Literaturverzeichnis

Bücher und Zeitschriften

BIELFELDT Maike / **BRISCH** Britta, in: Deutscher Industrie- und Handelstag (DIHT) (Hrsg.), Digitale Signatur, Bonn, 1998.
BIESER Wendelin / **KERSTEN** Heinrich, Elektronisch unterschreiben, 2. Aufl., Heidelberg, 1999.
BITZER Frank / **BRISCH** Klaus M., Digitale Signatur, Grundlagen, Funktion und Einsatz, Berlin, 1999.
BIZER Johann / **MIEDBRODT** Anja, Die digitale im elektronischen Rechtsverkehr, in: Detlef Kröger / Marc A. Gimmy, Handbuch zum Internetrecht, Berlin, 2000, S. 135ff.
BRISCH Klaus M., Gemeinsame Rahmenbedingungen für elektronische Signature, Richtlinienvorschlag der Europäischen Kommission, in: Computer und Recht, 8/1998, S. 492ff.
BUNDESAMT FÜR JUSTIZ, Gutachten: Digitale Signatur und Privatrecht, in: VPB 63, Nr. 46, S. 446ff.
EMMERT Ulrich, Haftung der Zertifizierungsstellen, in: Computer und Recht, 4/1999, S. 244ff.
ERBER-FALLER Sigrun, Elektronischer Rechtsverkehr und digitale Signaturen in Deutschland – Bisherige Entwicklungen, internationale Bezüge und Zukunftsperspektiven aus notarieller Sicht, in: Geis, Ivo (Hrsg.), Rechtsaspekte des elektronischen Geschäftsverkehr, Eschborn 1999, S. 85ff.
GEIS Ivo, Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen, in: Computer und Recht, 12/1998, S. 772ff.
GEISER Jean-Maurice, Signature numérique: Les enjeux du projet de réglementation, in: medialex, 4/99, S. 205.
GRAF FRINGUELLI Pietro / WALLHÄUSER Mattias, Formerfordernisse beim Vertragsschluss im Internet, in: Computer und Recht, 12/1999, S. 93ff.
HOEREN Th. / **SCHLÜNGEL** M., Rechtsfragen der digitalen Signatur – Eine Einführung in Recht und Praxis der Zertifizierungsstellen, Berlin, 1999.
HORSTER Patrick (Hrsg.), Digitale Signaturen, Grundlagen, Realisierungen, rechtliche

Aspekte, Anwendungen, Braunschweig/Wiesbaden, 1996.

JACCARD Michel, Droit de la concurrence et signature numérique, Quelques réflexions à la lumière de la concentration Swisskey SA, in: sic! 1/1999, S. 17ff.

JÖHRI Yvonne, Digitale Signatur, Tagung der Interdepartementalen Arbeitsgruppe „Digitale Signatur" vom 24. November 1998 in Biel, in: sic!, 1/1999, S. 73ff.

PESTALOZZI Simone R. / **VEIT** Marc D., Elektronische Signaturen: schweizerischen Regulierungsansätze im europäischen Umfeld, in: AJP, 5/2000, S. 599ff.

RASSMANN Steffen, Elektronische Unterschriften im Zahlungsverkehr, in: Computer und Recht, ?/1998, S. 36ff.

ROSENTHAL David, Digitale Signaturen: Der Bund will vorwärts machen, in: Revue SAV, 2/1999, S. 19f.

ROSENTHAL David, Projekt Internet, Zürich, 1997.

RUNGE Alexander, Elektronische Unterschriften, St. Gallen, 1997.

SANDL Ulrich, Wirtschaftspolitische Bedeutung digitaler Signaturen, Die etwas andere „Kryptodiskussion", in: Computer und Recht, 5/2000, S. 319ff.

SCHLECHTER Richard, Ein europäischer Rahmen für elektronische Signaturen, in: Geis, Ivo (Hrsg.), Rechtsaspekte des elektronischen Geschäftsverkehr, Eschborn 1999, S. 107ff.

SCHUMACHER Stephan, Digitale Signaturen in Deutschland, Europa und den USA, in: Computer und Recht, 12/1998, S. 758ff.

SCHUMACHER Stephan, Einigung auf EU-Signaturrichtlinie, in: Computer und Recht, 7/1999, S. 473ff.

SEIDEL Ulrich, Das Recht des elektronischen Geschäftsverkehr, Wiesbaden, 1997.

SEIDEL Ulrich, Dokumentenschutz im elektronischen Rechtsverkehr, in: Computer und Recht, 7/1993, S. 409ff. und 8/1993, S. 484ff.

WIDMER Ursula / BÄHLER Konrad, Rechtsfragen beim Electronic Commerce: sichere Geschäftstransaktionen im Internet, Zürich, 1997.

Zeitungen

o. V., Gegen das digitale Analphabetum, Bundesrat startet Bildungsoffensive im Informatikbereich, in: NZZ, 11. 07. 2000, S. 15.

o. V., Warten auf die Steuererklärung per Internet, Kantone Bern und St. Gallen wollen 2002 so weit sein, in: NZZ, 10. 07. 2000, S. 7.
LALIVE D'EPINAY Maya, Nationalrätin, "E-Switzerland" – auch eine politische Aufgabe, Aktionsfelder für den Staat bei den Informationstechnologien, in: NZZ, 13. 06. 2000, S. 15.
LEGLER Thomas, Startschuss für elektronische Zertifizierungsdienste – Bundesrätliche Verordnung schafft eine rechtliche Grundlage, in: NZZ, 20. 04. 2000, S. 87.
MURAL MÜLLER Hanna, Vizekanzlerin, E-Government – Herausforderung für Behörde, Direkter Austausch zwischen Bürger und Verwaltung?, in: NZZ, 14. 04. 2000, S. 15.
o. V., Gültige elektronische Unterschrift, in: NZZ, 13. 04. 2000, S. 14.
OPPLIGER Rolf, Dezentralisierung erhöht die Sicherheitsrisiken, Ungelöste Probleme beim Agent-based Computing, in: NZZ, 08. 02. 2000, S. 78.
BRUN Pierre, Vertrauen ist besser – Risikomanagement im Electronic Businell, in: NZZ, 04. 02. 2000, S. 76.
o. V., Die EU regelt digitale Signatur, Rechtssicherheit im E-Commerce, in: NZZ, 01. 12. 99, S. 23.
o. V., Zögerliche Anerkennung von digitalen Signaturen, in: NZZ, 29. 10. 99, S. 82.
HUSSEY Peter J., Sicherheit auf dem neuen „Extranet"-Marktplatz, Einsatz vertrauenschaffender Technologien im Internet, in: NZZ, 07. 10. 99, S. 100.
SCHLOSSER Peter, Standard für sichere Nachrichtenübermittlung, Die Public Key Infrastructures als Lösung, in: NZZ, 21. 09. 99, S. 115.
GRABER Christian, Zertifikate für digitale Identitäten, Bestandesaufnahme eines zentralen E-Commerce-Elements, in: NZZ, 21. 09. 99, S. 119.
ROSENTHAL David, Rechtliche Basis für den Einsatz digitaler Signaturen, Bund gibt Verordnung in Vernehmlassung, in: NZZ, 18. 06. 99, S. 77.
o. V., Erleichterung für Zahlungsverkehr via Internet, Vereinbarung einer EU-Richtlinie, in: NZZ, 23. 04. 99, S. 21.
o. V., Mehr Datensicherheit bei der Verwaltung, in: NZZ, 21. 01. 99, S. 16.
ROSENTHAL David, Unterschreiben mit einem Mausklick – Rechtliche Probleme bei der Anwendung digitaler Signaturen, in: NZZ, 20. 11. 98, S. 69.
o. V., Wo zu legiferieren wäre, in: NZZ, 07. 11. 98, S. 29.
JÖRG Florian S. / ARTER Oliver, Gesetzgeberischer Handlugsbedarf bei „electronic

commerce“?, Im Spannungsfeld zwischen grenzüberschreitendem Handel und nationalem Recht, in: NZZ, 07. 11. 98, S. 29.
MÜLLER Otto, Vertrauenswürdige digitale Identitäten – Vertrauen ist Grundlage des elektronischen Marktes, in: NZZ, 22. 09. 98, S. 92.
GRABER Christian, Werkzeuge für ein sicheres Internet, Digitale Unterschriften ersetzen die Handunterschrift, in: NZZ, 22. 09. 98, S. 95.
o. V., Elektronische Unterschrift erhöht Sicherheit im Internet, Zertifikate ab Herbst erhältlich, in: NZZ, 08. 05. 98, S. 68.
o. V., Das E-Geschäft harrt der E-Unterschrift, Im Oktober will der Bundesrat einen Gesetzesentwurf vorlegen, in: NZZ, 13. 06. 2000, S. 99.
FELLER Urs, Neue Regeln für den E-Commerce, Die Bedeutung der EU-Fernabsatzrichtlinie für die Schweiz, in: NZZ, 05./06. 08. 2000, S. 23.

Texte aus dem Internet

BÜRGE Urs, Digitale Signatur und Recht – Voraussetzungen, Stand und Aussichten der rechtlichen Anerkennung in der Schweiz. http://www.ofj.admin.ch/themen/ri-ir/digsig/intro-d.htm (verifiziert: 28. 07. 2000)
ROSENTHAL David, Digitale Signatur: Wo sie eine Rolle spielt, IPD Insider Presse Dienst, April 2000. http://www.ipd.ch/texte/ipd4006.htm (verifiziert: 23. 07. 2000)
ROSENTHAL David, Digitale Signatur: Ein elektronisches Siegel fürs Internet, IPD Insider Presse Dienst, April 2000. http://www.ipd.ch/texte/ipd4007.htm (verifiziert: 23. 07. 2000)
ROSENTHAL David, Digitale Signatur: Bundesrat schafft Qualitätslabel, IPD Insider Presse Dienst, April 2000. http://www.ipd.ch/texte/ipd4005.htm (verifiziert: 23. 07. 2000)
ROSENTHAL David, Stellungnahme zum Entwurf einer “Public Key Infrastruktur Veordnung” (PKIV-E) vom 3. Juni 1999, 09. 07. 99. http://www.rvo.ch/docs/pkiv-dr.pdf (verifiziert: 07. 08. 2000)
ROSENTHAL David, Digitale Zertifikate erhitzen die Gemüter, Online-Ausgabe Computerworld (Schweiz), 19. 07. 99.

http://www.computerworld.ch/domino/CWArchiv.nsf, dann im Archiv suchen (verifiziert: 22. 07. 2000)
ROSENTHAL David, Der Konsument als Spielverderber, Online-Ausgabe Computerworld (Schweiz), 09. 03. 98. http://www.computerworld.ch/domino/CWArchiv.nsf, dann im Archiv suchen (verifiziert: 22. 07. 2000)
LANDROCK Peter, Public Key Infrastruktur und elektronischer Handel – ein Pamphlet, Online-Ausgabe Computerworld (Schweiz), 08. 02. 99. http://www.computerworld.ch/domino/CWArchiv.nsf, dann im Archiv suchen (verifiziert: 22. 07. 2000)
ROSENTHAL David, E-Commerce: Die Kuh melken andere, Online-Ausgabe Computerworld (Schweiz), 09. 06. 2000. http://www.computerworld.ch/domino/CWArchiv.nsf, dann im Archiv suchen (verifiziert: 22. 07. 2000)
HAEFELY Andrea, CA, Online-Ausgabe Computerworld (Schweiz), 08. 02.99. http://www.computerworld.ch/domino/CWArchiv.nsf, dann im Archiv suchen (verifiziert: 22. 07. 2000)
HAEFELY Andrea, Wunder dauern länger, Online-Ausgabe Computerworld (Schweiz), 25. 10. 99. http://www.computerworld.ch/domino/CWArchiv.nsf, dann im Archiv suchen (verifiziert: 22. 07. 2000)
STARK Jens, Sicherheit ist relativ, Online-Ausgabe Computerworld (Schweiz), 31. 01. 2000. http://www.computerworld.ch/domino/CWArchiv.nsf, dann im Archiv suchen (verifiziert: 22. 07. 2000)
FRAVI Gondini A., Elektronische Signaturen, 28. 10. 99 http://www.fravi-law.ch/elektronische_signaturen1.htm (verifiziert: 07. 08. 2000)
FRAVI Gondini A., EU-Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 06. 03. 2000. http://www.fravi-law.ch/EU%20Rlfuer%20elektronische%20Signaturen.htm (verifiziert: 03. 09. 2000)
o.V., TeleTrustT, Wissensforum, Digitale Signatur, Wie unterschreibt ein Computer? http://www.teletrust.de/wf/ds.htm (verifiziert: 22. 07. 2000)
o. V., IuKdg, Initiative Informationsgesellschaft Deutschland, Wissensforum,

Einsatzmöglich- keiten der digitalen Signatur. http://www.iid.de/iukdg/wissensforum/einsatz.html (verifiziert: 22. 07. 2000)
o. V., TeleTrusT, Wissensforum, Biometrische Identifikationsverfahren. http://www.teletrust.de/wf/bio.htm (verifiziert: 30. 08. 2000)
o. V., Formvorschriften im digitalen Zeitalter, da trovare dove, chi è l'autore

Verzeichnis der Erlasse und Materialien

Nationale Erlasse

BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. Dezember 1998, (BV, SR 101).
ZertDV	Verordnung über Dienste der elektronischen Zertifizierung (Zertifizierungsverordnung) vom 12. April 2000, (ZertDV, SR 784.103).
FMG	Fernmeldegesetz vom 30. April 1997, (FMG, SR 784.10).
THG	Bundesgesetz über technischen Handelshemmnisse vom 6. Oktober 1995, (THG, SR 946.51).
AkkBV	vom 17. Juni 1996, (AkkBV, SR 946.512).
OR	Schweizerisches Obligationenrecht vom 30. März 1911, (OR, SR 220).
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, (ZGB, SR 210).
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs vom 11. April 1889, (SchKG, SR 281.1).
VwVG	Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1968, (VwVG, SR 172.021).

Nationale Materialien

Kommentar zur ZertDV	Kommentar zur Verordnung vom 12. April 2000 über Dienste der elektronischen Zertifizierung (ZertDV)
E-PKIV	Entwurf des Bundesrates zur Verordnung über eine PKI in der Schweiz vom 3. Juni 1999
E-PKIV-Bericht	Erläuternder Bericht des Bundesrates zum Entwurf zur Verordnung über eine PKI in der Schweiz. http://www.bakom.ch/ger/subsubpage/document/237/807 (verifiziert: 20. 07. 2000)
E-PKIV-Stellungnahmen	Anhörung der interessierten Kreise zum Entwurf zur Verordnung über eine PKI in der Schweiz, Zusammenfassung der Stellungnahmen, September 1999
2. Bericht-KIG	2. Bericht der Koordinationsgruppe Informationsgesellschaft (KIG) an den Bundesrat vom 16. Mai 2000
Amtliches Bulletin des Ständerates	Motion Leumann, Digitale Unterschrift, (99.3288), Wortlaut der Motion, schriftliche Stellungnahme des Bundesrates vom 8. September 1999, Schriftliche Begründung von Leumann vom 28. September 1999 und schriftliche Stellungnahme von Bundesräting Ruth Metzler vom 28. September 1999. http://www.parlament.ch/Poly/Suchen_amtl_Bulletin/ce99…/266.htm (verifiziert: 13. 08. 2000)
Amtliches Bulletin des Nationalrates	Interpellation Ehrler Melchior vom 22. Dezember 1999, Entwicklung zur Informationsgesellschaft. Wo bleibt die Schweiz? (99.3632), Wintersession. http://www.parlament.ch/afs/data/d/gesch/1999/d_gesch_19993632.htm (verifiziert: 14. 08. 2000)
Amtliches Bulletin des Nationalrates	Motion Kommission 00.016-NR vom 9. Mai 2000, E-Switzerland. Staat als Modellanwender, (00.3194). http://www.parlament.ch/afs/data/d/gesch/2000/d_gesch_20003194.htm (verifiziert: 13. 08. 2000)
Amtliches Bulletin des Nationalrates	Motion Adalbert Durrer vom 15. März 2000, E-Commerce. Regulierungsbedarf, (00.3057).

	http://www.parlament.ch/afs/data/d/gesch/2000/d_gesch_20003057.htm (verifiziert: 13. 08. 2000)
Amtliches Bulletin des Nationalrates	Interpellation Peter Hess vom 07. März, IT- und E-Commerce-Initiative, (00.3028). http://www.parlament.ch/afs/data/d/gesch/2000/d_gesch_20003028.htm (verifiziert: 14. 08. 2000)

Internationale Erlasse

ESig-RL	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Abl. Nr. L 013 vom 19/01/2000 S. 0012 – 0020. http://www.europa.eu.int/eur-lex/de/lif/dat/1999/de_399L0093.html (verifiziert: 19. 07. 2000)
FARL	Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, Abl. Nr. L 144 vom 04/06/1997 S. 0019 – 0027. http://europa.eu.int/eur-lex/de/lif/dat/1997/de_397L0007.html (verifiziert: 10. 08. 2000)
E-Commerce-RL	Richtlinie 2000/??/?? des eurokdfjdlkfjaölldlgjlgdljfdlflfdlkfjlajdljfdlfjdljfdljflkdalfjfl kjdfljdlfjalfjdjföladjfldjfldkjfdljfdlkjfldkjflöadjfjfdjflsdfjdf
OECD-Krypto-Leitlinien	Guidelines on Cryptography Policy of 27 March 1997, OECD/GD(97)204. (französische Version) http://www.oecd.org/dsti/sti/it/secur (verifiziert: 04. 08. 2000)
OECD-Verbraucherschutz-Leitlinien	OECD-Leitlinien für den Verbraucherschutz im Zusammenhang mit dem elektronischen Geschäftsverkehr

	(deutsche Übersetzung). http://www.oecd.org/dsti//sti/it/consumer/prod/guidelines-de.pdf (verifiziert: 04. 08. 2000)
UNCITRAL-E-Commerce-Modellgesetz	UNCITRAL – Model Law on electronic commerce, UNCITRAL General Assembly Resolution 51/162 of 16 Dec 1996, (französische Version) http://www.uncitral.org/french/texts/electcom/ml-ec.htm (verifiziert: 21. 08. 2000)

Internationale Materialien

Uniform Rules on Electronic Signatures	Draft Guide to Enactment of the UNCITRAL Uniform Rules on Electronic Signatures vom 18. August 2000, A/CN.9/WG.IV/WP.86. http://www.uncitral.org/english/sessions/wg_ec/index.htm#TOP (verifiziert: 27. 08. 2000)
Rapport Groupe de travail	Rapport du Groupe de travail sur le commerce électronique sur les travaux de sa trente-sixième session (New York, 14-25 février 2000) vom 5. April 2000, A/CN.9/467.
OECD-Inventory	Inventory of approaches to authentication and certification in a global networked society, vom 4. Oktober 1999, DSTI/ICCP/REG(99)13/FINAL. http://www.olis.oecd.org/olis/1990doc.nsf/linkto/dsti-iccp-reg(99)13-final (verifiziert: 04. 09. 2000)
OECD Letter 6/4	OECD Adopts guidelines for cryptography policy, in: OECD Letter 6/4 of May 1997. http://www.oecd.org/publications/letter/0604.html (verifiziert: 21. 08. 2000)

Verzeichnis der Auskunftspersonen

Dr. Felix Schöbi, Projektleiter der Gesetzgebung im E-Commerce beim Eidgenössichen Justiz- und Polizeidepartement, E-Mails vom 10./14./16./28. 08. 2000, s. Anhänge I, II, III und IV.

Lic. Iur. Urs Bürge, Abteilungschef, Leiter der Fachstelle für Rechtsinformatik und Informatikrecht, telefonische Befragung vom 1. 09. 2000.

Lic. Iur. Philippe Gerber, Projektleiter der Gesetzgebung im E-Governement beim Eidgenössischen Justiz- und Polizeidepartement, telefonische Befragung vom 1. 09. 2000.

Lic. Iur. Robert Dietschi, Wissenschaftlicher Adjunkt beim Bundesamt für Kommunikation, E-Mail vom 28. 08. 2000, s. Anhang V.

Christian Graber, Geschäftsführer der Swisskey AG, E-Mail vom 14. 08. 2000 und telefonische Befragung vom 31. 08. 2000.

Lic. Iur. David Rosenthal, Publizist und Rechtsberater, telefonische Befragung vom 31. 08. 2000.

1. Einleitung

1.2 Elektronischer Rechtsverkehr

Der Begriff des Rechtsverkehrs wird verwendet, um den Austausch rechtlich verbindlicher Nachrichten zu kennzeichnen. Von elektronischem Rechtsverkehr ist die Rede, soweit er mit Hilfe moderner Informations- und Kommunikationsmedien erfolgt. Das Papierdokument als tradiertes Trägermedium einer Nachricht wird durch das elektronische Medium substituiert. Zusammenfassend können also als elektronischer Rechtsverkehr die mit Mitteln der Informations- und Kommunikationstechnik unterstützten Handlungen und Erklärungen bezeichnet werden, die Rechtspflichten begründen, verändern, erfüllen oder beenden.[1]

Der elektronische Rechtsverkehr unterliegt aber ohne weitere Sicherungen erheblichen Risiken, denn elektronische Informationen sind flüchtig und können spurenlos verändert werden. Diese Risiken werden potenziert, weil technische Fehler oder absichtliche Manipulationen durch eine Partei oder Dritte von den Betroffenen nicht erkannt werden können. Dies hat zur Folge, dass die Teilnehmer am Rechtsverkehr nicht sicher sein können, ob ein übermitteltes elektronisches Dokument *unverfälscht* ist und auch tatsächlich von dem *Urheber* stammt, von dem es zu kommen scheint.[2]

Dazu kommt auch, dass eine traditionelle Kommunikation via Internet *nicht abhörsicher* ist, egal, ob sie im World Wide Web oder ob sie mit elektronischer Post erfolgt.

1.2 Vertrauen ist die Grundlage des elektronischen Marktes

Vertrauen in die Durchsetzbarkeit von Verträgen ist die Grundlage für das Funktionieren jedes Marktes. Dies gilt auch für den weltweiten elektronischen Handel im Internet.

Ohne Vertrauen in organisatorische und rechtliche Infrastrukturen entsteht kein grossräumiger Markt. Der Handel würde sich in lokalen Märkten versteifen.

Im Unterschied zu traditionellen Handels- und Dienstleistungen stehen sich die Vertragspartner im Internet nicht direkt gegenüber und kennen sich oft nicht aus vorhergehenden Geschäften.[3]

[1] Detlef Kröger, Marc A. Gimmy: Handbuch zum Internetrecht, Berlin Heidelberg, 2000, S. 139
[2] vgl. FN 1, S. 141
[3] Thomas Legler: Digitale Signaturen fördern den E-Commerce, NZZ, 20.04.2000

An dieser Stelle ist aber hinzuzufügen, dass Geschäfte unter Geschäftsleuten kaum Probleme verursachen. Wie sie bisher schon über Telefon oder Telefax gängig sind, stellen sie auch im Internet kein Problem dar. Die Gesetze räumen den Geschäftsleuten eine weitgehende Vertragsautonomie ein. Der Gesetzgeber will in der Tat diese Geschäfte nicht durch unnötige Schutzvorschriften in ihren Möglichkeiten beschränken, weil Geschäftsleute gut genug wissen oder wissen sollten, was sie tun und worauf sie sich einlassen dürfen.[4]

Was sie geregelt haben wollen, regeln sie per Vertrag – von der Geltung elektronischer Dokumente bis hin zum anwendbaren Recht. Die wichtigsten Grundsätze des internationalen Handelns sind ohnehin bereits seit Jahren durch internationale Abkommen und halbprivate Standards wie etwa jene der Internationalen Handelskammer (ICC) gut geregelt. Zunehmen wird vor allem die Zahl der Ad-hoc-Geschäfte mit unbekannten Partnern, so dass nicht wie im heutigen EDI (Electronic Data Interchange) vorher Rahmenverträge geschlossen werden können.[5]

Aber mit dem Internet nehmen Massengeschäfte mit dem Konsumenten zu. Bisher hatten die Konsumenten im internationalen Handel nicht viel zu suchen. Dank dem Internet wollen nun aber auch sie von billigeren und attraktiven Angeboten aus dem Ausland profitieren. Und da beginnen die Probleme. Leidtragend sind nicht die Konsumenten allein, sondern auch die Anbieter.

Der Bundesrat hat am 12. April 2000 einen ersten juristischen Schritt zur Förderung eines sicheren elektronischen Geschäftsverkehrs in der Schweiz getan. Er hat auf den 1. Mai 2000 die Verordnung über Dienste der elektronischen Zertifizierung in Kraft gesetzt.

1.3 Elektronische Signatur als Überbegriff

Elektronische Nachrichten ersetzen bereits in vielen Fällen den traditionellen Brief in Papierform. An die Stelle von Akten und Karteien in den Büros treten elektronische Speicher. Das bisherige Medium Papier wird damit in weiten Bereichen durch elektronische Datenträger ersetzt.

Elektronische Daten können jedoch nicht in der bisherigen Weise eigenhändig unterschrieben werden. Das Scannen der eigenen Unterschrift und das Anhängen derselben an den Text ist sicher nicht die beste Lösung, weil jede Person mit mittelmässigen

[4] David Rosenthal: Der Konsument als Spielverderber, Computerworld, 09.03.98, S. 2
[5] David Rosenthal: Der Konsument als Spielverderber, Computerworld, S. 2

Computerkenntnissen dieselbe Unterschrift kopieren und für eigene Zwecke nutzen könnte. Es würde damit nur das Missbrauchspotential erhöht werden.

Hier bedarf es eines neuen Mittels: der „elektronischen Unterschrift oder Signatur" – in der Fachsprache als „digitale Signatur" bezeichnet.[6]

Eigentlich ist die elektronische Signatur ein Überbegriff für verschiedene Arten von Unterschriften im elektronischen Rechtsverkehr. Die digitale Signatur ist eine bestimmte technologiespezifische Art von elektronischer Signatur, hingegen ist der Begriff der „elektronischen Signatur" weniger „technologiegebunden".[7] Er umfasst die digitale Signatur, schliesst aber andere Technologien nicht aus. In der Tat bestehen zur Zeit, abgesehen von der digitalen Signatur, biometrische Identifikationsverfahren. Diese können aber nicht als echte elektronische Signatur betrachtet werden. Solche Verfahren nutzen die Tatsache, dass verschiedene Körper- oder Verhaltensmerkmale einem bestimmten Menschen eindeutig zugeordnet werden können. Der Vorteil dieser Verfahren ist, dass diese personenspezifischen Merkmale nicht gestohlen, verloren, vergessen oder weitergegeben werden können.[8] Die wichtigsten Verfahren werten die folgenden Merkmale aus: Finger, Stimme, Gesicht, Tastenanschlag und Unterschrift (bezogen auf die Dynamik, also auf die Geschwindigkeit und der Druck). Diese Verfahren sind schon heute verfügbar, aber in Zukunft wird es so sein, dass man die digitale Signatur mit biometrischen Identifikationsverfahren kombinieren werden kann.

2. Grundlagen digitaler Signaturverfahren

2.1 Zweck

Die auf einer Public Key Infrastructure (PKI) beruhende digitale Signatur ist zur Zeit die sicherste Identifikationstechnologie.

Digitale Signaturen sollen sicherstellen:

- dass die von den Geschäftspartnern via Internet ausgetauschten Willensäusserungen auf ihrem Transportweg nicht verändert werden können (Integrität);

[6] Wendelin Bieser, Heinrich Kersten: Elektronisch unterschreiben, 2. Aufl., Heidelberg, 1999
[7] s. Thomas Hoeren, S. 387
[8] s. TeleTrustT- Wissensforum, Biometrische Identifikationsverfahren, http://www.teletrust.de/wf/bio.htm

- dass die Person, welche die Transaktionen ausgelöst hat, ist, wer sie zu sein vorgibt (Authentizität);
- dass erfolgte Transaktionen vom Sender nicht bestritten werden können und nachprüfbar bleiben (Nichtabstreitbarkeit);
- dass vertrauliche Dokumente bei der Übertragung im Internet nicht eingesehen werden können (Vertraulichkeit).[9]

Die digitale Signatur ist sicher die beste Lösung, und sie vermag eine handschriftliche Unterschrift ohne weiteres zu ersetzen.
Sie bietet sogar einen höheren Grad des Integritätsschutzes als eine handschriftliche Unterschrift.

2.3. Technische Aspekte der digitalen Signatur

2.3.1 Symmetrische vs. asymmetrische Kriptografieverfahren

„Kriptographie“ stammt aus dem Griechischen und heisst wörtlich übersetzt „Geheimschrift“. Die ersten Kryptografiesysteme waren sehr simpel zu knacken, aber damals waren sie wirksam. Cäsar z. B. verschlüsselte seine Meldungen, die er seinen Boten auf den Weg gab, in dem er das Alphabet um drei Buchstaben verschob.[10]
Bei den heutigen Verschlüsselungstechniken werden die Daten mit Hilfe von mathematischen Verfahren so verändert, dass diese auch mit grossem Aufwand nicht gelesen werden können.
Es gibt also symmetrische und asymmetrische Verschlüsselungsverfahren.

2.3.1.1 Symmetrisches Verfahren

Bei der symmetrischen Kryptographie wird sowohl für die Verschlüsselung als auch für die Entschlüsselung der gleiche Schlüssel verwendet.
Das an der ETH Zürich entwickelte IDEA (International Data Encryption Algorithm), das DES (Digital Encryption Standard), das von IBM entwickelt wurde und von der US-

[9] Thomas Legler: Digitale Signaturen fördern den E-Commerce, NZZ, 20. 4. 2000
[10] articolo Computerworld, se non erro

amerikanischen Regierung verwendet wird, und die DES-Verfeinerung Triple DES (3DES) funktionieren nach diesem Muster.[11]

Der Vorteil der symmetrischen Verschlüsselung besteht darin, dass dieses Verfahren schnell ist und mit kurzen Schlüsseln arbeitet.

Der Hauptnachteil ist, dass beide Seiten im Besitz des gleichen, hochgeheimen Schlüssels sein müssen. Wohnen die beiden Anwender in der Schweiz, so scheint es noch realisierbar, dass die beiden sich treffen, um sich die Diskette mit dem Geheimcode zu übergeben. Wohnt aber die eine Partei in Europa und die andere in den USA, wird der sichere Austausch des Codes schwer beziehungsweise unmöglich. Der Austausch des Schlüssels über ein unsicheres Medium wie das Internet unterliegt wie alles andere den oben genannten Gefahren.

2.3.1.2 Asymmetrisches Verfahren

Man kann das oben erwähnte Problem auf elegantere Weise lösen: Der Benutzer besitzt ein einmaliges mathematisches Schlüsselpaar. Mit dem einen Schlüssel wird verschlüsselt, und mit dem zweiten Schlüssel wird entschlüsselt. Es gibt nur genau einen Schlüssel, der zum Gegenschlüssel passt, und aus dem einen Schlüssel kann der zweite nicht abgeleitet werden. Sie sind verwandt, aber die Verwandtschaft ist so kompliziert, dass sie nicht errechnet werden kann.

Der eine Schlüssel ist geheim (Private Key) und dient der Erstellung der Signaturen, der andere Schlüssel ist öffentlich (Public Key) und dient zur Überprüfung der mit dem geheimen Schlüssel erstellten Signaturen.

Eine vertrauliche Nachricht wird mit dem öffentlichen Schlüssel des Empfängers, der kein Geheimnis ist, verschlüsselt. Nur der richtige Empfänger mit dem entsprechenden dazu-passenden privaten Schlüssel wird in der Lage sein, diese zu entschlüsseln und die Nachricht zu lesen. Dieses Verfahren ist aber noch keine digitale Signatur, weil damit noch nicht geprüft ist, ob die Person, welche die Nachricht gesandt hat, wirklich ist, wer sie zu sein vorgibt. Jede Person, die in Besitz des öffentlichen Schlüssels des Empfängers käme, könnte ihm eine Nachricht senden. Der Empfänger hätte in diesem Fall nicht die Sicherheit, dass die Botschaft wirklich vom angegebenen Absender stammen würde.

Die asymmetrische Verschlüsselung bietet nur (wie das Wort selber aussagt) die Codierung der Daten und nicht zugleich die drei anderen wichtigen Funktionen der

[11] Jens Stark: Sicherheit ist relativ, Computerworld, 31.01.2000

digitalen Signatur, namentlich die Prüfung der Authentizität, der Integrität und die Nichtabstreitbarkeit. Die Verschlüsselung dient nur der Vertraulichkeit der ausgetauschten Informationen.
Da die digitale Signatur sich auf die asymmetrische Verschlüsselung stützt, kann natürlich die wesentliche Funktion der Vertraulichkeit mit inbegriffen werden.

2.3.2 Fingerabdrücke von Dokumenten

Bei der Erzeugung einer digitalen Signatur kann man im einfachsten Fall so vorgehen, dass der Signieralgorithmus direkt auf die zu signierenden Daten angewendet wird. Bei den meisten Signaturverfahren entsteht dabei eine Signatur, die grössenordnungsmässig dieselbe Länge besitzt wie die signierten Daten selbst. Folglich wird sich das Datenvolumen mindestens verdoppeln. Um diesen unpraktikabel hohen Aufwand zu begrenzen, ist es üblich, von einem Dokument zuerst eine Kurzform zu erstellen und diese dann zu signieren; vorausgesetzt wird natürlich, dass die Nachricht selbst lesbar bleibt. Die Verfahren zur Erzeugung dieser Kurzform heissen *kryptographische Hashfunktionen*; die Kurzform wird auch *Fingerabdruck*, *Hashwert* oder engl. Finger print genannt.[12] Die Hashfunktion konzentriert den Inhalt eines Dokuments auf einen eindeutigen Wert von fixer Länge. Entscheidend ist dabei, dass aus zwei verschiedenen Dokumenten nicht der gleiche digitale Fingerabdruck entsteht. Dies bedeutet, dass bei der Veränderung von auch nur einem Bit im Originaldokument ein anderer Hashwert entsteht.[13]
Wichtig ist auch, dass der originale Inhalt sich nicht aus dem Fingerabdruck rekonstruieren lässt.

2.3.3 Erzeugung und Überprüfung von digitalen Signaturen

Die digitale Signatur wird aus dem Fingerabdruck, unter Benutzung des geheimen Signaturschlüssels des Senders, berechnet. Die Signatur wird nun der Nachricht angefügt und mit ihr verschickt. Das digital signierte Dokument besteht also aus dem Dokument selbst und der zugehörigen digitalen Signatur.
Die Überprüfung des digital signierten Dokuments läuft wie folgt ab:

[12] Thomas Hoeren: Rechtsfragen der digitalen Signatur, S. 73 - 74
[13] Christian Graber: Werkzeuge für ein sicheres Internet, NZZ 22.09.2000

Der Empfänger wird die digitale Signatur mit dem öffentlichen Schlüssel des Inhabers entschlüsseln, und er erhält so wieder den Fingerabdruck der ursprünglichen Nachricht; gleichzeitig berechnet er den digitalen Fingerabdruck der erhaltenen Nachricht neu.
Sind beide identisch, beweist dies die Authentizität des Absenders, da nur der Sender allein über den passenden privaten Schlüssel verfügt und somit auch nicht bestreiten kann, die Nachricht versandt zu haben.
Weiter wird garantiert, dass die Nachricht unterwegs nicht verändert wurde, sonst wären die Fingerabdrücke verschieden.[14]

Hingegen verläuft die Anwendung der digitalen Signatur in bezug auf eine vertrauliche Nachricht, die nicht lesbar bleiben soll, wie folgt:

1. Der Sender verschlüsselt zuerst die Nachricht mit seinem geheimen Schlüssel.
2. Er verschlüsselt danach die schon einmal codierte Nachricht mit dem öffentlichen Schlüssel vom Empfänger.
3. Der Empfänger hingegen entschlüsselt die Nachricht zuerst mit seinem geheimen Schlüssel,
4. Und danach entschlüsselt er das entstandene Dokument mit dem öffentlichen Schlüssel des Senders.

Da der Empfänger die Nachricht nur mit dem öffentlichen Schlüssel des Absenders entschlüsseln kann, ist garantiert, dass die Nachricht wirklich vom angegebenen Absender stammt. Gleichzeitig ist auch sicher, dass die Nachricht nicht abgehört worden ist, weil nur der Empfänger mit seinem Private Key die Nachricht decodieren kann.
Die Integrität ist auch gewährleistet, weil dazu auch ein Fingerabdruck der Nachricht erfolgt.

2.4 Organisatorische Aspekte der digitalen Signaturen

2.4.1 Funktion von Zertifizierungsstellen

Die Sicherheit von Public-Key-Anwendungen hängt nicht nur von den verwendeten Verschlüsselungssystemen ab.[15] Ebenso entscheidend ist auch, dass der Empfänger einer digitalen Signatur darauf vertrauen kann, dass der dazu verwendete öffentliche Schlüssel

[14] Christian Graber: Werkzeuge für ein sicheres Internet, NZZ 22.09.2000
[15] David Rosenthal, Projekt Internet, 1997, S. 246

tatsächlich von der angegebenen Person stammt. Dieses Problem lässt sich dadurch lösen, dass eine dritte Person, der vertraut werden kann, bescheinigt, dass ein bestimmter öffentlicher Schlüssel tatsächlich der genannten Person gehört.[16] Öffentliche oder private Zertifizierungsstellen dienen der Lösung dieses Problems. Sie werden auch „Trusted Third Party“ oder „Certification Authority“ (CA) genannt.

Sie stellen die sogenannten digitalen Zertifikate aus, in denen der Name der Person und ihr öffentlicher Schlüssel unzertrennlich voneinander angeführt werden. Hierdurch können auch einander unbekannte Personen ihre Schlüssel austauschen. In der Tat müssen die Zertifikate nicht notwendigerweise dem Kunden ausgehändigt werden. Es ist möglich, die Zertifikate dem Publikum über einen Verzeichnisdienst zur Verfügung zu stellen.

Certification Authorities braucht es nur dort, wo sich Geschäftspartner nicht kennen und vorweg verständigen können oder ihre Zertifikate nicht selbst verwalten können.[17]

„Zertifizierungsstelle“ ist ein sehr breiter Begriff. Neben der Bereitstellung der kryptographischen Dienste ist auch die Verwaltung der Schlüssel und der digitalen Zertifikate die wichtigste Aufgabe einer Zertifizierungsstelle. Aus diesem Grund können die verschiedenen Aufgaben auf verschiedene Stellen verteilt werden. Man spricht auch von „Public Key Infrastructure“ (PKI). Damit wird der gesamte Apparat von Einrichtungen bezeichnet, der nötig ist, um digitale Unterschriften verwenden und verifizieren zu können.[18]

Jede PKI kann drei zentrale Elemente haben:

1. Certification Authority (CA): eine vertrauenswürdige Drittstelle, die sogenannte Trusted Third Party, die für die Ausgabe, die Bestätigung der Gültigkeit und das Sperren von digitalen Zertifikaten sorgt.
2. Registration Authority (RA): Diese Stelle ist für die Überprüfung und Beglaubigung der Identität eines Antragstellers zuständig.
3. Directory Services (DIR): Diese Stelle führt eine Datenbank für die Speicherung und die Publikation der Public Keys und der digitalen Zertifikate, einschliesslich einer Liste der gesperrten und abgelaufenen Zertifikate.[19]

In der Schweiz übernimmt die Swisskey, ein Joint venture von Swisscom, Telekurs und Digi-Signa (ein Verein der Handelskammern der Schweiz und des Fürstentums

[16] Rosenthal, Projekt Internet, S. 246
[17] David Rosenthal, Der Bund will vorwärts machen, in SAV Revue 2/1999 s. 19ff.
[18] s. David Rosenthal, Projekt Internet, 1997, s. 246
[19] Peter Schlosser: Standard für sichere Nachrichtenübermittlung, NZZ 21.09.99

Liechtenstein), die Funktion der Certification Authority und der Directory Services.[20] Als Registration Authority sind hingegen die verschiedenen angeschlossenen Handelskammern zuständig. Vorteil dieses Systems ist, dass man über ein breites Netz an Registrierungsstellen verfügt. In Zukunft könnten aber auch die Banken eine solche Funktion übernehmen. Zur automatischen Statusabfrage der Zertifikate ist seit kurzer Zeit OCSP (Online Certificate Status Protocol) als Standard definiert.[21]

2.4.1.1 Die Rolle des digitalen Zertifikats

Digitale Zertifikate werden heute in der Regel dazu benutzt, um im elektronischen Datenverkehr die Identität einer Person verifizieren zu können. Diese „Identifikations-Zertifikate“ funktionieren als elektronischer Identitätsausweis.[22]
Zertifikate für digitale Identität sind also einerseits die Ausweise im Internet, mit denen der Zugang zu Dienstleistungen geregelt wird. Andererseits erlauben sie das digitale Unterschreiben und Verschlüsseln.
Dank digitalen Zertifikaten wird E-Mail ein sicherer Informationskanal, der auch für vertrauliche Informationen eingesetzt werden kann. Informationsaustausch zwischen Ärzten und Anwälten, Krankengeschichten, Geschäftsgeheimnisse, kritische Unternehmensdaten können mittels Zertifikaten und eines E-Mail-Programms sicher verschickt werden.
Auch z. B. der Zugang zu geschützten Diensten, wie beispielsweise zum Internet-Banking, wird drastisch erleichtert. Die unhandliche Strichliste mit den nur einmal verwendbaren Nummern, die verschiedenen Passwörter, die man immer braucht, Benutzernummern bzw. -namen und die sogenannte „Security-Identity-Card“ werden vollständig durch digitale Zertifikate ersetzt.
Neben den Schlüsselzertifikaten, welche Identitäten bestätigen, werden neue Zertifikatstypen wie Zeitstempel, welche die Zeitinformationen an Daten binden, und Attributszertifikate angeboten werden. Attributszertifikate sind Zusatzzertifikate zu Schlüsselzertifikaten, welche Informationen wie Zutritts-, Unterschrifts- und Kauf-berechtigung bescheinigen.[23]

[20] Schlosser Peter, Die Public Key Infrastructures als Lösung, NZZ, 21. 09. 99
[21] Christian Graber: Zertifikate für digitale Identitäten NZZ, 21.09.99
[22] David Rosenthal, Projekt Internet s. 248
[23] Christian Graber: Zertifikate für digitale Identitäten, NZZ 21.09.1999

2.4.2 Vertrauenswürdigkeit von Zertifikaten

Doch nicht jedem Zertifikat darf dieselbe Bedeutung zugemessen werden: Es muss jeweils abgeklärt werden, was genau mit einem digitalen Zertifikat bescheinigt wird und welche Gewähr für den Inhalt gegebenenfalls geboten wird.[24]

Ausschlaggebend sind die Voraussetzungen, unter welchen eine Zertifizierungsstelle ein Zertifikat ausgibt. Es kann vorkommen, dass eine Zertifizierungsstellen das Zertifikat ausgibt, ohne dass der Antragsteller persönlich erscheint und Ausweisdokumente vorlegt. In diesem Falle würde die Zertifizierungsstelle das Zertifikat ausgeben nur beim Vorhandensein von Angaben über Name, Adresse und weitere persönliche Daten des Antragstellers, ohne sich zu vergewissern, ob die Person, die das Zertifikat braucht, wirklich so heisst.

Die Vertrauenswürdigkeit eines gültigen digitalen Zertifikats hängt davon ab, wie die Zertifizierungsstelle eingeschätzt wird, die es ausgestellt hat.[25]

Deshalb wird in jedem Zertifikat auch der Name der Zertifizierungsstelle genannt.

Kommerzielle Zertifizierungsstellen ohne staatliche Aufsicht sorgen dafür, dass ihre Vertrauenswürdigkeit so hoch wie möglich ist. Sie unterstellen sich in der Tat einer Art „Verhaltenskodex“.

Staatliche Zertifizierungsstellen dürfen das grösste Vertrauen geniessen, und gleich danach folgen Zertifizierungsstellen unter staatlicher Aufsicht und Kontrolle.

Auf den 1. Mai 2000 ist eine Verordnung über Dienste der elektronischen Zertifizierung in Kraft getreten. Ihr Ziel ist es einen rechtlichen Rahmen festzulegen, der Gewähr dafür bietet, dass Zertifizierungsstellen gewisse grundlegende Anforderungen erfüllen. Zertifizierungsstellen würden der staatliche Aufsicht unterliegen.

2.5 Rechtliche Aspekte der digitalen Signaturen

Vertragsabschlüsse sind heute zwar per Internet in den meisten Fällen ohne weiteres möglich. Der Beweis eines solchen Abschlusses mit einem unterzeichneten Stück Papier ist jedoch nach wie vor um ein Vielfaches einfacher als mit einem digital unterzeichneten

[24] David Rosenthal, Projekt Internet, S. 248
[25] Rosenthal, Projekt Internet, S. 249

Dokument, denn die Gerichte in der Schweiz wollten und konnten mit digitalen Dokumenten bislang nichts anfangen.[26]

2.5.1 Die Rechtswirkung digitaler Signaturen

2.5.1.1 Generelle rechtliche Anforderungen

Die Rechtswirkung einer digitalen Signatur kann sich auf dreierlei Weise ergeben. Zwei Parteien können miteinander vereinbaren, in ihrem Geschäftsverkehr eine digitale Signatur als rechtsverbindlich gelten zu lassen; die Verbindlichkeit basiert in diesem Fall auf einem Vertrag. Eine Person kann unter Umständen auch durch eine einseitige Erklärung ihre digitale Signatur für verbindlich erklären.[27]
Es ist schliesslich denkbar, dass eine digitale Signatur bereits vom Gesetz zum rechtsgültigen Ersatz für eine handschriftliche Unterschrift erklärt wird und deren Gebrauch somit rechtsverbindlich wie eine handschriftliche Unterschrift wird.

2.5.1.2 Im Rahmen der Vertragsfreiheit

Das schweizerische Vertragsrecht baut auf den Grundsatz der Vertragsfreiheit. Die Formfreiheit ist Teil der Vertragsfreiheit (Art. 11 Abs. 1 OR, bezüglich internationaler Verträge vgl. auch Art. 11 Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf vom 11. April 1980, Wiener Kaufrecht). Das bedeutet, dass der rechtlich relevante Wille, ungeachtet der Einhaltung bestimmter Formen, zum Ausdruck gebracht werden kann.[28] Es genügt also der Austausch übereinstimmender Willenserklärungen in irgendeiner Form für den Eintritt der Wirkung der digitalen Signatur. Wird also in einem Vertrag der Einsatz der digitalen Signatur vereinbart, so richten sich die Voraussetzungen an die Gültigkeit einer digitalen Signatur nach den jeweiligen Vertragsabmachungen. Digitale Signaturen lassen sich also ohne weiteres verwenden, falls die beteiligten Parteien das wollen. Formfreiheit bedeutet aber auch, dass die Parteien das Recht haben zu bestimmen, dass Schriftlichkeit als Voraussetzung für den Vertragsabschluss zu betrachten ist (OR 16 Abs. 1).[29]

[26] David Rosenthal, Der Konsument als Spielverderber, S. 3
[27] David Rosenthal, Projekt Internet, S.267
[28] Gutachten S.4
[29] Gutachten S. 4

2.1.5.3 Bei Schriftformbedürftigkeit

Von der Formfreiheit gibt es Ausnahmen. Es gibt Fälle, wo die Schriftform, sei es einfache Schriftlichkeit oder öffentliche Beurkundung, gesetzlich vorgeschrieben ist.
Die Ausnahmen dienen unter anderem dem Schutz der schwächeren Vertragspartei bzw. dem Übereilungsschutz, den Interessen Dritter und der Sicherung des Beweises. Auch im Kontakt mit dem Handelsregister und dem Grundbuch ist die Schriftlichkeit erfordert.[30]
In Art. 13 Abs. 1 OR ist die Definition der einfachen Schriftlichkeit enthalten. Folglich muss ein Vertrag, für den die schriftliche Form gesetzlich vorgeschrieben ist, die Unterschriften aller Personen tragen, die durch ihn verpflichtet werden sollen. Art. 14 Abs. 1 OR ergänzt, dass die Unterschrift eigenhändig zu setzen ist. Dem elektronischen Geschäftsverkehr sind in diesen Fällen enge Grenzen gesetzt.
Man könnte Art. 14 Abs. 1 OR analog auf die digitale Signatur anwenden. Sinn und Zweck der handschriftlichen Unterschrift ist es gemäss der herrschenden Rechtslehre, die Person des Erklärenden zu identifizieren und den festgehaltenen Inhalt anzuerkennen. Diese Erfordernisse erfüllt die digitale Unterschrift zweifelsohne.[31]
Aber wo Schriftlichkeit vorgeschrieben ist, muss die Schriftlichkeit verschiedene Funktionen erfüllen: ausser der Identifikation des Erklärenden und der Feststellbarkeit auch die Unverfälschbarkeit, die Konservierung oder Archivierung, die Reproduzierbarkeit, die Registerführung, die Kontrolle, die Nichtabstreitbarkeit und den Übereilungsschutz.[32]
Mit der digitalen Signatur kann ein Teil dieser Funktionen ebensogut oder gar besser wahrgenommen werden, so z. B. die Unverfälschbarkeit des Inhaltes. Bei mehreren Funktionen, wie z. B. der Identifikation der Erklärenden, gibt es schon gewisse Unterschiede. Solange keine biometrischen Elemente verwendet werden, ist beispielsweise nur der Bezug zum Inhaber des privaten Schlüssels, jedoch nicht zu einer physischen Person gesichert. Die Funktion des Übereilungsschutzes kann die digitale Signatur nach heutiger Technik gar nicht erfüllen. Sie könnte es allenfalls, wenn auch die Verwendung ganz bestimmter Programme für das Anbringen der digitalen Signatur vorgeschrieben und feststellbar wäre.[33]

---

[30] Gutachten, S. 1
[31] David Rosenthal, Projekt Internet, S. 270
[32] s. Formvorschriften im digitalen Zeitalter, da ritrovare in Internet
[33] Urs Bürge: Digitale Signatur und Recht – Voraussetzung, Stand und Aussichten der rechtlichen Anerkennung in der Schweiz, in: Die Volkswirtschaft – Magazin für WirtschaftsPolitik 6.99, Bern, 1999

Eine allgemein formulierte Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift bedarf der vorgängigen Beantwortung der Frage nach dem Schutz der schwächeren Vertragspartei vor Übereilung.[34]
Auf dieses Anliegen werde ich in Kapital 3.2 eingehen.

2.5.2 Der Beweiswert digital signierter elektronischer Dokumente

Digital signierte elektronische Dokumente sind vor Gericht wie andere Beweismittel (Parteiverhör, Zeugen, Sachverständige, schriftliche Urkunden) brauchbar. Aber wie alle Beweismittel unterliegen sie der freien richterlichen Beweiswürdigung, und weder sie noch schriftliche Dokumente geniessen eine besondere Privilegierung, die über die im Einzelfall und unter Berücksichtigung aller Umstände zukommende faktische Beweiskraft hinausgeht. Wie stark die Beweiskraft der digital signierten Dokumente ist, hängt nicht von der gesetzlichen Anerkennung der digitalen Signatur, sondern hauptsächlich von der Regelung bzw. Qualität der benutzten Public Key Infrastructure ab.[35] Der Wert einer digitalen Signatur misst sich also an der Art und Weise, wie die Identität des Inhabers einer digitalen Signatur überprüft worden ist.

3. Vorhandene und zukünftige schweizerische Regulierungsansätze

3.1 Die Verordnung über Dienste der elektronischen Zertifizierung

3.1.1 Ihre Tragweite

Zum ersten Mal kümmert sich der Schweizer Gesetzgeber um die digitale Signatur. Die rechtliche Anerkennung der digitalen Signatur ist noch nicht Wirklichkeit, aber die Schweiz ist dieser Anerkennung mindestens näher gekommen. Der zweite wichtige Schritt, d. h. die gesetzgeberische Gleichstellung der elektronischen mit der handschriftlichen Unterschrift, lässt noch auf sich warten. Im Herbst 2000 wird das Vernehmlassungsverfahren betreffend den Bundesgesetzesentwurf über die elektronische Signatur eröffnet.

[34] Gutachten des Bundesamts für Justiz vom 24. November 19998, VPB 63.46, Digitale Signatur und Privatrecht (Vertragsrecht)
[35] Urs Bürge, S. 5

Die Verordnung schreibt freiwillige Regeln für die Beglaubigung von digitalen Signaturen vor, verleiht dem Verfahren der digitalen Signatur in breiteren Kreisen eine gewisse Akzeptanz und Ernsthaftigkeit und fördert die Anwendung von digitalen Signaturen und die grenzüberschreitende Anerkennung der Anbieterinnen von Zertifizierungsdiensten und ihrer Dienste.

Diese neue Verordnung stützt sich aber nicht auf eine klare und solide Gesetzesgrundlage. Formell stützt sie sich auf das Fernmeldegesetz (FMG, Art. 28, 62, 64) und auf das Bundesgesetz über die technischen Handelshemmnisse (THG, Art. 10, 14, 15).

In der Tat ist ihr Regelungsspielraum sehr eingeschränkt. Sie darf nichts von Amtes wegen vorschreiben: die Anerkennung ist für die Zertifizierungsdienste freiwillig. Auch die Rechtswirkung einer digitalen Signatur kann sie nicht festlegen, sondern nur auf deren Regelung hinwirken – und das tut sie auch. Die Verordnung wirkt indirekt.[36] Aus diesem Grunde wird die Verordnung als *Versuchsregelung* erlassen (Art. 1 Abs. 1). Sie gilt so lange, bis eine formelle Gesetzesgrundlage zu diesem Bereich ausgearbeitet worden ist (höchstens aber bis zum 31. Dezember 2009).[37] Ein Bundesgesetz über die elektronische Signatur könnte diese Verordnung auf eine stärkere Grundlage stellen, die digitale Signatur anerkennen und ihr ähnlich der eigenhändigen Unterschrift eine gesetzliche Rechtswirkung verleihen, die in verschiedenen Rechtsgebieten gelten würde.

3.1.2 Der Zweck

Die Verordnung bezweckt die *freiwillige Anerkennung* der Anbieterinnen von Zertifizierungsdiensten. Diese unterliegen den Bestimmungen der Verordnung nur, wenn sie dies wünschen. Somit bezweckt die Verordnung also keineswegs eine Regelung des Zugangs zum Markt für Zertifizierungsdienste, sondern zielt darauf ab, den Anbieterinnen, die es wünschen, ein *Qualitätssiegel* zu verleihen.[38] Diese Anerkennung kann daher für Werbezwecke eingesetzt werden. Eine staatlich konzessionierte Stelle könnte unter Umständen ihre Zertifikate auch teurer verkaufen. Gleichermassen erhalten die Drittpersonen, die den von einer anerkannten Anbieterin von Zertifizierungsdiensten

[36] David Rosenthal: Digitale Signatur: Bundesrat schafft Qualitätslabel, IPD, Homepage Rosenthal, April 2000
[37] vgl. Art. 21 Abs. 2 Verordnung über Dienste der elektronische Zertifizierung (Zertifizierungsdiensteverordnung, ZertDV)
[38] Kommentar zur ZertDV, s. 1

ausgestellten Zertifikaten vertrauen, eine zusätzliche Garantie für die Zuverlässigkeit dieser Zertifikate.[39]

Für eine Zertifizierungsstelle kann es sogar wichtiger sein, mit ausländischen „Schwesterorganisationen" Allianzen zu bilden und so für eine gegenseitige Anerkennung der Zertifikate des anderen zu sorgen. Das macht es für den Kunden einfacher, die Echtheit von Dokumenten aus dem Ausland zu prüfen, selbst wenn er die ausländische Zertifizierungsstelle gar nicht kennt. Die bisher einzige Schweizer Zertifizierungsstelle, die Swisskey, hat zum Beispiel mit anderen Institutionen einen internationalen Zertifizierungsverbund mit dem G77-Netzwerk der Handelskammern geschaffen – ganz ohne gesetzliche Regelung.[40]

Die Verordnung regelt, unter welchen Voraussetzungen ein Zertifizierungsdienst eine Anerkennung erhalten kann. Sie regelt aber nur in den Grundzügen die technischen, administrativen und finanziellen Anforderungen an die Zertifizierungsanbieterinnen. Die wichtigen und heiklen Details sollen erst in den Ausführungsvorschriften nach Art. 20 ZertDV geregelt werden. Diese werden vom BAKOM in Zusammenarbeit mit dem Informatikstrategieorgan Bund (ISB) und der SAS entwickelt. Dadurch können die Regeln rasch an die technische Entwicklung und die internationalen Harmonisierungsbestrebungen angepasst werden.[41]

Es ist denkbar, dass in Zukunft eine Behörde für ihren Verkehr mit Privaten nur digitale Signaturen annehmen könnte, die von einer staatlich anerkannten Zertifizierungsstelle beglaubigt worden sind.

3.1.3 Die Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Das System für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten beruht auf einem hierarchischen Konzept. Zertifizierungsdiensteanbieterinnen werden von einer Anerkennungsstelle (sog. Certification Body) anerkannt, welche ihrerseits von der Schweizerischen Akkreditierungsstelle (SAS) des Eidgenössischen Amtes für Messwesen akkreditiert wird. Dieses System basiert auf dem Bundesgesetz über technische Handelshemmnisse (THG) und auf der Akkreditierungs- und Bezeichnungsverordnung (AkkBV). Die Anerkennung ist ein privatrechtliches Rechtsgeschäft. Sie gilt somit nicht

[39] Erläuternder Bericht der Verordnung über eine PKI in der Schweiz, s. 2
[40] David Rosenthal, Der Bund will vorwärts machen, SAV Revue, 2/1999 s. 19ff.
[41] Kommentar Zur ZertDV s. 8

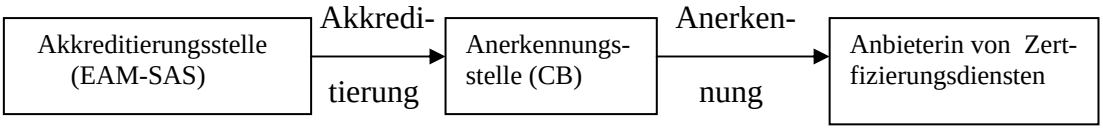
als Verfügung im Sinne von Art. 5 des Bundesgesetzes über das Verwaltungsverfahren. Mögliche Streitigkeiten zwischen Anerkennungsstellen und Anbieterinnen von Zertifizierungsdiensten unterliegen somit nicht der Verwaltungsrechtspflege, sondern werden von Zivilgerichten entschieden.

Nach Art. 2 AkkBV wird mit der Akkreditierung die Kompetenz einer Stelle, nach international massgebenden Anforderungen bestimmte Prüfungen oder Konformitäts-bewertungen durchzuführen, formell anerkannt. Die Bewertung nach international massgebenden Anforderungen zielt auf eine bessere Anerkennung der akkreditierten Stellen und Konformitätsbescheinigungen. In der Tat müssen die Anerkennungsstellen die Kriterien der europäischen Norm EN 45012 erfüllen.[42] Diese Stellen können in vier Hauptkategorien aufgeteilt werden: Prüfstellen, Kalibrierstellen, Zertifizierungsstellen und Inspektionsstellen.[43] Nach Art. 14 Abs. 1 AkkBV erfolgt die Akkreditierung dieser Stellen durch den Direktor des Eidgenössischen Amtes für Messwesen (EAM) auf der Grundlage der Bewertung durch die Schweizerische Akkreditierungsstelle (SAS) und der Stellungnahme der Akkreditierungskommission.

Nach Art. 3 Abs. 3 darf die SAS selber Anbieterinnen von Zertifizierungsdiensten anerkennen, wenn keine Anerkennungsstelle existiert, und nach Art. 5 Abs. 1 müssen die Anerkennungsstellen der SAS die von ihnen anerkannten Anbieterinnen von Zertifizierungsdiensten anmelden. Zudem müssen nach Art. 5 Abs. 2 und 3 die SAS und die anerkannten Anbieterinnen von Zertifizierungsdiensten selbst die Liste der gesamten anerkannten Zertifizierungsstellen mit deren öffentlichen Schlüsseln publizieren. Ziel dieser Veröffentlichungen ist die Schaffung von grösstmöglicher Transparenz und von einem Mindestmass an Integration des Systems. Die anerkannten Anbieterinnen von Zertifizierungsdiensten können sich zwar durch „Cross Certifications“ gegenseitig anerkennen, sind aber nicht verpflichtet, dies mit allen anderen anerkannten Anbieterinnen zu tun. Somit fördert die beabsichtigte Transparenz auch einen gesunden und wirksamen Wettbewerb zwischen den anerkannten Anbieterinnen.[44]

[42] Kommentar zur ZertDV s. 3
[43] Kommentar zur ZertDV, s. 2
[44] Kommentar zur ZertDV s.3

Die dreistufige hierarchische Struktur, auf der die Anerkennung der Anbieterinnen von Zertifizierungsdienste beruht, sieht wie folgt aus:



System ohne Wurzel-Instanz („root“)

Der Gesetzgeber hat sich für ein System ohne staatliche „Root“ entschieden.
Bezüglich dieses Themas ist eine heftige Auseinandersetzung entstanden. Im Entwurf wurde vorgeschlagen, dass das BAKOM die Funktion der Behörde für die Primärzertifizierung („Root“) von Anbieterinnen von Zertifizierungsdiensten im Zusammenhang mit der digitalen Signatur übernehmen sollte. In dieser Funktion hätte das BAKOM mit seiner eigenen digitalen Signatur den öffentlichen Schlüssel der anerkannten Anbieterinnen von Zertifizierungsdiensten zertifiziert. Diese wären somit Teil einer hierarchisch organisierten Kette der elektronischen Zertifizierung gewesen, wodurch sich die gegenseitige Zertifizierung („Cross Certification“) erübrigt hätte.[45]
Die Alternative dazu waren private Wurzel-Instanzen oder die direkte gegenseitige Anerkennung der Zertifizierungsanbieterinnen.
Die Befürworter einer obligatorischen staatlichen „Root“ waren unter anderem der Meinung, dass nur so eine gewisse Vertrauenswürdigkeit, Sicherheit, Transparenz und Vereinfachung des Systems, vor allem im Hinblick auf eine internationale Anerkennung, gewährleistet werden konnte. Die Gegner einer nationalen „Root“ argumentierten hingegen, dass dieses System zusätzliche Kosten, die natürlich die Benutzer schlussendlich tragen müssten, verursacht hätte. Im übrigen erklärten sie auch, dass nach dem Grundsatz der Subsidiarität und der Selbstregulierung der Staat diese Aufgabe den Privaten überlassen muss, wenn sie dieselbe Aufgabe wahrnehmen können. Hinzu besteht auch das Risiko, dass ein unberechtigter Zugang zum Schlüssel, mit welchem das BAKOM seine Zertifikate für die Zertifizierungsdiensteanbieterinnen erstellt, der gesamten Public Key Infrastructure schaden würde. Dazu kommt, dass eine nationale Lösung, wie es die staatliche „Root“ wäre, die internationale Einbindung der schweizerischen anerkannten Zertifizierungsstelle einschränken oder hemmen würde.[46]

[45] Erläutender Bericht zur E-PKIV, S. 3
[46] s. Anhörung der interessierten Kreise zur Verordnung über eine PKI in der Schweiz (PKIV), Zusammenfassung der Stellungnahmen, Bakom, September 1999, s. 3 ff.

Der Gesetzgeber hat die Argumente der Gegner für ein „Bundes-Root“ höher eingeschätzt und ein Hierarchiemodell eingeführt, aber ohne Einbezug einer Primärzertifizierung durch das BAKOM.

3.1.4 Anforderungen für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten

3.1.4.1 Generierung und Verwendung der kryptografischen Schlüssel

Aus Sicherheitsgründen sind Vorschriften zur Länge der kryptografischen Schlüssel und zu den zu verwendenden Algorithmenarten für die Generierung der kryptografischen Schlüssel notwendig. Diese Vorschriften zielen darauf, nur sichere digitale Signaturen in den Geltungsbereich der Verordnung fallen zu lassen und daher indirekt eine grössere rechtliche Anerkennung der digitalen Signaturen zu bewirken.[47]
Nach Art. 6 ZertDV sind diese Fragen in den vom BAKOM erlassenen Ausführungsvorschriften nach Art. 20 näher geregelt. Diese Ausführungsvorschriften sind zur Zeit noch nicht veröffentlicht worden. Sie werden in den Grundzügen, den in den Anhängen III und IV der europäischen Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen[48] (ESiG-RL) enthaltenen Anforderungen und Empfehlungen entsprechen.[49] Nach Art. 1 ESiG-RL soll die Richtlinie die Verwendung elektronischer Signaturen im europäischen Binnenmarkt erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist. Diese Richtlinie verlangt von den EU-Mitgliedstaaten bis zum 19. Juli 2001 entsprechende nationale Vorschriften. Anhang III enthaltet die Anforderungen für sichere Signaturerstellungseinheiten zur Gewährleistung der Funktionalität fortgeschrittener elektronischer Signaturen.[50] Nach Art. 2 Nr. 5 ESiG-RL sind Signaturerstellungseinheiten konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet werden. Nach Art. 2 Nr. 4 ESiG-

[47] Kommentar zur ZertDV, s 4
[48] Abl. 2000 L-13/12, in Kraft seit dem 19. Januar 2000
[49] Kommentar zur ZertDV, s 4
[50] ESiG-RL, Erwägungen
[32] J. Bizer /A. Miedbrodt, Die digitale Signatur im elektronischen Rechtsverkehr, in DETLEF KRÖGER/MARC A. GIMMY, Handbuch zum Internetrecht, Berlin 2000, s. 155

RL sind Signaturerstellungsdaten einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden. Sichere Signaturerstellungseinheiten erfüllen die Anforderungen des Anhangs III (Art. 2 Nr. 6 ESiG-RL) und müssen durch geeignete Technik und Verfahren gewährleisten, dass:

a) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal auftreten können;
b) ihre Geheimhaltung hinreichend gewährleistet ist;
c) die Signaturerstellungsdaten nicht errechnet werden können und vor einem Betrug sicher sind;
d) die Signaturerstellungseinheit für die Erstellung der Signatur durch den berechtigten Inhaber vor der Nutzung durch andere geschützt werden kann. Gefordert wird mit anderen Worten, dass der private Signaturschlüssel erst nach der Identifikation des Inhabers durch Besitz und Wissen angewendet und bei der Anwendung nicht freigegeben werden kann. [51]
e) die Signaturerstellungseinheiten die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass diese Daten dem Unterzeicher vor dem Signaturvorgang vorgelegt werden. Mit anderen Worten: Es muss gewährleistet sein, das die Daten, die signiert werden, die sind, die der Unterzeichner signieren wollte.[52]

Anhang IV betrifft die Anforderungen an die Signaturverifizierung. Während des Signaturprüfungsvorgangs ist mit hinreichender Sicherheit zu gewährleisten, dass:[53]

a) die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden;
b) die Signatur verlässlich verifiziert und das Ergebnis der Prüfung korrekt angezeigt wird;
c) der Überprüfer bei Bedarf den Inhalt der signierten Daten feststellen kann;
d) die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden;
e) die Identität des Signierenden bzw. die Verwendung eines Pseudonyms richtig angezeigt wird;
f) sicherheitstechnische Änderungen erkannt werden können.

[52] s. Bizer/Miedbrodt, S. 155
[53] s. ESigG-RL Anhang IV

Die sicherheitstechnischen Anforderungen bezüglich der Generierung und Verwendung der kryptografischen Schlüssel, die das BAKOM in den Ausführungsvorschriften erlassen wird, werden im Grunde genommen den obengenannten Bedingungen entsprechen. Da aber die Anhänge selber noch einen hohen Abstraktionsgrad aufweisen, werden die Ausführungsvorschriften noch detaillierter sein. Sie werden sich in der Tat nicht nur auf die Anhänge der europäischen Richtlinie beziehen, sondern vor allem auf die von CEN und EESSI veröffentlichten Ausführungsvorschriften.[54]
Nach Art. 6 ZertDV bezwecken diese die Gewährleistung eines der technischen Entwicklung entsprechenden hohen Sicherheitsniveaus, im Hinblick vor allem auf den vorhandenen europäischen technischen Standard.

3.1.4.2 Elektronische Zertifikate

Die Verordnung schreibt in Art. 7 ZertDV auch vor, welche Angaben ein elektronisches Zertifikat mindestens aufweisen muss:

- Seriennummer,
- mögliche Nutzungsbeschränkungen,
- Name des Inhabers des beglaubigten öffentlichen Schlüssels,
- den beglaubigten öffentlichen Schlüssel,
- die Gültigkeitsdauer,
- Name und digitale Signatur der Anbieterin des Zertifizierungsdienstes, die das Zertifikat ausgestellt hat.

Die Anforderungen entsprechen den in Anhang I enthaltenen Bedingungen der europäischen Richtlinien.[55]
Aus Gründen der Transparenz ist es besonders wichtig, dass das Zertifikat den Hinweis enthält, dass es in den Geltungsbereich der Verordnung fällt (Absatz 1 lit. b) und ob es sich beim Inhaber um eine natürliche Person, eine juristische Person, eine Verwaltungseinheit oder gegebenenfalls um ein Pseudonym handelt (Absatz 1 lit. d).[56] Nach Art. 2 lit. b können auch juristische Personen und Verwaltungseinheiten Inhaber eines eigenen Schlüsselpaars sein und somit ein Zertifikat bekommen. In der virtuellen Welt kann also auch eine juristische Person über ein eigenes Schlüsselpaar verfügen, das sich von jenem

[54] s. Anhang V: Kontaktnahme mit BAKOM, vom 28. August 2000
[55] s. Kommentar zur ZertDV s. 4
[56] Kommentar zur ZertDV s. 4

unterscheidet, welches die gewöhnlich in ihrem Namen handelnden natürlichen Personen verwenden. Somit ist die korrekte Verwendung des privaten Schlüssels ein Aspekt, der durch die juristische Person intern zu regeln ist. Die Gültigkeit ihrer Rechtsgeschäfte unterliegt jedoch den privatrechtlichen Vorschriften über die Stellvertretung von juristischen Personen.

Die Gültigkeit der Zertifikate ist zeitlich befristet, weil der mit dem Zertifikat bescheinigte Zustand sich seit der Ausstellung des Zertifikates hätte ändern können.[57] Aus diesem Grund muss die Gültigkeitsdauer auf dem Zertifikat angezeigt werden.

Bezüglich eventueller Nutzungsbeschränkungen muss darauf hingewiesen werden, dass in Zukunft digitale Zertifikate benutzt werden können, um ihre Inhaber für bestimmte Zwecke zu legitimieren (indem eine Berechtigung bescheinigt wird oder die Zugehörigkeit zu einer bestimmten Organisation).[58] Solche Zertifikate werden deshalb auch „Autorisierungs-Zertifikate“ genannt. Sie könnten z. B. eine Zugriffsberechtigung zu einem Computersystem bescheinigen oder eine Begrenzung des Wertes der Transaktionen begründen.

3.1.4.3 Anbieterinnen von Zertifizierungsdiensten

In Art. 4 und Abschnitt 3 ZertDV sind die Voraussetzungen und grundlegenden Anforderungen für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten durch die Anerkennungsstellen vorgeschrieben. Sie entsprechen Anhang II der europäischen Richtlinie.

a) Gemäss Art. 4 Abs. 1 lit. a ZertDV müssen die Anbieterinnen von Zertifizierungsdienste im Handelsregister eingetragen sein. Das hat zur Folge, dass auch die Regeln über den Konkurs und die kaufmännische Buchführung zur Anwendung kommen. Wenn die Anbieterinnen von Zertifizierungsdiensten keine Personen (natürliche oder juristische) sind, müssen sie Verwaltungseinheiten des Bundes, der Kantone oder der Gemeinden sein. Wie schon oben angedeutet, können also auch Verwaltungen Zertifizierungsdienste anbieten oder elektronische Zertifikate für den Eigengebrauch ausstellen.

b) Gemäss Art. 4 Abs. 1 lit. b müssen sie Personal mit den erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen.

[57] David Rosenthal, Projekt Internet, s. 249
[58] David Rosenthal, Projekt Internet, s.250

c) Gemäss Art. 4 Abs. 1 lit. c müssen sie zuverlässige Informatiksysteme und -produkte verwenden, die vor Veränderungen geschützt sind und die die technische und kryptographische Sicherheit der von ihnen unterstützten Verfahren gewährleisten.
d) Gemäss Art. 4 Abs. 1 lit. d müssen sie über ausreichende Finanzmittel und -garantien verfügen, um anerkannt zu werden.
e) Art. 4 Abs. 1 lit. f schreibt vor, dass Zertifizierungsstellen in ihren allgemeinen Geschäftsbedingungen sich verpflichten, für Schäden, die infolge eines fehlerhaften elektronischen Zertifikats oder wegen Missachtung von Publikationspflichten entstehen, auch gegenüber Dritten zu haften, sofern sie nicht nachweisen können, dass sie kein Verschulden trifft.
Da, wie schon oben erwähnt, die Verordnung sich auf keine solide Gesetzesgrundlage stützt, kann sie nur indirekt wirken. Die Haftungsfrage der Zertifizierungsstelle ist ein typischer Fall dieses Problems. Sie kann keine Haftung für Zertifizierungsdienste, die bei der Beglaubigung unsorgfältig arbeiten, direkt verordnen, sondern sie kann nur vorschreiben, dass Anbieter in ihren Geschäftsbedingungen eine solche Haftung gegenüber ihren Kunden und gegenüber Dritten, die auf ihre Zertifikate vertrauen, vorsehen müssen, wenn sie anerkannt werden wollen. Diese Haftungsvorschrift ist grundlegend, weil der Empfänger einer Signatur mit beiliegendem digitalem Zertifikat darauf vertrauen kann, dass die Identität des Inhabers von der Zertifizierungsstelle wirklich geprüft wurde. Diese Vorschrift vermeidet, dass ein Graben zwischen Sein und Soll entsteht.
Diese Vorschrift ist eine der umstrittensten. Im wesentlichen wird befürchtet, dass die Haftung für die Zertifizierungsstelle zu weit gehe und diese folglich davon abhalte, sich freiwillig anerkennen zu lassen. Laut anderen ist hingegen gerade zu verhindern, dass die Zertifizierungsstellen ihre Haftung zum Nachteil ihrer Kunden und Dritten weitgehend ausschliessen könnte.[59]
Bezüglich einer Haftungsvorschrift muss eine Abwägung getroffen werden. Die Verantwortlichkeit und die Haftung der Zertifizierungsstellen entscheiden über die Bereitschaft zur Investition und zur Nutzung. Einerseits muss ein ideales Investitionsklima für die Anbieter digitaler Signaturen geschaffen werden, andererseits muss das Vertrauen der Verbraucher für digitale Signaturen gestärkt werden.[60] Das deutsche Signaturgesetz mit der Signaturverordnung und den Massnahmenkatalogen baut die Förderung des Vertrauens

[59] Zusammenfassung der Stellungnahmen, Anhörung der interessierten Kreise über PKIV, s. 13
[60] Ivo Geis, Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen, CR 12/1999

auf einen hohen (und damit auch teuren) Sicherheitsstandard. Die Vorschriften sind aber derart streng, dass nur mittels eines immens grossen finanziellen Aufwandes, geschätzt auf mindestens 750 000 DM, der Aufbau derartiger Zertifizierungsstellen möglich wird und dass dies viele Institutionen vom Aufbau neuer Zertifizierungsstellen abhalten wird.[61] Die Haftung der nach § 4 des Signaturgesetzes genehmigten Zertifizierungsstellen für digitale Signaturen ist im Gesetz nicht geregelt und richtet sich daher nach dem allgemeinen Haftungsrecht.[62]

Die Europäische Richtlinie setzt demgegenüber in Anlage II deutlich niedrigere Hürden für den Betrieb einer Zertifizierungsstelle. Die Sicherheit soll hier im wesentlichen durch strenge Haftungsregelungen erreicht werden, und diese Regelungen sind daher trotz geringerer Regulierungsdichte in der Lage, Vertrauen in die Sicherheit der Zertifizierungsstellen zu geben, da der Schaden, der durch eine Pflichtverletzung der Zertifizierungsstellen entstanden ist, ohne Verschuldensprüfung zu erstatten ist.[63]

Im Hinblick auf die europäische Entwicklung und vor allem im Hinblick auf das Verfahren zur Anerkennung von Zertifizierungsstellen ausserhalb der EU konnte eine Regelung der Beweislast in Form einer Kausalhaftung (Haftung ohne Verschulden) mit Entlastungsmöglichkeit in die Verordnung integriert werden. So werden Zertifikate von ausländischen Zertifizierungsstellen von der EU nur anerkannt, wenn diese innerhalb der EU die Haftung für Schäden aus diesen Zertifikaten übernehmen.[64]

Es handelt sich, wie schon oben angedeutet, um eine Kausalhaftung mit Entlastungsmöglichkeit. Eine solche Haftung kommt aber ökonomisch analysiert einer Verschuldenshaftung gleich. Man konnte sich wegen der auf keine solide Grundlage gestützten Zertifizierungsdiensteverordnung nicht zu weit von den allgemeinen Regeln des OR entfernen. Unterschiedlich ist nur die Beweislast: Nach Art. 4 Abs. 1 lit. f muss die Zertifizierungsstelle nachweisen, dass sie kein Verschulden trifft.

Ohne dieser Kausalhaftung hätte man ganz verschiedene „Haftungkonstellationen“ gehabt. Es müsste zwischen Haftung gegenüber den eigenen Kunden, für die die Zertifizierungsstellen ihre Zertifikate ausstellen, und gegenüber den Dritten, denen die Zertifikate vorgewiesen werden und die ihnen vertrauen, unterschieden werden. Im ersten Fall hätte es sich um eine Haftung aus Vertrag gehandelt. Der Vertrag zwischen dem Kunden und der Zertifizierungsstelle umfasst normalerweise das Erstellen des Zertifikats

[61] Ulrich Emmert, Haftung der Zertifizierungsstellen, CR 4/1999. S. 249
[62] FN 42 s. 245
[63] FN 42 s. 249
[64] FN 41 s. 249

mit oder ohne Nachforschungsbedarf, eventuell auch das Erstellen des geheimen Schlüssels sowie das Verfügbarmachen des Zertifikats im Verzeichnisdienst.

Eine Haftung der Zertifizierungsstelle hätte von der Art der erbrachten Dienste abgehangen.

Im zweiten Fall handelt es sich hingegen um eine ausservertragliche Haftung. Der Geschädigte dritte hätte nach Art. 41 OR gegen die Zertifizierungsstelle vorgehen müssen. Er hätte das widerrechtliche Verhalten der Zertifizierungsstelle, den Kausalzusammenhang zwischen dem Schaden und dem unrechtmässigen Verhalten der Zertifizierungsstelle sowie deren Verschulden nachweisen müssen. Das wäre unter Umständen eine sehr schwierige und aufwendige Aufgabe gewesen. Mit Art. 4 Abs. 1 lit. f muss aber jetzt die Zertifizierungsstelle nachweisen, dass sie kein Verschulden trifft. Ihr Verschulden ist also vermutet, und die lästige Aufgabe des Verschuldensnachweises oder besser des Unschuldnachweises ist die Zertifizierungsstelle abgewälzt.

Eine Haftung kann sich aus folgenden Pflichtverletzungen einer Zertifizierungsstelle ergeben:

- Falschangaben im Zertifikat,
- Falschangaben im Verzeichnis,
- Preisgabe der Identität bei Pseudonym,
- Speicherung des privaten Schlüssels,
- fehlende Veröffentlichung im Verzeichnis,
- verspätete/unterbliebene Sperrung,
- fehlende Erreichbarkeit,
- fehlende Betragsbeschränkung.[65]

Es kann aber keine Haftung begründet werden, wenn die Zertifizierungsstelle kein Verschulden trifft, d. h. z. B., dass die Zertifizierungsstelle nicht für Falschangaben des Teilnehmers haftet, wenn sie sich in zumutbarer Weise von der Richtigkeit der Angaben überzeugt hat.

Anbieterinnen von Zertifizierungsdiensten können aber die Identifizierung der Antragsteller oder andere Aufgaben an Dritte delegieren (Outsourcing), beispielsweise an Poststellen oder Bankfilialen. Für die korrekte Ausführung dieser Aufgaben durch Dritte haftet jedoch allein die anerkannte Anbieterin von Zertifizierungsdiensten, insbesondere gegenüber der akkreditierten Zertifizierungsstelle, welche sie anerkannt hat und die für ihre

[65] Ulrich Emmert, Haftung der Zertifizierungsstellen, CR 4/1999 s. 245

Aufsicht zuständig ist (vgl. Artikel 17). Auf privatrechtlicher Ebene gelangt Artikel 101 OR (Haftung für Hilfspersonen) zur Anwendung.[66]

g) Ohne haftendes Kapital ist aber eine Haftungsregelung nichts wert. Es muss entweder ein Mindestkapital oder eine Versicherungspflicht der Zertifizierungsstelle für Haftungsfälle eingeführt werden. So schreibt Art. 4 Abs. 1 lit. e vor, dass sie die notwendigen Versicherungen zur Deckung allfälliger Haftungsansprüche abschliessen muss. Die obligatorischen Versicherungen dienen auch zur Deckung der Kosten, welche durch die Massnahmen aus freiwilliger oder erzwungener Einstellung der Tätigkeit erwachsen könnten (Art. 4 Abs. 1 lit. e).

h) Art. 8 Abs. 1 schreibt vor, dass die Person, die einen Antrag auf Ausstellung eines elektronischen Zertifikates stellt, um ihre Identität nachzuweisen, sie bei der Zertifizierungsstelle oder bei einer ihrer Registrierungsstellen persönlich erscheinen und sich dort ausweisen muss. Wenn es um den Nachweis der Identität einer natürlichen Person geht, muss sie nach lit. a Identitätskarte oder Pass vorweisen.

Wenn es um den Nachweis der Vertretungsmacht einer Verwaltungseinheit geht, müssen nach lit. b die Vollmacht und die Identitätskarte oder der Pass der Personen, die für Verwaltungseinheiten handeln, vorgewiesen werden.

Der Handelsregisterauszug und die Identitätskarte oder der Pass der Handlungsbevollmächtigten müssen nach lit. c bei juristischen Personen vorgewiesen werden.

Dies ist eine sehr wichtige Bedingung für die Erlangung der Anerkennung, weil die wesentliche Tätigkeit der CA genau die Bestätigung der Zuordnung einer bestimmten Person zu einem öffentlichen Schlüssel ist. Und dies kann nur mit Sicherheit bestätigt werden, wenn man die genaue Identität der Person kennt.

Wie schon unter Punkt 2.4.2 erwähnt, können Zertifizierungsstellen unter unterschiedlichen Bedingungen Zertifikate ausstellen. Die US-Firma Verisign bietet eine vierstufige Zertifizierung an. Auf der untersten Stufe (Class 1) wird lediglich bescheinigt, dass die Zertifizierungsstelle niemand anderen mit derselben E-Mail-Adresse und demselben Namen registriert hat. Auf der teuersten Stufe (Class 4) nimmt Verisign zusätzlich zum persönlichen Erscheinen bei Verisign und zum Vorweisen von offiziellen Ausweisdokumenten umfangreichere Abklärungen über die Unbescholtenheit und Kreditwürdigkeit der Person vor.[67] Nach der Zertifizierungsdiensteverordnung sind die

[66] Kommentar ZertDV s. 5
[67] David Rosenthal, Projekt Internet, s. 248

Mindestanforderungen das persönliche Erscheinen und das Vorweisen von Identitätsdokumenten.

Allerdings wird das persönliche Erscheinen nicht bei jeder Erneuerung des elektronischen Zertifikats verlangt. Liegt die formelle Identifizierung (durch persönliches Erscheinen) nicht länger als zehn Jahre zurück, so muss lediglich ein elektronischer Antrag gestellt werden, der mit einer digitalen Signatur versehen ist, welche bereits früher zertifiziert wurde (Art. 8 Abs. 2).[68]

Art. 8 Abs. 3 sieht die Möglichkeit vor, anstelle des Namens des Inhabers des beglaubigten öffentlichen Schlüssels ein Pseudonym aufzuführen. Dies kann die Anonymität der Personen, die dies wünschen, gewährleisten. Damit wird aber die Zertifizierungsstelle nicht davon befreit, die betreffende Person korrekt zu identifizieren.

i) Nach Art. 9 Abs. 1 ZertDV müssen die anerkannten Anbieterinnen von Zertifizierungsdiensten aus Transparenzgründen ihre allgemeinen Vertragsbedingungen (AGB) und ihre Zertifizierungspolitiksregeln publizieren.

k) Nach Art. 9 Abs. 2 ZertDV müssen sie ihre Kunden spätestens bei der Ausstellung der elektronischen Zertifikate auf die Folgen eines möglichen Missbrauchs oder Verlusts des privaten Schlüssels aufmerksam machen. Und sie müssen ihnen geeignete Massnahmen zur Geheimhaltung des privaten Schlüssels vorschlagen.

Wer die Chipkarte mit dem privaten Signaturschlüssel und dem dazugehörigen PIN einer Person besitzt, kann im Namen dieser Person Rechtsgeschäfte tätigen oder ihr Konto ausrauben. Deshalb muss man den privaten Schlüssel vor Missbrauch oder Verlust schützen. Die Chipkarte mit dem privaten Signaturschlüssel muss in persönlichem Gewahrsam gehalten werden. Das Signaturschlüssel-Zertifikat muss sofort gesperrt werden, wenn die Chipkarte verlorengeht oder in die Hände Unbefugter gelangt. Die Chipkarte muss zur Vernichtung übergegeben werden, wenn man sie nicht mehr benötigt, und das Signaturschlüssel-Zertifikat muss gesperrt werden, sofern es nicht bereits abgelaufen ist. Der PIN-Code muss geheimgehalten, und abgeändert werden, wenn er Unbefugten bekannt wird. Zur zusätzlicher Sicherheit kann man die technischen Komponenten zum Erzeugen digitaler Signaturen (die Chipkarte, die den privaten Schlüssel und eine Software zum Erzeugen der digitalen Signaturen enthält) mit einer zusätzlichen Identifikation durch biometrische Merkmale benutzen.[69] So können z. B. Referenzdaten über die Fingerstrukturen einer Person auf der Chipkarte mit dem privaten

[68] Kommentar ZertDV s.
[69] Bieser Wendelin, Elektronisch unterschreiben, Heidelberg, 1999, s. 56

Signaturschlüssel gespeichert werden. Der Signaturschlüssel wird dann erst nach einem Vergleich der Fingerstrukturen mit den gespeicherten Referenzwerten zur Anwendung freigegeben.[70]

l) Nach Art. 10 ZertDV dürfen die anerkannten Anbieterinnen von Zertifizierungsdiensten keine Kopien der privaten Schlüssel ihrer Kunden anfertigen und aufbewahren. Sie können die kryptographischen Schlüssel für ihre Kunden generieren, aber diese weder speichern noch kopieren. Diese Vorschrift dient auch der Sicherheit, dass eine Kopie des Geheimschlüssels nicht in die Hände eines Dritten fällt.

m) Für die Vertrauenswürdigkeit des elektronischen Geschäftsverkehrs ist es wesentlich, dass nur die Zertifikate benutzt werden, denen Rechtswirkung zukommt. Falls der geheime Schlüssel innerhalb des Gültigkeitsrahmens verlorengeht oder in die Hände Unbefugter gerät, muss das Zertifikat für ungültig erklärt werden. Die Ungültigerklärung eines elektronischen Zertifikats hat eine Ex-nunc-Wirkung. Sie stellt also die Verbindlichkeit der zwischen dem Zeitpunkt der Zertifikatsausstellung und dem Zeitpunkt von dessen Ungültigerklärung abgewickelten Geschäfte nicht in Frage. Deshalb muss die Ungültigerklärung immer unverzüglich veröffentlicht werden.[71]

In diesem Fall stammt der Antrag auf Ungültigerklärung vom Kunden selbst (Art. 11 Abs. 1 ZertDV). Die Zertifizierungsstellen müssen sich versichern, dass die Person, welche die Ungültigerklärung verlangt, dazu berechtigt ist. Diese Anforderung gilt nach Abs. 2 als erfüllt, wenn der Antrag mit der anhand des privaten Schlüssels erzeugten digitalen Signatur versehen ist, der dem öffentlichen Schlüssel zugeordnet werden kann, dessen Zertifikat für ungültig erklärt werden soll.

Es kann aber auch vorkommen, dass das Zertifikat gegen den Willen des Benutzers durch die Anbieterin von Zertifizierungsdiensten für ungültig erklärt wird. Nach Abs. 3 sind die anerkannten Anbieterinnen von Zertifizierungsdiensten verpflichtet, die von ihnen ausgestellten elektronischen Zertifikate unverzüglich für ungültig zu erklären, wenn sich herausstellt, dass diese unrechtmässig erlangt wurden oder falsche Angaben enthalten, welche die sichere Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Person gefährden.

Die Verordnung bietet den Zertifizierungsstellen auch die Möglichkeit, eine maximal drei Tage dauernde Suspendierung eines Zertifikats anzuordnen (Abs. 4). So kann die Rechtmässigkeit des Antrags auf eine Ungültigerklärung geprüft werden. Gleiches gilt im

[70] Beiser Wendelin, Elektronisch nterschreiben
[71] Kommentar ZertDV, s. 5

Fall einer automatischen Ungültigerklärung eines Zertifikats. Das Zertifikat wird nach einer dreitägigen Suspendierung wieder für gültig oder aber definitiv für ungültig erklärt. Im ersten Fall hat die Suspendierung keine Wirkung auf die Gültigkeit des Zertifikats. Im zweiten Fall wird die Ungültigerklärung zum Zeitpunkt der Suspendierung des Zertifikats wirksam.

n) Nach Art. 12 Abs. 1 müssen die anerkannten Anbieterinnen von Zertifizierungsdiensten ein Verzeichnis erstellen der von ihnen ausgestellten elektronischen Zertifikate, in das die Kunden ihre elektronischen Zertifikate eintragen lassen können. Die Kunden sind also nicht verpflichtet, ihre elektronischen Zertifikate in das Verzeichnis eintragen zu lassen.

Die Zertifizierungsstellen publizieren die von ihnen ausgestellten Zertifikate entweder selbst über ein Verzeichnis, das die Zertifizierungsstelle unterhält (z. B. auf ihren Web-Sites), oder übertragen die Aufgabe einem Dritten, der sie in einer Datenbank zum Abruf für jedermann bereithält, oder händigen sie den bescheinigten Personen zum Verteilen an ihre Geschäftspartner aus. Im letzteren Fall wird das Zertifikat an die Nachricht angehängt.

Die Zertifizierungsdiensteverordnung verpflichtet also die Anbieterinnen von Zertifizierungsdiensten, ein Verzeichnis zu führen, und überlässt den Inhabern des elektronischen Zertifikates die Wahl der Eintragung in das online abrufbare Verzeichnis.

Nach Absatz 2 sind sie auch verpflichtet, eine Liste aller für ungültig erklärten oder suspendierten Zertifikate zu führen, auch wenn diese nicht im Verzeichnis eingetragen worden sind. Diese Liste soll ausschliesslich die Seriennummer des elektronischen Zertifikats, den Hinweis auf die Ungültigerklärung oder Suspendierung sowie das Datum und die Uhrzeit der Ungültigerklärung oder Suspendierung enthalten. Sie muss durch die digitale Signatur der anerkannten Anbieterin von Zertifizierungsdiensten authentifiziert werden.

Nach Absatz 3 muss der Zugang zu den Verzeichnissen (der gültigen Zertifikate und der für ungültig erklärten oder suspendierten Zertifikate) jederzeit und ohne zusätzliche Kosten neben jenen für die Nutzung der öffentlichen Telekommunikationsmittel möglich sein.

o) Nach Art. 13 Abs. 1 ZertDV müssen die anerkannten Anbieterinnen von Zertifizierungsdiensten die abgelaufenen oder für ungültig erklärten elektronischen Zertifikate sowie die Listen der für ungültig erklärten Zertifikate aufbewahren und die Einsicht in Zertifikate und die Listen während mindestens elf Jahren nach Ablauf oder Ungültigerklärung der Zertifikate gewährleisten. Es kann passieren, dass die Abgabe von Willenserklärungen in elektronischer Form während der Gültigkeitsdauer des Zertifikats nach mehreren Jahren nachgewiesen werden muss. Nur die Anforderung nach Art. 13

ZertDV können dies gewährleisten. Die Frist von 11 Jahren entspricht der allgemeinen Verjährungsfrist von Artikel 127 des OR und der in Artikel 962 Abs. 1 OR vorgesehenen Frist zur Aufbewahrung der Geschäftsbücher (10 Jahre) unter Berücksichtigung der Berechnungsmethode gemäss Artikel 962 Abs. 3 OR (bzw. Artikel 962 Abs. 2 OR gemäss der von der Bundesversammlung am 22. Dezember 1999 verabschiedeten Änderung, BBl 2000 61).[72]

Nach Art. 13 Abs. 2 ist die Einsicht in Zertifikate und in die Listen während der ersten sechs Jahre jederzeit und ohne andere Kosten als denjenigen für die Nutzung der öffentlichen Telekommunikationsmitteln online zu gewährleisten.

Die Frist von sechs Jahren entspricht einem allgemeinen Bedürfnis und berücksichtigt insbesondere Artikel 40 Abs. 1 und Artikel 41 Abs. 1 der Verordnung vom 22. Juni 1994 über die Mehrwertsteuer (SR 641.201) sowie Artikel 49 Abs. 1 und Artikel 50 Abs. 1 der zukünftigen MWStG (BBl 1999 6752).[73]

p) Nach Art. 14 ZertDV müssen die anerkannten Zertifizierungsstellen ihre Aktivitäten im Zusammenhang mit der Ausstellung, der Ungültigerklärung und der Suspendierung der elektronischen Zertifikate in einem Tätigkeitsjournal vermerken. Diese Vorschrift steht im Zusammenhang mit der Aufsicht nach Art. 17 ZertDV, die die Anerkennungsstellen über die Zertifizierungsstellen ausüben. In der Tat ist die Aufsicht dank einem Tätigkeitsjournal erheblich erleichtert. Dazu soll ihnen ein Tätigkeitsjournal die Erbringung des Beweises, dass sie ihrer Identifizierungspflicht nachgekommen sind, in einem Gerichtsverfahren ermöglichen.

q) Art. 15 ZertDV schreibt das Verfahren bei Einstellung der Geschäftstätigkeit vor.

Nach Abs. 1 müssen die Zertifizierungsstellen die Einstellung der Tätigkeit 30 Tage im voraus der SAS melden. Eine gegen sie gerichtete Konkursandrohung ist hingegen unverzüglich anzumelden.

Bei freiwilliger Einstellung der Geschäftstätigkeit sind nach Abs. 2 die anerkannten Zertifizierungsstellen verpflichtet, die von ihnen ausgestellten, noch gültigen elektronischen Zertifikate für ungültig zu erklären. Die SAS beauftragt dann eine andere anerkannte Zertifizierungsstelle, die Liste der für ungültig erklärten Zertifikate zu führen und die abgelaufenen oder für ungültig erklärten Zertifikate, das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren.

[72] Kommentar ZertDV s. 6
[73] Kommentar ZertDV s. 6

Bei konkursbedingter Einstellung der Geschäftstätigkeit oder bei Entzug der Anerkennung einer Zertifizierungsstelle verläuft das Verfahren ein bisschen anders. Nach Abs. 3 beauftragt die SAS eine andere anerkannte Zertifizierungsstelle, die von jener ausgestellten, noch gültigen elektronischen Zertifikate für ungültig zu erklären (bei freiwilliger Einstellung konnte das noch von den einstellungswilligen Zertifizierungsstellen selber vorgenommen werden), die Liste der für ungültig erklärten Zertifikate zu führen und die abgelaufenen oder für ungültig erklärten Zertifikate, das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren.
Unterschiedlich ist also nur die Zuständigkeit bezüglich der Ungültigerklärung der noch nicht abgelaufenen Zertifikate.
Die Kosten, die der beauftragten Zertifizierungsstelle, der SAS und eventuell der Anerkennungstelle entstehen, sind durch die Versicherungen, die die Zertifizierungsstellen nach Art. 4 Abs. 1 lit. e abzuschliessen verpflichtet sind, gedeckt.
r) Nach Art. 16 ZertDV dürfen die Anbieterinnen von Zertifizierungsdiensten nur diejenigen Personendaten erheben und weiterbearbeiten, die zur Erfüllung ihrer Aufgaben notwendig sind. Art. 16 will also den Schutz der Personendaten der Kunden gewährleisten. Mit dieser Bestimmung soll der Zweck der Erhebung und Bearbeitung der Personendaten durch die Anbieterinnen von Zertifizierungsdiensten klar festgelegt werden.[74] Im übrigen gilt die Datenschutzgesetzgebung.

3.1.5 Die Aufsicht

Nach Art. 17 Abs. 1 ZertDV müssen die Anerkennungsstellen nach den Regeln des Akkreditierungsrechts die anerkannten Anbieterinnen von Zertifizierungsdiensten beaufsichtigen und kontrollieren, dass sie die Voraussetzungen für die Anerkennung und die grundlegenden Anforderungen erfüllen.
Nach Art. 17 Abs. 2 ZertDV kann die Anerkennungsstelle den Anbieterinnen von Zertifizierungsdiensten die Anerkennung entziehen, wenn sie die grundlegenden Anforderungen nicht erfüllen oder ihre Pflichten verletzen. Der Entzug muss unverzüglich der SAS angemeldet werden. Die Regeln nach Art. 15 Abs. 3 kommen dann zur Anwendung.

3.1.6 Die Anerkennung der ausländischen Anbieterinnen von Zertifizierungsstellen

Nach Art. 14 FHG kann der Bundesrat internationale Abkommen zur Anerkennung ausländischer Anbieterinnen von Zertifizierungsdiensten schliessen, welche ein den Bestimmungen der Verordnung entsprechendes Sicherheitsniveau aufweisen.[75]
Nach Art. 18 ZertDV stellt die SAS der Öffentlichkeit die Liste der ausländischen Anbieterinnen von Zertifizierungsdiensten zur Verfügung.
Fraglich ist, ob Art. 14 FHG eine ausreichende gesetzliche Grundlage für den Abschluss von internationalen Abkommen zur Anerkennung ausländischer Zertifizierungsstellen durch den Bundesrat ist.

3.1.7 Bestätigung der Konformität einer digitalen Signatur mit dieser Verordnung

In einem Gerichtsverfahren gilt der Grundsatz der freien richterlichen Beweiswürdigung. Mit der Gleichstellung des digital signierten Dokuments mit der schriftlichen Urkunde würde sich nichts ändern. Erstens, weil die schriftlichen Urkunden kein besonderes Privileg geniessen, zweitens, weil das Problem, wie digital signierte Dokumente vor Gericht vorgelegt werden können, weiter besteht.
Braucht es ein Sachverständigengutachten? Oder müsste mittelfristig das Gericht über die Infrastruktur zur Beurteilung des elektronischen Dokuments verfügen?
Sinnvoll ist aber, dass es Instanzen zur Beglaubigung digital signierter Dokumente gibt. Eine solche Stelle könnte im Konfliktfall rasch und mit wenig Aufwand und Kosten ein Papierdokument ausstellen, das Inhalt, Unterzeichnende und Entstehungszeitpunkt des digital signierten Dokuments beglaubigt.[76]
Mit Art. 19 ZertDV wurde die sinnvollste Lösung getroffen. Als zuständige Stelle wurde die SAS eingesetzt. Nach Art. 19 ZertDV würde die SAS gegen Gebühr bestätigen, dass die auf einem elektronischen Dokument vorhandene digitale Signatur erstens mit Hilfe des privaten Schlüssels angebracht wurde, der einem öffentlichen Schlüssel zugeordnet werden kann, für den zweitens ein anerkannter Anbieter ein elektronisches Zertifikat ausgestellt hat, und dass drittens dieses Zertifikat zu einem bestimmten Zeitpunkt gültig war.

---

[74] Kommentar ZertDV s. 6
[75] Kommentar ZertDV, s. 7
[76] Urs Bürge: Digitale Signatur und Recht – Voraussetzung, Stand und Aussichten der rechtlichen Anerkennung in der Schweiz, in: Die Volkswirschaft – Magazin für WirtschaftsPolitik, 6.99 Bern, 1999

Die Bestätigung bezieht sich auf die Gültigkeit eines elektronischen Zertifikats zu einem bestimmten Zeitpunkt, garantiert aber nicht, dass dieses zu einem bestimmten Zeitpunkt übermittelt wurde, ausser es würde ein vertrauenswürdiger Zeitstempel angebracht (time stamping).[77] Solche digitalen Zeitangaben werden zurzeit jedoch noch nicht eingesetzt, weil technische Standards fehlen,[78] aber ihre Bedeutung wird in den nächsten Jahren sicher stark zunehmen. In bestimmten Ländern (z. B. Deutschland) soll ihr Einsatz in gewissen Fällen sogar gesetzlich vorgeschrieben werden, um den Zeitpunkt festzustellen, zu dem ein rechtsverbindliches Dokument digital unterzeichnet wurde.

3.1.8 Fazit

Diese Verordnung ist auf jeden Fall zu begrüssen. Sie baut die Einrichtung auf, die für den Electronic Commerce notwendig ist. Die Verordnung lehnt sich in ihren Grundzügen an das Signaturgesetz Deutschlands. Das Resultat dieser Verordnung besteht aber nur in einer vertrauensbildenden und anregenden Wirkung und nicht in einer Rechtswirkung.[79] Sie fördert die Diskussion über ein in der Schweiz sehr vernachlässigtes Thema. Man kann sicher nicht sagen, dass der entscheidendste und wichtigste Schritt bereits gemacht wurde.
Dies ist besser als nichts, aber der Mangel an Ausführungsvorschriften, die die wichtigen und heiklen Details regeln und Anhaltspunkte an die Zertifizierungsstellen für ihre Tätigkeit zur Verfügung stellen, verhindert die Sammlung von Erfahrungswerten. Die Sammlung von Erfahrungswerten ist wichtig, um konkrete Hinweise zu haben und um Lösungen für künftige problemgerichtete Rechtsvorschriften zu entwickeln.
Mit einer Verordnung ohne Ausführungsvorschriften wurde also nicht viel geleistet.
Auch die Tatsache, dass die Verordnung als eine Versuchsregelung zu betrachten ist, ist unbefriedigend. Wir haben mit einer Versuchsregelung zu tun, die beinahe nichts oder höchstens etwas indirekt regelt, aber vieles regeln möchte. Eine derartige lückenhafte Regelung birgt das Risiko in sich, dass sich jede durch der Verordnung benachteiligte Partei auf die Nichtanwendbarkeit der ZertDV mangels gesetzlicher Rechtsgrundlage berufen kann.

[77] Kommentar ZertDV s. 7
[78] Thomas Legler: Digitale Signaturen fördern den E-Commerce – Bundesrätliche Verordnung schafft eine rechtliche Grundlage, NZZ, 20.4.2000
[79] s. David Rosenthal, Stellungnahme zum Entwurf einer “Public Key Infrastruktur Verordnung” (PKIV-E) vom 3. Juni 1999

Man kann sich die Frage stellen, warum plötzlich innerhalb von fünf Monaten eine solide Grundlage für ein Bundesgesetz über digitale Signatur gefunden wurde. Warum stand sie nicht schon für die sogenannte Versuchsregelung zur Verfügung? Wurde die Verordnung über Dienste der elektronischen Zertifizierung unsonst gemacht?
Wurde ein solcher Weg vielleicht aus politischen Gründen gewählt? Ziel dieser ohne solide Gesetzesgrundlage, als Versuchsregelung erlassenen Verordnung war eine kurzfristig zur Verfügung gestellte Regelung, die mindestens eine sichere und vertrauenswürdige Public Key Infrastructure aufgebaut hätte. Den nachfolgenden Schritt (die Regelung der Rechtswirkung der digitalen Signatur) hätte man dann ohne Eile vorgenommen. Aber eine auch kurzfristig, ohne Ausführungsvorschriften zur Verfügung gestellte Verordnung wird den Anforderungen der Wirtschaft nicht gerecht und kann ihre Anliegen nicht erfüllen.
Es ist zu hoffen, dass mit dem Bundesgesetz über die elektronische Signatur nunmehr eine systematisch anwendbare und umfassende rechtliche Regelung realisiert wird. Infolgedessen wird sich die Verordnung auf eine sichere gesetzliche Grundlage stützen und der digitalen Signatur eine ähnliche Wirkung wie der eigenhändigen Unterschrift verleihen. Zu hoffen ist aber auch, dass die normative Arbeit sich nicht auf das Obengenannte beschränken wird. Wünschenswert sind auch Regelungen im Vertragsrecht allgemein, im Zwangsvollstreckungsrecht, im Prozessrecht, im Verwaltungsrecht, im Registerrecht und in der kaufmännischen Buchführung.

3.2 Die geplante Vorlage

Nach Kontaktnahme mit dem Verantwortlichen für das Projekt E-Commerce beim Eidgenössischen Justiz- und Polizeidepartement (EJPD), Herrn Felix Schöbi, habe ich die wichtigsten Bestandteile der geplanten Vorlage, über der das Vernehmlassungsverfahren im Herbst 2000 eröffnet wird, erfahren. [80]
Es ist geplant, ein eigenständiges Gesetz und verschiedene Revisionen von bestehenden Gesetzen in das Vernehmlassungsverfahren zu schicken.

3.2.1 Bundesgesetz über die elektronische Signatur

3.2.1.1 Bestand

Das Bundesgesetz über die elektronische Signatur wird wie folgt aussehen:
1. Im Vorentwurf betreffend das Bundesgesetz über die elektronische Signatur, über den das Vernehmlassungsverfahren im Herbst eröffnet wird, wird die am 1. Mai 2000 in Kraft getretene Zertifizierungsdiensteverordnung möglichst unverändert aufgenommen. Zum Bundesgesetz ist eine Vollziehungsverordnung geplant, die die obengenannten technischen Ausführungsvorschriften enthalten wird. Das Bundesgesetz stützt sich auf Art. 95 Abs. 1 und Art. 122 Abs. 1 BV.
2. Geändert wird nur die Vorschrift über die Haftung der Zertifizierungsstellen und des Inhabers eines privaten Schlüssels gegenüber einem Dritten, welcher auf den öffentlichen Schlüssel bzw. auf das Zertifikat vertraut hat.
3. Die Vorlage wird auch Bestimmungen über die elektronische Kommunikation mit Registern (Handelsregister und Grundbuch) enthalten. Noch nicht ausdiskutiert ist der Umfang des Projekts im Hinblick auf das sogenannte eGovernment.[81]

3.2.1.1.1 Anpassung der Vorschriften der Zertifizierungsdiensteverordnung

Der momentane Gesetzestitel lautet: „Bundesgesetz über die elektronische Signatur“. Da die Verordnung nur Regeln über die digitale Signatur aufweist, muss im Bundesgesetz terminologisch ein wenig Distanz gewonnen werden. Die vorgeschlagenen Bestimmungen werden ein bisschen mehr technologieneutral sein. Diese Anpassungen werden im besten Fall nichts schaden, dass d. h. sich in der Praxis nichts ändern würde; im schlimmsten Fall werden diese Anpassungen eine Verringerung der Qualitätsanforderungen an elektronische Signaturen zur Folge haben.[82]

---

[80] s. Anhang I: erste Kontaktnahme mit Felix Schöbi.
[81] s. Anhang I: Auskunft von Felix Schöbi Leiter des Projekt E-Commerce beim Eidgenössischen Bundesamt für Justiz und Polizei, der sich mit der Vorlage befasst hat.
[82] S. Anhang IV: III. Fragenfolge / Anhang V: Kontakt mit BAKOM

3.2.1.1.2 Änderung der Vorschrift über Haftung der Zertifizierungsstellen

Wie schon oben erwähnt, wird die Zertifizierungsverordnung möglichst unverändert in das Bundesgesetz eingegliedert. Die einzige Änderung wird die Haftung der Zertifizierungsdiensteanbieterinnen betreffen. Die heutige Norm, Art. 4 Abs. 1 lit. f ZertDV, schreibt vor, dass die Zertifizierungsdiensteanbieterinnen eine gewisse Haftung gegenüber ihren Kunden und gegenüber Dritten, die auf ihre Zertifikate vertrauen, zu übernehmen haben. Da die Verordnung auf wackligen Füssen steht, kann sie eine Haftung nur indirekt vorschreiben. Heute muss die Zertifizierungsstelle für Schäden einstehen, die infolge eines fehlerhaften elektronischen Zertifikats oder wegen Missachtung von Publikationspflichten entstehen, sofern sie nicht nachweist, dass sie kein Verschulden trifft. Es handelt sich um eine milde Kausalhaftung, die ökonomisch analysiert beinahe einer Verschuldenshaftung gleichkommt. Unterschiedlich ist nur die Beweislast.
Das EJPD schlägt immer noch eine Kausalhaftung vor, aber entscheidend für die Haftung der Zertifizierungssstelle wird einzig noch die **Widerrechtlichkeit** sein. Widerrechtlichkeit ist zu verstehen als Verstoss gegen das geplante Gesetz (über die elektronische Signatur) bzw. die dazu erlassene Verordnung. Fragen des Verschuldens werden keine Rolle spielen. Aufgabe des Geschädigten wird das Vorlegen des Beweises für die von ihm geltend gemachte Widerrechtlichkeit sein.[83] Der Geschädigte wird also von seiner Beweislast diesbezüglich nicht befreit. Das war hingegen bei der älteren Verordnung der Fall. Dieser Nachweis wird nicht immer einfach zu führen sein.

3.2.1.1.3 Bestimmungen über die elektronische Kommunikation mit Registern

Diese Bestimmungen zielen auf die Annahme von digital signierten Anmeldungen oder Belegen durch das Grundbuch und das Handelsregister. Elektronisch beglaubigte Auszüge, versehen mit der digitalen Signatur der Registerführer, werden die auf Papier erstellten Auszüge ersetzen. In einem ersten Schritt wird die gesetzliche Grundlage dafür geschaffen, die es dem Bundesrat in einem späteren Zeitpunkt erlaubt, die elektronische Kommunikation (auf der Basis elektronisch signierter Dokumente) zu gestatten. Vorausgesetzt wird natürlich, dass die Register selber informatisiert sind, und dies bedeutet kostspielige Investitionen. Die Beteiligten müssen auch vorerst die notwendige Übung im geschäftsmässigen Umgang mit elektronischen Kommunikationsformen gewinnen. Die

Einreichung von digital signierten Belegen oder Anmeldungen wird nur langfristig möglich sein.[84]

3.2.1.1.4 Exkurs: Die Vollziehungsverordnung

Nach Kontaktnahme mit den Verantwortlichen für das Projekt Zertifizierungsdienste-verordnung beim BAKOM habe ich den Inhalt der nächsten Schritte, die bezüglich den Ausführungsvorschriften vorgenommen werden, erfahren.[85]

Die Ausführungsvorschriften werden Ende des Jahres 2000 veröffentlicht. Dies so spät, weil man die schweizerischen Vorschriften mit denjenigen der EU und des CEN (Comité européen de normalisation) koordinieren wollte. In der Tat weist auch die europäische Richtlinie über Rahmenbedingungen für elektronische Signaturen einen hohen Abstraktionsgrad auf, und der EESSI (European Electronic Signature Standardization Initiative) und das CEN beschäftigen sich deswegen zur Zeit mit der Vorbereitung eines Entwurfes von Ausführungsvorschriften. Die schweizerischen Ausführungsvorschriften werden sich also an den veröffentlichten Arbeiten des CEN und der EESSI orientieren.

Die Ausführungsvorschriften zielen auf eine Präzisierung der folgenden in der Zertifizierungsdiensteverordnung enthaltenen Vorschriften:

- Voraussetzungen für die Anerkennung (Art. 4 ZertDV);
- Art und Umfang der Veröffentlichung der Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten sowie deren öffentlichen Schlüssel (Art. 5 ZertDV);
- Erzeugung und Prüfung der digitalen Signatur (Art. 6 ZertDV);
- Inhalt und Format der Zertifikate (Art. 7 ZertDV);
- Modalitäten betreffend die Führung der Verzeichnisse der elektronischen Zertifikate und der „Revocation List“ (Liste der für ungültig erklärten oder suspendierten Zertifikate) sowie deren Zugang (Art. 12 ZertDV).

[83] S. Anhang II:
[84] s. Anhang II
[85] s. Anhang V: Kontanahme mit BAKOM

3.2.2 Revision der bestehenden Gesetze

Die Revisionen werden die folgenden Gebiete betreffen:
1. Revision des Obligationenrechts, die zur Gleichstellung der elektronischen Signatur (im Sinne des obengenannten Bundesgesetzes) mit der eigenhändigen Unterschrift führen wird. Im Vorentwurf der Revision werden auch (am einschlägigen europäischen Recht orientierte) Bestimmungen über den Fernabsatz und den Fahrniskauf im Interesse des Konsumentenschutzes im Obligationenrecht aufgenommen;
2. Eine Revision des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) wird auch im Interesse des Konsumentenschutzes vorgeschlagen.

3.2.2.1 Revision des Obligationenrechts

3.2.2.1.1 Die Gleichstellung der elektronische Signatur mit der eigenhändigen Unterschrift

Nach schweizerischem Recht kommen Verträge grundsätzlich mündlich zustande. Für gewisse Verträge gibt es hingegen gesetzliche Formvorschriften.
Dies gilt beispielsweise für den Abzahlungskauf, einen sehr verbreiteten Vertrag des Konsumgeschäftes. Nebst den gesetzlich zwingenden minimalen Formvorschriften liegt es aber auch häufig im Interesse der Parteien, Verträge schriftlich abzuschliessen, obwohl sie theoretisch auch mündlich zustande kommen. Die Parteien machen dies aus Beweis- und/oder Schutzgründen.[86] Das Problem ist das folgende: Über das Thema E-Commerce haben viele Leute geschrieben, und viele Leute haben kleine Geschäfte über Internet abgeschlossen, aber sobald es sich um wichtigere Verträge handelt, werden diese nach wie vor in traditioneller Papierform festgehalten und eigenhändig unterschrieben. Die effektive und effiziente Nutzung des Internets für den E-Commerce ist somit gehemmt, und die Schriftlichkeit setzt dem E-Commerce enge Grenzen. Die Anerkennung der digitalen Signatur als rechtsverbindlicher Ersatz für eine eigenhändige Unterschrift ist die einzige Lösung.
Die Gleichstellung der digitalen Signatur mit der handschriftlichen Unterschrift wäre jedoch irreführend. Ein Papierdokument kann nicht digital signiert werden. Es ist nur eine

[86] Schriftliche Begründung zu Motion Leumann vom 16. Juni 1999, 99.3288, indirizzo Internet?

Gleichstellung von digital signierten Dokumenten mit eigenhändig unterschriebenen Papierdokumenten möglich.
In der Vorlage wird in der Tat ein **neuer Artikel 15a E-OR** vorgeschlagen, in dem festgehalten wird, dass die elektronische Signatur – in Frage kommt dafür nur ein elektronisches Dokument – rechtlich gleich zu bewerten ist wie die eigenhändige Unterschrift eines Papierdokuments.[87]

3.2.2.1.2 Neue Regelungen bezüglich empfangsbedürftiger Willenserklärungen?

Eine ganze Reihe von Fragen ist mit den empfangsbedürftigen Willenserklärungen verbunden. Die Frage, ob, wo und wann die Willenserklärung in den Bereich des Empfängers gekommen ist, hat einen materiell- und einen beweisrechtlichen Gehalt.[88]
Auf den materiellrechtlichen Aspekt wird der Entwurf erneut nicht eingehen. Es wird der Praxis überlassen, darüber zu befinden, wann eine Willenserklärung im elektronischen Geschäftsverkehr nach Treu und Glauben (Art. 2 Abs. 1 ZGB) als zugegangen bzw. zur Kenntnis genommen gelten kann.
Bezüglich der beweisrechtlichen Seite wird es in absehbarer Zeit so sein, dass der Erklärende vom Empfänger der Willenserklärung eine Eingangsbestätigung verlangt, um sicher zu sein, dass seine Willenserklärung angekommen ist. In gewissen Fällen sieht das europäische Recht sogar explizit eine Empfangsbestätigung vor. Art. 11 Abs. 1 der Richtlinie 2000/ /… des Europäischen Parlaments und des Rates vom 4. Mai 2000 über elektronischen Geschäftsverkehrs im Binnenmarkt[89] schreibt vor, dass der Dienstanbieter den Eingang der Bestellung durch einen Nutzer unverzüglich auf elektronischem Wege zu bestätigen hat. Vorbehalten sind natürlich abweichende Vereinbarungen zwischen Parteien, die nicht Verbraucher sind.
Würde zudem die Eingangsbestätigung elektronisch signiert, würde deren Empfänger von einer geplanten Beweislastumkehr profitieren (bezüglich Authentizität und Identität). So würde, wenn das Dokument digital signiert ist, die Vermutung bestehen, dass die Willenserklärung ohne Mängel und rechtsgültig angekommen ist, und bei einer gesetzlichen Vermutung findet eine Umkehrung der Beweislast statt, und es würde

[87] S. Anhang II: Interwiew an Felix Schöbi
[88] s. Anhang II: Interwiew mit Felix Schöbi
[89] Numero della Richtlinie, dove si trova, da rivedere! Abbreviazione E-Commerce-RL

demnach Aufgabe des Senders sein nachzuweisen, dass er die Eingangsbestätigung nicht geschickt und die Willenserklärung nie bekommen hat.
Ferner würde der Inhaber der elektronischen Signatur dafür haften, dass er seinen privaten Schlüssel einem Dritten zugänglich gemacht hat.
Die Forderung der Eingangsbestätigung ist eine vernünftige Lösung, es stellt sich einzig die Frage, was geschieht, wenn der Empfänger der Willenserklärung, trotz Empfang der Willenserklärung, böswillig keine Eingangsbestätigung sendet. Wie kann der Sender der Nachricht trotzdem die Sicherheit haben, dass der Empfänger sie bekommen hat?

3.2.2.1.3 Regelungen über den gültigen Verweis auf Allgemeine Geschäftsbedingungen (AGB)?

Ein anderes Problemfeld, das das Vertragsrecht betrifft, ist der gültige Verweis auf AGB. Wie kann man sicherstellen, dass eine bestimmte Version der AGB im Zeitpunkt des Vertrages vertrags- und rechtsverbindlich ist? Die Vorlage wird diesbezüglich keine Regel enthalten, sondern es wird der Praxis überlassen, die Frage zu beantworten, wann bzw. unter Beachtung welcher Voraussetzungen AGB gültig in einen Vertrag einbezogen werden.[90]

3.2.2.1.4 Bestimmungen betreffend den Konsumentenschutz

Wie schon in Kapitel 2.5.1.3 gesehen, kann eine pauschale Gleichstellung der digitalen Unterschrift mit der eigenhändigen Unterschrift Schutzbedürfnisse, wie Schutz der schwächeren Partei vor übereilten Vertragsabschlüssen, nicht abdecken. Wer etwas von Hand unterschreibt, ist oft vorsichtig. Eine digitale Signatur wird, weil mit einem Mausklick erzeugt, meist hemmungsloser ausgeführt.
Eine umfassende Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift ruft daher nach gesetzlichen Kompensationsmassnahmen, so beispielsweise einem Widerrufsrecht bei elektronisch geschlossenen Verträgen.[91]
Nach Leumanns Meinung[92] ist Internet ein neues Medium, mittels dessen Verträge abgeschlossen und zum Teil auch erfüllt werden können. Aus dieser Tatsache ergeben sich

[90] s. Anhang II: Interwiew mit Felix Schöbi
[91] Schriftliche Stellungnahme des Bundesrates vom 8. September 1999 zu Motion Leumann vom 16. Juni 1999

grundsätzlich keine neuen Regelungsbedürfnisse, wie zum Beispiel das Bedürfnis eines generellen Widerrufsrechtes, das bei Verträgen durch Verwendung von Telefon oder Fax auch nicht vorhanden ist. Nach Leumann ist ein erweiterter Kundenschutz, unabhängig von der Frage der Gleichsetzung der digitalen mit der eigenhändigen Unterschrift, auf politischer Ebene zu diskutieren; dies darf nicht dazu führen, dass das dringlich erforderliche Handeln noch weiter verzögert wird.

Der Bundesrat behauptet aber, dass bei Beschleunigung des Vertragsabschlusses und der Vertragsabwicklung im Zeitalter des elektronischen Handels der mit der Schriftlichkeit verfolgte Übereilungsschutz nur mit einem zeitlich befristeten Widerrufsrecht durch den Konsumenten gewährleistet werden kann.[93]

Ein solches Widerrufsrecht ist auf europäischer Ebene mit der Richtlinie über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz[94] bereits beschlossene und umgesetzte Sache, und die schweizerischen Bestimmungen werden sich an der sogenannten Fernabsatzrichtlinie orientieren. Spätestens auf den 5. Juni mussten die Mitgliedstaaten der EU die neuen Regeln in nationales Recht umsetzen. Die Regeln der Fernabsatzrichtlinie kommen nur zur Anwendung bei Verträgen, welche mittels gängiger Kommunikationsmittel angebahnt oder abgeschlossen werden. Darunter fallen Drucksachen mit oder ohne Anschrift, Briefe, Kataloge, Telefon, Telefax, Teleshopping und natürlich jede Form elektronisch übermittelter Informationen (z. B. elektronische Post). Ein wichtiger Anwendungsbereich ist also der E-Commerce.

Der Anwendung der Fernabsatzrichtlinie unterliegen auch nur Verträge zwischen Unternehmen und Konsumenten, nicht aber Verträge zwischen Unternehmen unter sich und Konsumenten unter sich.

Art. 6 Fernabsatzrichtlinie sieht ein Widerrufsrecht des Konsumenten vor, das als Herz der Richtlinie betrachtet werden kann.[95] Jedem Konsumenten steht ein voraussetzungsloses (ohne Angabe von Gründen und ohne Strafzahlung) Recht auf Widerruf während mindestens sieben Tagen zu. Die Frist zum Widerruf beginnt bei Dienstleistungen erst mit Erfüllung der Informationspflicht auf dem dauerhaften Datenträger, bei Warenlieferungen erst mit dem Empfang der Ware. Wird die Informationspflicht nicht oder nicht vollständig

[92] Antwort von Leumann zu schriftlicher Stellungnahme des Bundesrates vom 8. Sempterber 1999, 99.3288, indirizzo Internet?

[93] S. Antwort von Bundesrätin Ruth Metzler nach Aufforderung von Leumann bezüglich Motion Leumann, 99.3288

[94] Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz , Amtsblatt nr. L144 vom 04/06/1997 S.0019-0027

erfüllt, kann eine bis zu drei Monate gültige Widerrufsfrist eintreten. Das Widerrufsrecht erlischt spätestens drei Monate nachdem die Ware geliefert wurde (bei Warenlieferungen) oder drei Monate nach Vertragsabschluss (bei Dienstleistungen).[96] Bei erfolgtem Widerruf hat der Konsument die Ware zurückzusenden, und der Unternehmer hat die vom Verbraucher geleisteten Zahlungen innerhalb eines Monats nach Zugang der Widerrufserklärung zu leisten, andernfalls gerät er ohne weiteres in Verzug. Gemäss deutschem Fernabsatzgesetz trägt sogar der Unternehmer die Kosten für die Rücksendung der Ware wie auch die Gefahr des zufälligen Untergangs.[97]

Die obengenannte Informationspflicht bezieht sich auf die Unterrichtung des Konsumenten über die folgenden Informationen:

a) Identität und Adresse des Unternehmers;
b) Wesentliche Eigenschaften der Ware oder der Dienstleistung;
c) Preis der Ware oder der Dienstleistung einschliesslich aller Steuern;
d) Lieferkosten;
e) Einzelheiten hinsichtlich der Zahlung und der Lieferung oder Erfüllung;
f) Bestehen eines Widerrufsrechtes;
g) Kosten für den Einsatz der Fernkommunikationstechnik, sofern nicht nach dem Grundtarif berechnet;
h) Gültigkeitsdauer des Angebots oder des Preises;
i) Mindestlaufzeit des Vertrages über die Lieferung von Waren oder Erbringung von Dienstleistungen, wenn dieser eine dauernde oder regelmässig wiederkehrende Leistung zum Inhalt hat.

Nach Art. 4 Fernabsatzrichtlinie sind diese Informationen vor Vertragsabschluss auf klare und verständliche Weise auf jedwede der verwendeten Fernkommunikationstechnik angepasste Weise zu erteilen. Nach Art. 5 Fernabsatzrichtlinie müssen die Informationen a) bis f) rechtzeitig während der Erfüllung des Vertrages, bei nicht zur Lieferung an Dritte bestimmten Waren spätestens zum Zeitpunkt der Lieferung, schriftlich oder auf einem anderen für den Verbraucher verfügbaren dauerhaften Datenträger bestätigt werden.

Die Schweiz wird (nach verwaltungsinterner Auskunft) den europäischen Bestimmungen nicht blind folgen (es ist nicht gesagt, dass die Schweiz möglichst immer dieselben Rahmenbedingungen wie in der EU anstreben muss, sie kann auch bessere

[95] Urs Feller: Neue Regeln für den E-Commerce, NZZ 5./6. August 2000
[96] s. FN 77
[97] s. FN 79

Voraussetzungen schaffen, weil sie letztendlich noch zu der EU in Konkurrenz steht), sondern es werden von den obengenannten Vorschriften Abweichungen vorgenommen.[98] Die mit der Richtlinie angestrebte Rechtsharmonisierung wird sowieso nicht erreicht, weil die Mitgliedstaaten auch weiter gehende Bestimmungen zum Schutze der Verbraucher erlassen dürfen (Deutschland hat zum Beispiel eine zweiwöchige Widerrufspflicht eingeführt).[99] Die Richtlinie muss als Mindestanforderung für den relevanten europäischen Binnenmarkt betrachtet werden, aber man kann von ihr nicht verlangen, dass sie eine Rechtsharmonisierung oder sogar eine Rechtsvereinheitlichung bewirkt.

Die schweizerische Frist zur Ausübung des voraussetzungslosen Widerrufsrechts wird, so von EJPD vorgeschlagen, sieben Tage (wie EU-Richtlinie) betragen.[100]

Die Frist wird mit der Erfüllung der Informationspflichten auf dem dauerhaften Datenträger und mit dem Vertragsabschluss zu laufen beginnen, soweit es sich um die Lieferung von Sachen handelt. Allerdings setzt hier der Lauf der siebentägigen Frist voraus, dass der Verbraucher die für die Ausübung des Widerrufsrechts nötigen Informationen erhalten hat, wie bspw. die Adresse, an den er den Widerruf schicken kann.[101]

Bezüglich des Umfanges der Informationen, die die Unternehmen zu erbringen haben, hat sich das EJPD für eine Differenzierung der Informationen in drei Klassen entschieden:

1. Auf gewisse in der Richtlinie vorgesehene Informationen wird nicht eingegangen;
2. Andere Informationen betreffen die vorvertragliche Phase und berühren den Vertragsabschluss nur am Rande und führen daher, nach Vorschlag des EJPD, zu einer Revision des Bundesgesetz gegen den unlauteren Wettbewerb;
3. Eine dritte Gruppe von Informationen betreffen direkt oder indirekt das Widerrufsrecht; diese werden neu im Obligationenrecht verankert mit der geschilderten Folge, dass die Widerrufsfrist nicht zu laufen beginnt, wenn der Kunde noch nicht über die entsprechenden Informationen verfügt.[102]

In die dritte Gruppe könnten das Bestehen eines Widerrufsrechts, die Adresse, an den der Widerruf geschickt werden kann, die Bedingungen und Einzelheiten zur Ausübung des Widerrufsrechts, die Identität des Lieferers, die wesentlichen Eigenschaften der Ware oder

[98] s. Anhang III: 2. Fragenfolge an Felix Schöbi des EJPD
[99] s. Urs Feller, Neue Regeln für den E-Commerce, NZZ 5./6. August 2000
[100] s. Anhang III: 2. Fragenfolge
[101] s. Anhang III
[102] s Anhang III

Dienstleistungen, der Preis der Ware hineinfliessen;[103] in die zweite Gruppe die Kosten für den Einsatz der Fernkommunikationstechnik, sofern sie nicht nach dem Grundtarif berechnet werden.[104]

Die Art und Weise der Mitteilung wird von der Richtlinie übernommen (sie spricht von Schriftlichkeit und von dauerhaftem Datenträger). Es zeichnet sich ab, dass dem zweiten Erfordernis (bereits) Genüge getan wird, wenn der Empfänger die entsprechenden Informationen abspeichern und ausdrucken kann.[105]

Von einer digitalen Signatur ist in diesem Zusammenhang, laut Herrn Felix Schöbi, selten bis nie die Rede, obwohl nur sie die Integrität der Daten „einigermassen" garantieren könnte.

3.2.2.2 Revision des Bundesgesetzes gegen den unlauteren Wettbewerb

Nach Ansicht des verantwortlichen Teams des EJPD ist es sinnvoll, dass der schweizerische Konsument (und nicht nur er) über gewisse in der Fernabsatzrichtlinie und in der Richtlinie über den elektronischen Geschäftsverkehr erwähnte Informationen verfügt. Es handelt sich um Informationen, die den Vertragsabschluss nur am Rande berühren, z. B. Angaben zum Geschäftsdomizil (Art. 5 Abs. 1 lit. b E-Commerce-RL) bzw. die Darstellung der technischen Schritte, die zu einem Vertragsabschluss führen (Art. 10 Abs. 1 lit. a E-Commerce-RL). Die Details stehen allerdings noch aus.[106] Meines Erachtens könnten dazu die folgenden Vorschriften in die UWG-Revision aufgenommen werden: die obengenannten Kosten für den Einsatz der Fernkommunikationstechnik, sofern nicht nach dem Grundtarif berechnet werden (Art. 4 Abs. 1 lit. g Fernabsatzrichtlinie), die klare Erkennung der Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben, Geschenke und leichte Zugänglichkeit sowie klare und unzweideutige Angabe der Bedingungen für ihre Inanspruchnahme (Art. 6 Abs. 1 lit. c E-Commerce-RL), die klare Angabe, ob Steuern und Versandkosten in den Preisen enthalten sind (Art. 5 Abs. 2 E-Commerce-RL), die verständliche und unzweideutige Angabe der technischen Mittel zur Erkennung und Korrektur von Eingabefehlern vor Abgabe der Bestellung (Art. 10 Abs. 1 lit. c E-Commerce-RL), die Angabe der für den

[103] Nach Felix Schöbi, Leitender des Projekt E-Commerce beim EJPD, sollten die letzten zwei nicht in die Informationspflichten hineinfliessen, weil sie typischerweise zum Konsens gehören und können wegen ihrer Natur nicht unter der Informationspflichten behandelt werden.
[104] s.für den zweiten Kapitel 3.2.5
[105] s.Anhang III

Vertragsabschluss zur Verfügung stehenden Sprachen (Art. 10 Abs. 1 lit. d E-Commerce-RL).

3.2.3 Ausblick in andere Rechtsgebiete

3.2.3.1 Im Schuldbetreibungs- und Konkursrecht

Nach Art. 82 SchKG hat Aussicht auf provisorische Rechtsöffnung nur wer eine öffentliche Urkunde oder eine durch Unterschrift bekräftigte Schuldanerkennung präsentiert. Die in Art. 82 SchKG verwendete Formulierung – eine durch Unterschrift bekräftigte Schuldanerkennung – lässt Raum für die Vorstellung, dass auch eine digital signierte elektronische Urkunde als Rechtsöffnungstitel taugt.[107] Diese Auslegung würde nicht in Einklang mit der bisherigen Praxis stehen. In der Tat werden z.B. von den Gerichten Vorlagen von Fotokopien akzeptiert, aber nur wenn dahinter ein vom Schuldner unterzeichnetes Original steht. Gerichten sind also in der Annahme von Surrogaten einer durch Unterschrift bekräftigten Schuldanerkennung sehr zurückhaltend. Auch Daniel Staehelin ist gegen eine erweiterte Auslegung von Art. 82 SchKG.[108] Eine Revision vom Art. 82 SchKG wurde vom EJPD nicht vorgeschlagen.

Dieses Problem wird erst mit der allgemeinen Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift durch den Gesetzgeber gelöst werden. Nach der Arbeitsgruppe des Project E-Commerce vom EJPD bedarf es keiner zusätzlichen Änderung des SchKG. Die Gleichstellung der digitalen Signatur im Obligationenrecht wird nach ihrer Ansicht reichen. Zu lösen bleibt allerdings das Problem, wie sich der Rechtsöffnungsrichter Zugang zu einer digital signierten Schuldanerkennung verschafft.[109]

Noch wichtiger als die elektronische Schuldanerkennung ist zum Beispiel die Möglichkeit, Betreibungsbegehren elektronisch signiert gültig einreichen zu können.[110]

Der Hauptgrund für den Einsatz digitaler Signaturen wird in der Tat zunächst nicht die höhere Rechtssicherheit in Online-Geschäften sein, sondern eine höhere Effizienz bei all

---

[106] s. Anhang IV: III Fragenfolge an Felix Schöbi

[107] s. Gutachten des Bundesamt für Justiz vom 24. November 1998, Digitale Signatur und Privatrecht (Vertragsrecht) s. 7

[108] Daniel Staehelin in: Adrian Staehelin/Thomas Bauer/Daniel Staehelin (Hrsg.), Kommentar zum Bundesgesetz über Schuldbetreibung und Konkurs, Basel 1998, N 12 zu Art. 82

[109] s Anhang IV: III Fragenfolge an Felix Schöbi

[110] David Rosenthal, Digitale Signatur: Wo sie eine Rolle spielt, IPD Insider Presse Dienst, april 2000 + indirizzo Internet

jenen Geschäftsabläufen, die bisher nicht elektronisch abgewickelt werden konnten.[111] Für einen solchen Einsatz der digitalen Signatur reicht es die Gleichstellung der digitalen Signatur im Obligationenrecht nicht. Man sollte das SchKG ausdrücklich ändern.
Am gewichtigsten dürften aber die Einsparungsmöglichkeiten im Verkehr mit Behörden sein.

3.2.3.2 Im Verwaltungsrecht

Der elektronische Behördenverkehr kann dank der Anerkennung von der digitalen Signatur sicher abgewickelt werden. Digitale Signaturen können überall benutzt werden, wo ein Dokument einer Behörde rechtsverbindlich eingereicht werden muss. Das könnten Zollpapiere, ebenso eine Steuererklärung oder andere Anträge sein. Zu denken ist z. B. auch an Rechnungs-Belege für den Vorsteuerabzug bei der Mehrwertsteuer.
Vor allem jüngere Bevölkerungsgruppen empfinden schon heute Schalteröffnungszeiten und papiergebundene Abläufen im Verkehr mit den Behörden als schwerfällig. Wieso sollen z.B. neue Ausweispapiere, Adressänderungen, verschiedene Gesuche, nicht elektronisch – rund um die Uhr und um den Globus – abgewickelt werden können?
Das vielzitierte Abstimmen per Internet liesse sich mit digitalen Signaturen und entsprechenden Zertifikaten, zumindest rein technisch, schon heute realisieren.[112] Es wäre sinnvoll, wenn die Schweiz mit ihrer Kompetenz in direktdemokratischen Fragen (mit Initiative und Referendum) bei der elektronischen Abstimmung eine Vorreiterrolle übernehmen könnte.[113] Wieso sollen auch politische Diskussionen, Meinungsumfragen (z.B. über E-Chatting) nicht elektronisch stattfinden?[114]
Dazu muss jedoch nicht primär das Vertragsrecht, sondern das Verwaltungsrecht – dies nicht nur des Bundes, sondern auch der Kantone angepasst werden. Wo etwas schon geschehen ist, sind bis jetzt erst die rechtlichen Grundlagen für den Einsatz von Signaturen geschaffen worden.[115] Die technischen, organisatorischen und finanziellen Hürden sind damit noch nicht genommen.[116]

---

[111] vgl. FN 92
[112] David Rosenthal: Ein elektronisches Siegel fürs Internet, IPD Insider Presse Dienst, April 2000
[113] s. Vizekanzlering Hanna Muralt Müller, NZZ, 14.04.2000
[114] Vizekanzlerin Hanna Muralt Müller, E-Goverment – Herausforderung für Behörden, NZZ, 14.04.2000
[115] Es gibt aber schon realisierte Projekte, s. Kanton Genf (www.geneve.ch/infos/welcome.html) und Städte Zürich und Winterthur
[116] David Rosenthal, E-Commerce: Die Kuh melken andere, Computerworld, 9.6.2000

Es müssen verschiedene Gesetzesanpassungen in den verschiedenen Rechtsgebieten des Verwaltungsrecht im Gange, mit dem Ziel die elektronische Kommunikation mit den Behörden zu ermöglichen, vorgenommen werden. So vorbereitet zur Zeit das Eidgenössischen Finanzdepartement (EFD) in Zusammenarbeit mit dem EJPD eine Anpassung der verschiedenen Steuergesetzen- und Verordnungen. Zu denken ist z. B. an Rechnungs-Belege für den Vorsteuerabzug bei der Mehrwertsteuer.
Zu erwarten im Moment ist es nur, dass die zur Zeit schon vorbereitete Vorlage Bestimmungen über die elektronische Kommunikation mit Registern (Handelsregister und Grundbuch) enthalten wird.

3.2.3.3 Im Verfahrensrecht

Nach Kontaktnahme mit dem Verantwortlichen des EJPD für Verfahrensrecht, Herr Philippe Gerber, habe ich die wichtigsten Grundzüge über die Änderung der verschiedenen Verfahrensgesetzen erfahren.
Erstens ist eine Totalrevision des Bundesgesetz über das Verwaltungsverfahren (VwVG) vorgesehen. Bei dieser Gelegenheit wird die elektronische der Kommunikation zwischen Behörden und Bürgern betreffend Einreichung der Beschwerden, Anträgen und Zustellung von Verfügungen geregelt. In der Tat muss Art. 21 VwVG revidiert werden. Art. 21 VwVG betrifft die rechtsgültige Einhaltung der Frist für die Einreichung der Eingaben. Dort ist die schriftliche Einreichung der Eingaben vorgeschrieben. Die Änderung zielt auf der Annahme von elektronisch eingereichte Eingabe.
Problematisch scheint die Berechnung der Frist zu sein oder besser die Feststellung des Zeitpunkt mit dem Frist zu laufen beginnt. Nach Art. 20 VwVG Abs. 1 beginnt die Frist am dem auf ihre Mitteilung folgenden Tage zu laufen. Nach Abs. 2 beginnt sie, wenn sie nicht der Mitteilung an die Parteien bedarf, an dem auf ihre Auslösung folgenden Tage zu laufen. Bei der elektronische Kommunikation ist aus technischen Gründen nicht einfach zu wissen, ob und wann eine Botschaft beim Empfänger angekommen ist. Mögliche Lösungsansätzen ist die Festsetzung einer pauschale Frist, nachdem angenommen werden könnte, dass die Botschaft angekommen ist, oder eine Empfangsbestätigung seitens des Empfängers. Die erste Lösung ist sehr problematisch, weil es sehr schwierig ist eine solche Frist festzusetzen. Die zweite Lösung weist die Lücke auf, dass der Empfänger trotz rechtsgültigen Empfang die Empfangsbestätigung nicht senden könnte. Zur Umgehung

dieses Problem sollte man auf die traditionelle Beförderung durch die Post ausweichen oder eine Empfangsbestätigung nur von denjenigen, die man trauen kann, verlangen.
Diskussionen und Recherchen sind zur Lösung dieses Problems sind noch im Gange.
Im neuen Bundesgerichtsgesetz, das der heutige Bundesgesetz über die Organisation der Bundesrechtspflege ersetzen wird, ist auch die elektronische Einreichung und Zustellung von Beschwerden und Entscheide geregelt. Darin werden die Voraussetzung für eine gültige elektronische Beförderung aufgezeichnet. Da es sich um wenige Bestimmungen handelt, werden sie direkt dem schweizerischen Parlament zur Abstimmung vorgelegt.
Auch das zukünftigen Bundesgesetz über Zivilverfahren, das die kantonale Zivilprozessordnungen ersetzen wird, nimmt auf die elektronische Kommunikation Rücksicht.
Zuständig für das Prozessrecht sind zur Zeit noch die Kantone. Das Bundesrecht stellt einzig klar, dass die Kantone für die Beweisbarkeit eines Rechtsgeschäftes keine besondere Form vorschreiben dürfen, wenn das Bundesrecht selber keine solche kennt (Art. 10 ZGB). Öffentliche Register und öffentliche Urkunden erbringen für die durch sie bezeugten Tatsachen vollen Beweis (Art. 9 Abs. 1 ZGB). Der Nachweis, dass diese Tatsachen nicht der Wahrheit entsprechen, darf an keine besondere Form gebunden werden (Art. 9 Abs. 2 ZGB).
Ausgehend von den obigen Regeln basiert das Beweisrecht auf verschiedene Beweismittel: Zeugen, Urkunden, Parteiverhör, Augenschein und Gutachten. Unter Berücksichtigung der freien richterlichen Beweiswürdigung hängt die Anerkennung von digital signierten Dokumenten nicht von der Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift ab. Die Gerichte konnten schon lange digital signierten Dokumenten Beweiskraft anerkennen, wenn sie nur wollten und sich trauten.[117] Die Beweiskraft von digital signierten Dokumenten hängt aber auf jeden Fall von der Qualität der digitalen Signatur selbst, von der Zuverlässigkeit der Zertifikate, und von der Vertrauenswürdigkeit der Anbieterinnen von Zertifizierungsdiensten.
Im vorgeschlagenen Bundesgesetz über die elektronische Signatur wird einen Artikel aufgenommen, der eine gesetzliche Vermutung gründet. So wird einem digital signierter Dokument Authentizität zuführt. Die vorgeschlagene Vorschrift besagt, dass es wird vermutet, der digital signierter Dokument von der angegebene Person stamme, ausser sie nachweist, dass die technischen Komponenten zur Erzeugung der digitalen Signatur in den Händen dritten gelangen ist.

3.2.3.4 In der kaufmännischen Buchführung

Auch bezüglich dieses Gebiet wurden in der Vorlage keine Regelungsvorschläge vorgenommen. Nach Art. 962 Abs. 2 OR ist den buchführungspflichtigen Unternehmen gestattet, Geschäftskorrespondenz und Buchungsbelege als Aufzeichnungen auf Bild- oder Datenträger aufzubewahren, wenn die Aufzeichnungen mit den Unterlagen übereinstimmen und jederzeit lesbar gemacht werden können. Eine Verpflichtung, die entsprechenden Datenträger digital zu signieren, damit sie als Geschäftskorrespondenz und Buchungsbelege taugen, besteht nicht.[118] Nicht ganz ausgeschlossen werden kann, dass sich in der Praxis oder gestützt auf eine bundesrätliche Verordnung (Art. 962 Abs. 2 OR) in Zukunft ein Standard durchsetzt, wonach Geschäftskorrespondenz und Buchungen nur dann als dem Papier gleichwertige Belege Anerkennung finden, wenn diese digital signiert worden sind.[119] In der näheren Zukunft ist auch nicht vorgesehen, dass eine digital signierte Urkunde an die Stelle der von Hand unterzeichneten Betriebsrechnung und Bilanz treten könnte.

4. Bewertung der rechtlichen Regelungen in der Schweiz

Die Anhaltspunkte für die Bewertung sind das eigenständige Gesetz (Bundesgesetz über die elektronische Signatur) und die Revisionen des OR und des UWG. Objekte der Analyse werden also nicht nur die rechtlichen Regelungen über die elektronische Signatur i.e.S. sein, sondern auch die Regulierungsansätze, die aus den Auswirkungen der Anwendung der elektronischen Signaturen entstehen.

[117] David Rosenthal: E-Commerce: Die Kuh melken andere, Computerworld, 9.6.200
[118] vgl. FN 90 s. 7
[119] vgl. FN 90 s. 8

4.1 Im Allgemein

4.1.1 Eine Regelung mit Verspätung

Ist die Schweiz auf den richtigen Weg? Auf den richtigen Weg ist sie sicher, aber man kann sich die Frage stellen, ob sie sich schnell genug an die technische Entwicklung angepasst. Die Zertifizierungsdiensteverordnung hat schon ihren Sinn, aber die alleinige Regelung der Public Key Infrastructure genügt nicht. Die Zertifizierungsdiensteverordnung war ein dringend nötiger erster Schritt, aber der zweite – zur rechtlichen Wirkung der digitalen Signatur - muss umgehend folgen, weil eine Zertifizierungsdiensteverordnung ohne Anerkennung der digitalen Signatur nützt nicht viel. Im Herbst 2000 wird das Vernehmlassungsverfahren, wenn alles nach dem Plan verläuft, über das Bundesgesetz betreffend elektronischen Signaturen durchgeführt. Aber im allgemein kommt jede neue gesetzliche Grundlage zu spät. Der erste Vorstoss zur Regulierung der Rechtswirkung von digitaler Signaturen wurde im Jahre 1994 vorgenommen (Motion Spoerry)[120], und ein erneuter Vorstoss wurde im Juni 1999 vorgenommen (Motion Leumann).[121]

Das dringlich erforderliche Handeln wurde immer weiter verzögert. Der erste Vorstoss geht auf das Jahre 1994 zurück und nach sechs Jahren ist die Anerkennung der digitalen Signatur noch nicht Wirklichkeit. Zudem ist nur eine Zertifizierungsdiensteverordnung in Kraft getreten (1. Mai 2000) und die technischen Ausführungsvorschriften sind noch nicht veröffentlicht. Es ist zu hoffen, dass sie in einer Vollziehungsverordnung zum Bundesgesetz über die elektronische Signatur endlich in Kraft gesetzt werden. Sehr beliebt was die zweifellos trendige, jedoch nicht besonders vorantreibende „Laissez-faire“-Politik: die Wirtschaft soll es zunächst einmal selbst machen, während der Staat erst auf konkrete Forderungen hin reagiert.[122] Die Wirtschaft hat in der Tat konkrete Forderungen gestellt, aber der Staat hat nicht unverzüglich reagiert. Der Bundesrat hatte die Thematik aufgenommen und im Jahre 1998 eine passende Strategie für die Informationsgesellschaft der Zukunft formuliert. Aber aus dieser Strategie und einer dazu gegründeten, verwaltungsinternen Koordinationsgruppe gingen entsprechend dicke Berichte der diversen Bereiche der Bundesverwaltung hervor. Darin werden unterschiedlichste

[120] s. Motion Spoerry (94.3115), Rechtsverbindlichkeit elektronischer Unterschriften. Änderungs von Artikel 14 OR, Amtliches Bulletin der Bundesversammlung 1994, Nationalrat, 1883 f.
[121] s. Motion Leumann (99.3288), Digitale Unterschriften, Amtliches Bulletin der Bundesversammlung 1999, Ständerat, 819; http://www.parlament.ch/Poly/Suchen_amtl_Bulletin/ce99…/266.HTM?servlet=get_conten
[122] David Rosenthal

Aktionspläne, Bedürfnisse und andere Aspekte der Informationsgesellschaft diskutiert.[123] Darauf reagierend hatte der Schweizerischen Wirtschaftsverband Vorort nachgedoppelt und Mitte März 2000 an den Bund geschrieben. Darin hiess es, dass mit theoretischen Überlegungen und Vorarbeiten allein der Wirtschaft nicht gedient sei und dass konkrete Schritte in kurzer Zeit gewünscht seien.
Zurückblickend nach über zwei Jahren Arbeit ist das Ergebnis ernüchternd, zumindest auf den ersten Blick: Während zum Beispiel in der EU unterschiedlichste Richtlinien ausgearbeitet und in Kraft gesetzt wurden, hat die Schweiz nichts Vergleichbares vorzuweisen – oder so gut wie fast nichts - um das besagte günstige E-Commerce-Umfeld zu fördern.[124] Eine der wenigen Ausnahmen ist die Zertifizierungsdiensteverordnung, die seit Anfang Mai gilt und eine erste Grundlage für digitale Signaturen bietet; zustandegekommen ist sie erst im zweiten Anlauf.

4.1.2 Technologiebehafteten Konzept

Ein weiterer Kritikpunkt betrifft die Zertifizierungsdiensteverordnung selber. Die Verordnung ist zu einseitig technologiebehaftet, weil sie einzig die digitale Signatur (welche auf der Technik der asymmetrischen Kryptologie aufbaut) reguliert und dabei „vergisst“, dass noch andere Formen der elektronischen Signatur existieren oder in naher Zukunft entwickelt werden.[125] In der Tat sind Regulierungsansätze immer in einem Spannungsfeld zwischen technologischer Neutralität und rechtlicher Bestimmtheit.[126] Je mehr elektronische Authentifizierungsverfahren vom Gesetzgeber gefasst werden, desto schwieriger wird die Spezifikation der Rechtswirkungen solcher Verfahren.[127]
Es können verschiedene Modelle und Lösungsansätze für die Sicherung und Gewährleistung des elektronischen Handels. Es gibt Gesetze, die die rechtliche Anerkennung von „elektronischen Signaturen“ allein eine auf einer PKI beruhende digitalen Signatur zulassen.[128] Der „Utah Digital Signature Act“ war das erste Gesetz, das der elektronischen Geschäftsverkehr mittels digitalen Signaturen erliess.

[123] David Rosenthal, E-Commerce: Die Kuh melken andere, Computerworld, 9.6.2000
[124] vgl. FN 102 s. 1
[125] Gondini A. Fravi: Elektronische Signaturen, Homepage Anwaltskanzlei Fravi, 28. Oktober 1999; http://www.fravi-law.ch/elektronische_signaturen1.htm
[126] s. Simone R. Pestalozzi/Marc D. Veit, Elektronische Signaturen: schweizerische Regulierungsansätze im europäischen Umfeld, AJP, 5/2000
[127] s FN 105
[128] s. Thomas Hoeren, s. 388 mit Bezug auf Koch FN 5

Es gibt aber auch Alternativen zum PKI Modell. Diese Gesetze sind auf eine „Technologieneutralität“ ausgerichtet, um so alle aktuellen und zukünftigen Authentifikationsmechanismen erfassen zu können und nicht lediglich einen Standard festzulegen, der sich zur Zeit als der günstigste erweist. Unter diesen Alternativen sind das „criteria-based“ Modell, das „signature-enabling“ Modell und das „Hybrid-Modell“ zu zählen.[129] Nach dem „criteria-based“ Modell (die EU-Richtlinie über elektronischen Signaturen folgt diesen Modell) wird die Authentizität einer digitalen oder elektronischen Signatur nur anerkannt, wenn sie gewisse Kriterien hinsichtlich der Vertrauenswürdigkeit und Sicherheit erfüllt. Nach der EU-Richtlinie erhalten elektronische Signaturen von Zertifizierungsdiensteanbieterinnen, welche die Anforderungen für ein höheres Sicherheitsniveau erfüllen, darüber hinaus weitere Rechtswirkungen, wie z.B. die Erfüllung gewisser handschriftlicher Formerfordernisse oder die (widerlegbare) Vermutung der Richtigkeit des Empfängers und des Inhaltes.[130] Damit soll die Richtlinie offen und anwendbar für zukünftige technologische Entwicklungen sein.[131]
Nach dem „signature-enabling“ Modell werden hingegen elektronische Signaturen generell den traditionellen Signaturen gleichgestellt.
Beim „Hybrid-Modell“ werden sowohl digitale Signaturen als auch elektronische Signaturen gleichwertig anerkannt.
Die Zertifizierungsdiensteverordnung hat den PKI-Modell gefolgt, ohne aber die rechtliche Anerkennung der digitale Signatur zu regeln. Hingegen wird sich der vorgeschlagene Bundesgesetz über die elektronische Signatur von dem Begriff der digitalen Signatur etwas entfernen. Es zielt auf mehr Technologieneutralität. Es wird aber, wie die Zertifizierungsdiensteverordnung, die Rechtswirkung der elektronische Signatur nicht regeln. Dies wird den einzelnen Gebieten überlassen. Was das Privatrecht betrifft, wird die Anerkennung der elektronische Signatur im Obligationenrecht geregelt.

4.1.3 Förderung der Effizienz

Man muss aber nicht meinen, dass mit der rechtlichen Anerkennung der digitalen Signatur der E-Commerce sich sofort radikal verändern würde. Es ist immerhin erforderlich, dass der Bund mit der rechtlichen Anerkennung der digitalen Signatur vorwärts macht. Die

[129] s. derselbe s. 400
[130] s. FN 105
[131] s. Stephan Schumacher, Digitale Signaturen in Deutschland, Europa und den U.S.A., Computer und Recht, 12/1998, s. 758 ff.

Bedürfnisse sind aber oft anderer Art als landläufig diskutiert werden mag. So lassen sich digitale Signaturen in vielen Fällen, in denen sie angezeigt sind, heute schon ohne weiteres einsetzen, sofern die beteiligten Parteien nur wollen.[132] Der Hauptgrund für den Einsatz digitaler Signaturen ist nicht unbedingt die höhere Rechtssicherheit in Online-Geschäften, sondern eine höhere Effizienz bei all jenen Geschäftsabläufen, die bisher nicht elektronisch abgewickelt werden konnten. Dem sollte der Gesetzgeber auch Rechnung tragen. Anscheinend betrachtet der Gesetzgeber das als kein interessantes und dringendes Thema. In der Vorlage betreffend das Bundesgesetz über die elektronische Signatur werden nur Bestimmungen über die elektronische Kommunikation mit Registern aufgenommen und werden nur eine erste gesetzliche Grundlage bilden. Vorlagen betreffend das E-Governement sind noch in der Entwicklungsphase und können in absehbare Zeit nicht erwartet werden. Die konkrete elektronische Kommunikation mit Registern wird noch lange auf sich warten lassen. Bezüglich den anderen Bereichen des E-Governement ist leider nicht die Rede.
Im allgemein kann man ohne weiteres behaupten, dass die Schweiz den Zug verloren hat und ihm ständig nachlaufen muss. Dies ist eine häufige Kritik an die schweizerische Bewältigung des Problems.

4.1.4 Änderung der Haftung von Zertifizierungsstellen

Bezüglich der Änderung der Vorschrift über die Haftung der Anbieterinnen von Zertifizierungsdiensten muss gesagt werden, dass auch in diesem Fall ein Kompromiss gefunden worden ist. Es wurde ein Konstrukt zwischen einer Kausalhaftung mit Exkulpationsmöglichkeit und einer Gefährdungshaftung vorgeschlagen. Nach der vorgeschlagene Vorschrift spielt das Verschulden keine Rolle mehr, sondern entscheidend wird nur die Verletzung der Vorschriften des Bundesgesetz über die elektronische Signatur sein. Die Zertifizierungsstelle wird sich nicht mehr von ihrer Haftung befreien können, in dem sie beweist, dass sie ohne Verschulden gehandelt hat. Die Zertifizierungs- stellen muss aber nicht für jedes entstandenen Schaden haften, sondern nur für diejenige Schäden, die aus einer Pflichtverletzung entstehen. Vergisst z. B. die Zertifizierungsstelle das gesperrte Zertifikat in die „Certificate Revocation List“ (CRL) einzutragen, handelt sie in pflichtverletzende Weise und muss dafür einstehen, auch wenn ihr kein Verschulden trifft. Hingegen muss die Zertifizierungsstelle nach der vorgeschlagene Bestimmung nicht für die

[132] vgl. FN 102 s. 4

Schäden, die nicht aus ihrer Macht entstehen. Kann ein Dritte z. B. das online-abrufbare Verzeichnis der gültige Zertifikate wegen einem Stromausfall nicht einsehen, haftet die Zertifizierungs- stelle nicht, weil der Stromausfall aus höhere Gewalt entsteht. Knackt z. B. jemand den Schlüssel zur Erzeugung der digitale Signatur einer anderen Person, muss die Zertifizierungsstelle für den entstandenen Schaden nicht einstehen, ausser es kann ihr vorgeworfen werden einen nicht den Sicherheitsstandard entsprechenden Schlüssel angeboten zu haben. (Z. B. einen zu kurze Schlüssellänge).
Eine zu weitgehende Haftung kann auch also solchen Gründen nicht vorgeschrieben werden: Zertifizierungsstellen haben grosse Mühe eine Versicherung zu finden, die bereit ist die Schäden zu decken.[133] Wenn sie eine finden, verlangt die Versicherung so hohe Versicherungsprämien, dass die Zertifizierungsstelle gezwungen wird, die zusätzlichen Kosten auf dem Preis des Zertifikats überzuwälzen. Das Resultat wäre dann zu teure Zertifikate, die niemand bereit ist, sie zu bezahlen.[134] Auch wenn die Zertifizierungsstelle keine Versicherung finden würde, würden die Folgen dieselben sein.
Die vorgeschlagene Vorschrift ist ein guter Kompromiss, dass die Interessen der Kunden und der Zertifizierungsstellen gleichmässig berücksichtigt.

4.1.5 Auswirkungen der Konsumentenschutzbestimmungen

Bezüglich der Bestimmungen betreffend den Konsumentenschutz ist noch Folgendes hinzufügen. Solche Bestimmungen sind zu begrüssen, aber deren Nachteil ist es dass, mit einem siebentägigen Widerrufsrecht jeder Kauf praktisch zum Kauf auf Probe wird.[135]
Weil das Widerrufsrecht in einer bestimmten Anzahl von Fällen ausgeübt werden wird, sind unter Umständen Anpassungen in der Preiskalkukation vorzusehen. Für viele Unternehmen drängt sich sodann eine Überarbeitung ihres Internet-Auftritts auf, soweit sie bereits heute E-Commerce betreiben.[136]

4.1.6 Public Key Infrastructure ohne staatliche „Root“

Die Streichung eines staatlichen „Root“ ist auch zu begrüssen. Dies war der einzige richtige Weg, der von der Wirtschaft (oder deren Teil, der etwas von der Sache versteht)

[133] E-Mail und telefonische Befragung mit Christian Graber
[134] Landrock Peter, Computerworld, S. 3
[135] s. Urs Feller, Neue Regeln für den E-Commerce, NZZ 5./6. August 2000
[136] s. Urs Feller

vehement gefordert wurde. Eine hierarchische Struktur, die für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten sorgt, ist immerhin besser, als ein Netz gegenseitiger Anerkennungen. Eine hierarchische Struktur würde die Qualität, das Schutz der Konsumenten und das Vertrauen erhöhen, hingegen ist ein Netz gegenseitiger Anerkennungen viel komplizierter und undurchsichtiger. In Zukunft wird es so sein, dass mehrere supranationale internationale Zertifizierungsstelle geben (z.B. der UNCITRAL), aus denen alle anderen Zertifizierungsstellen ableitbar werden sein.
Schliesslich sieht auch die ESiG-RL keine „Wurzelinstanz" vor, von der die innerhalb der Union ansässigen Dienstleister ihre Zertifikate ableiten können. Der einzige Staat, der eine staatliche „Root" vorsieht ist Deutschland.

4.2 Im Hinblick auf dem europäischen Umfeld

4.2.1 EU-Richtlinien

Der elektronische Rechtsverkehr kennt keine Grenzen. Es ist also wichtig, dass die vorhandenen nationalen Regelungen auch im europäischen Bereich keine Hindernissen für den E-Commerce darstellen.[137] Für die internationale kommerzielle Verwendung von digitalen Signaturen ist eine gegenseitige Anerkennung der von den Zertifizierungsdiensteanbietern ausgestellten Zertifikate von herausragender Bedeutung. Die Frage, nach welchen Kriterien und von welchen Instanzen bzw. in welchem Verfahren die national ausgegebenen Zertifikate im internationalen Verkehr anerkannt werden, ist also zentral.[138]

4.2.1.1 Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ESiG-RL)

Nach Art. 14 THG kann der Bundesrat internationale Abkommen zur Anerkennung ausländischer Zertifizierungsdiensteanbieter und ihrer Dienstleistungen abschliessen. Nach Art. 18 ZertDV stellt dann die SAS der Öffentlichkeit die Liste der ausländischen Anbieterinnen von Zertifizierungsdiensten zur Verfügung. Die Anforderungen, welche

[137] s. Jean-Maurice Geiser: Signatur numérique: Les enjeux du projet de réglementation, in: Medialex, 4/99. S. 205
[138] s. FN 105 s. 604

ausländische Zertifizierungsdiensteanbieter erfüllen müssen, um in der Schweiz anerkannt zu werden, wurden vom Bundesrat bis jetzt noch nicht ausgearbeitet.[139]

Hingegen hat die EU in der ESiG-RL die Anforderungen zur Anerkennung ausländischer Zertifizierungsdiensteanbieter ausdrücklich vorgeschrieben. Hierbei wird zwischen Anbieterinnen von Zertifizierungsdiensten innerhalb der EU sowie aus Drittländern unterschieden: nach Art. 7 ESigG-RL werden qualifizierte Zertifikate von in Drittländern ansässigen Zertifizierungsdiensteanbieterinnen den von einer in der Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieterin ausgestellten Zertifikaten rechtlich gleichgestellt, wenn die Zertifizierungsdiensteanbieterin die Anforderungen der ESigG-RL erfüllt und im Rahmen eines freiwilligen Akkreditierungssystems eines Mitgliedstaates akkreditiert ist (Abs. 1 lit. a). Alternativ kann eine Zertifizierungsdiensteanbieterin eines Mitgliedstaates, der den Anforderungen der ESiG-RL entspricht, für den drittländischen Kollegen eintreten (Art. 7 Abs. 1 lit. b ESiG-RL). Es besteht auch die Möglichkeit, das Zertifikat oder die Zertifizierungsdiensteanbieterin im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der EU und Drittländern oder internationalen Organisationen anzuerkennen. (Art. 7 Abs. 1 lit. c ESiG-RL).

Es stellt sich somit die Frage, ob die von einer anerkannten schweizerischen Zertifizierungsdiensteanbieterin ausgestellten Zertifikate die Anforderungen der ESiG-RL erfüllen. Im Lichte der Ausführungen im Kapital 3.1.4 entsprechen die Anforderungen an der Generierung und Verwendung der kryptografischen Schlüssel nach Art. 6 ZertDV den in den Anhängen III u IV ESiG-RL ausgeführten Voraussetzungen. Die Anforderungen an die elektronische Zertifikate nach Art. 7 ZertDV entsprechen denjenigen in Anhang I ESiG-RL und die Anforderungen an die Zertifizierungsdiensteanbieterinnen nach Art. 4 und Abschnitt 3 entsprechen implizit oder explizit denjenigen in Anhang II ESiG-RL.

Die Anforderungen an Zertifikate und die fachlichen, technischen und organisatorischen Anforderungen an die Zertifizierungsdiensteanbieterinnen stimmen überein und daher sollte eine Gleichstellung der Zertifikate möglich sein.[140]

Auch bezüglich die Ausführungsvorschriften zur Zertifizierungsdiensteverordnung wird mit Bezug auf die europäischen Projekte genommen.

Die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift, die im Art. 15 E-OR vorgeschlagen wurde, führt eine Harmonisierung mit den EU-Vorschriften mit sich.

[139] FN 105 Pestalozzi, Veit s. 604
[140] s. Pestalozzi/Veit

Man kann also ruhig behaupten, dass die schweizerische Vorschriften mit denjenigen der EU kompatibel sind.

4.2.1.2 Richtlinie über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz (Fernabsatzrichtlinie)

Wie schon in Kapitel 3.2.4 geschrieben, wird die Schweiz die EU-Fernabsatzrichtlinie nicht blind folgen.
Auf jeden Fall müssen Unternehmen mit Sitz in der Schweiz mit der Fernabsatzrichtlinie in dem Sinne rechnen, dass sie am ausländischen Wohnsitz des Verbrauchers verklagt werden können und in diesem Fall an den Massstäben der Richtlinie bzw. deren innerstaatlichen Umsetzung gemessen werden.[141]
Die Frage, inwieweit hingegen schweizerische Konsumenten, die von Unternehmen aus der EU beliefert werden, sich ihrerseits auf die Vorteile der Richtlinie werden berufen können, würde sich mit der Annahme der vorgeschlagene Bestimmungen über den Konsumentenschutz durch das schweizerische Parlament nicht mehr stellen, weil schweizerische Konsumenten nach schweizerischen Recht mehr oder weniger den gleichen Schutz geniessen würden.
Im gegenteiligen Fall würde die Anwendung der Vorteile der Richtlinie auch für Konsumenten in der Schweiz wegen des dem Verbraucherrecht immanenten „Günstigkeitsprinzips“ nicht von vornherein ausgeschlossen.[142]

4.2.1.3 Richtlinie über den elektronischen Geschäftsverkehr (E-Commerce-Richtlinie)

Die Schweiz hat keine vergleichbare Regulierung im Bereich des elektronischen Geschäftsverkehrs.
Am 28. Februar 1996 hat der Bundesrat die Groupe de réflexion für eine Informationsgesellschaft in der Schweiz eingesetzt. Er hat ihr das Mandat erteilt, die sozialen und wirtschaftlichen Auswirkungen der Verbreitung der neuen Informations- und Kommunikationstechnologien zu untersuchen und die Grundlagen für die Ausarbeitung einer Strategie für eine Informationsgesellschaft in der Schweiz zu schaffen.[143]

[141] s. Urs Feller, Neue Regeln für den E-Commerce, NZZ 5./6. August 2000
[142] s FN 113
[143] s. Stellungnahme des Bundesrates vom 17.05.200 zur Motion Durrer, E-Commerce. Regulierungsbedarf vom 15.03.2000, 00.3057; http:// www.parlament.ch/afs/data/d/gesch/2000/d_gesch_20003057.htm

Gestützt auf die Erkenntnisse der Groupe de réflexion, die Erfahrungen aus der Teilnahme der Schweiz an den G7-Pilotprojekten, die Studien des Schweizerischen Wissenschaftsrates sowie der Bonner Ministererklärung, hat der Bundesrat eine Strategie für eine Informationsgesellschaft in der Schweiz ausgearbeitet und am 18. Februar 1998 verabschiedet, sowie eine interdepartementale Koordinationsgruppe Informationsgesellschaft (KIG) beauftragt, die nötigen Konzepte und Aktionspläne zu erstellen und dem Bundesrat jährlich Bericht über den Stand der Arbeiten zu erstatten.[144] Unter diesen Aktionsplänen gibt es auch einen Aktionsplan E-Commerce. Dieser Aktionsplan behandelt ordnungspolitische Leitlinien und die verschiedenen Gebiete des E-Commerce (Verschlüsselung, digitale Signatur, Verbraucherschutz, Internationales Vertragsrecht, Datenschutz, Domainnamen und Markenschutz, Urheberrecht, schädliche und illegale Inhalte, Wettbewerbsrecht, Steuern, Arbeits- und Gesellschaftsrecht, elektronischer Zahlungsverkehr und Internet-Banking sowie Auswirkungen der Konvergenz auf Fernmelde- und Mediengesetzgebung).[145]

Die europäische E-Commerce-Richtlinie regelt hingegen die Anforderungen an die elektronischen Verträge und die Verantwortlichkeit der Anbieter von Diensten der Informationsgesellschaft.[146] Sie zielt auf die Umgestaltung des nationalen Vertragsrechts, mit dem Ziel, Hindernisse des elektronischen Geschäftsverkehrs zu beseitigen. Die Definition „Dienste der Informationsgesellschaft“ folgt der des Artikels 1 Absatz 2 der Richtlinie 98/34/EG, geänderten Fassung. Man findet hier folgende Definition für die Dienste der Informationsgesellschaft im Sinne des Dienstleistungsbegriffs der Artikel 59 und 60 EG-Vertrag: „Eine Dienstleistung der Informationsgesellschafts, d.h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“.[147]

Der schweizerische Aktionsplan E-Commerce ist sehr anspruchsvoll und braucht für seine Umsetzung sehr viel Zeit. Er zielt auf die Schaffung der rechtlichen Rahmenbedingungen für den E-Commerce in allen Rechtsgebieten. Die Umsetzung aller Massnahmen gemäss den Aktionsplan E-Commerce wird nur langfristig möglich sein. Hingegen ist die

[144] s. Stellungnahme des Bundesrates vom 13.06.2000 zur Motion der Kommission 00.016-NR, E-Switzerland. Staat als Modellanwender, vom 09.05.2000, 00.3194; http://www.parlament.ch/afs/data/d/gesch/2000/d_gesch_20003194.htm

[145] Antwort des Bundesrates vom 23.02.2000 zur Interpellation Melchior, Entwicklung zur Informationsgesellschaft. Wo bleibt die Schweiz?, vom 22.12.1999, 99.3632; http://www.parlament.ch/afs/data/d/gesch/1999/d_gesch_19993632.htm

[146] s. Ivo Geis, Die europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen, Computer und Recht, 12/1999, s 772 ff.

europäische E-Commerce-Richtlinie vielleicht in ihren Regulierungsgebieten detaillierter, aber sie stellt wenigstens einen unentbehrliches Minimum dar, der mehr oder weniger kurzfristig zur Verfügung gestellt wurde. Es stellt sich die Frage, ob die Schweiz auch diesen Weg als Überbrückungsregelung einschlagen sollte.

4.3 Im Hinblick auf dem weltweiten Umfeld

Ein grosses Risiko der momentan „boomenden" Regulierungsbestrebungen auf nationaler Ebene besteht darin, dass diese Regulierungsbestrebungen der internationalen Verwendung elektronischer Signaturen eher hinderlich denn förderlich sind: unterschiedliche rechtliche und technischen Anforderungen an elektronische Signaturen können einerseits zu neuen technischen Handelshemmnissen führen, andererseits kann schon die reine Notwendigkeit eines Anerkennungsverfahrens in den einzelnen nationalen Jurisdiktionen zu einer Beschränkung des Marktzuganges für Zertifizierungsdiensteanbieter führen.[148]
Deswegen denken weltumspannenden Gremien über die Beseitigung von Hemmnissen sowie über die Schaffung einheitlicher Mindestrahmenbedingungen für den elektronischen Rechtsverkehr, insbesondere für elektronische Signaturen, nach.
Die Kernfrage ist folgende: welche tatsächlichen Voraussetzungen müssen elektronische Signaturen erfüllen, damit sie rechtlich als „gleichwertig" anerkannt werden können?[149]

4.3.1 OECD

Die OECD hat sich aufgrund der kontroversen Debatte und der vom gewerblichen Bereich befürchteten weltweiten Handelshindernisse ebenfalls in die Diskussion eingeschaltet und im Mai 1997 Leitlinien für die Kryptographiepolitik[150] verabschiedet, die die Mitgliedsstaaten veranlassen sollen, einen möglichst freien, rechtlichen geregelten Zugang zu den Signaturverfahren zuzulassen, ohne in die Diskussion über innere Sicherheit einzugreifen.[151]

---

[147] s. Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, 18.12.1998
[148] s. FN 105, s. 604
[149] s. Ulrich Sandl, Wirtschaftspolitische Bedeutung digitaler Signaturen, Computer und Recht, 5/2000, 319 ff.
[150] s. OECD-Leitlinien zur Kryptopolitik ("Guidelines on Cryptography Policy") vom 27.3.1997; http://www.oecd.org/dsti/iccp/cryptoe.html
[151] s. Dr. IvoGeis, Rechtsaspekte des elektronischen Geschäftsverkehrs, AWV-Eigenverlag, Eschborn 1999, s. 97

Die Leitlinien legen acht Grundprinzipien dar, die nicht isoliert betrachtet werden müssen, sondern ganzheitlich angewendet werden sollen:[152]

1. Die zugelassenen kryptographischen System sollen so vertrauenswürdig sein, um das Vertrauen in den Informations- und Kommunikationstechnologien steigern zu lassen. Der Markt, die staatlichen Regulierungsansätze, die Konzessionen der Lizenzen und der Gebrauch der kryptographischen Methoden sollten auch das Vertrauen der Anwendern steigern. Bezüglich Punkt 1: Die Zertifizierungsdiensteverordnung zielt auf die Vertrauensförderung in der Anwendung von digitalen Signaturen.

2. Die Nutzer sollen bezüglich der kryptographischen Systemen die freie Wahl haben. Es wird davon ausgegangen, dass es verschiedene kryptographischen Systemen zur Befriedigung der verschiedenen Bedürfnissen im Bereich Datenschutz zur Verfügung gibt. Der Nutzer muss auch selber entscheiden können, welchen Grad an Sicherheit beanspruchen will. Der kann aber bestimmte, einen Mindestmass an Sicherheit aufweisende Kryptographien vorschreiben, insbesondere im Falle von Schutz von persönlicher Daten und von elektronischem Geschäftsverkehr. Bezüglich Punkt 2: Die Zertifizierungsdiensteverordnung bildet die Voraussetzung für eine sichere Anwendung der digitalen Signaturen, aber die Anwendung der andere kryptographischen Methoden mit unterschiedlichen Sicherheitsniveaus wird nicht ausgeschlossen.

3. Die Entwicklung der kryptographischen Methoden soll den Bedürfnissen von Einzelpersonen, der Wirtschaft und der Regierungen folgen und das Angebot von kryptographischen Systemen soll durch einen offenen und wettbewerbsfreudigen Markt bestimmt werden. Bezüglich Punkt 3: Dieses Grundsatz ist in der Schweiz selbstverständlich erfüllt.

4. Die technischen Grundlagen sollen auf nationaler und internationaler Ebene entwickelt und verbreitet werden. Dieser Grundsatz zielt auf die Interoperabilität, Mobilität und Anpassungsfähigkeit. Regierungen und Experten sollen technischen Standards, Kriterien und technische Protokolle entwickeln, auf internationaler Ebene kompatibel sind. Bezüglich Punkt 4:

[152] s. FN 129

5. Grundsätzliche Persönlichkeitsrechte Einzelner, insbesondere das Recht auf den Schutz persönlicher Daten, sollen von der nationalen Kryptographiepolitik sowie nationalen Umsetzungen respektiert werden. Die Sammlung von persönlichen Daten und die Schaffung von Identifikation-Systemen muss unter Schutzmassnahmen unterstellt werden. Bezüglich Punkt 5: In Art. 16 ZertDV wird auf die geltende Datenschutzgesetzgebung verwiesen.

6. Der Zugang zu geheimen Schlüsseln bei der Verschlüsselung soll nur unter möglichst weitgehender Berücksichtigung der anderen Belange ermöglicht werden; Bezüglich Punkt 6:

7. Es soll klare Haftungsregeln, sei es durch Gesetz oder durch Vertrag, geben; Bezüglich Punkt 7: Eine solche Haftungsregel ist und wird in den legislativen Akten sein.

8. Die Regierungen sollen ihre Kryptopolitiken koordinieren, insbesondere mit dem Ziel, Handelshemmnisse zu vermeiden.[153] Bezüglich Punkt 8: Wie oben gesehen, sind die vorhandenen schweizerischen Vorschriften mit denjenigen der EU kompatibel und diese Feststellung bestätigt, dass die Schweiz die Schaffung der Grundlagen für einen grenzüberschreitenden elektronischen Geschäftsverkehr anstrebt. In der Tat ist die Schweiz in den verschiedenen OECD-Kommitees vertreten und hat immer an supranationale Aktivitäten, wie z.B. auch diejenigen des UNCITRAL, teilgenommen.[154] Aus diesem Grund kann vielleicht die andauernde Verzögerung des schweizerischen Gesetzgebers in dem Erlass von Vorschriften geklärt werden.

Im Lichte des Dargestellten kann bestätigt werden, dass die Schweiz in ihren Regulierungsansätze mit der OECD-Leitlinie kompatibel ist.

Der Rat der OECD hat am 9. Dezember auch die Leitlinien für den Verbraucherschutz im Zusammenhang mit dem elektronischen Geschäftsverkehr erlassen.[155] Auf der OECD-Ministerkonferenz über dem elektronischen Geschäftsverkehr, die im Oktober 1998 in Ottawa stattfand, hatten die dort vertretenen Minister bekräftigt, dass zu vereinbarende Leitlinien zum Verbraucherschutz beim elektronischen Geschäftsverkehr eine

[153] s. FN 126, s. 97-98
[154] s. Rapport OECD sulle nazioni
[155] Leitlinien für den Verbraucherschutz im Zusammenhang mit dem elektronischen Geschäftsverkehr vom 9. Dezember 1999; http://www.oecd.org/dsti//sti/it/consumer/prod/guidelines-de.pdf (da ricontrollare il trattino)

Notwendigkeit seien, und deshalb die OECD aufgefordert, diese Leitlinien noch im Laufe des Jahres 1999 auszuformulieren.
Solche Leitlinien sollten darauf zielen, den Verbrauchern bei Online-Käufen zumindest einen ebenso hohen Schutz zu gewährleisten wie bei Offline-Transaktionen. Sie sollten für die Regierungen, die Unternehmen und die Verbraucher eine wichtige Stütze dabei sein, Verbraucherschutzmechanismen für Online-Transaktionen zu entwickeln und umzusetzen, ohne dass dadurch Handelshemmnisse aufgerichtet werden. Die Leitlinien decken sich weitgehend mit den Verbraucherschutzbestimmungen und –grundsätzen der EU.[156]
Verbraucherschutzbestimmungen betreffend Online-Geschäften sind in der Schweiz gar noch nicht veröffentlicht worden und dem Parlament unterbreitet worden. Wenn die oben ausgeführten Bestimmungen in Kraft treten würden, würde die Schweiz die OECD-Leitlinien mehr oder weniger achten.

4.3.2 UNCITRAL

Die UN-Kommission für internationales Handelsrecht (UNCITRAL: United Nations Commission on International Trade Law) hat am 16. Dezember 1998 ein Modellgesetz für den elektronischen Geschäftsverkehr verabschiedet.[157] Dieses Modellgesetz zielt im Bereich von Handelsaktivitäten auf eine Gleichbehandlung von Kommunikation auf „Papierbasis“ und elektronischer Kommunikation und ist einem funktionalen und in technischer Hinsicht neutralen Ansatz verpflichtet.[158] Das Modellgesetz folgt das „signature-enabling“ Modell.[159] Nach Art. 5 soll kein Dokument nur aufgrund der Tatsache, dass es in Form einer Datennachricht vorliegt, seine Rechtswirkung, Gültigkeit oder Durchsetzbarkeit verlieren.[160] Art. 6 des Modellgesetzes umschreibt die Voraussetzungen, welche an elektronische Mitteilungen im Hinblick auf eine Gleichstellung mit der Schriftform zu stellen sind. Von zentraler Bedeutung ist dabei, dass die Informationen abrufbar bleiben und somit nachträglich auch als Beweis oder Beleg dienen können, was die Verwendung eines dauerhaften Datenträgers impliziert.[161]

[156] IP/99/966 boh! Non so più dove l’ho trovato su internet
[157] s. UNCITRAL General Assembly Resolution 51/162 of 16 Dec 1996; http://www.uncitral.org/english/texts/electcom/ml-ec.htm
[158] s. Gutachten des Bundesamt für Justiz vom 24. November 1998, Digitale Signatur und Privatrecht (Vertragsrecht); 63.46, s. 12
[159] s. Thomas Hoeren, s. 406
[160] s. Thomas Hoeren s. 406
[161] s. FN 137 und FN 136

Die Frage der Gleichstellung elektronischer Signaturen mit der eigenhändigen Unterschrift ist in Art. 7 geregelt. Nach Ziff. 1 buchstabe a soll überall dort, wo ein Gesetz die Signatur einer Person erfordert, dieses Erfordernis durch eine Datennachricht erfüllt werden können, wenn die Datennachricht mittels einer Methode erstellt wurde, bei der der Aussteller der Datennachricht identifiziert werden kann und sichergestellt ist, dass er die in der Datennachricht enthaltenen Informationen in der vorliegenden Art und Weise gebilligt bzw. abgeschickt hat. Nach buchstabe b muss zudem der angewandte Methode in dem Masse zuverlässig sein, wie es in Anbetracht aller äusseren Umständen und Vereinbarungen für die Datennachricht notwendig ist.[162]

Von Art. 7 des Modellgesetzes ausgehend und aufbauend wurden Arbeiten zur Entwicklung einheitlicher Regeln für elektronische Signaturen aufgenommen.[163] Der Entwurf für ein mögliches Modellgesetz für elektronische Signaturen wurde als „Draft Uniform Rules on Electronic Signatures“[164] während des 32. Treffens der Kommission vorgestellt.[165] Zur Zeit ist noch ungewiss, ob die „Uniform Rules“ in einer erweiterte Fassung des Modellgesetzes (z.B. als dritte Teil) einfliessen werden oder ob sie als eigenständiges Gesetz erlassen werden.[166] Dieser Entwurf wurde mehrmals revidiert und die letzte Version wurde während des 36. Treffens der Arbeitsgruppe „Electronic Commerce“, der am 14.-25. Februar 2000 stattfand, ausgearbeitet.[167] Die Draft Uniform Rules on Electronic Signatures folgen das „Hybrid-Modell“. Die Draft Uniform Rules on Electronic Signatures sollen eine einheitliche Gesetzgebung für elektronische Signaturen in den Mitgliedstaaten der Vereinten Nationen ermöglichen.

Die Arbeitsgruppe hat erkannt, dass die Public-Key-Kryptographie im elektronischen Handel eine vorherrschende Rolle übernommen hat, dieser Entwurf aber den Gebrauch und die Entwicklung anderer Authentifizierungstechniken nicht verhindern soll, im Hinblick vor allem auf dem technologieneutralen Ansatz des Modellgesetzes für den elektronischen Geschäftsverkehr. Aus diesem Grunde ist der Entwurf technologieneutral gehalten worden,

[162] s. Thomas Hoeren, s. 406
[163] Dr. Ivo Geis, s. 109
[164] Draft Uniform Rules on Electronic Signatures, A/CN.9/WG.IV/WP.73; http://www.uncitral.org/english/sessions/wg_ec/index.htm#TOP
[165] Thomas Hoeren, Rechtsfragen der digitalen Signatur, s. 415
[166] s. A/CN.9/WG.IV/WP.86, Draft Guide to Enactment of the UNCITRAL Uniform Rules on Electronic Signatures, vom 18 August 2000; http://www.uncitral.org/english/sessions/wg_ec/index.htm#TOP (da ritrovare qua sotto, da rivedere)
[167] s. A/CN.9/WG.IV/WP.84

unterstützt aber dennoch das zur Zeit sicherste Verfahren – die Public Key Infrastructure.[168]

Nach Art. 6 Ziff. 1 kann eine elektronische Signatur die rechtlichen Anforderungen wie eine handschriftliche Unterschrift nur erfüllen wenn sie einen Mindestmass an Sicherheit und Vertrauen erfüllt. Nach Ziff. 3 kann eine sichere elektronische Signatur nur gegeben sein, wenn die folgenden Voraussetzungen erfüllt sind:

- die angewandten Mittel zur Schöpfung der elektronischen Signatur muss ausschliesslich dem Unterzeichner zugeordnet werden können;
- die angewandten Mittel zur Schöpfung der elektronischen Signatur muss unter der alleinigen Kontrolle des Unterzeichner stehen;
- jede Veränderung der elektronische Signatur muss erkennbar sein?;
- wo die Integrität der Informationen geschützt werden muss, muss jede Änderung der Informationen erkennbar sein?

Nach Art. 7 kann ein Organ oder eine staatliche Behörde bestimmen, welche elektronische Signaturen die Anforderungen nach Art. 6 Ziff. 3 erfüllen.

Nach Art. 8 Ziff. 1 buchstabe a muss der Inhaber einer elektronischen Signatur die nötigen Vorkehrungen vornehmen, um eine unerlaubte Anwendung der Vorrichtung zur Erzeugung von elektronischen Signaturen zu vermeiden. Nach Art. 8 Ziff. 1 buchstabe b muss der Inhaber der elektronischen Signatur jeder, der auf die elektronische Signatur vertraut, unverzüglich, auch im Falle eines Verdacht, über die unerlaubte Anwendung der Vorrichtung zur Erzeugung von elektronischen Signaturen. Nach Art. 8 Ziff. 1 buchstabe c muss jeder Inhaber einer elektronischen Signatur aufpassen, dass jede gegebene Auskunft, die den Lebenszyklus des Zertifikats betrifft oder die im Zertifikat selbst ausgewiesen ist, der Realität entspricht.[169]

Die folgenden Bestimmungen betreffen, ohne dies ausdrücklich zu nennen, die Regulierung einer sicheren Public Key Infrastructur.

Da aber die Arbeiten noch im Fluss sind und in jede Sitzung der Arbeitsgruppe die vorgeschlagenen Artikel jedes Mal geändert oder ergänzt werden, ist die der 36. Sitzung sicher nicht die endgültige Fassung.

Im Lichte des oben Ausgeführten kann aber festgestellt werden, dass die Schweiz mit der UNCITRAL Uniform Rules mehr oder weniger kompatibel ist. Die interdepartementale

[168] s. Thomas Hoeren, s. 417

[169] s. A/CN.9/467, Rapport du Groupe de travail sur le commerce électronique sur les travaux de sa trente-sixième session (New York, 14-25 février 2000), 5 avril 2000; http://www.(da ritrovare)

Arbeitsgruppe „DigSig“, eine vom EJPD und vom BAKOM im Jahre 1998 eingesetzte Gruppe, hat bei der Entwicklung ihrer Projekte zur Einführung der digitalen Signatur zur Errichtung einer PKI, im Hinblick auf eine Kompatibilität mit internationalen Harmonisierungsbestrebungen, die internationalen Rechtsvorschriften oder Rechtsvorschläge, wie diejenigen der EU oder des UNCITRAL, immer berücksichtigt.[170]
Es muss einzig kritisiert werden, dass die schweizerischen Regelungen zu wenig technologieneutral sind, weil sie sich zu viel über die digitale Signatur und die Public Key Infrastructur konzentriert.
Man muss aber auch sagen, dass die (auf internationaler Ebene) viel beschworene Technologieneutralität primär ein Schlagwort ist[171] und ihrer Umsetzung wesentlich schwieriger liegt.

5. Schlussfolgerungen

Das Thema der digitalen Signatur kann nicht isoliert behandelt werden. Die digitale Signatur ist nur ein Teilbereich des umfassenden Thema des elektronischen Geschäftsverkehrs, das unsere gut besiedelte Gewohnheiten radikal ändern wird. Internet wird die Geschäftsregeln so ändern, das der gesamte Recht des Vertragsschlusses und des Handels angepasst werden müssen.
Die digitale Signatur und die Informatisierung der Behörde wird auch den Kontakt mit den Verwaltung radikal ändern. Es müssen dafür aber sämtliche Vorschriften des Verwaltungsrechtes, die den Kontakt mit den Behörden regeln. Letztendlich ist der Einsatz der digitalen Signatur nicht dafür, weil er eine sicheren elektronischen Geschäftsverkehr erlaubt, sondern weil auch höhere Effizienz in dem täglichen Geschäftsverwaltung ermöglicht.
Es besteht allerdings das Gefahr, dass es eine Gesellschaft mit zwei Geschwindigkeiten geben wird. Ein Teil der Bevölkerung weiss überhaupt noch nicht war Internet ist. Und das nicht nur unter den älteren. Deswegen hat der Bundesrat eine Bildungsoffensive im Informatikbereich gestartet, um eine Zweiklassengesellschaft zu vermeiden.
Neue Notariatregeln hinzufügen.

[170] s. Yvonne Jöhri, Digitale Signatur: Tagung der Interdepatementalen Arbeitsgruppe “Digitale Signatur1” vom 24. November 1998 in Biel, sic! 1/1999, s. 73 ff.
[171] s. Anhang IV: III. Fragenfolge an Felix Schöbi

Vorgeschlagene Regelungen müssen noch im Vernehmlassungsverfahren gehen. Es können völlig anders auskommen.