Übrigen will Artikel 59a OR klarstellen, dass der Inhaber des Signaturschlüssels auch für so genannte reine Vermögensschäden haftet.

Die Lehre bezeichnet gewisse Haftungen im Anschluss an Artikel 41 OR als "milde Kausalhaftungen" (namentlich die Art. 56, 58 OR, Art. 333 und 679 ZGB). Die genaue Tragweite dieser Aussage bleibt jeweils recht diffus. Als gemeinsamer Nenner bleibt höchstens die Vorstellung, dass jemand unabhängig von einem subjektiven

Vorwurf zur Verantwortung gezogen werden kann, im Extremfall also auch ein Urteilsunfähiger haftet. Den "Praxistest" hat diese Theorie allerdings bisher meines Wissens noch nie bestehen müssen, d.h. mir ist kein Fall bekannt, dass (beispielsweise) ein Werkeigentümer aus Artikel 58 OR zur Verantwortung gezogen worden wäre, obwohl er urteilsunfähig war. Vor diesem Hintergrund besteht für mich kein Anlass, die in ihrer Nützlichkeit umstrittene Kategorie milder Kausalhaftungen um den Tatbestand von Art. 59a OR zu ergänzen.“

Anhang E – MAC

MAC ist eine mit einer Hashfunktion und einem Schlüssel hergestellte Prüfsumme und dient der Authentisierung der versandten Datenpakete.

Alice und Bob haben ein digitales Geheimnis G, einen Schlüssel, vereinbart. Alice will das Paket P Bob zustellen. Alice fertigt eine Kopie des Pakets P an und fügt dem Paket P das Geheimnis G hinzu. Aus Paket P und Geheimnis G wird eine Prüfsumme mit einer Hashfunktion angefertigt. Diese Prüfsumme heisst MAC. Das ursprüngliche Paket P (ohne Geheimnis) zusammen mit dem MAC Wert wird nun Bob zugestellt.

Beim Empfang des Pakets P und dem MAC Wert stellt Bob mit P und G auch einen MAC Wert her. Sind der empfangene und der selber hergestellte MAC Wert identisch, glaubt Bob zu wissen, dass das Paket von Alice stammt. Nur sie kennt das Geheimnis G und kann folglich die richtige Prüfsumme hergestellt haben.

Anhang F – Urheberrechte

Wer *eCH*-Standards erarbeitet, behält das geistige Eigentum an diesen Arbeitsergebnissen. Allerdings verpflichtet sich der Erarbeitende mittels spezieller, schriftlicher Vereinbarung, sein Arbeitsergebnis, sofern möglich, den jeweiligen Fachgruppen und dem Verein *eCH* kostenlos zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von *eCH* unentgeltlich genutzt werden. *eCH*-Standards sind frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die 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 werden. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Wichtig: Die Standards einiger hier angegebenen Organisationen sind **nicht frei verfügbar** und sind **kostenpflichtig**. Ebenso kann der Einsatz und die Verwendung der hier aufgeführten Technologien lizenz- und/oder kostenpflichtig sein.

Bei einigen Technologien und Verfahren, wo uns bekannt, ist darauf hingewiesen worden, dass die Nutzung lizenz- und/oder kostenpflichtig ist.

Wird diesbezüglich nichts erwähnt, besteht keine Gewähr dafür, dass weitere hier aufgeführten Technologien/Verfahren nicht lizenz- und/oder nicht kostenpflichtig sind. **Vor einem etwelchen Gebrauch dieser Technologien/Verfahren** sind die **Lizenzbedingungen** unbedingt umfassend **abzuklären** und einzuhalten.