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

Name	Relevantes und Wissenswertes zur Anwendung der elektronischen Signatur (im eGovernment), ein Dossier
Version	**2.0 Juni 2007**
Status	Revidiertes Arbeitsergebnis der eCH Fachgruppe Digitale Signatur („White Paper“). Die Version 1.3 des Dokuments enthielt den endgültigen Text, welchen die Fachgruppe Digitale Signatur Ende 2005 erarbeitet hat. Infolge des Inkrafttretens neuer Gesetze oder der Änderungen bestehender Gesetze im Januar 2007 erweist sich nun eine Anpassung des Dokuments als unumgänglich. Wie bei allen früheren Versionen handelt sich auch hier um eine Version des Dokuments der Fachgruppe, welches dem **Expertenausschuss** von ***eCH*** **nicht** unterbreitet worden ist.
Basiert auf	u.a. auf dem Gutachten des Bundesamtes für Justiz VPB 63.46
Sprache	Deutsch
Herausgeber	Verein ***eCH***, Amthausgasse 18, 3011 Bern Tel. 031 560 00 20, Fax 031 560 00 25 www.ech.ch / info@ech.ch
Autoren	Daniel Muster (Bit Pattern Security) Jean-Maurice Geiser (BAKOM) Christian Jenny (BAKOM) Maria Winkler (IT & Law Consulting GmbH)
Weitere Mitwirkende	Attila Laczko (EVD) Michael R. Vetterli (SignPool Group AG), Leiter der Fachgruppe Lorenz Neher (Swisscom Solutions AG) Daniel Gabi (Schweizerische Bundeskanzlei) Dr. Jacques Bühler (Schweizerisches Bundesgericht) Dr. Thomas Hügi (OPENLiMiT Holding AG) Peter Balsiger (Bundesamt für Informatik) Michael Doujak (SwissSign AG) Daniel Gerber Ralf Hauser Elena Jent-Dellis (Telekurs Paynet AG) Carl Rosenast (Quovadis AG)
Redaktionelle Hoheit	Fachgruppe Digitale Signatur Verein ***eCH***

Ansprechpartner	Michael Vetterli, SignPool Group AG, michael.vetterli@signpool.com Daniel Muster, Bit Pattern Security, 8048 Zürich, daniel.s.muster@bluewin.ch Verein ***eCH***, Amthausgasse 18, 3011 Bern Tel. 031 560 00 20, Fax 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.**

Noch nicht viele praktische Fragen lassen sich 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 7.3.2)
- Archivierung von elektronisch signierten Dokumenten (s. Kapitel 7.3“)
- Tipps bei der Namensgebung im Zertifikat (s. Kapitel 6.7)
- Tipps bei der Nutzung von vertraulichen E-Mails in Zusammenhang mit Spam (s. Kapitel 6.6) und beim Einsatz qualifizierter Zertifikate (s. Kapitel 4.1).

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).

Es kann durchaus sein, dass ein oder mehrere Mitglieder 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 Geschäftstelle
E-Mail: info@eCH.ch
Homepage und Download der digitalen Version: www.eCH.ch

Inhaltsverzeichnis

BEGRIFFE (GLOSSAR) 7

1 EGOVERNMENT ANWENDUNGEN 11

1.1 Akteure und Beziehungen 11

1.2 Der elektronische Zugang zu Behörden 11

1.3 Das hoheitliche Handeln der öffentlichen Verwaltung 11

1.4 Eingaben an Gerichte und Behörden 12

1.5 Die Zustellung 13

2 WIRKSAMKEIT ELEKTRONISCHER SIGNATUREN 14

2.1 Einleitung 14

2.2 Elektronische Signatur und Privatrecht 14

2.2.1 Kontext zu Europa 15

2.3 Die Verwendung der elektronischen Signatur im Bereich eGovernment 16

2.3.1 Die Ausgabe von Zertifikaten nach ZertES 16

2.3.2 Gleichstellung der elektronischen Unterschrift mit der Handunterschrift im eGovernment 16

2.3.3 Überblick 16

2.3.4 Zugang zum Bundesgericht 17

2.3.5 Bundesverwaltungsverfahren 17

2.3.6 Zugang zum Bundesverwaltungsgericht 17

2.3.7 Zugang zum Bundesstrafgericht 17

2.3.8 Empfehlung im Umgang mit den Behörden 18

2.4 Technischer Zugang 18

2.5 Zusammenfassung 18

3 ABSICHERUNG (HAFTUNG) 19

3.1 Haftungsbestimmungen im OR 19

3.2 Haftungsbestimmungen im ZertES 20

3.3 Haftungsbestimmungen im VG 20

3.4 Schlussfolgerung 22

3.5 Anmerkung zu qualifizierten elektronischen Zertifikaten 23

3.6 Zusammenfassung 24

4 ZUGANG ZU SENSITIVEN INFORMATIONEN 25

4.1 Einleitung 25

4.1.1 Funktionsweise der online Authentisierung 26

4.2 Authentisierung mit elektronischer Signatur 26
4.3 Authentisierung mit Entschlüsselung 27
4.3.1 Wie funktioniert es? 27
4.3.2 Rechtliche Probleme 28
4.3.3 Mindestvorschriften 29
4.4 Anmerkung 29
4.5 Digitale ID und Zertifikate 30
5 FUNKTIONSZERTIFIKATE 31
5.1 Einleitung 31
5.2 Angst vor funktionellen Signaturen 31
5.3 Einsatzgebiete für Funktionszertifikate 32
5.3.1 Besonders wichtige Einsatzgebiete 33
5.4 Lösungsansätze 33
5.5 Anmerkung 34
5.6 Beispiel zur Haftung 35
5.7 Beispiel zu einer praktischen Implementation 36
6 SICHERHEITSANFORDERUNGEN 37
6.1 Einleitung 37
6.2 Überblick 37
6.3 Zusammenstellung der bestehenden Vorschriften 38
6.4 Handhabung der Zertifikate 39
6.5 Weiterführende Sicherheitsmassnahmen 39
6.6 Spam und Vertraulichkeit 40
6.7 Namensgebung 41
6.7.1 Einleitung 41
6.7.2 Massnahmen 41
6.8 Bemerkungen zu den Sicherheitsvorschriften 42
7 ARCHIVIERUNG ELEKTRONISCH SIGNIERTER DOKUMENTE 43
7.1 Elektronische Beglaubigung 43
7.2 Signatur und Schutz der Integrität 43
7.3 Erhaltung der Beweiskraft digital signiert Dokumente 44
7.3.1 Massnahmen zum Erhalt der Beweiskraft 44
7.3.2 Prüfung der elektronischen Signatur 45
7.3.3 Lösungsansätze 45

8 PRODUKTZERTIFIZIERUNG 46

9 BEANTWORTUNG VON FRAGEN 47

9.1 Beantwortung der Fragen im Antrag 47

9.2 Häufig gestellte Fragen 48

10 ZUSAMMENFASSUNG 49

10.1 Allgemeines 49

10.2 eGovernment Anwendungen 49

10.3 Wirksamkeit elektronischer Signaturen 49

10.4 Absicherung (Haftung) 50

10.5 Zugang zu sensitiven Informationen 50

10.6 Funktionszertifikate 51

10.7 Sicherheitsanforderungen 51

10.8 Archivierung elektronisch signierter Dokumente 52

10.9 Produktzertifizierung 52

ANHANG A – REFERENZEN 54

ANHANG B – MITARBEIT & ÜBERPRÜFUNG 55

ANHANG C – ABKÜRZUNGEN UND GESETZESTEXTE 55

ANHANG D – HAFTUNG GEMÄSS OR 59A 57

ANHANG E – MAC 59

ANHANG F PRINZIP DER PUBLIC KEY KRYPTOGRAPHIE 60

ANHANG G – URHEBERRECHTE 61

INDEX 62

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	Rechtlicher Begriff aus dem BGG (Art. 42 Abs. 4) und dem revidierten VwVG (Art. 21a Abs. 2 und Art. 34 Abs. 1^{bis}). In Art. 4 Abs. 3 ReRBGer wird festgelegt, dass die vom Bundesgericht anerkannten elektronische Signaturen in einer Liste bei der Zustellplattform für die Eingabe von Rechtsschriften ans Bundesgericht aufgeführt sind. In einer Verordnung zum VwVG wird festgelegt werden, welche elektronischen Signaturen als anerkannt im Sinne des VwVG gelten. Eine qualifizierte elektronische Signatur, welche mit einem qualifizierten Zertifikat eines nach ZertES anerkannten CSP verifiziert werden kann, sollte den Anforderungen genügen.
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	Certification Authority. Institution, welche Zertifikate ausstellt.
Crypto Card	Die Crypto Card hat die Form einer Bankkarte mit einem Mikroprozessor-Chip und stellt eine mögliche Ausprägung einer sicheren Signaturerstellungseinheit dar.
CSP	Anbieterin von Zertifizierungsdiensten, engl. Certification 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. Technische Definition: Die elektronische Signatur eines Dokuments ist der mit dem privaten Schlüssel verschlüsselte Hashwert des Dokuments. Der Hashwert ist eine kryptographische Prüfsumme des signierten Dokuments. Für weitere Informationen zur elektronischen Signatur, s. [Sch] und [Mud]. Die Sicherheit der elektronischen Signatur basiert sowohl auf der Sicherheit der Verschlüsselungsverfahren als auch auf der Herstellung der Hashwerte.
Fortgeschrittene elektronische Signatur	Definition s. Art. 2 lit. b ZertES. Zur Abgrenzung siehe auch „Qualifizierte elektronische Signatur“ im Glossar.
Fortgeschrittenes Zertifikat	Zertifikat, welches für die Prüfung einer fortgeschrittenen elektronischen Signatur verwendet wird.
Funktionelle elektronische Signatur	Eine elektronische Signatur, welche mittels eines Funktionszertifikats verifiziert werden kann.
Funktionszertifikate	Zertifikate, welche nicht einer natürlichen Person zugeordnet werden, z.B. Zertifikate für eine juristischen Person, eine öffentlich-rechtliche Institution oder eine Behörde ausgestellt worden sind oder 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.
Hashfunktion	Funktion, welche Hashwerte herstellt, zu Hashfunktionen s. [Sch].
Hashwert	Kryptographische Prüfsumme
Öffentlicher Schlüssel	Bei der Signatur ist es der Signaturprüfschlüssel, bei der Vertraulichkeit der Verschlüsselungsschlüssel, engl. Public Key, Zertifikatsschlüssel (Schlüssel im Zertifikat)
Online Authentisierung	Authentisierung für die online Datenkommunikation. Bei der online Datenkommunikation werden die versandten Daten unmittelbar nach Empfang weiterverarbeitet, wie z.B. bei der Client Server Kommunikation. Im Gegensatz dazu werden z.B. E-Mails einmal versandt und in ein „Postfach“ abgelegt. Das Lesen und Verarbeiten der E-Mail kann zu einem beliebigen Zeitpunkt später erfolgen. Deswegen wird der Austausch von E-Mails nicht der online Datenkommunikation zugeordnet.
Privater Schlüssel	Bei der Signatur ist es der Signaturschlüssel, bei der Vertraulichkeit der Entschlüsselungsschlüssel, engl. Private Key.

Provisorische Rechtsöffnung	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.). 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.).
Qualifizierte elektronische Signatur	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.
Qualifiziertes Zertifikat	s. Art. 2 Bst. f ZertES: Ein digitales Zertifikat, das die Anforderungen des Artikels 7 ZertES erfüllt.
Qualifiziertes Zertifikat einer anerkannten CA	Ein qualifiziertes Zertifikat, welches von einer nach ZertES anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt worden ist.
Revokation	Ungültigkeitserklärung, Vorgang, etwas für ungültig zu erklären.
Schriftlichkeit	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. 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. Schriftlichkeit im Rahmen von Verwaltungs- und Gerichtsverfahren bedeutet, dass die Information in Schriftform abgefasst und zugestellt und nicht mündlich mitgeteilt wird. 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).
Server	Server ist ein Computer, ein Programm oder Applikation, welche eine bestimmte Dienstleistung bietet. Das englische Verb „to serve“ hat die Bedeutung „Dienen“. In gewissen nicht technischen Kreisen wird Server auch lediglich mit einem Web Server assoziiert, welcher über das http Protokoll angesprochen werden kann.

Signaturprüfschlüssel	Schlüssel zur Prüfung der Signatur, öffentlicher Schlüssel, welcher im Zertifikat enthalten ist.
Signaturschlüssel	Privater und geheim zu haltender Schlüssel. Für die qualifizierte elektronische Signatur hat sich der Schlüssel in einer sicheren Signaturerstellungseinheit zu befinden.
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	Zeitstempel: Eine mit dem Datum, der Uhrzeit und der elektronischen Signatur versehene Bescheinigung, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt existiert haben. Zeitstempeldienst: Dienst, der eine mit dem Datum, der Uhrzeit und der elektronischen Signatur versehene Bescheinigung abgibt, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt existiert haben. Definition eines nach ZertES anerkannten Zeitstempeldienst: „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] Ein gemäss ZertES anerkannter CSP hat nach ZertES anerkannte Zeitstempeldienste anzubieten (Art. 12 ZertES).

1 eGovernment Anwendungen

1.1 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.

1.2 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. Der elektronische Zugang zu den Behörden wurde für das Bundesverwaltungsverfahren auf Bundesebene (nicht aber auf kantonaler und kommunaler Ebene) mit der Revision des Bundesgesetzes über das Verwaltungsverfahren (VwVG) geregelt. Die Revision des VwVG ist seit 1.1.2007 in Kraft. Eine Vollzugsverordnung ist in Bearbeitung.

1.3 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 Verwaltungsaufgaben 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 nichtstreitigen 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 „anderen“ 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.

1.4 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. 42 Abs. 1 BGG[1]) oder bei Beschwerden in einem Verwaltungsverfahren (Art. 52 Abs. 1 und 3 VwVG). Nach dem Inkrafttreten des Bundesgerichtsgesetzes (BGG) und des revidierten VwVG ist seit dem 1.1.2007 möglich, Rechtsschriften auch elektronisch ans Bundesgericht und in einem bundesrechtlichen Verwaltungsverfahren einzureichen. Gemäss Art. 42 Abs. 4 BGG müssen die Rechtsschriften, welche elektronisch an das Bundesgericht eingereicht werden, aber mit einer „anerkannten, elektronischen“ Signatur versehen werden. Das gilt auch für die Eingaben im Bundesverwaltungsverfahren (Art. 21a Abs. 2 VwVG).

[1] Das BGG hat am 1.1.2007 das OG abgelöst.

Wichtig: Der Bundesrat hat gemäss Schlussbestimmung zur Änderung des VwVG aber die Möglichkeit, die elektronische Eingabe von Schriften auf bestimmte Behörden und Verfahren während 10 Jahren einzuschränken oder zu unterbinden. Eine Verordnung dazu liegt im Entwurf vor, wurde aber noch nicht verabschiedet.

1.5 Die Zustellung

Die **Eröffnung der Verfügung** oder die Zustellung eines Gerichtsentscheids ist grundsätzlich eine empfangsbedürftige einseitige Rechtshandlung. 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]).

Die Zustellung von Verfügungen auf Bundesebene im Verwaltungsverfahren (Art. 34 Abs. 1^{bis} VwVG) und die Eröffnung eines Entscheids des Bundesgerichts (Art. 60 Abs. 3 BGG) können seit 1.1.2007 bei Einverständnis der Partei auch auf elektronischem Weg erfolgen. Zur Zustellung von Verfügungen auf elektronischem Weg siehe auch Kapitel 5.3.1 „Besonders wichtige Einsatzgebiete“.

2 Wirksamkeit elektronischer Signaturen

2.1 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.

2.2 Elektronische Signatur und Privatrecht

Verträge, für welche das Gesetz oder die Parteien selbst die einfache Schriftform vorgesehen haben, können nun auch gültig elektronisch abgeschlossen werden (Art. 14 Abs. 2^{bis} OR). Das Schweizerische Vertragsrecht baut aber auf dem Grundsatz der Vertragsfreiheit auf. Teil der Vertragsfreiheit ist die **Formfreiheit** (Art. 11 Abs. 1 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.:

- 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)

Auch nach dem Inkrafttreten des ZertES können 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 Vereinbarungen 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 per se 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.

Die Gleichstellung gemäss Art. 14 Abs. 2^{bis} OR ist nicht anwendbar:

- Wenn dies die Vertragsparteien ausschliessen oder sich die Parteien auf eine andere Art oder Güte der elektronischen Signatur einigen (Art. 14 Abs. 2^{bis} OR).
- Bei einer öffentlichen Beurkundung und beim Wertpapierrecht.
- Wenn das Gesetz bei der Unterschrift Eigenschriftlichkeit verlangt.
- Wo ein Formularzwang gilt und die Behörde das Formular noch nicht digital zur Verfügung stellt.
- Oder wenn nach der Rechtssprechung des Bundesgerichts der qualifizierte Formzwang nur durch eine Originalunterschrift erfüllt werden kann.

2.2.1 Kontext zu Europa

Die Richtlinie RL 1999/93/EG trägt den EU-Mitgliedstaaten auf, bis zum 19.7.2001 die rechtlichen Anforderungen für die Gleichstellung der elektronischen Signatur mit der Handunterschrift zu schaffen. Die Mitgliedstaaten können jedoch bestimmte Rechtsbereiche ausnehmen. Vorbehalten bleiben bestehende Gültigkeits- und Formvorschriften für Verträge sowie die Gleichbehandlung beim Abschluss von Verträgen (BBl 2001 5713).

Der Bundesrat schliesst internationale Abkommen, um die internationale Verwendung elektronischer Signaturen und deren rechtliche Anerkennung zu erleichtern (Art. 19 ZertES). Bei Redaktionsschluss dieses Dokuments sind noch keine solchen Abkommen abgeschlossen worden.

2.3 Die Verwendung der elektronischen Signatur im Bereich eGovernment

2.3.1 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.

2.3.2 Gleichstellung der elektronischen Unterschrift mit der Handunterschrift im 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. 42 Abs. 1 BGG[2]; Art. 52 Abs. 1 VwVG; Art. 23 Bst. g und 29 Bst. g BZP), kann diese handschriftlicher oder elektronischer Art sein. 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].

2.3.3 Überblick

Mit der Revision des Bundesgesetzes über das Verwaltungsverfahren (VwVG) und mit dem Inkrafttreten des Bundesgerichtsgesetzes (BGG) ist auf Bundesebene seit 1.1.2007 nun grundsätzlich möglich, einen Teil des „behördlichen Geschäftsverkehrs“ elektronisch abzuwickeln. Auf kantonaler Ebene bedarf es aber noch unter Umständen der (gesetzlichen) Anpassungen, wie das Bereitstellen der erforderlichen elektronischen Formulare.

[2] In Kraft seit 1.1. 2007

2.3.4 Zugang zum Bundesgericht

Am 1.1.2007 ist das Bundesgerichtsgesetz (BGG) in Kraft getreten. Gemäss Art. 42 Abs. 4 BGG können die Rechtsschriften nun auch elektronisch ans Bundesgericht eingereicht werden, sofern sie mit einer anerkannten elektronischen Signatur versehen sind. Zudem können bei Einverständnis der Parteien Zustellungen vom Bundesgericht auch elektronisch erfolgen (Art. 39 Abs. 2 BGG). So kann ein Entscheid des Bundesgerichts auf elektronischem Weg eröffnet werden (Art. 60 Abs. 3 BGG).

Wie die Eingabe der Rechtsschriften an und die Zustellung der Entscheide vom Bundesgericht genau erfolgen soll, sind im Reglement ReRBGer festgelegt.

2.3.5 Bundesverwaltungsverfahren

Das revidierte Bundesgesetz über das Verwaltungsverfahren (VwVG) ist seit dem 1.1.2007 in Kraft. Die Dokumente können im Verwaltungsverfahren vor den Bundesbehörden elektronisch eingereicht werden (Art. 21a Abs. 1 VwVG). Bei den Eingaben ist das vom Bundesrat vorgeschriebene Format zu beachten. Die ganze Sendung ist mit einer anerkannten elektronischen Signatur zu versehen (Art. 21a Abs. 2 VwVG).

Bei Zustimmung der Parteien und bei Nennung einer Zustelladresse können Zustellungen der Behörden auch elektronisch erfolgen (Art. 11b Abs. 2 VwVG). So können Verfügungen im Verwaltungsverfahren seit 1.1.2007 bei Einverständnis der Partei auf elektronischem Weg eröffnet werden (Art. 34 Abs. 1^{bis} VwVG). Die Verfügungen sind mit einer anerkannten elektronischen Signatur zu versehen.

Es ist eine Verordnung geplant, wie im Detail die Dokumente im Verwaltungsverfahren auszutauschen sind. Der Bundesrat hat aber gemäss Schlussbestimmung des VwVG die Möglichkeit, die elektronische Eingabe von Schriften auf bestimmte Behörden und Verfahren während 10 Jahren einzuschränken oder zu unterbinden.

2.3.6 Zugang zum Bundesverwaltungsgericht

Am 1.1.2007 ist das Bundesverwaltungsgerichtsgesetz (VGG) in Kraft getreten. Der Geschäftsverkehr mit dem Bundesverwaltungsgericht fällt unter das bundesrechtliche Verwaltungsverfahren (Art. 1 Abs. 2 Bst. c^{bis} VwVG).

2.3.7 Zugang zum Bundesstrafgericht

Gemäss Artikel 99 des Bundesgesetzes über die Bundesstrafrechtspflege (BStP) gilt für die elektronische Zustellung von Rechtsschriften an das Bundesstrafgericht der Art. 42 Abs. 4 des Bundesgerichtsgesetzes. Das Format richtet sich nach dem entsprechenden Reglement des Bundesgerichts (ReRBGer). Demzufolge kann man ebenfalls seit dem 1.1.2007 Rechtsschriften elektronisch beim Bundesstrafgericht einreichen.

2.3.8 Empfehlung im Umgang mit den Behörden

Dort, wo reelle Government Prozesse digitalisiert werden und dabei bisher eine Handunterschrift verlangt wird, sollte bei der elektronischen Abwicklung eine anerkannte Signatur verwendet werden. Deshalb ist sinngemäss die anerkannte elektronische Signatur vorzusehen, wie dies in Art. 42 Abs. 4 BGG, Art. 21a Abs. 2 VwVG und Art. 34 Abs. 1bis VwVG verlangt wird.

Weil das Potenzial für Missbrauch und Fahrlässigkeit in der digitalen Welt beträchtlich grösser ist, sind beim Umgang mit sensitiven Informationen in der digitalen Welt vermehrt Anwendungen von Zertifikaten (Authentisierung und Verschlüsselung) einzusetzen, wie dies bei der elektronischen Zustellung von Verfügungen seit 1.1.2007 der Fall ist.

2.4 Technischer Zugang

Für das Einreichen und den Empfang von Rechtsschriften an und vom Bundesgericht ist eine (technisch und rechtlich) klar definierte Zustellplattform eingerichtet worden. Es ist zu erwarten, dass bei dem Austausch von Rechtsschriften im Bundesverwaltungsverfahren von und an die entsprechenden Ämter bei den jeweiligen Verfahren ebenfalls eine Zustellplattform definiert werden wird.

2.5 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, was im Bundesrecht u.a. mit der Revision[3] des VwVG und des BGG geschaffen worden ist. Bei elektronischen Unterschriften von natürlichen Personen sollte der Gesetzgeber aber nur die **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] Seit 1.1.2007 in Kraft

3 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 überwälzt 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, anderseits im OR für den Inhaber des privaten Schlüssels geregelt, welcher zu einem öffentlichen Schlüssel in einem qualifizierten Zertifikat eines anerkannten CSP passt.

3.1 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 notwendigen 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.

3.2 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 Ausführungsbestimmungen 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 sensitiven Daten gewährt werden soll.

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

3.3 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 einstehen muss, auf die Entstehung oder Verschlimmerung des Schadens eingewirkt hat (Art. 4 VG; HUGM, N 1748 ff.).

3.4 Schlussfolgerung

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

- Beim Einsatz unterschiedlichster Zertifikatsklassen (im Sinne von unterschiedlichen Vertrauens- oder Güteklassen) in verschiedenen eGovernment Anwendungen besteht das beträchtliche Risiko zur Unklarheit, welche entsprechenden elektronischen Signaturen in welcher eGovernment Anwendung eingesetzt werden müssen, damit die Formvorschriften erfüllt sind und die Rechtskonformität eingehalten werden kann. Dies kann zu langwierigen Diskussionen führen, was einer schnellen Realisierung und Abwicklung von eGovernment Projekten und der Ökonomie 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 Bundes[4]- und Staatsbeamtenhaftung[5] 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.

[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.

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.

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 nach ZertES 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. eine Formvorschrift für die elektronische Eingabe von Rechtsschriften an das Bundesgericht.)
- Seit dem Inkrafttreten des BGG im Januar 2007 wird man mit anerkannten elektronischen Signaturen Rechtsschriften elektronisch ans Bundesgericht einreichen können. Zudem werden diese Signaturen nach dem Inkrafttreten der Revision des VwVG im Januar 2007 auch im bundesrechtlichen Verwaltungsverfahren „theoretisch“ (unter Vorbehalt des Übergangsrechts) zugelassen.
- 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 ist[6].

[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 sensitiven Informationen

4.1 Einleitung

Gemäss der [TAV] vor 1.12.06 durfte das qualifizierte Zertifikat ausschliesslich für die Verifikation einer verbindlichen Signatur (engl. Non Repudiation) verwendet werden. Folglich konnte die (anerkannt) qualifizierte elektronische Signatur ausschliesslich für die (rechtlich) verbindliche elektronische Signatur eingesetzt und nur für die der Handschrift gleichgestellten Unterzeichnung (z.B. von Verträgen) genutzt werden.

Damit man die elektronische Signatur nicht nur zur Unterzeichnung eines Rechtsgeschäfts aber lediglich zur Prüfung der Authentizität von Dokumenten oder abgelegten Daten verwenden kann, ist der Verwendungszweck für qualifizierte Zertifikate seit 1.12.06 erweitert worden Neben der Nichtabstreitbarkeit (engl. Non Repudiation) wird neu seit 1.12.06 die Möglichkeit eröffnet, die qualifizierte Signatur auch für die Bestätigung der Integrität und Authentizität eines Dokuments und für „Digitale Signaturen" jeglicher Art einzusetzen.

Grundsätzlich sollte aber unterschieden werden, *ob eine qualifizierte elektronische Signatur für die Authentizität (Bestimmung der Herkunft) und Integrität eines Dokuments oder zur online Authentisierung eingesetzt wird.* Vor dem Einsatz qualifizierten elektronischen Signaturen bei der online Authentisierung **ist aber ausdrücklich zu warnen**. Eine elektronische Signatur könnte nun eventuell auch für Authentisierungen im Rahmen der online Kommunikation (z.B. für die Authentisierung, den Aufbau und später für die Verschlüsselung von SSL oder IPSEC[7] Verbindungen) eingesetzt werden. Erfolgt dies mit einer qualifizierten Signatur, dann hat der Benutzer nicht mehr die Möglichkeit, alle seine einmal geleisteten qualifizierten Signaturen zu sammeln und zu archivieren, denn z.B. die Sicherheitstechnologien SSL und IPSEC ermöglichen dies nicht. Zudem kann er die von ihm geleistete Signatur später nicht verifizieren und den Inhalt des zu signierenden Objekts vor der Signatur anschauen, wie dies eigentlich CWA 14 170 vorschlägt.

Die **bei der Authentisierung einer online Kommunikation verwendete Signatur** sollte deshalb **keine qualifizierte** sein. Andere Signaturen sollten hierfür eingesetzt werden. Für unbedarfte Benutzer sind deshalb entsprechend andere als qualifizierte Zertifikate mit entsprechendem Verwendungszweck zusätzlich auszustellen und bei der online Kommunikation für die Verifikation der Signatur einzusetzen.

Es wird empfohlen, drei Zertifikate für Benutzer auszustellen; ein qualifiziertes, eines für die Verschlüsselung von Daten und eines für die Verifikation der Signatur bei einer online Authentisierung. Der Verwendungszweck des qualifizierten Zertifikats ist auf die Verifikation der „Nicht Abstreitbarkeit" (engl. NON Repudiation oder Content Commitment) und der Authentizität und Integrität eines Dokuments (engl. digital Signature) zu beschränken.

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

Anmerkung: Die Nichtabstreitbarkeit eines Dokuments enthält immer die Authentizität und Integrität dessen. Mit dem Schutz der Authentizität und Integrität mittels Signatur will man sich aber nicht immer zum Inhalt eines Dokumentes bekennen (engl. commit). D.h. man will mit der Signatur nicht immer die „Nicht Abstreitbarkeit“ schützen.

Anmerkung: Zu den Risiken beim Leisten einer elektronischen Signatur siehe auch Kapitel 6 „Sicherheitsanforderungen“.

4.1.1 Funktionsweise der online Authentisierung

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 elektronischen Signatur eignet sich auch für den geschützten Zugang zu sehr sensitiven Informationen.

Dies ist insbesondere dann empfehlenswert, wenn:

1. Die Bekanntgabe von Daten, welche gemäss Art. 3 Bst. c DSG besonders schützenswert sind[8]; 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.

Es liegt nahe und empfiehlt sich deshalb auch, Zertifikate für die online Authentisierung bei einem nach ZertES anerkannten CSP zu beziehen. Die Prozesse für die Ausstellung von nicht qualifizierten Zertifikate (z.B. Zertifikate für die online Authentisierung) laufen meist nicht

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

anders ab als bei der Vergabe qualifizierter Zertifikate. Die Vergabe von nicht qualifizierten Zertifikaten untersteht aber nicht dem ZertES, sondern ausschliesslich dem allgemeinen Vertragsrecht nach OR. Die AVB des CSP sind deshalb zu konsultieren.

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 Chiffrat wird der verschlüsselten E-Mail beigefügt. 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.

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 $E_{Alice}(R)$ wird nun Alice zugestellt.
- Alice entschlüsselt $E_{Alice}(R)$ 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 E 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 elektronischen Signatur, nicht aber für die Verschlüsselung verwendet werden darf, s. auch [TAV] Kapitel 3.4.2, Abschnitt c.

Nicht sinnvoll wird erachtet, dass der Otto Normalverbraucher die qualifizierten Signaturen neben der rechtsverbindlichen Unterschrift noch für die online Authentisierung einsetzt. Der Verwendungszweck des qualifizierten Zertifikats ist entsprechend einzuschränken.

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 einem 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 erfüllt.
- 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 Authentizität 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.

4.5 Digitale ID und Zertifikate

Anhand von digitalen Identitätskennungen im Zertifikat kann das Zertifikat einer Person oder einer (öffentlichen) Körperschaft zugeordnet werden. Ob die Identitätskennungen im Zertifikat alleine für eine Zuordnung ausreichen oder ob weitere Informationen von der CA für die eindeutige Zuordnung benötigt werden, bleibt offen. Aber eine eindeutige Zuordnung muss für fortgeschrittene und somit auch für qualifizierte Zertifikate aber jederzeit möglich sein (Art. 2 lit. b ZertES).

Nun ist es grundsätzlich möglich, auch ein Pseudonym in ein qualifiziertes elektronisches Zertifikat einzufügen (Art. 7 Abs. 1 lit. c ZertES). Die Verwendung eines Pseudonyms kann zur Folge haben, dass alleine vom Inhalt des Zertifikats keinen direkten Rückschluss auf den Besitzer des Zertifikats gemacht werden kann.

Der Einsatz eines Pseudonyms in einem qualifizierten Zertifikat macht unter anderem dann Sinn, wenn eine natürliche Person im Namen eines Unternehmens elektronisch signiert. In den Identitätskennungen stehen dann hauptsächlich Angaben zum Unternehmen und nicht zur natürlichen Person.

Grundsätzlich darf aber ein qualifiziertes Zertifikat ausschliesslich für eine natürliche Person ausgestellt werden (s. AB 2003 N 813). Wenn das qualifizierte Zertifikat ausschliesslich für die Verifikation von elektronischen Signaturen im Namen der juristischen Person oder einer Behörde verwendet wird, stellt sich nun die Frage der Haftung bei missbräuchlichem oder fehlerhaftem Einsatz von elektronischen Signaturen. Etwelche Haftung lässt sich unter anderem aus folgenden Gesetzesartikeln ableiten:

- Vertrag (Art. 97 ff OR)
- Geschäftsherrenhaftung für private Unternehmen (Art 55 OR)
- Verantwortlichkeitsgesetz (VG), falls ein Beamter im Rahmen seiner amtlichen Tätigkeit eine elektronische Signatur leistet.
- Haftung des Inhabers sei aus Verschuldenshaftung (Art. 41 ff OR) und aus Haftung für Missbrauch der elektronischen Signatur (Art 59a OR).

Dass der Inhaber des Zertifikats selber (persönlich) haftet, auch wenn er die elektronische Signatur einzig im Dienste des privaten Unternehmens verwendet, dazu [KeA] S. 152:

> „Die Haftung der Geschäftsherrin oder des Geschäftsherrn schliesst eine Haftung der Angestellten nicht aus. Diese können gegebenenfalls nach OR 41 belangt werden (siehe z.B. BGE 80 II 250). Dies ist von um so grösserer Bedeutung als die Versicherungsgesellschaften durch ihre Betriebshaft-Policen regelmässig auch die persönliche Haftpflicht der Angestellten (mit Ausnahme von Rückgriffsansprüchen) decken.“

Kommt das Verantwortlichkeitsgesetz aber zum Tragen, dann besteht kein direktes Forderungsrecht auf den fehlbaren Beamten (Art. 3 Abs. 3 VG).

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. Trotzdem 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 Zertifikat[9], 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
- Empfangsbestätigung 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)
- Authentisierter und bezüglich Vertraulichkeit geschützter Zugang zu sensitiven Daten
- Transaktionen zwischen Server
- Backup von einem Server zum anderen

[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.

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.

Beispiel: Im bundesrechtlichen Verwaltungsverfahren gilt ein elektronisches Dokument als fristgerecht zugestellt, wenn das entsprechende IT-System den Empfang vor Ablauf der Frist quittiert (Art. 21a Abs. 3[10] VwVG). Wie dieser Beleg zu gestalten ist, ist noch nicht definiert worden.

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 ElDI-V entsteht, welche die funktionellen Signaturen regelt. Sofern erforderlich, wird dann dieses Dokument entsprechend dieser Verordnung noch angepasst werden.

[10] Seit 1.1.2007 in Kraft

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 - 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 ElDI-V an interessierte Kreise verteilt. Die definitive Fassung der Verordnung konnte aber für dieses Dokument nicht mehr berücksichtigt werden.

5.6 Beispiel zur Haftung

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

- Anerkennungsstelle (Ankst.)
- Anerkannter Zertifizierungsdienstanbieter (CSP)
- Benutzer oder Bezüger eines qualifizierten Zertifikats (Be)
- Juristische Person (JuP), welche ein Serverzertifikat (Funktionszertifikat) eines nach ZertES anerkannten CSP bezogen hat.

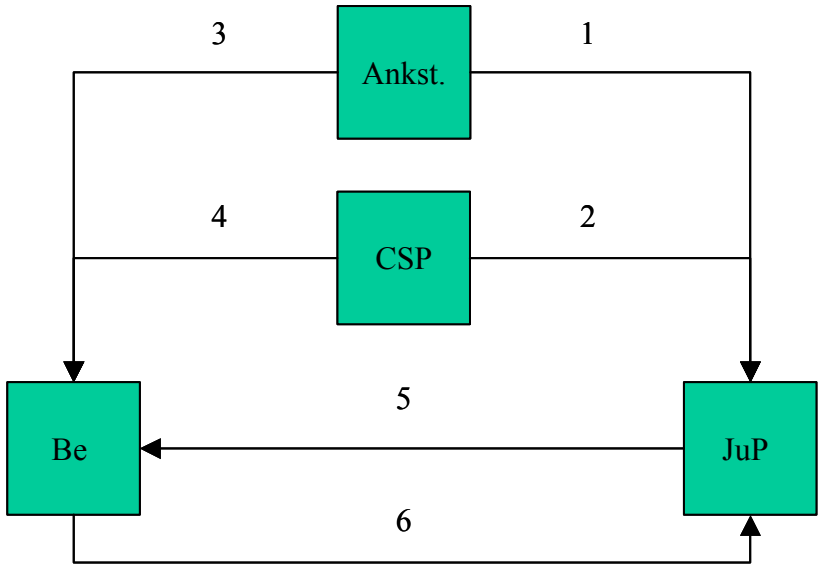

Abbildung 1 Haftungsszenario

1. Art. 17 ZertES, weil sich die juristische Person auf die Gültigkeit des qualifizierten Zertifikats des Benutzers verlassen hat.
2. Art. 16 ZertES, weil sich die juristische Person 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 (Funktionszertifikat)** verlassen hat.
4. Art. 41 OR aus unerlaubter Handlung, **weil der Benutzer sich** auf **die Gültigkeit des Serverzertifikats (Funktionszertifikat)** verlassen hat.
5. Art. 41 OR aus unerlaubter Handlung, eventuell Art. 97 ff OR wegen Verletzung des Vertrags zwischen der juristischen Person und dem Benutzer

6. Art. 59a OR, weil sich die juristische Person 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.

Wenn einer der Parteien, z.B. der CSP, der Bezüger des Zertifikats oder der Betreiber des Server Teil einer Behörde sind, wird auch das Verantwortlichkeitsgesetz VG oder die Staatshaftung angewandt werden, wenn die Voraussetzungen dafür erfüllt sind.

5.7 Beispiel zu einer praktischen Implementation

Zur Eingabe von Rechtsschriften ist eine IT-Plattform geschaffen worden, damit der eingeschriebene Brief elektronisch nachgebildet werden kann. Vereinfacht ausgedrückt werden die Rechtsschriften beim Versand auf einen Server deponiert. Der Server benachrichtigt den Empfänger, dass eine Nachricht für ihn zum Abholen bereit ist. Der Empfänger holt innerhalb einer vorgesehenen Frist die elektronische Post ab, ansonsten erhält der Absender eine Mitteilung, dass die elektronische Post vom Adressat nicht abgeholt worden ist.

Sowohl der Versand der Rechtsschrift als auch die Zustellung an den Empfänger werden dem Absender vom Server quittiert. Der Versand der Rechtsschrift entspricht der Aufgabe des eingeschriebenen Briefes bei der Post. Die Quittungen sind dabei vom Server elektronisch signiert worden, wobei darin eine Zeitangabe enthalten ist. Zur Verifikation wird ein Funktionszertifikat benötigt.

Die Rechtsschrift (z.B. die Beschwerde) wird vom Verfasser anerkannt elektronisch signiert.

Die Kommunikation zum Server wird verschlüsselt und authentisiert. Dazu wird ein Zertifikat für die Verschlüsselung eingesetzt.

6 Sicherheitsanforderungen

6.1 Einleitung

In diesem Kapitel werden u.a. 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.

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 [Mud]

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 3.3.2 [TAV] mit Hinweis unter anderem auf folgende technische Standards: ETSI TS 101 456, FIPS 140-1, FIPS 140-2, ITSEC, ISO/IEC 15408:1999, CWA 14167-3

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

- Kapitel 3.3.3 [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 oder nach FIPS 140-2 Level 3[11] 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 - 5 VZertES (Aktivierung der Signaturerstellungseinheit und Umgang mit den Aktivierungsdaten, beziehungsweise mit der PIN)
- Kapitel 3.3.3 [TAV] (Eingabe der PIN, Sperrung und Freischaltung der Signaturerstellungseinheit)

[11] Seit 1.12.06 ist der Einsatz von FIPS 140-2 Level 3 Produkte nebst zusätzlichen technischen Massnahmen ebenfalls möglich.

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

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

6.4 Handhabung der Zertifikate

Die Handhabung der Zertifikate umfasst grob die Herstellung, die Publikation, die Ungültigkeitserklärung (Revokation) und die Aufbewahrung der Zertifikate.

Die Pflichten bezüglich Handhabung von qualifizierten Zertifikaten ist für einen anerkannten Zertifizierungsdienstanbieters in den Artikeln 8, 9 und 10 ZertES geregelt, wobei die VZertES dies in den Artikeln 5 - 8 präzisiert.

Bei der Erstellung und Herausgabe von qualifizierten Zertifikaten eines anerkannten CSP müssen die Antragsteller persönlich erscheinen und dabei den Nachweis ihrer Identität erbringen (Art. 8 ZertES). Dazu ist u.a. die Identitätskarte oder der Pass vorzuweisen (Art. 5 Abs. 1 VZertES).

Der Inhalt eines qualifizierten Zertifikats wird in [TAV] bestimmt, wobei sich die Legitimation dazu aus Art. 4 Abs. 1 VZertES und Art. 7 Abs. 3 ZertES ergibt.

Der anerkannte CSP darf zwar den Signaturschlüssel für ein qualifiziertes Zertifikat erzeugen, aber es ist ihm untersagt, eine Kopie des Signaturschlüssels aufzubewahren (Art. 8 VZertES).

Unter welchen Bedingungen und Voraussetzungen ein qualifiziertes Zertifikat bei einem anerkannten CSP für ungültig erklärt und was dabei beachtet werden muss, ist in Art. 10 ZertES und Art. 7 VZertES festgehalten. Unter anderem muss der anerkannte CSP Dritten einen online Zugang gewähren, um Informationen zur Ungültigkeitserklärung eines qualifizierten Zertifikats bis zu dessen regulären Ungültigkeit zu erhalten (Art. 7 Abs. 2 VZertES).

Zudem müssen die anerkannten CSP die Informationen zur Überprüfung von nicht mehr gültigen qualifizierten Zertifikaten während elf Jahren ab Ablauf der Zertifikate angeben können (Art. 7 Abs. 3 VZertES).

Anmerkung: Zudem sind in [TAV] mit Verweis auf den ETSI Standard TS 101 456 weitere detailliertere Vorschriften zum Verwalten der Zertifikate enthalten.

6.5 Weiterführende Sicherheitsmassnahmen

In SAGA.ch Kapitel 8 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 Entschlüsselung[12] 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 Applet, 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.

6.6 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 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.

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

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.

6.7 Namensgebung

6.7.1 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 [Mud] 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.

6.7.2 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.ch:

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.

6.8 Bemerkungen zu den Sicherheitsvorschriften

In vielen Fällen wird beklagt, dass die Sicherheitsbestimmungen in der digitalen (elektronischen) Welt so viel grösser sind, als in der realen Welt, insbesondere die Bestimmungen und die Haftungsregelung im Bereich der elektronischen Signatur. Hierzu folgende Argumente, warum es u.a. sinnvoll ist, die Sicherheitsbestimmungen und die Haftung im Zertifikatsumfeld entsprechend hoch anzusetzen:

- Eine Handunterschrift ist mit der Person verbunden, eine digitale Identität jedoch ist übertragbar, wenn der Inhaber der Identität dies auch so will. Dies erfolgt z.B. durch Übergabe oder Entwendung der PIN und der sicheren Signaturerstellungseinheit. „Identifizieren heisst in der digitalen Welt, das Zuordnen der Verantwortlichkeit“.
- **Bei der Ausstellung der Zertifikate werden digitale Identitäten vergeben!** Deswegen sind entsprechende Gesetze im ZertES und dessen Ausführungsvorschriften erlassen worden, wie eine Person bei Herstellung von qualifizierten Zertifikaten zu identifizieren ist und wie die Zertifikate und Schlüssel zu verwalten sind.
- Ein digitaler Prozess läuft für den Benutzer unsichtbar und somit weniger kontrollierbar ab, als z.B. ein reeller Dokumentationsfluss. Somit sind die visuellen Kontrollen in der IT normalerweise für den Otto-Normalverbraucher sehr eingeschränkt oder gar nicht vorhanden.
- Mit Anschluss ans Internet ist man mit „der ganzen Welt“ in Kontakt. Damit ist möglicherweise auch eine Fülle von Missbrauchspotenzial verbunden.
- Andere Länder, andere Sitten, Gesetze und Prozessvorschriften. Die Rechtsdurchsetzung, falls überhaupt möglich, ist unter Umständen langwierig. Zudem ist fraglich, ob der einmal verursachte Schaden auch wirklich später ersetzt werden wird.

Anmerkung: Grundsätzlich empfiehlt es in der digitalen wie auch in der realen Welt zuerst zu prüfen, was signiert werden soll und von wem die Signatur stammt, bevor irgendwelche weiteren Schritte unternommen werden.

7 Archivierung elektronisch signierter Dokumente

Für öffentlichrechtliche Organisationen gelten andere Bestimmungen in Bezug auf die Archivierung relevanter geschäftlicher Informationen (verschiedene Archivgesetze) als für privatrechtliche Gesellschaften. Für öffentlichrechtliche gelten verschiedene Archivgesetze, wie das Bundesgesetz über die Archivierung (BGA) oder weitere kantonale und kommunale Archivierungsbestimmungen mit unterschiedlichen Geltungsbereichen. Für privatrechtliche ist unter anderem die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung; GeBüV) verbindlich.

Grundsätzlich soll in diesem Kapitel aber keine Abhandlung über die Archivierung und deren rechtliche Aspekte vorgenommen. Dazu wird auf Literatur wie [LeAt] oder auf die entsprechenden ISO und eCH Standards zu Records Management verwiesen.

Hier werden lediglich einige Aspekte der elektronischen Signatur im Kontext zur Archivierung erläutert. Hauptsächlich werden elektronische Signaturen dabei in folgenden Bereichen eingesetzt:

1. Elektronische Beglaubigung, dass die Information auf Papier oder auf sonst einem reellen Medium korrekt digitalisiert worden und ins elektronische Archiv überführt worden ist.
2. Elektronische Signatur zum Schutz der Integrität der digitalen Information
3. Archivierung von digital empfangenen, elektronisch signierten Dokumenten, so dass die Beweiskraft der elektronischen Signatur nicht erlischt.

7.1 Elektronische Beglaubigung

In vielen Fällen wird mittels einer elektronischen Signatur beglaubigt, dass das betreffende Dokument korrekt digitalisiert worden ist. Falls noch wichtig ist, wann dies geschehen ist, werden auch noch Zeitstempeldienste eingesetzt.

7.2 Signatur und Schutz der Integrität

Ein wichtiger Aspekt der digitalen Archivierung gemäss GeBüV ist die Forderung, dass eine nachträgliche Veränderung der archivierten Dokumente eindeutig feststellbar sein muss (Art. 3 GeBüV zur Integrität). Dies ist eine besondere Herausforderung, wenn für die elektronische Archivierung (vor allem aus Kostengründen) veränderbare elektronische Datenträger (z.B. handelsübliche Festplatten) eingesetzt werden. Gemäss GeBüV Art. 9 Abs. b sind veränderbare auch zulässige Informationsträger, doch müssen in diesem Fall technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen schützen (z.B. digitale Signaturverfahren).

Betreffend den Einsatz der elektronischen Signatur zum Schutz der Integrität soll auf den folgenden Punkt 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 dann nicht den Ursprungszustand der Daten vor der Veränderung oder vor dem Integritätsverlust herstellen. Deshalb sind elektronische Signaturen als einzige Massnahme für den Schutz (der Integrität) der gelagerten Dateien ungenügend.

Es empfiehlt sich deshalb neben der elektronischen Signatur weitere organisatorische und technische Massnahmen, wie lückenlose Journalisierung, periodische Prüfung der Lesbarkeit, Verfügbarkeit, Kopie auf nicht veränderbare Datenträger oder Datenmigration.

7.3 Erhaltung der Beweiskraft digital signiert 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 und verifiziert werden kann. Gleichzeitig muss aber auch definiert werden, wie die Verifikation elektronisch signierter Dokumente erfolgen soll. Ansonsten können keine Massnahmen zur Archivierung getroffen und umgesetzt werden. Zur Problematik der Archivierung von elektronischen Signaturen, siehe auch www.archisig.de. Eine Einführung in die Problematik der Nachhaltigkeit elektronischer Signaturen, siehe [Mud] Kapitel 15. Eine umfassende Erläuterung dazu ist in [Bea] erhältlich.

7.3.1 Massnahmen zum Erhalt der Beweiskraft

Die Massnahmen zum Erhalt 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.

7.3.2 Prüfung der elektronischen Signatur

Grundsätzlich gilt es zu unterscheiden, ob eine elektronische Signatur für die online Authentisierung (s. Kapitel 4.2 Authentisierung mit elektronischer Signatur“) 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 SAGA.ch:

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 (z.B. bei 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 7.3.1 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.

Anmerkung: Die Prüfung der elektronischen Zertifikate wird erleichtert, wenn die Gültigkeitsdauer des Zertifikats A innerhalb der Gültigkeitsdauer des zu A übergeordneten Zertifikats liegt, welches für die Verifikation des Zertifikats A benötigt wird.

7.3.3 Lösungsansätze

In CWA 14171 sind grundsätzliche Empfehlungen dazu enthalten, was bei der Archivierung von elektronisch signierten Dokumenten zu beachten gilt. Es handelt sich hier aber nur um Lösungsansätze, keineswegs aber um ein ausgearbeitetes Konzept oder um eine verbindliche Richtlinie. Eine verbindliche Richtlinie, wie eine elektronische Signatur langfristig zu prüfen und folglich zu archivieren ist, gibt es in der Schweiz noch nicht.

8 Produktzertifizierung

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

- Schlüsselgenerierung (Kapitel 3.3.2)
- Sicherheitsanforderung an die Signaturerstellungseinheit (Kapitel 3.3.3)

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 7.3.2 beschriebenen Sicherheitsanforderungen genügt. Deswegen ist z.B. im Kapitel 3.3.3 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), ITSEC oder nach FIPS Level 3[13] 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 u.a., ob der CSP die von der [TAV] geforderten Produkte dem Kunden zur Verfügung stellt oder zum Kauf anbietet.

[13] Seit 1.12.06 ist der Einsatz von FIPS 140-2 Level 3 zertifizierten Produkte zulässig.

9 Beantwortung von Fragen

9.1 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 2 „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 ElDI-V geplant, die Server- oder Funktionszertifikate einzuführen und die Anforderungen an diese zu definieren.

3. Welche Identitätskennungen (z. B. Personennamen, E-Mail Adressen) sollen im eGovernment 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. [Mud]. Selbstverständlich gibt es Unterschiede in der Identitätskennung bei der Behörde, doch diese sollten absolut minimal gehalten werden, s. dazu Kapitel 6.7 „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. [Mud].

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

   s. Kapitel 7, insbesondere 7.3.2 „Prüfung der elektronischen 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 6.6 „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“

9.2 Häufig gestellte Fragen

Das Bakom führt auf dessen Internetseite unter anderem zum Thema elektronische Signatur eine Liste von häufig gestellten Fragen und deren Antworten.

- Link auf die deutschsprachige Seite:
  http://www.bakom.ch/dienstleistungen/faq/01834/01836/index.html?lang=de
- Link auf die französischsprachige Seite:
  http://www.bakom.ch/dienstleistungen/faq/01834/01836/index.html?lang=fr

10 Zusammenfassung

10.1 Allgemeines

Weitgehend praxisorientierte Gesetze insbesondere im europäischen Umfeld führen zu international zahlreichen Gesetzen und Rechtsnormen betreffend die elektronische Signatur mit hohem „Ähnlichkeitsfaktor“. Die Einhaltung internationaler Standards erlaubt die leichte Integration von am Markt vorhandenen Signaturlösungen in bestehende Anwendungen, was die technische Umsetzung der elektronischen Signatur wesentlich vereinfacht. Vielzählige Projekte in den Bereichen eGovernment, eInvoicing, eArchiving, eBanking oder eForms belegen die beschleunigte Entwicklung der elektronischen Signatur, nachdem diese während Jahren nur für technische Spezialisten ein Thema war. Dies ist der Grund für ***eCH***, mit dem vorliegenden Themenpapier Antwort auf offene Fragen zu geben.

10.2 eGovernment Anwendungen

Der elektronische Zugang zu den Behörden ist in der Schweiz noch nicht vollständig möglich. Mit dem neuen Bundesgerichtsgesetz (BGG) und der Revision des Bundesgesetzes über das Verwaltungsverfahren (VwVG), in Kraft seit 1. Januar 2007, werden auf Bundesebene die Eingaben an Gerichte und Behörden sowie die Zustellung von Verfügungen in elektronischer Form geregelt.

10.3 Wirksamkeit elektronischer Signaturen

Verträge, für welche das Gesetz oder die Parteien selbst einfache Schriftform vorsehen, können gestützt auf Art. 14 Abs. 2^{bis} OR rechtsgültig auch in elektronischer Form abgeschlossen werden. Der handschriftlichen Unterschrift gleichgestellt sind nur qualifizierte elektronische Signaturen, die auf Basis eines qualifizierten Zertifikats von einer nach dem Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt wurden.

Gestützt auf die EU-Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen haben praktisch alle EU-Mitgliedstaaten in nationalen Gesetzen der elektronischen Unterschrift eine rechtliche Relevanz zugeordnet, wobei in den meisten Fällen die qualifizierte elektronische Unterschrift der handschriftlichen Unterschrift gleichgestellt wurde. Gestützt auf internationale Abkommen wird die gegenseitige Anerkennung von digitalen Signaturen, Zertifikaten und Anerkennungsstellen geregelt.

Im Bereich des eGovernment ist durch die Revision des Bundesgesetzes über das Verwaltungsverfahren sowie den Erlass des Bundesgerichtsgesetzes (BGG, in Kraft seit 1. Januar 2007) die gesetzliche Grundlage für den Einsatz der elektronischen Signatur auf Bundesebene geschaffen worden. Wo der behördliche „Geschäftsverkehr“ bislang eine handschriftliche Signatur vorsah, sollte für die künftige elektronische Abwicklung die anerkannte elektronische Signatur vorgesehen werden. Wo in diesem Bereich keine Formvorschriften bestehen,

kann die Behörde selbst bestimmen, wie sie mit den Bürgern elektronisch kommuniziert. Empfehlenswert ist die Anwendung eines standardisierten Vorgehens in der Ausgestaltung, Umsetzung und Durchführung der entsprechenden IT-Prozesse.

10.4 Absicherung (Haftung)

Die Haftungsbestimmungen betreffend die qualifizierten Zertifikate sind einerseits im Bundesgesetz über die elektronische Signatur (Art. 16 ZertES und folgende Bestimmung) und andrerseits im Schweizerischen Obligationenrecht (Art. 59a OR) geregelt. Nach der privatrechtlichen Haftung gestützt auf das OR haftet der Inhaber eines Signaturschlüssels Dritten für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinn des ZertES verlassen haben, ausser er kann glaubhaft machen, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern.

Die Anbieterin von Zertifizierungsdiensten haftet gemäss Art. 16 Abs. 1 ZertES gegenüber dem Inhaber eines Signaturschlüssels und Dritten, die sich auf ein gültiges qualifiziertes Zertifikat verlassen haben für Schäden, die diese erleiden, weil die Anbietern den Pflichten aus dem ZertES und den entsprechenden Ausführungen nicht nachgekommen ist, ausser sie beweist, die entsprechenden Pflichten erfüllt zu haben.

Schliesslich haftet der Staat (auf Bundesebene) gestützt auf das Verantwortlichkeitsgesetz (Art. 3 VG) für Schäden, die ein Beamter in Ausübung seiner amtlichen Tätigkeit Dritten zufügt, im Zusammenhang mit der elektronischen Signatur im Fall der missbräuchlichen Verwendung des Signaturschlüssels für die Schäden gegenüber Dritten, welche diese erleiden, weil sie sich auf das gültige qualifizierte Zertifikat verlassen haben. Weil der Bürger dem Staat gegenüber gefühlsmässig nur eine Stufe von Vertrauensklasse hat, führt der Einsatz unterschiedlichster Zertifikatsklassen (im Sinn von unterschiedlichen Vertrauens- und Güteklassen) zu erheblichen Unsicherheiten, welche elektronischen Signaturen in welcher eGovernment Anwendung eingesetzt werden müssen, um Formvorschriften und generell Rechtskonformität einzuhalten. Dies hindert die Förderung des elektronischen Rechtsverkehrs mit Behörden.

Um entsprechende Unsicherheiten zu vermeiden, ist der qualifizierten elektronischen Signatur, welche mit einem qualifizierten Zertifikat eines anerkannten Zertifizierungsdienstanbieters verifiziert werden kann, gegenüber den übrigen elektronischen Unterschriften den Vorzug zu geben. Der Empfänger einer elektronischen Signatur muss sich auf die Wirksamkeit der Signatur allein auf Grund der ihm möglichen Prüfung der Signatur und des Zertifikats verlassen können.

10.5 Zugang zu sensitiven Informationen

Die fortgeschrittene elektronische Signatur dient der Bestätigung der Integrität und Authentizität (eines Dokuments); die qualifizierte zusätzlich noch der Nichtabstreitbarkeit (Non Repudiation).

Für die Authentisierung im Rahmen einer online Kommunikation empfiehlt sich grundsätzlich der Einsatz anderer als der qualifizierten elektronischen Signaturen. Der Inhalt des signierten Objekts kann vor dem Signieren nicht angeschaut werden, die vom Benutzer geleistete Signatur kann unter Umständen nicht archiviert und folglich später nicht verifiziert werden. Hingegen können anerkannt qualifizierte Signaturen im Rahmen von elektronischen Registrierungsprozessen behilflich sein oder zumindest als Ausgangspunkt für die online Authentisierung dienen.

In diesem Zusammenhang ist zu bedenken, dass die Ausstellung unterschiedlicher Zertifikate an einen Benutzer unter Umständen zu Verwirrung führt.

10.6 Funktionszertifikate

Grundsätzlich dürfen qualifizierte Zertifikate nur an natürliche Personen ausgegeben werden. Trotzdem werden funktionelle Signaturen (u.a. elektronische Signaturen von Server) benötigt, bspw. bei digitalen Belegen oder Quittungen, digitalen Belegen für die Eingabe von elektronischen Rechtsschriften an das Bundesgericht, digitale Belegen für den elektronischen Geschäftsverkehr zwischen Privaten und Behörden, Massensignaturen, etc.

Bei der Verwendung von Funktionszertifikaten sollten folgende Mindestvorschriften beachtet werden:

- Zertifikate für den Server werden mit dem gleichen öffentlichen Schlüssel aus dem von einer anerkannten Anbieterin von Zertifizierungsdiensten ausgestellten Zertifikat geprüft wie die qualifizierten Zertifikate;
- Die Signaturerstellung mittels eines Server muss die gleichen Sicherheitsanforderungen einer sicheren Signaturerstellungseinheit nach ZertES erfüllen;
- Im Zertifikat muss erkennbar sein, welche Organisation das Zertifikat bezogen hat, da es nicht an eine natürliche Person ausgestellt wurde;
- Die Ausstellung eines Serverzertifikats muss sich nach denselben Bestimmungen wie für die Ausstellung eines qualifizierten Zertifikats richten;
- Es muss eine klare Zuordnung des Zertifikats zur (juristischen) Person ersichtlich sein.

10.7 Sicherheitsanforderungen

Die Sicherheitsanforderungen an das Erstellen einer elektronischen Signatur sind von Bedeutung, weil der Einsatz qualifizierter elektronischer Signaturen zum Anschein der Echtheit einer in elektronischer Form vorliegenden Willenserklärung führt und eine Zurechnung zum Verwender erfolgt. Dabei kann er die Haftung vermeiden, wenn er die Einhaltung zumutbarer Sicherheitsvorschriften zur Verhinderung des Missbrauchs des Signaturschlüssels glaubhaft machen kann. Dies wird ihm vor allem durch den Einsatz geeigneter Technologien möglich. Der Einsatz von Produkten für qualifizierte Signaturen (Hardware und Software), die tatsächlich die Anforderungen des Signaturrechts (und damit insbesondere die bestehen-

den Vorschriften des ZertES betreffend sichere Signaturerstellungseinheiten) erfüllen, liegt daher im Interesse des Verwenders.

10.8 Archivierung elektronisch signierter Dokumente

Die Archivierung elektronisch signierter Dokumente sollte so gestaltet werden, dass die Beweiskraft der elektronischen Signatur im Lauf der Zeit nicht verloren geht. Gleichzeitig muss aber auch definiert werden, wie die Prüfung elektronisch signierter Dokumente erfolgen soll.

Falls rechtlich eine Archivierung der elektronisch signierten Dokumente gefordert ist, dann sollten diese Dokumente mittels eines von der Behörde oder vom Gesetz anerkannten Zeitstempeldienstes archiviert werden. wie z.B. dies im CWA Standard 14171, Kapitel 8 skizziert wird. Falls u.a. qualifizierte elektronische Signaturen archiviert werden müssen, der Zeitstempel unter Umständen später als Beweis oder Beleg herangezogen werden soll oder ein erhöhtes Sicherheitsbedürfnis besteht[14], dann wird der Einsatz von nach ZertES anerkannten Zeitstempeln empfohlen.

10.9 Produktzertifizierung

Beim Einsatz elektronischer Signaturen kann weder der Ersteller noch der Empfänger von elektronischen Signaturen verifizieren, ob die von ihm eingesetzten Produkte, insbesondere für qualifizierte elektronische Signaturen (Hardware und Software), den gesetzlichen Sicherheitsanforderungen entsprechen. Obwohl die Verwendung von zertifizierten Produkten keine Wirksamkeitsvoraussetzung für die mit Hilfe der Produkte erstellten qualifizierten elektronischen Signatur darstellt, muss sich der Empfänger jedoch auf die Wirksamkeit der Signatur allein auf Grund der ihm möglichen Prüfung der Signatur und des Zertifikats verlassen können. Der Einsatz von Produkten für qualifizierte Signaturen, die tatsächlich die Sicherheitsanforderungen des Signaturrechts erfüllen, liegt daher im Interesse des Verwenders. Dadurch erhält er gegebenenfalls die Möglichkeit zur Haftungsabwendung nach Art. 59a Abs. 2 OR; er kann glaubhaft darlegen, dass er bei der Auswahl und bei der Verwendung der SW für die Signaturerstellung und –verifikation die notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat.

[14] Die hier vorgenommene Aufzählung ist nicht als abschliessend zu verstehen.

Die entsprechende Sicherheit erhält der Benutzer über die Verwendung zertifizierter Produkte, die damit über ein Gütezeichen verfügen. Eine nur behauptete Sicherheit durch eine Herstellererklärung kann die nachgewiesene Sicherheit durch Prüfung und Bestätigung nicht ersetzen. Aufgrund von Staatsübereinkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten für die Bewertung der Sicherheitseigenschaften von informationstechnischen Produkten und Systemen (bspw. nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik/Common Criteria for Information Technology Security Evaluation (CC), derzeit Version 2.3“) können Mehrfachzertifizierungen vermieden, und Produktzertifikate aus anderen Ländern international anerkannt werden.

Anhang A – Referenzen

[01.023]	Botschaft zur Totalrevision der Bundesrechtspflege vom 28. Februar 2001 (BBl 2001 4202)
[01.044]	Botschaft des Bundesrates vom 3. Juli 2001 zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (BBl 2001 5679)
[AkGd]	Kurt Amonn, Dominik Glauser, Grundriss des Schuldbetreibungs- und Konkursrechts, Stämpfli Verlag, Bern 1997
[Bea]	Bertsch Andreas, Digitale Signaturen, Springer Verlag, 2002
[GSSR]	Gauch, Schluep, 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
[LeAt]	Beat Lehmann und andere, Records Management, Kompetenzzentrum Records Management vom SWICO, 1. Auflage 2004, ISBN 3 033 00186 6
[Mud]	Muster Daniel, Digitale Unterschriften und PKI, 3. Auflage 2006
[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 TS 101 456 v.1.4.1	Policy Requirements for Certification Authorities Issuing Qualified Certificates

ISO/IEC 15408: 2005	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, V3.0, Standard des Vereins ***eCH***
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). Die dritte Fassung ist seit 1.12.06 in Kraft.
1999/93/EG	Richtlinie der Europäischen Union über die gemeinschaftliche Rahmenbedingungen für elektronische Signaturen
AB	Amtliches Bulletin
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
BGA	Bundesgesetz vom 26. Juni 1998 über die Archivierung (SR 152.1)
BGer	Bundesgericht
BGG	Bundesgesetz vom 17. Juni 2005 über das Bundesgericht (SR 173.110)
Bst.	Buchstabe
BStP	Bundesgesetz 15. Juni 1934 über die Bundesstrafrechtspflege (SR 312.0)
BZP	Bundesgesetz vom 4. Dezember 1947 über den Zivilprozess (SR 273)
CA	Certification Authority (Ausstellerin von Zertifikaten)

CEN	Comité Européen de Normalisation
CSP	Certificate Service Provider
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (SR 235.1)
EA	European Agreement
EFD	Eidgenössische Finanzdirektion
ElDI-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
IRSG	Bundesgesetz vom 20. März 1981 über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG) (SR 351.1)
IT	Informationstechnologie
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)
ReRBGer	Regelement des Bundesgerichts vom 5. Dezember 2006 über den elektronischen Rechtsverkehr mit Parteien und Vorinstanzen (SR 173.110.29)
Rz	Randziffer
s.	siehe
SchKG	Bundesgesetz vom 11. April 1889 über Schuldbetreibung und Konkurs (SR 281.1)
SSCD	Engl. Secure Signature Creation Device - sichere Signaturerstellungseinheit
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 Bundesverwaltungsgericht (SR 173.32)
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 widerrechtlich[15] sein.
- Der Beklagte muss den Schaden verursacht haben (Adäquater Kausalzusammenhang[16] 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.

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

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

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.

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 schmächtigem Körperbau. Der Velofahrer stützt und erleidet dabei Schürfungen und eine leichte Hirnerschütterung. Das defekte Vorderrad des Velos muss ersetzt werden. Der widerrechtliche Schaden (Schürfungen, 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 Zertifizierungsdienstanbieter 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 Prinzip der Public Key Kryptographie

In sehr rudimentärer Art und Weise wird das Prinzip der Publik Key Kryptographie erklärt. Für weitere Informationen sei der Leser auf die Fachliteratur verwiesen.

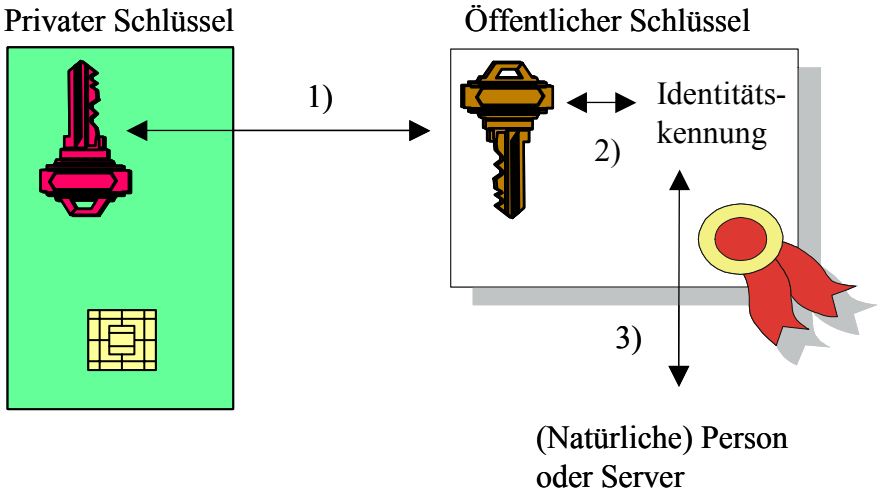

Abbildung 2 Skizze der Funktionsweise der Public Key Kryptographie

Grundsätzlich beruht das Public Key Verfahren auf einem kryptographischen Verfahren. Das Verfahren hat die Eigenschaft, dass zwei unterschiedliche Schlüssel erzeugt und verwendet werden, für die Verschlüsselung und Entschlüsselung. **Doch aus dem einen Schlüssel lassen sich keine Rückschlüsse auf den anderen ziehen 1).**

Die beiden Schlüssel sind aber eindeutig miteinander verbunden wie ein Ehepaar. Vom dem einen Ehegatten lassen sich normalerweise keine Rückschlüsse auf den anderen ziehen. Trotzdem sind sie miteinander eindeutig verbunden (vorausgesetzt, Bigamie ausgeschlossen).

Weil keine Rückschlüsse möglich sind, kann der eine Schlüssel veröffentlicht werden und der andere privat gehalten werden. Die Authentisierung funktioniert so, dass man das Gegenüber davon überzeugt, dass man den anderen, dazu passenden, privaten Schlüssel kennt. Z.B. man verschlüsselt etwas, und der andere kann es so entschlüsseln, dass etwas Plausibles entsteht.

Nun kann jeder behaupten, er sei z.B. der Verwaltungsratspräsident des Unternehmens XY mit dem entsprechenden öffentlichen Schlüssel. Deswegen sind digitale Zertifikate unerlässlich, welche die Zugehörigkeit von öffentlichem Schlüssel und der Identitätskennung beglaubigen 2). Anhand der Identitätskennung im Zertifikat kann ein Rückschluss auf die natürliche Person oder Server gemacht werden 3).

Wenn der private Schlüssel bekannt wird, so kann sich jemand anderer als die betreffende Person ausgeben. Deswegen werden die privaten Schlüssel in sicheren Einheiten wie einer Crypto Card (eine mögliche Ausprägung der sicheren Signaturerstellungseinheit) aufbewahrt.

Anhang G – 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 können 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.

Index

A

Adäquater Kausalzusammenhang 21
Adäquater Kausalzusammenhang 57
Anerkannt qualifizierte elektronische Signatur 7
Anerkannt qualifiziertes Zertifikat 7
Anerkannte CA 7
Anerkannte elektronische Signatur 7
Anerkannter CSP 7
Anerkanntes Zertifikat 7
Anerkennungsstelle 7
Anerkennungsstelle 35
Authentisierung 27, 28, 29, 34
  elektronische Signatur 26
  mit Entschlüsselung 27
  online Kommunikation 27

B

beweisen 7, 20, 32, 57
Bundesgericht 17, 24, 28

C

CA 7
Certification Authority 7
Certification Service Provider 7
CSP 7

D

Distinguished Name 7, 34, 42

E

eGovernment 11
  Elektronische Zugang 11
Eigenschriftlichkeit 15
Eingabe von Rechtsschriften 17
Elektronische Signatur 8
  anerkannt qualifizierte 7
  anerkannte 7
  Archivierung 45
  funktionelle 8, 31
  Prüfung 45
  qualifizierte 9
E-Mail 27
Eröffnung eines Entscheids 17

F

Fahrlässig 58
Fahrlässigkeit 58
Formfreiheit 14
Formularzwang 15
Formzwang 15
Fortgeschrittene elektronische Signatur 8
Fortgeschrittenes Zertifikat 8
Funktionelle elektronische Signatur 8
Funktionszertifikat 8, 31, 32
  Einsatzgebiete 31, 32
  wichtige Einsatzgebiete 33

G

Generierung der Schlüssel 38
glaubhaft machen 8, 19, 23, 32, 58

H

Haftung 19, 20, 24, 35, 57
  anerkannter CSP 20
  Anerkennungsstelle 20
  Bundesbeamten 22
  Geschäftsherr 30
  Inhaber des Signaturschlüssels 19
  OR 19
  OR 59a 19
  Privater 19
  Staatsbeamten 22
  VG 20
  ZertES 20
Handhabung der Zertifikate 39
Handunterschrift 12, 16, 18, 31
Hashfunktion 8
Hashwert 8
hoheitlich 18
Hoheitliches Handeln 11

M

MAC 27, 59

N

Namensgebung 41
Non Repudiation 25

Ö

Öffentlicher Schlüssel 8

O

online Authentisierung 25, 26, 28

P

Privater Schlüssel 8
Produktzertifizierung 46
Provisorische Rechtsöffnung 9, 15, 24
Prüfung elektronischer Signatur 45
Pseudonym 30
Public Key Kryptographie 60

Q

Qualifizierte elektronische Signatur 9
Qualifiziertes Zertifikat 9
Qualifiziertes Zertifikat einer anerkannten CA 9

R

Revokation 9

S

Schaden 21
Schriftlichkeit 9
  Eigenschriftlichkeit 15
  einfache 9
  qualifizierte 9
Server 9, 28
Signaturerstellungseinheit 38
  Umgang 38
Signaturprüfschlüssel 8
Signaturschlüssel 8, 10
Spam 10, 40
Staatshaftung 21

U

Unversehrtheit der Daten 44

V

Verantwortlichkeitsgesetz 20
Verfügung 13, 17, 22
  Zustellung 13, 17
Verschlüsselung 27, 28
Verschlüsselungsschlüssel 8
Verschulden 21
Verschuldenshaftung 57, 58
Vertrag 14
Vertraulichkeit 32, 40
Verwaltungsgericht 17
Verwaltungsverfahren 12, 17, 18, 24, 33
  nicht streitig 12
  streitig 12

W

Widerrechtlichkeit 21, 57

Z

Zeitstempel 10
Zeitstempeldienste 10, 32
Zertifikat
  Anerkannt qualifiziertes 7
  Aufbewahrung 39
  Erstellung 39
  Funktionszertifikat 8
  Handhabung 39
  Herausgabe 39
  Inhalt 39
  Qualifiziertes 9
  Qualifiziertes einer anerkannten CA 9
  Ungültigkeitserklärung 39