Institut für Allgemeine Wirtschaftsforschung

Abteilung für Wirtschaftspolitik

INSTITUTIONELLER RAHMEN DES ELECTRONIC COMMERCE: EINE ORDNUNGSÖKONOMISCHE ANALYSE AM BEISPIEL DER DIGITALEN SIGNATUR

HANSUELI STAMM

01/3

ISSN 1437-1510

FREIBURGER DISKUSSIONSPAPIERE ZUR ORDNUNGSÖKONOMIK

FREIBURG DISCUSSION PAPERS ON CONSTITUTIONAL ECONOMICS

Albert-Ludwigs-Universität Freiburg i. Br.

INSTITUTIONELLER RAHMEN DES ELECTRONIC COMMERCE: EINE ORDNUNGSÖKONOMISCHE ANALYSE AM BEISPIEL DER DIGITALEN SIGNATUR

HANSUELI STAMM

01/3

Universität Freiburg i. Br.

Beitrag zum 2. Workshop „Ordnungsökonomik und Recht“
vom 11. – 13. Oktober 2000 in Heuweiler

FREIBURGER DISKUSSIONSPAPIERE ZUR ORDNUNGSÖKONOMIK
FREIBURG DISCUSSIONPAPERS ON CONSTITUTIONAL ECONOMICS
01/3
ISSN 1437-1510

Albert-Ludwigs-Universität Freiburg im Breisgau; Institut für allgemeine Wirtschaftsforschung; Abteilung für Wirtschaftspolitik; Kollegiengebäude II; Platz der Alten Synagoge; D - 79085 Freiburg i. Br.
Tel. Nr.: +49 +761 / 203 2317; Fax. Nr.: +49 +761 / 203 2322
http://www.vwl.uni-freiburg.de/fakultaet/wipo/wipo.htm

INSTITUTIONELLER RAHMEN DES ELECTRONIC COMMERCE: EINE ORDNUNGSÖKONOMISCHE ANALYSE AM BEISPIEL DER DIGITALEN SIGNATUR

Von Hansueli Stamm, Universität Freiburg i. Br.

Inhalt

1. Einleitung
2. Was ist neu am Electronic Commerce?
3. Ordnungsökonomische Betrachtungsweise
4. Vertrauensprobleme bei digitalen Signaturen
5. Überblick über einige existierende Regulierungsansätze
6. Schlussbemerkungen

   Anhang

Zusammenfassung

Das Paper beschäftigt sich mit dem Auseinanderfallen von Authentizität und Identität bei digitalen Signaturen als einer Quelle von Unsicherheit und den daraus entstehenden Vertrauensproblemen beim elektronischen Handel. Es wird gezeigt, dass diese Vertrauensprobleme dem beim Handel zwischen Unbekannten üblichen Gefangenen-Dilemma-Problem um eine Stufe vorgelagert ist und somit nicht mit den bekannten Institutionen gelöst werden kann. Dennoch kann es im bisherigen institutionellen Rahmen dank dem Entstehen von sog. Zertifizierungsstellen auf rein privater Basis gelöst werden. Trotzdem sind an vielen Orten zur Zeit staatliche Regulierungsbemühungen zu beobachten. Diese haben u.a. zum Ziel, Transaktionen, für deren Gültigkeit Schriftform verlangt wird, dem elektronischen Handel zugänglich zu machen, indem sie entsprechende Standards festgelegt werden, die es ermöglichen sollen, die digitale der handschriftlichen Unterschrift rechtlich gleichzusetzen.

Abstract

Subject of this paper are the problems of trust in electronic commerce that have originated because of the disparity between authenticity and identity of digital signatures. It is shown, that this problem of trust between unknown persons is one step ahead of the usual prisoner-dilemma-problem. It is possible, however, to solve it on a private basis by so called “certification authorities”. Nevertheless, there is a lot of state regulation in the area of digital signature. The respective regulations define standards which have to be met for formal recognition of the equivalence of electronic and handwritten signatures. This is a condition for electronic commerce to be used in contracts for which the written form is required or for using digital signatures as proof in trade disputes in a state court.

1. EINLEITUNG

Keine Zeitung, die nicht fast täglich einen Artikel dazu publiziert[1] und keine Börsendiskussion, bei der es nicht um das Thema geht - Electronic Commerce und Internet sind zur Zeit in aller Munde. Der rasante und anhaltende Fortschritt in der Informationstechnologie führt zu einem spürbaren Wandel in Wirtschaft und Gesellschaft. Distanzen verkürzen sich oder fallen ganz weg, neue Märkte entstehen, andere verschwinden, neue Fähigkeiten und neues Wissen ist gefragt. Diese strukturellen Veränderungen generieren neue Anreizstrukturen und wirken über diese auf unser Verhalten: Der institutionelle Rahmen, in dem wir uns bewegen, ändert sich.

Die grundsätzlichen Prinzipien, die unsere Handlungen motivieren, bleiben jedoch die selben. So ist das Ziel von Handel auch im „E"-Zeitalter das Verwirklichen von möglichen Tauschgewinnen, indem jeder die Güter, bei deren Produktion er komparative Vorteile besitzt gegen jene tauscht, die er zwar benötigt, andere aber günstiger produzieren können. Die Voraussetzung, damit dieser Tausch zustande kommt ist das Vertrauen darauf, dass sich die anderen am Tausch Beteiligten an die Abmachungen halten. Nur wenn der mögliche Gewinn höher ist als die Kosten der Unsicherheit, kommt Handel zustande.

Als neues, elektronisches und offenes[2] Medium eröffnet das Internet dem Handel ganz neue Möglichkeiten. Diese neuen Möglichkeiten werden meist zusammengefasst unter der Bezeichnung „elektronischer Handel oder „Electronic Commerce.[3] Neuheiten, die in eine gewohnte Umgebung „einbrechen", können Unsicherheit verursachen. Unsicherheit wiederum verursacht Kosten und diese Kosten verhindern unter Umständen eine Transaktion. Diese Unsicherheit kann viele Gründe haben, eine davon ist das fehlende Vertrauen in unbekannte Handelspartner aufgrund der Abwicklung der Transaktion über das neue Medium.[4]

---

1 Durchsucht man den Index der Jahresausgaben der Neuen Zürcher Zeitung nach dem Stichwort "Internet", so ergeben sich für das Jahr 1997 genau 1000 Einträge, 1999 sind es bereits knapp doppelt so viele und im Jahr 2000 taucht der Begriff schon über 2700 mal in der NZZ auf.

2 Elektronischer Handel in geschlossenen Netzen, d.h. Netzwerken, die von den beteiligten Unternehmen angelegt wurden und für Dritte nicht zugänglich sind, existiert seit den 60er Jahren (sog. Electronic Data Interchange EDI) (vgl. GREENSTEIN & FEINMAN 2000: Chapter 4).

3 Der Begriff Electronic Commerce wird in der Literatur unterschiedlich definiert (vgl. z.B. OECD 1999:28f, BACHETTA ET AL. 1998:5 oder MESENBOURG 1999). Da es in dieser Arbeit einzig um den Akt des Vertragsschlusses, d.h. um die gemeinsame Willenserklärung der beteiligten Parteien als einem grundlegenden Bestandteil aller Transaktionen (nicht nur) über das Internet geht, wird hier bewusst auf eine Definition von „Electronic Commerce verzichtet. Es wird daher auch nicht unterschieden zwischen den üblichen Kategorisierungen in „business to business" (B2B)- oder „business to consumer" (B2C)-Electronic Commerce.

4 Vertrauensproblem heisst in diesem Zusammenhang konkret, dass ein Vertrag nicht zustande kommen wird, weil bspw. nicht sicher ist, ob die übermittelten Daten nicht verändert wurden, oder nicht klar ist, wer überhaupt der Vertragspartner ist.

Grundsätzlich sind Vertrauensprobleme nichts Neues in der Wirtschaftsgeschichte. Bisher haben sich immer Lösungen gefunden, die diese soweit reduzieren konnten, dass die „bedrohten" Transaktionen trotzdem zustande kommen. Diese Lösungsansätze können grob unterteilt werden in private Lösungen, die spontan unter den Beteiligten entstehen und vom Staat geplante und implementierte Lösungen.

Das auch in Umfragen bestätigte Vertrauensproblem beim Electronic Commerce soll in dieser Arbeit an einem für das Zustandekommen einer elektronischen Transaktion grundlegenden Akt, der digitalen Unterschrift, untersucht werden. Es wird gezeigt, dass durch das Auseinanderfallen von Authentizität und Identität beim elektronischen Signieren ein bisher nicht existierendes Problem für das Aufkommen von Vertrauen entstanden ist und dass dieses Problem im Rahmen der bestehenden staatlichen Regelrahmen durch spontan entstandene Institutionen gelöst werden kann. In einem nächsten Schritt wird das Problem der staatlichen Anerkennung der Äquivalenz von elektronischen und handschriftlichen Signaturen beleuchtet und die Auswirkungen der entsprechenden regulatorischen Ansätze auf die Möglichkeit der spontanen Bildung von gleichwertigen Institutionen besprochen.

2. WAS IST NEU AM ELECTRONIC COMMERCE?

Der Bedarf für eine Änderung am institutionellen Rahmen eines Systems tritt erst auf, wenn der alte Rahmen nicht mehr genügt. Damit ein bestehender Rahmen seine Aufgaben wie insbesondere die Unsicherheitsreduktion nicht mehr erfüllt, muss in seinem Umfeld eine Änderung eingetreten sein, die grösser ist als diejenigen, die aufgrund der zu erwartenden Dynamik des Wirtschaftsprozesses antizipierbar sind, und die durch die Offenheit der bestehenden Regeln „abgefangen" werden. Besteht beim elektronischen Handel tatsächlich der Bedarf an neuen Regeln, so muss vorab gezeigt werden, dass es dabei tatsächlich Probleme gibt, die zuvor, d.h. im herkömmlichen Handel über traditionelle Medien nicht existierten und dass sie sich unter den bestehenden Regeln nicht lösen lassen.

Ziel dieses Abschnittes ist es, mittels Ergebnissen einiger Umfragen zum Thema Electronic Commerce, Elemente zu identifizieren, die von den Befragten als Unsicherheit stiftend wahr-

genommen werden. Daraus können dann Rückschlüsse gezogen werden, was zumindest in der Wahrnehmung der Unternehmen resp. deren Repräsentanten am elektronischen Handel "neu" ist.

In den letzten drei Jahren sind einige Untersuchungen zum Thema Electronic Commerce erschienen, die sich neben den hauptsächlich betriebswirtschaftlichen Erfolgsfaktoren auch mit den zur Zeit noch existierenden Hemmschuhen für das Handeln über das Internet beschäftigen.[5] Auch wenn der Fokus der verschiedenen Arbeiten nicht immer identisch ist, so sind die Resultate bei allen doch recht ähnlich. Ein wichtiger Punkt, der immer wieder genannt wird, sind die fehlenden allgemein üblichen Geschäftsgepflogenheiten.[6] Dabei handelt es sich aber sicherlich nicht um etwas genuin Neues, das einzig auf das elektronische Medium zurückzuführen ist.

Nicht weit hinter dieser Aussage folgen aber Punkte, die direkt auf das Internet Bezug nehmen. Da wird beispielsweise die Beweisbarkeit von Online-Transaktionen, die Gewährleistung der Integrität der übertragenen Informationen oder Probleme mit der Sicherheit von Zahlungen über das Internet genannt. Sehr prominent vertreten sind auch die Vertrauensprobleme mit zunächst unbekannten Web-Teilnehmern sowie – davon nicht unabhängig – Probleme im Zusammenhang mit elektronisch signierten Verträgen.

Wie sind diese Probleme zu gewichten? Wo sind sie einzuordnen? NORTH (1990:34f) unterscheidet drei generelle Formen von Tausch, die sich im Laufe der Zeit entwickelt haben. Seine Aufzählung beginnt mit dem während langer Zeit vorherrschenden persönlichen Tausch, bei dem keine dritte Instanz existiert, die Verträge durchsetzt. Die Kosten der Produktion zu jener Zeit bestehen einerseits aus hohen Transformationskosten aufgrund der geringeren Arbeitsteilung, aber niedrigen Transaktionskosten, da ein Simultantausch mit nur wenig Unsicherheit behaftet ist. Mit der Ausdehnung der Reichweite des Handels u.a. aufgrund von technischen Innovationen im Infrastrukturbereich nehmen dank zunehmender Spezialisierung die Transformationskosten ab. Die Unsicherheit bei einer Transaktion nimmt allerdings wegen der sich laufend vergrös-

[5] Vgl. dazu u.a. die drei hauptsächlich an der Universität Freiburg entstandenen Untersuchungen „Electronic Commerce Enquête I und II“ von MÜLLER & SCHODER (1999) bzw. von EGGS & ENGELERT (2000), sowie die e-Reality 2000 – Studie von STRAUSS & SCHODER (2000). Interessant in diesem Zusammenhang sind aber auch die Arbeiten von KURBEL & TEUTEBERG (1998) oder SMEDINGHOFF (1998).

[6] In der Untersuchung von MÜLLER & SCHODER (1999) haben über 71% der Befragten diesen Punkt als zutreffend eingestuft. Er steht damit an der Spitze von 32 abgefragten potentiellen Hemmnissen für den elektronischen Handel. Bei STRAUSS & SCHODER (2000) befindet er sich immer noch an der Spitze der „zehn wichtigsten Hürden des Electronic Commerce“.

sernden Gruppe der am Handel Beteiligten und der fehlenden staatlichen Institutionen (Durchsetzungsinstanz) zu, [7] was zu hohen Transaktionskosten führt. In der dritten Stufe kommt es dann zum unpersönlichen Tausch mit niedrigen Transformationskosten dank der institutionellen Innovation einer Durchsetzungsinstanz in Form des Nationalstaates mit seinem Gewaltmonopol. Diese institutionelle Neuerung reduziert die Transaktionskosten drastisch.

Wie lässt sich nun der elektronische Tausch in diese Aufzählung einordnen? Durch die neuen Möglichkeiten der Informationsbeschaffung und -verarbeitung verschwindet die Dimension Distanz fast völlig. Die dadurch mögliche weitere Ausdehnung des Marktes im elektronischen Handel[8] lässt eine weitere Reduktion der Transformationskosten erwarten.

Bei den Transaktionskosten ist das Bild nicht so eindeutig. Zwar ist es unbestritten, dass die Vereinfachung des Informationsaustausches Transaktionskosten drastisch reduziert. Auf der anderen Seite aber existieren, wie die Umfragen gezeigt haben, diverse Situationen, die unter den Handeltreibenden zu Unsicherheit führen. Die Transaktionskosten erhöhen sich dadurch u.U. wiederum so weit, dass sie das Zustandekommen eines Tausches verhindern. Dazu kommt, dass Electronic Commerce häufig internationaler Handel ist und bei diesem die bekannten Probleme des unvollständigen Rechtssystems im Aussenhandel zu einer weiteren Erhöhung der Transaktionskosten führen. In der NORTH'schen Systematik bedeutet das Aufkommen von elektronischem Handel im Bereich der Produktionsmöglichkeiten einen weiteren Schritt nach vorne, institutionell aber vorläufig noch ein Zurückfallen auf die zweite Stufe.

3. ORDNUNGSÖKONOMISCHE BETRACHTUNGSWEISE

Ziel dieser Arbeit ist es, am Beispiel der digitalen Unterschrift etwaige institutionelle Defizite, die der bisherige Regelrahmen nicht abzudecken vermag, aufzuzeigen und denkbare und tatsächlich realisierte Lösungsansätze darzustellen. Der theoretische Rahmen, in dem diese Analyse geschehen soll, ist derjenige der Ordnungs- oder Konstitutionenökonomik. Diese ist

[7] Oder noch schlimmer: Der „Staat" wirkte damals eher als zusätzlicher Unsicherheitsfaktor, da sein Verhalten grösstenteils unberechenbar war (vgl. NORTH 1990:35).

[8] Genauer müsste hier die Rede sein vom Handel mit elektronischen, d.h. digitalisierbaren Gütern. Für den Handel mit „traditionellen" Gütern gelten die neuen Möglichkeiten immerhin für die Vertragsvereinbarung (weltweite Informationsmöglichkeiten über unterschiedliche Angebote), die entsprechenden Verhandlungen und den Vertragsabschluss.

bestrebt, in Form von hypothetischen Imperativen Empfehlungen abzugeben, wie ein bestimmtes soziales Problem aus ökonomischer Sicht gelöst werden soll, damit sich ein für die Betroffenen wünschenswertes Resultat abzeichnet. Die Implementation des in einem hypothetischen Imperativ der Form „wenn man X will, sollte man Y tun" Geforderten, bedarf einerseits des Nachweises, dass X im Interesse aller Betroffenen liegt und andererseits, dass Y ein geeignetes Mittel ist, X zu erreichen.[9]

Bei ordnungsökonomischen Empfehlungen gilt es zwischen konsensfähigen und nicht konsensfähigen Interessen zu unterscheiden. Zusätzlich spielt die Unterscheidung zwischen konstitutionellen und subkonstitutionellen Entscheidungen eine wichtige Rolle. Auf der konstitutionellen Ebene wird über die Regeln, nach denen ein „Spiel" gespielt wird, entschieden, auf der subkonstitutionellen über die Spielzüge, die im Rahmen der Regeln möglich sind.[10] Das Ziel einer ordnungsökonomischen Analyse von wirtschaftspolitischen Massnahmen muss ein Urteil darüber sein, ob diese wünschenswert, d.h. im konsensfähigen konstitutionellen Interesse aller Betroffenen sind.

Was heisst das nun konkret für die Probleme des Electronic Commerce, insbesondere das in den Umfragen häufig genannte und im Zusammenhang mit der digitalen Unterschrift entscheidende Vertrauensproblem? Es heisst, dass vom hypothetischen Imperativ „Wenn man die Vertrauensprobleme des elektronischen Handels lösen will, dann muss Massnahme Y ergriffen werden" zunächst gezeigt werden muss, dass die Wenn-Komponente im konsensfähigen konstitutionellen Interesse der Beteiligten liegt und dass anschliessend für Y Empfehlungen abgegeben werden müssen, die aus ordnungsökonomischer Sicht diese Vertrauensprobleme adäquat lösen.

Da aufgrund der möglichen zusätzlichen Ausdehnung des Marktes zu erwarten ist, dass neue Wohlstandsgewinne realisiert werden können, kann davon ausgegangen werden, dass ein Konsens unter allen Beteiligten möglich ist, die neuen institutionellen Probleme des elektronischen Handels in den Griff zu bekommen.

[9] Vgl. VANBERG (1997:709f).
[10] Vgl. VANBERG (1996:11ff).

Zur Beurteilung der zu treffenden Massnahmen kann man sich drei Schritte vorstellen. In einem ersten Schritt muss das konkrete Problem identifiziert werden, das Händler beim Handel über das Internet vor ein so grosses Vertrauensproblem stellt, dass die Transaktion nicht zustande kommt. In einem zweiten Schritt ist die Frage zu beantworten, ob der bestehende Regelrahmen, der die bisherigen Vertrauensprobleme des traditionellen Handels scheinbar befriedigend gelöst hat, nicht auch für die neu entstandene Unsicherheit die Möglichkeit offenlässt, dass sich entsprechende unsicherheitsreduzierende Institutionen bilden können. Besteht diese Möglichkeit, so ist zu erwarten, dass keine Verbesserung der Situation durch neue Regeln stattfindet, da diese höchstens bisher zulässige Handlungsmöglichkeiten einschränken, ohne einen zusätzlichen sicherheitsstiftenden Effekt zu bewirken.[11] Stellt sich eine Anpassung der Regeln als notwendig heraus, so müssen in einem dritten Schritt die vorgeschlagenen neuen Regeln darauf überprüft werden, ob deren Wirkung gemäss bestehendem (ordnungsökonomischen) Wissensstand die Vertrauensprobleme im elektronischen Handel tatsächlich löst.[12]

4. VERTRAUENSPROBLEME BEI DIGITALEN SIGNATUREN

Dieses Kapitel zeigt am Beispiel der digitalen Signatur, dass es beim Electronic Commerce neue Vertrauensprobleme aufgrund des Auseinanderfallens von Authentizität und Identität bei der elektronischen Unterschrift gibt. Es stellt sich heraus, dass zur Überwindung dieses Problems neue institutionelle Lösungen gefunden werden müssen, da die Kosten der Unsicherheit grösser sind als der mögliche Gewinn aus der Transaktion. Es werden verschiedene Lösungsmöglichkeiten aufgezeigt, die sich im Rahmen des existierenden staatlichen Regelrahmens entwickeln könnten sowie die Argumente dargestellt, warum der Staat mit neuen Regeln in diesen Prozess eingreift.

[11] Die rechte Seite des obigen hypothetischen Imperatives bestünde dann also aus einer leeren Menge, d.h. es sind keinerlei Massnahmen zu empfehlen.

[12] Diese Darstellung in drei Schritten ist insofern vereinfacht, als sie die Dynamik des bestehenden Regelrahmens ausblendet. Diese Simplifizierung ist aber gerechtfertigt, da eine Überprüfung i.d.R. kein einmaliges Ereignis darstellt, sondern periodisch oder zu gegebenen Anlässen wiederholt wird.

4.1 Der digitale Vertragsabschluss

Der zentrale Bestandteil einer ökonomischen Transaktion ist der Vertragsabschluss. Dieser kann auf unterschiedliche Arten zustande kommen. Eine wichtige Variante eines solchen Abschlusses ist die schriftliche Fixierung des Vertragsinhaltes, versehen mit der handschriftlichen Unterschrift der beiden bzw. aller Vertragsparteien. Durch diese handschriftlichen Signaturen können die Unterzeichnenden identifiziert und im Falle einer Verletzung der Vertragsbedingungen dafür haftbar gemacht werden. Der Vertragspartner kann also sicher sein, dass die Unterschrift tatsächlich von seinem Geschäftspartner stammt (Authentizität) und dass er diesen auch identifizieren kann. Diese für handschriftliche Signaturen im Grunde unnötige Trennung von Authentizität und Identität ist notwendig, um die Probleme, die mit dem Aufkommen elektronischer Verträge entstanden sind, zu verstehen.

Eine digitale Signatur[13] besteht aus Daten, die dank einer entsprechenden Rechenvorschrift die gesamte zu signierende Meldung repräsentiert[14] und die mit dem privaten Schlüssel[15] des Unterzeichnenden verschlüsselt werden. Sie wird den signierten Daten angehängt.[16]

Dank dieser kryptographischen Verfahren ist es technisch möglich, eine digital signierte Nachricht zweifelsfrei dem privaten Schlüssel zuzuordnen, mit dem sie signiert wurde. Authentizität, d.h. das Feststellen der Herkunft einer Nachricht ist damit sichergestellt. Im Gegensatz zu einer handschriftlichen Unterschrift enthält eine digitale Signatur aber keinerlei Informationen über die Identität des Unterzeichnenden.

---

[13] In dieser Arbeit wird der Ausdruck „digitale Signatur bzw. Unterschrift“ synonym verwendet mit dem Begriff „elektronische Signatur bzw. Unterschrift“. An verschiedenen Orten werden die beiden Begriffe unterschiedlich verwendet, allerdings nicht einheitlich. Insbesondere bei Gesetzestexten wird die digitale Signatur direkt mit der Technik des Public Key-Verfahrens (vgl. Anhang) in Verbindung gebracht. Die elektronische Unterschrift hingegen wird technikneutral definiert (vgl. z.B. den Wechsel des Namens vom alten zum neuen deutschen Signaturgesetzes: das alte heisst „GESETZ ZUR *DIGITALEN* SIGNATUR“, das neue, in Angleichung an die Vorgabe aus Brüssel, „GESETZ ÜBER DIE RAHMENBEDINGUNGEN FÜR *ELEKTRONISCHE* SIGNATUREN“).

[14] Hergestellt werden diese Daten mittels einer sogenannten Hashfunktion, die eine (beliebig lange) Nachricht auf den Informationsgehalt weniger Buchstaben mit an Sicherheit grenzender Wahrscheinlichkeit eindeutig reduziert (s. Anhang).

[15] Seit einiger Zeit existieren in der Kryptographie sogenannte asymmetrische Verschlüsselungsverfahren. Dabei besteht der Schlüssel aus einem privaten und einem öffentlichen Teil. Während der private Schlüssel geheim, d.h. nur dem Besitzer bekannt ist, kann der öffentliche Teil des Schlüssels von jedermann verwendet werden. Eine mit dem privaten Schlüssel verschlüsselte Mitteilung kann mit dem zugehörigen öffentlichen Schlüssel entschlüsselt werden, eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht nur vom Inhaber des privaten Schlüssels (s. Anhang).

Genau diese Lücke zwischen Authentizität und Identität ist es, die eines der neuen Probleme des Electronic Commerce darstellt. Sie ist eine der Ursachen der neu entstandenen Unsicherheit bei Transaktionen über das Internet. Ohne Sicherheit über die Identität und somit die Vertrauenswürdigkeit seines Vertragspartners, wird sich ein Händler auf einen Abschluss nicht einlassen.

4.2 Struktur des Problems: die Authentizitäts-Identitäts - Lücke

Bei Vertrauensproblemen im Bereich des Handels liegt es nahe, die Situation theoretisch auf ein Gefangenendilemma-Problem zurückzuführen, wie dies z.B. im Falle des mittelalterlichen Handels[17] oder bei der modernen lex mercatoria bspw. im Bereich des unvollständigen Rechtssystems im Aussenhandel getan wird.[18] Üblicherweise bieten sich zwei Möglichkeiten an, das Handelsdilemma zu lösen und Austausch auch zwischen sich Unbekannten zu ermöglichen. Entweder existiert eine dritte Instanz (z.B. der Staat mit seinem Gewaltmonopol) der die Durchsetzung von Verträgen garantiert oder es muss sich um ein repetitives Spiel mit hoher Wiederbegegnungswahrscheinlichkeit der Akteure handeln,[19] deren potentieller Reputationsverlust sie negativ sanktionieren würde.

Das Problem der Lücke zwischen Authentizität und Identität (AI-Lücke) einer digitalen Unterschrift ist jedoch dem Gefangenendilemmaproblem um eine Stufe vorgelagert, d.h. bevor die Lösungsmechanismen des Gefangenendilemmas einsetzen können muss sowohl Authentizität als auch Identität aller am Handel Beteiligten gesichert sein. Am einfachsten lässt sich dies am Beispiel eines elektronischen Vertragsabschlusses zeigen, der in einer einzigen Jurisdiktion stattfindet, in der davon ausgegangen werden kann, dass der Staat das Einhalten von Verträgen garantiert, das Gefangenendilemmaproblem somit gelöst wäre. Ist ein Händler zwar sicher über die Authentizität der digitalen Unterschrift unter einem Vertrag, kennt er jedoch die Identität des elektronisch Signierenden nicht, so kann ihm im Falle der Nichterfüllung des Vertrages durch seinen Vertragspartner auch die Durchsetzungsgewalt des Staates nicht helfen, zu seinem Recht zu kommen. Auch der Staat hat keine Möglichkeit aufgrund der digitalen Signatur die Identität des Unterzeichnenden festzustellen. Dieses Problem besteht ebenso im Falle des Lösungsansatzes

---

16 Vgl. die ausführlichere Beschreibung der Entstehungsweise einer digitalen Signatur im Anhang.
17 Vgl. z.B. MILGROM ET AL. (1990).
18 Vgl. z.B. SCHMIDT-TRENZ (1990).
19 Vgl. z.B. NORTH (1990: 55f).

über ein repetitives Spiel, da Reputation personen-(identitäts-)gebunden ist und im Falle ohne lückenschliessende Institution keine Gewähr dafür besteht, dass hinter der (authentischen) Signatur sich bei jeder Transaktion die selbe Person (Identität) verbirgt.

Die Lücke zwischen Authentizität und Identität bei Unterschriften, die mit der Einführung des neuen Mediums Internet auftaucht, stellt somit ein Problem dar, das eine neue Lösung erfordert. Die bisher in Situationen von Unsicherheit aufgrund fehlenden Vertrauens angewandten Reputationsmechanismen oder die Delegation der Lösung an den Staat mit dessen Durchsetzungsmöglichkeiten versagen solange, bis klar ist, wessen Reputation beschädigt ist bzw. bei wem das staatliche Gewaltmonopol ausstehende Forderungen eintreiben kann.

Solange die Lücke zwischen Identität und Authentizität institutionell nicht gefüllt werden kann, ist elektronischer Handel zwischen sich nicht bekannten Partnern nicht zu erwarten. Elektronischer Handel ist aber zu beobachten, was den Schluss nahelegt, dass es Möglichkeiten gibt, die Authentizitäts-Identitäts-Lücke zu schliessen.

4.3 Lösungsansätze

Damit elektronischer Handel überhaupt zustande kommt, muss zunächst die Authentizitäts-Identitäts-Lücke geschlossen werden. Ohne zusätzliche Institution ist dies einzig dann möglich, wenn sich die am Handel Beteiligten gegenseitig kennen. Im elektronischen Handel wäre dies beispielsweise bei Unternehmen gegeben, die bereits vor der „E“-Zeit miteinander im Kontakt standen.[20] Zwar kann mit der Umstellung bestehender Geschäftsbeziehungen auf das neue Medium die Effizienz der zur Verfügung stehenden Ressourcen gesteigert werden, der eigentliche Vorteil des Netzes, den eigenen Markt auszudehnen, ist erst dann möglich, wenn es gelingt, die AI-Lücke mittels geeigneter Institutionen zu schliessen.

Im Bereich des elektronischen Handels sind im Zusammenhang mit der digitalen Unterschrift Zertifizierungsstellen („Certification Authorities“ (CA)) genannte Institutionen entstanden, die

[20] Ein Beispiel aus den B2C-Bereich ist die Einführung von Electronic Banking bei Bankkunden, die bereits ein Konto oder Depot bei der entsprechenden Bank haben.

diese Aufgabe übernehmen, indem sie sogenannte „Public-Key"-Infrastrukturen zur Verfügung stellen.

4.3.1 Privater Lösungsansatz: Public Key - Infrastrukturen

Public Key[21]-Infrastrukturen (PKI) werden von privaten, meist kommerziellen Institutionen angeboten. Es handelt sich dabei um drei zusammengehörige Dienstleistungen: Als erstes werden elektronische Zertifikate[22] ausgegeben, die eine digitale Signatur mit der Identität ihres Inhabers verbindet. Um dies glaubhaft tun zu können, muss diese Institution zweitens eine Form der Registrierung eines neuen Kandidaten für ein Zertifikat anbieten können, die die Identität des Zertifikateinhabers bestätigt (Registration Authority) und schliesslich muss sie eine öffentlich zugängliche Datenbank führen, der die gültigen sowie die abgelaufenen und gesperrten Zertifikate (Revocation List) zu entnehmen sind. Diese drei Funktionen ermöglichen es, die Informationslücke zwischen Authentizität der digitalen Signatur und der Identität des Inhabers prinzipiell zu schliessen.[23, 24]

---

[21] Der Begriff „Public Key" bezeichnet diejenige kryptographische Methode, mit der digitale Signaturen hergestellt werden (siehe Anhang).

[22] Ein Zertifikat ist ein öffentlicher, d.h. für jedermann abfragbarer Datenbankeintrag bei einer Zertifizierungsstelle, der einerseits die Identität des Inhabers des Zertifikates und andererseits den öffentlichen Schlüssel, mit dem die digitale Unterschrift entschlüsselt werden kann, enthält. Zertifikate haben eine bestimmte Güligkeitsdauer und müssen nach deren Ablauf erneuert werden. Verletzt ein Inhaber die Voraussetzungen, die er für die Registrierung erbringen musste, so wird sein Zertifikat in der Datenbank als gesperrt gekennzeichnet.

[23] Neben der reinen „Lückenschliessfunktion" ist es grundsätzlich vorstellbar, dass Zertifizierungsstellen auch als Informationsdrehscheibe zu Lösung des Reputationsproblems bei grossen Gruppen von am Handel Beteiligten auftreten könnten. Dabei würde die Information, die ein Zertifikat über dessen Inhaber enthält, zusätzlich eine Eintragung über dessen früheres „Geschäftsgebaren" enthalten. Bevor ein Händler mit einem anderen einen Vertrag abschliesst, konsultiert er dessen Eintrag und entscheidet dann, ob er mit ihm in Kontakt treten will. Erste Ansätze solcher Institutionen sind bspw. bei Online-Versteigerungen im C2C-Bereich zu beobachten (vgl. z.B. das Feedback-System von eBay.de (http://pages.ebay.de/services/forum/feedback.html)).

[24] Der Typ der „Zertifizierungsinstitution", die dank ihrer eigenen Reputation jemandem bestimmte Informationen bezüglich gewisser Eigenschaften über einen Dritten zukommen lässt, ist nicht neu. Beispiele sind das Handelsregisteramt, das u.a. die Zeichnungsberechtigung der Vertreter von Unternehmen ausweist und auf Anfrage entsprechende „Zertifikate" ausstellt oder das Prüfungsamt einer Universität, das „Zertifikate" in Form von Diplomurkunden ausstellt, die bestätigen, dass der Inhaber einen gewissen Kanon an Qualifikationen besitzt. Der Unterschied solcher bestehender Zertifizierungsinstitutionen zu denjenigen, die das Schliessen der AI-Lücke ermöglichen, ist, dass sie zwar die Informationsbeschaffung erleichtern, Handel oder die Besetzung von offenen Stallen aber auch ohne sie denkbar sind (Reputationsmechanismus bzw. Prüfung der Qualifikationen durch den potentiellen Arbeitgeber). Certification Authorities (CAs), die Public Key-Infrastrukturen anbieten, vereinfachen aber nicht nur das Zustandekommen von Verträgen unter Unbekannten im Internet, sie ermöglichen sie erst. Ohne CAs ist Handel über das neue Medium aufgrund der in Abschnitt 4.2 dargelegten Gründe nicht zu erwarten.

Ein Problem ist durch diese Konstruktion der externen dritten PKI-Institutionen aber noch nicht gelöst. Das Vertrauensproblem ist zwar auf der untersten Ebene verschwunden, damit aber nur um eine Stufe nach oben verschoben worden. Mit anderen Worten: wer garantiert die Vertrauenswürdigkeit der PKI-Anbieter, d.h. der Zertifizierungsstellen?

Vier Lösungsmöglichkeiten sind denkbar:

a) Die Institutionen zertifizieren sich gegenseitig, d.h. der Reputationsverlust der einen Zertifizierungsstelle hinge somit auch vom Ruf der anderen ab.
b) Die Trägerschaft der Institutionen garantiert mit deren Namen für die Reputation der PKI-Institutionen. Die Zertifizierungsstelle „erbt" dadurch den Ruf ihrer Geldgeber.[25]
c) Der Wettbewerb unter den Zertifizierungsstellen und die günstigen und schnellen Informationsmöglichkeiten im Netz (Rating-Agenturen die entsprechende Informationen für Anleger bekanntgeben, wären bspw. denkbar[26]) werden dafür sorgen, dass ein Reputationsverlust für die betroffene Institution grosse negative Auswirkungen nach sich ziehen würde.
d) Die Zertifizierungsstellen gründen eine gemeinsame Institution mit einer Menge von Standards, die für die Mitglieder als verbindlich gelten. Mitglieder, die sich nicht an diese Vorgaben halten, werden ausgeschlossen.

4.3.2 Rolle des Staates

Das mit dem Aufkommen des Electronic Commerce neue Unsicherheitsproblem im Zusammenhang mit der digitalen Signatur ist dank dem Schliessen der Lücke zwischen Authentizität und Identität mittels Zertifizierungsstellen gelöst. Handelsabschlüsse über ein elektronisches Medium – so sollte man meinen – kommen also mit dem bestehenden Regelrahmen aus, die neue Institution „Zertifizierungsstelle" entwickelt sich spontan im schon existierenden Rechtsumfeld. Wozu braucht es dann die in letzter Zeit in den meisten Industriestaaten entstandenen Gesetze, die u.a. die Anforderungen an die digitale Signatur und deren Gültigkeit regulieren?

[25] Ein solches Beispiel ist Swisskey, eine Zertifizierungsstelle, die getragen wird von zwei Schweizer Grossbanken, dem ehemaligen Schweizer Telekom-Monopolisten und einem Zusammenschluss der kantonalen Handelskammern. (Vgl. SWISSKEY 1999).

[26] Dies käme allerdings bereits wieder der Einführung einer weiteren Ebene gleich, auf der theoretisch das selbe Spiel wieder beginnt.

Ein Grossteil möglicher Rechtsgeschäfte sind formfrei abschliessbar, d.h. für deren Rechtsgültigkeit existieren keine besonderen Vorschriften ausser der gemeinsamen Willenserklärung. Diese Formfreiheit gilt für die meisten privatrechtlichen Verträge. Für bestimmte Rechtsvorgänge schreiben die nationalen Rechtsordnungen aber die Schriftform mit eigenhändiger Unterschrift vor.[27] Alle diese Geschäfte können erst dann auf elektronischem Wege abgewickelt werden, wenn die digitale Signatur der handschriftlichen gleichgestellt wird. Dies gilt ebenso für die Anerkennung elektronischer Unterschriften als Beweismittel bei der Beilegung von Handelsstreitigkeiten vor staatlichen Gerichten.[28]

Genau so wie vom Staat an eine handschriftliche Unterschrift formale Ansprüche gestellt werden,[29] damit sie z.B. vor Gericht Gültigkeit besitzt, ist zu erwarten, dass der Gesetzgeber für digitale Unterschriften, die den traditionellen gleichgestellt sein sollen, ebenfalls gewisse Standards aufstellt, die diese erfüllen müssen. Die Rechtfertigung für staatliche Aktivitäten im Bereich der digitalen Signatur besteht also in der formalen Anerkennung der Äquivalenz von elektronischen und handschriftlichen Unterschriften und dem Setzen von Standards, welche digitale Unterschriften für diese Anerkennung erfüllen müssen. In der Praxis sieht das so aus, dass der Staat selbst die digitalen Unterschriften derjenigen Zertifizierungsstellen zertifiziert, die Zertifikate ausstellen, welche den staatlichen Kriterien genügen.

Ein Problem, das mit dem Setzen nationaler Standards immer verbunden ist, ist die Anerkennung in anderen Staaten zugelassener digitaler Signaturen. Das Vertrauensproblem in die „Zuverlässigkeit" der Regulierungen anderer Staaten ist vergleichbar mit demjenigen der Händler über die Vertrauenswürdigkeit der Zertifizierungsstellen. Auch hier sind verschiedene Lösungsmöglichkeiten denkbar:

---

[27] Im deutschen Rechtssystem existieren davon immerhin über 3000 Stück (vgl. KUNER & MIEDBRODT 1999: 6, Fussnote 20).

[28] Ein Beispiel von BAKER & HURST (1998:266) soll dies illustrieren: „Imagine A wishes to sell Blackacre for $5000 and publishes an offer to sell his property to the first person who submits a ‚signed and binding acceptance of this offer.' B accepts the offer using an email and his digital signature. Another bidder then submits a handwritten and hand-signed offer to pay $6000. Is A bound by B's acceptance because it came first? Or can he refuse to accept a digitally signed bid?"

[29] U.a. eben Handschriftlichkeit, im Gegensatz zu einer einkopierten, gestempelten oder gefaxten Unterschrift (vgl. bspw. die entsprechenden deutschen Gesetzesstellen und Gerichtsurteile in KUNER & MIEDBRODT 1999:6).

a) Die Staaten schliessen bilaterale Abkommen untereinander ab, in denen sie ihre staatlich reglementierten elektronischen Unterschriften gegenseitig anerkennen. Die Staaten zertifizieren sich quasi gegenseitig ihre digitalen Signaturen.
b) Die Staaten versuchen ihre Anforderungen international zu koordinieren, z.B. in einer supranationalen Organisation.

4.4 Zusammenfassung

Die Vertrauensprobleme, die aufgrund des Auseinanderfallens von Authentizität und Identität bei der digitalen Signatur entstanden sind, können dank dem Entstehen von privaten Zertifizierungsdiensten gelöst werden. Auch das Problem des Vertrauens in die Zuverlässigkeit dieser Zertifizierungsstellen ist auf privater Ebene mittels der im Kapitel 4.3.1 vorgestellten Mechanismen denkbar und in der Realität auch beobachtbar. Um die neuen Unsicherheitsprobleme aus der Welt zu schaffen reichen die bestehenden Spielregeln aus. Es ist zu erwarten, dass neue Regeln, die diesen Bereich tangieren, keine Mehrheit finden werden.

Es existieren in den bestehenden nationalen Rechtsrahmen jedoch Passagen, in denen für die Gültigkeit einer Transaktion die Schriftform verlangt wird. Um diesen Teil des Handels ebenfalls dem Electronic Commerce zugänglich zu machen, ist eine Änderung des Regelrahmens notwendig:[30] Entweder wird die Verpflichtung zur Schriftlichkeit an allen entsprechenden Stellen aufgehoben, oder die digitale Unterschrift wird der handschriftlichen gleichgesetzt. Unter der (vereinfachenden) Annahme, dass der bisherige Regelrahmen konsenfähig ist, ist zu erwarten, dass die Anerkennung der Äquivalenz von handschriftlicher und elektronischer Unterschrift neu als Regel aufgenommen wird. Abhängig ist die Entscheidung, ob eine solche Regel von allen Beteiligten befürwortet wird, aber von weiteren Faktoren, wie der Diskriminierungsfreiheit der Regel[31] oder der Anerkennung in anderen Rechtssystemen, etc.

[30] Entsprechendes gilt, wie oben beschrieben, bspw. für die Anerkennung von digitalen Signaturen bei Streitfällen vor staatlichen Gerichten.

[31] Eine diesbezüglich nicht konsensfähige Regel stand im ursprünglichen digitalen Signaturgesetz des US-Teilstaates Utah. Dieses beschränkte die Haftung für die vom Staat anerkannten Zertifizierungsstellen. Die nicht staatlich anerkannten Stellen hafteten dagegen voll. Vgl. BAKER & HURST (1998: 268). Die beiden Autoren kommentieren den Sachverhalt treffend: „If Utah´s rule becomes the norm, the freedom to act as a certificate authority without a state license may be illusory."

Im nächsten Kapitel werden in einem groben Überblick drei reale Regulierungsansätze vorgestellt.

5. ÜBERBLICK ÜBER EINIGE EXISTIERENDE REGULIERUNGSANSÄTZE

Die Freigabe des Internets 1991 für private, kommerzielle Anbieter von elektronischen Dienstleistungen war der Startschuss für den Electronic Commerce.[32] Dank der asymmetrischen Verschlüsselungstechnik war es möglich, die Authentizität der übertragenen Daten zu garantieren. Um die Identität des elektronisch Unterzeichnenden sicherzustellen, entstanden Mitte der 90er Jahre die ersten kommerziellen Zertifizierungsdienste. Auch staatliche Stellen realisierten bald, dass dem elektronischen Handel in absehbarer Zukunft eine wichtige Rolle im Wirtschaftsprozess zukommen wird. In diversen Absichtserklärungen taten sie kund, welche Rolle sie bei der Gestaltung des entsprechenden institutionellen Rahmens übernehmen wollen.[33] Seither sind diverse Gesetzgeber aktiv geworden und haben insbesondere im Bereich der digitalen Signaturen neue Regeln erlassen.

Ziel der folgenden Abschnitte ist es nicht, eine detaillierte Analyse der beabsichtigten und tatsächlichen Intentionen und Wirkungen der drei vorgestellten Regulierungsansätze zu machen. Vielmehr soll ein Eindruck vermittelt werden, wie solche Ansätze in der Realität aussehen und welche Dynamik zur Zeit auf diesem Gebiet herrscht. Dazu wird auf diejenigen Regeln bzw. Richtlinien der USA, der EU und Deutschlands, die die elektronische Unterschrift betreffen, ein kurzer Blick geworfen.

5.1 USA

Die US-Administration hat im Juli 1997 ein „Framework for Global Electronic Commerce“ (CLINTON & GORE 1997) veröffentlicht, in dem sie die Prinzipien, nach denen sie mit den gesetzgeberischen Herausforderungen des elektronischen Handels umgehen will sowie konkrete Themen, denen sie sich widmen will, darlegt. Das erste dieser Prinzipien lautet „The private

[32] Vgl. OECD (1999:9).
[33] Vgl. CLINTON & GORE (1997), MITI (1997), EU-KOMMISSION (1997).

sector should lead“ (CLINTON & GORE 1997:2);[34] in den Ausführungen dazu heisst es u.a.: „Innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry” (ebd.).[35]

Erwartungsgemäss klingt auch die entsprechende Passage, in der es um Datensicherheit und digitale Unterschrift geht: „The Administration, in partnership with industry, is taking steps to promote the development of market-driven standards, public-key management infrastructure services and key recoverable encryption products“ (ebd:15).

Mit dem am 30. Juni 2000 von Präsident Clinton unterzeichneten „ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT“ endet der in den USA bisher vorherrschende Wildwuchs von digitalen Signatur-Gesetzen in den einzelnen Teilstaaten.[36] Der Kern des neuen Gesetzes, das ab dem 1. Oktober 2000 gültig ist, ist die Gleichstellung der elektronischen Unterschrift mit der handschriftlichen und das Setzen von Standards, die eine elektronische Transaktion erfüllen muss. Es ersetzt ausserdem allzu restriktive Vorschriften in einigen Teilstaaten, die bspw. eine bestimmte Sicherheitstechnik vorgeschrieben haben. Die Standards, die das Gesetz vom 30. Juni vorschreibt, gehen zu einem guten Teil auf Konzessionen zugunsten von Verbraucherverbänden zurück, die lange gegen das Gesetz opponierten.[37]

5.2 Europäische Union

Auch die EU hat 1997 in einem Grundsatzpapier[38] ihre Absichten bezüglich der Aktivitäten und Prinzipien, die sie im Bereich elektronischer Handel zu unternehmen bzw. zu verfolgen gedenkt, bekannt gegeben. Ziel der Initiative ist „eine kräftige Ankurbelung des elektronischen Geschäfts-

[34] Die restlichen vier lauten: „Governments should avoid undue restrictions on electronic commerce“, „Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce“, „Governments should recognize the unique qualities of the Internet“, „Electronic Commerce over the Internet should be facilitated on a global basis“ (CLINTON & GORE 1997:2f).

[35] Im Bereich des Datenschutzes äussert sich dieses Prinzip beispielsweise folgendermassen: „We [the Administration] believe, that private efforts of industry working in cooperation with consumer groups are prefarable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy“ (CLINTON & GORE 1997:14).

[36] GIDARI ET AL. (1998) sprechen von einem „patchwork of inconsistent state regulation and an absence of standards for the cross-border recognition of electronic signatures.“ Vgl. dazu auch BAKER & HURST (1998).

[37] Vgl. LERNER (2000), EILPERIN & SCHWARTZ (2000).

[38] Vgl. EU-KOMMISSION (1997).

verkehrs in Europa“ (EU-KOMMISSION 1997:6). Dabei will die EU einen aktiven Part übernehmen, indem sie u.a. einen „günstigen ordnungspolitischen Rahmen“ (ebd.:21ff) schafft sowie ein „günstiges unternehmerisches Umfeld“ (ebd.:30ff) fördert. Im Gegensatz zur amerikanischen Absichtserklärung von CLINTON & GORE (1997), sieht die EU ihre Aufgabe neben der Schaffung der ihrer Ansicht nach notwendigen Regeln auch in einer gezielten Förderung des elektronischen Handels bspw. mittels Pilotprojekten.[39]

Die digitale Unterschrift wird an verschiedenen Stellen angesprochen. Wichtig sei ihre rechtliche Anerkennung im Binnenmarkt sowie die Festlegung von Mindestkriterien für Zertifizierungsstellen. Ferner seien weltweite Vereinbarungen über digitale Unterschriften erforderlich (EU-KOMMISSION 1997:27). Die Umsetzung dieser Forderungen erfolgte am 13. Dezember 1999 mit der RICHTLINIE ÜBER GEMEINSCHAFTLICHE RAHMENBEDINGUNGEN FÜR ELEKTRONISCHE SIGNATUREN. Punkt 16 der dem eigentliche Rechtstext vorangestellten Begründungen fasst die wesentlichen Punkte der EU-Richtlinie sehr schön zusammen:

> „Diese Richtlinie leistet einen Beitrag zur Verwendung und rechtlichen Anerkennung elektronischer Signaturen in der Gemeinschaft. Es bedarf keiner gesetzlichen Rahmenbedingungen für elektronische Signaturen, die ausschliesslich in Systemen verwendet werden, die auf freiwilligen privatrechtlichen Vereinbarungen zwischen einer bestimmten Anzahl von Teilnehmern beruhen. Die Freiheit der Parteien, Bedingungen zu vereinbaren, unter denen sie elektronisch signierte Daten akzeptieren, sollte respektiert werden, soweit dies im Rahmen des innerstaatlichen Rechts möglich ist. Elektronischen Signaturen, die in solchen Systemen verwendet werden, sollte rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht abgesprochen werden.“

Die Richtlinie legt in diversen Anhängen u.a. die Anforderungen an qualifizierte Zertifikate und qualifizierte Zertifizierungsdiensteanbieter (Zertifizierungsstellen) fest. Erfüllt ein Zertifikat diese Anforderungen, so muss der entsprechenden Signatur die selbe Rechtswirkung zugestanden werden, wie einer handschriftlichen. Erfüllt eine Zertifizierungsstelle die entsprechenden Bedingungen, so ist sie berechtigt, qualifizierte Zertifikate auszugeben. Zusätzlich muss bei der Anerkennung ausländischer Signaturen (aus dem EU-Raum) das Herkunftslandprinzip beachtet werden, d.h. eine elektronische Unterschrift, die in einem anderen EU-Land als qualifiziert gilt,

[39] So heisst es bspw. auf der Seite 31: „Pilotprojekte zur Ermittlung der besten Verfahren spielen eine wichtige Rolle im Hinblick darauf, die Unternehmen auf die neuen Möglichkeiten aufmerksam zu machen.“

muss auch im eigenen Land als solche akzeptiert werden.[40] Über den Umgang mit entsprechenden elektronischen Unterschriften aus Nicht-EU-Ländern macht die Richtlinie keine verbindlichen Aussagen.

In die Richtlinie, die bis Mitte 2001 von den Mitgliedern umgesetzt werden muss, sind die bisherigen Erfahrungen der nationalen Gesetzgebungen eingeflossen. Insbesondere Länder mit relativ restriktiven Regelungen werden ihre Gesetze der relativ liberalen Vorgabe aus Brüssel anpassen müssen.[41]

5.3 Deutschland

Deutschland besitzt eines der „ältesten" Gesetze zur Regelung der digitalen Signatur (SIGG). Es besteht aus Artikel 3 des GESETZES ZUR REGELUNG DER RAHMENBEDINGUNGEN FÜR INFORMATIONS- UND KOMMUNIKATIONSDIENSTE vom 22. Juli 1997 und der daraus abgeleiteten VERORDNUNG ZUR DIGITALEN SIGNATUR (SIGV) vom 23. Oktober des selben Jahres. Zweck des Gesetzes gemäss § 1 Absatz 1 ist es, „Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten [...]."

Charakteristikum des deutschen Signaturgesetzes ist die in § 4 verankerte Genehmigungspflicht für den Betrieb einer Zertifizierungsstelle.[42] Zuständige Behörde ist die REGULIERUNGSBEHÖRDE FÜR TELEKOMMUNIKATION UND POST (REG TP). Nur wer die restriktiven Kriterien im Bereich Personal, technische Komponenten und Sicherheit erfüllt, kann mit einer entsprechenden Bewilligung der REG TP rechnen.[43] Im Gegenzug zertifiziert diese dann das höchste Zertifikat der antragstellenden Institution.

Die deutsche Regelung krankt an dem Umstand, dass es zwar die Möglichkeit gibt, staatlich anerkannte Zertifikate anzubieten bzw. zu erwerben, die entsprechenden Signaturen vom selben Staat aber noch nicht den Handschriftlichen gleichgestellt sind. Dieser mangelnde Anreiz zum Einsatz

[40] Vgl. Artikel 7 Abs. 1.
[41] Vgl. BAKER & YEO (1999:13) bzw. Abschnitt 5.3.
[42] § 4 Abs1 SIGG: „Der Betrieb einer Zertifizierungsstelle bedarf einer Genehmigung der zuständigen Behörde. Diese ist auf Antrag zu erteilen."
[43] Vgl. die entsprechenden Vorgaben im SIGG und der SIGV sowie REG TP (o.J.: 12).

elektronischer Unterschriften, gepaart mit sehr restriktiven Vorgaben für das Betreiben einer Zertifizierungsstelle, mögen Ursache dafür sein, dass es bisher erst drei vom Staat zugelassene Zertifizierungsstellen gibt.[44] Trotz der de facto Genehmigungspflicht[45] bieten aber weitere Unternehmen[46] Zertifikate für digitale Signaturen an, weisen ihre Kunden allerdings darauf hin, dass diese (noch) nicht gesetzeskonform seien. Dabei verweisen sie u.a. auf die bis Mitte 2001 umzusetzende EU-Richtlinie, bei deren Umsetzung ihr Produkt „legal" würde.

Ein erster Schritt in Richtung dieser Öffnung ist für das erste Halbjahr 2001 geplant. Am 16. August 2000 verabschiedete das Bundeskabinett den Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen, das im Herbst vom Bundestag beschlossen werden soll. Im Bestreben, die Vorgaben der EU-Richtlinie zu erfüllen, senkt es die Ansprüche an die elektronische Unterschrift und hebt die Genehmigungspflicht für Zertifizierungsstellen auf. U.a. ist auch das in der EU übliche Herkunftslandprinzip für die Anerkennung ausländischer elektronischer Unterschriften in das Gesetz neu aufgenommen worden. Was in Deutschland aber auch nach der Inkraftsetzung des neuen SigG noch immer fehlt, gemäss der EU-Richtlinie aber umzusetzen ist, ist die Anerkennung der Äquivalenz von handschriftlicher und elektronischer Unterschrift. Ein Gesetzesentwurf zur Anpassung der Formvorschriften des Privatrechts an den elektronischen Geschäftsverkehr ist in Arbeit.[47]

6. SCHLUSSBEMERKUNGEN

Auf privater Ebene steht dem Handel über das Internet in Bezug auf die Sicherheit über die Identität des Transaktionspartners institutionell nichts mehr im Wege. Hohe Informationskosten bezüglich der sich rasant entwickelnden Technik und der Anwendung der neuen Möglichkeiten, dürften zur Zeit in diesem Bereich die wichtigsten Gründe sein, die eine Unternehmung noch

[44] Die Zertifizierungsstelle der Deutschen Telekom AG (http://www.telesec.de/), diejenige der Deutschen Post (http://www.signtrust.de/start.htm/) sowie eine der Bundesnotarkammer (http://www.bnotk.de/). Die ersten beiden verwalten zusammen nur 20´000 Zertifikate (vgl. KRÄGENOW (2000). Verisign, die in den USA domizilierte Marktführerin im Bereich digitaler Zertifikate, bringt es immerhin auf 4 Millionen Zertifikate (vgl. http://www.verisign.com/about/index.html).

[45] Das deutsche SIGG bietet für das Betreiben nicht genehmigter Zertifizierungsstellen in § 1 Abs. 2 auch ein „Schlupfloch": „Die Anwendung anderer Verfahren für digitale Signaturen ist freigestellt, soweit nicht digitale Signaturen nach diesem Gesetz durch Rechtsvorschrift vorgeschrieben ist." BAKER & YEO (1999:13, insbesondere Fussnote 15) verweisen aber auf einen Widerspruch mit §13 Abs. 4, so dass §1 Abs. 2 gar nicht zur Geltung kommen kann.

[46] Ein Beispiel ist die Firma TC TrustCenter GmbH in Hamburg (http://www.trustcenter.de/).

vom Einstieg in den Electronic Commerce abhält. Die in den im Kapitel 2 vorgestellten Umfragen am häufigsten genannten fehlenden üblichen Geschäftsgepflogenheiten sind ein Teil dieser hohen Informationskosten.

Auf der Seite der staatlichen Regulierungen ist zur Zeit eine „Phase der Konsolidierung" im Gange. In der EU und in den USA werden die individuellen staatlichen Gesetze zur digitalen Signatur mittels zentraler Richtlinien koordiniert. Der Wettbewerb um die geeignetste Lösung wird damit nicht aufgehoben, sondern zumindest teilweise um eine Stufe nach oben verlagert.[48] Es ist zu erwarten, dass dieser Prozess der Suche nach geeigneten Regeln auf staatlicher Ebene parallel mit der technischen Entwicklung weitergeht.[49] Dass aber ein Regelrahmen, der sich ständig ändert, keine optimale Voraussetzung ist, Rechtssicherheit und somit Vertrauen unter den davon Betroffenen zu schaffen, ist naheliegend. Auch hier ist also die momentane Skepsis vieler potentieller Teilnehmer am Electronic Commerce verständlich.

Die institutionellen Voraussetzungen für den „Durchbruch" eines sicheren Handels über das Internet sind also theoretisch vorhanden. In absehbarer Zeit ist somit – um auf NORTH's dreistufige Entwicklung des Tausches aus Abschnitt 2 zurückzukommen – auch im Bereich des Electronic Commerce die dritte Stufe mit niedrigen Produktions- *und* niedrigen Transaktionskosten erreicht.

Wie geht es weiter? Was heute noch umständlich und kompliziert klingt, wird in absehbarer Zeit eine Selbstverständlichkeit sein. Der Regelrahmen wird sich festigen, die Geschäftsgebräuche einspielen. Es wird eine spannende Aufgabe bleiben, diesen Prozess auf allen Ebenen weiter zu verfolgen.

---

47 Vgl. Die Pressemitteilung des BUNDESMINISTERIUMS FÜR WIRTSCHAFT UND TECHNOLOGIE vom 16. August 2000.

48 Vgl. zum Standortwettbewerb um einen geeigneten Regelrahmen für den Electronic Commerce z.B. die Passage in der Europäischen Initiative für den elektronischen Geschäftsverkehr (EU-KOMMISSION 1990: 3): „Europas grösste Konkurrenten haben die Möglichkeit des elektronischen Geschäftsverkehrs bereits entschlossen genutzt. So haben sich die USA einen beachtlichen Vorsprung verschafft." Ähnlich klingt es in einem entsprechenden Papier des japanischen Handels- und Industrieministeriums: „However [...] the introduction of electronic commerce in Japan lags behind those efforts of the United States in particular, due to restrained investment in information technology after the bursting of the economic bubble" (MITI 1997:1).

49 In der Schweiz gilt seit dem 1. Mai 2000 eine VERORDNUNG ÜBER DIENSTE DER ELEKTRONISCHEN ZERTIFIZIERUNG, die in ihrem Artikel 1 explizit als „Versuchsregelung" bezeichnet wird. Die Absicht des Gesetzgebers ist, damit Erfahrungen zu sammeln, die in ein für später geplantes Gesetz, dessen Entwurf sich zur Zeit (Januar 2001) in der Vernehmlassung befindet, einfliessen sollen.

ANHANG

Die direkt Internet-bezogenen Sicherheitsprobleme lassen sich in vier Kategorien unterteilen:[50]

- **Vertraulichkeit (Confidentiality)**

  Nachrichten, die über das Netz verschickt werden und vertraulichen Inhalts sind, müssen vor der Einsicht Unbefugter geschützt werden.

- **Unversehrtheit (Integrity)**

  Durch die Garantie der Unversehrtheit der Daten soll sichergestellt werden, dass die Meldung, die vom Sender abgeschickt wurde mit derjenigen identisch ist, welche beim Empfänger eintrifft, d.h. dass sie von niemandem „unterwegs" verändert wurde.

- **Authentiziät (Authenticity)**

  Beim Austausch von elektronischen Meldungen ist es von entscheidender Bedeutung zu wissen, ob der Absender auch tatsächlich derjenige ist, den er vorgibt zu sein, d.h. seine Identität muss verifizierbar sein.

- **Nichtabstreitbarkeit (Non-Repudiation)**

  Es muss verhindert werden, dass die Existenz einer Verpflichtung trotz deren tatsächlichen Vorhandenseins, abgestritten werden kann. Es muss also sichergestellt werden, dass eine Nachricht tatsächlich versandt wurde (proof of origin), was verhindert, dass der Sender später behaupten kann, den Auftrag nie erteilt zu haben. Dann muss der Empfänger bestätigen, die Nachricht erhalten zu haben (proof of receipt), um für eine allfällige Nichtausführung des Auftrages haftbar gemacht werden zu können. Schliesslich braucht es noch einen „proof of content", mit dem belegt werden kann, was genau in der Meldung gestanden hat.

In einem ersten Schritt sind diese Probleme technisch durch Verschlüsselung der zu übermittelnden Daten zu lösen. Dabei werden diese mittels eines mathematischen Algorithmus in eine Form gebracht, die nur noch von demjenigen in den Ursprungszustand versetzt werden kann, der die entsprechenden Schlüssel dazu besitzt. Man unterscheidet zwischen symmetrischer und asymmetrischer Verschlüsselung, letztere besser bekannt unter der Bezeichnung "public key"-Verfahren.[51]

---

[50] Vgl. z.B. GREENSTEIN & FEINMANN (1999: 228f).

[51] Unabhängig von der Art der Verschlüsselung, gilt die Länge des Schlüssels (ausgedrückt in Bit) als Mass für deren Sicherheit. Je schneller die Computerhardware, desto länger muss der Schlüssel sein, um den Rechenaufwand für das Entschlüsseln ohne Kenntnis des Schlüssels so gross werden zu lassen, dass sich dieser nicht mehr lohnt. Zur Zeit (2001) gelten 128 Bit-Verschlüsselungen als sicher.

Bei **symmetrischen Verschlüsselungsverfahren** wird für die Verschlüsselung und die Entschlüsselung der selbe Schlüssel benutzt. Das Problem bei der symmetrischen Verschlüsselung ist der sichere Austausch der Schlüssel.

Bei der **asymmetrischen Verschlüsselung** fällt der Schlüssel in einen privaten, d.h. geheimen (private key) und einen öffentlichen, jedermann zugänglichen Teil (public key) auseinander. Will nun der Sender dem Empfänger eine vertrauliche Nachricht übermitteln, so verschlüsselt er diese mit dem öffentlichen Schlüssel des Empfängers und übermittelt sie an diesen. Die so verschlüsselte Nachricht ist nur noch mit dem zum öffentlichen Schlüssel gehörigen privaten Schlüssel zu entziffern. Der Empfänger entschlüsselt also den bei ihm eingetroffenen verschlüsselten Text mit dem privaten, nur ihm bekannten Teil seines Schlüssels.

Durch die Verschlüsselung einer Nachricht mit dem öffentlichen Teil eines Schlüssels kann **Vertraulichkeit** hergestellt werden, da sichergestellt ist, dass nur der Besitzer des privaten Teils des entsprechenden Schlüssels die Mitteilung entschlüsseln kann.

Werden die Schlüssel in umgekehrter Reihenfolge benutzt, d.h. wird die Meldung vom Sender mit seinem privaten Schlüssel verschlüsselt, so ist (zumindest technische) **Authentizität** gewährleistet, da es niemand anderen gibt, der eine verschlüsselte Nachricht erstellen könnte, die mit dem entsprechenden öffentlichen Teil des Schlüssels entschlüsselt werden könnte. Die Vertraulichkeit ist dann aber nicht mehr gewährleistet, da die verschlüsselte Nachricht mit dem öffentlichen Schlüssel von jedermann entschlüsselt werden kann.

Die verbreitetste Methode, die **Unversehrtheit** der Daten zu gewährleisten, ist das sogenannte Hashing. Dabei wird die gesamte Mitteilung mittels einer geeigneten Rechenvorschrift in einen Hash-Wert abgebildet.[52] Dieser Wert wird an die eigentliche Nachricht angehängt und zusammen mit dieser übermittelt. Nach dem Eintreffen der Meldung, wird der Hash-Wert ein zweites Mal, diesmal vom Empfänger berechnet. Stimmen der übermittelte und der berechnete Wert überein, so kann davon ausgegangen werden, dass die Meldung nicht verändert wurde.

Durch geeignete Kombinationen der oben beschriebenen Verfahren auf die zu versendenden Daten kann ein Grossteil der eingangs beschriebenen Probleme beseitigt werden (vgl. Tabelle 1). Von besonderer Bedeutung ist dabei die sogenannte digitale Unterschrift.

Sicherheitsproblem	Verschlüsseln (Sender)	Entschlüsseln (Empfänger)	
Vertraulichkeit	Öffentlicher Schlüssel des Empfängers	Privater Schlüssel des Empfängers	
Unversehrtheit	Berechnung des Hashwertes	Berechnung des Hashwertes und Vergleich	} Digitale Unterschrift
Authentizität	Privater Schlüssel des Senders	Öffentlicher Schlüssel des Senders	
Nichtabstreitbarkeit[53]	Generieren der digitalen Unterschrift	Entschlüsseln der digitalen Unterschrift	

Tabelle 1: Anwendung kryptographischer Verfahren als Beitrag zur Lösung von Sicherheitsproblemen beim Electronic Commerce

Um eine **digitale Unterschrift** zu generieren wird in einem ersten Schritt der Hashwert der Meldung erstellt. Als zweites wird diese Prüfziffer mit dem privaten Schlüssel des Senders verschlüsselt. Das Resultat dieses Vorganges ist dann die digitale Unterschrift, eine einmalige Kombination des Inhalts einer Meldung mit dem privaten Schlüssel des Senders. Der Empfänger berechnet ebenfalls als erstes den Hashwert der eingetroffenen Nachricht. Dann entschlüsselt er die zusammen mit der Nachricht eingetroffene digitale Unterschrift mit dem öffentlichen Schlüssel des Senders und erhält dadurch den Hashwert, den die Nachricht beim Sender repräsentierte. Stimmen die beiden Hashwerte überein, so kann der Empfänger sicher sein, dass die Mitteilung tatsächlich mit dem privaten Schlüssel des Sender verschlüsselt wurde (Authentizität) und ihr Inhalt nicht verändert wurde (Unversehrtheit).[54]

[52] Dieser Hash-Wert, auch „digitaler Fingerabdruck“ genannt, ist 128 Bit lang, was dem Informationsgehalt von 16 Buchstaben entspricht. Ändert sich nur ein einziges Bit in der gesamten Nachricht, so verändert sich auch der berechnete Hashwert.

[53] Zusätzlich können hier zum Beispiel sogenannte „Timestamps“ eingesetzt werden, die die exakte Versendungs- und Eintreffenszeit dokumentieren oder „Confirmation Services“, die das Eintreffen automatisch bestätigen.

[54] Ist zusätzlich Vertraulichkeit gefordert, muss die gesamte Meldung zusätzlich vom Sender mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden. Die erneute Verschlüsselung der digitalen Unterschrift ist nicht notwendig, da vom Hashwert nicht auf den Inhalt geschlossen werden kann.

BACCHETTA, MARC; LOW, PATRICK; MATTOO, AADITYA; SCHUKNECHT, LUDGER; WAGNER, HANNU; WEHRENS, MADELON (1998): Electronic Commerce and the Role of the WTO. Special Studies 2. Geneva: WTO.

BAKER, STEWART A. & HURST, PAUL R. (1998): The Limits of Trust: Cryptography, Governments, and Electronic Commerce. The Hague: Kluwer International.

BAKER, STEWART & YEO, MATTHEW (1999): Survey of International Electronic and Digital Signature Initiatives. Internet Law & Policy Forum (ILPF) (http://www.oecd.org/dsti/sti/it/secur/act/wksp_ilpf.pdf).

BUNDESMINISTERIUM FÜR WIRTSCHAFT UND TECHNOLOGIE (2000): Pressemitteilung vom 16. August 2000. (http://www.bmwi.de/presse/2000/0816prml.html).

CLINTON, WILLIAM J & GORE ALBERT (1997): Framework for Global Electronic Commerce. Washington. (http://www.ecommerce.gov/framewrk.htm).

EGGS, HOLGER & ENGELERT, JÜRGEN (2000): Electronic Commerce Enquête 2000. Empirische Untersuchung zum Business-to-Business Electronic Commerce im deutschsprachigen Raum. Computer Zwitung, Leinfelden-Echterdingen; Institut für Informatik und Gesellschaft, Albert-Ludwigs-Universität Freiburg.

EILPERIN, JULIET & SCHWARTZ, JOHN (2000): "Electronic Signature Bill Passes the House." The Washington Post, 15. Juni 2000.

EU-KOMMISSION (1997): Europäische Initiative für den elektronischen Geschäftsverkehr vom 14.4.1997. (http://www.cordis.lu/esprit/src/ecomcom.htm).

GIDARI, ALBERT; MORGAN, JOHN P.; COIE, PERKINS (1998): Update: Survey of Electronic and Digital Signature Legislative Initiatives in the United States. Internet Law and Policy Forum. (http://www.ilpf.org/digsig/update.pdf).

GREENSTEIN, MARILYN & FEINMAN, TODD M. (2000): Electronic Commerce. Security, Risk Management and Control. Boston: Mc Graw Hill.

KRÄGENOW, TIMM (2000): "Bundesregierung fördert die digitale Unterschrift." Financial Times Deutschland, 16. August 2000.

KUNER, CHRISTOPHER & MIEDBROD, ANJA (1999): Written Signature Requirments and Electronic Authentication: A Comparative Perspective (http:/www.oecd.org/dsti/sti/it/secur/act/wksp_kuner.pdf).

KURBEL, KARL & TEUTEBERG, FRANK (1998): Betriebliche Internet-Nutzung in der Bundesrepublik Deutschland - Ergebnisse einer empirischen Untersuchung. Arbeitsbericht des Lehrstuhls für Wirtschaftsinformatik der Europa-Universität Viadrina, Frankfurt (Oder).

LERNER, DAN (2000): "E-Signature Given Legal Status." Financial Times, 14. Juni 2000.

MESENBOURG, THOMAS L. (1999): Measuring Electronic Business: Definitions, Underlying Concepts, and Measurement Plans. US Census Bureau. (http://www.census.gov/epcd/www/ebusines.htm).

MILGROM, PAUL R.; NORTH, DOUGLASS C.; WEINGAST, BARRY R. (1990): "The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs." Economics and Politics, Vol. 2, 1 - 23.

MITI (1997): Towards the Age of the Digital Economy. For Rapid Progress in the Japanese Economy and World Economic Growth in the 21st Century. (Draft). Ministry of International Trade and Industry, Japan. (http://www.miti.go.jp/intro-e/a228101e.htm bzw. http://www.gip.jipdec.or.jp/~hirai/fujimori/digital02-e.html).

MÜLLER, GÜNTER & SCHODER, DETLEF (1999): Electronic Commerce - Hürden, Entwicklungspotential, Konsquenzen. Ergebnisse aus der Electronic Commerce Enquête. Arbeitsbericht Nr. 137 des Instituts für Informatik und Gesellschaft/Telematik der Universität Freiburg i. Br.

NORTH, DOUGLASS C. (1990): Institutions, Institutional Change and Economic Performance. New York: Cambridge University Press.

OECD (1999): The Economic and Social Impact of Electronic Commerce. Preliminary Findings and Research Agenda. Paris: OECD.

REGTP (o.J.): Die digitale Signatur. Regulierungsbehörde für Telekommunikation und Post (http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/10.pdf).

SCHMIDT-TRENZ, HANS-JÖRG (1990): Aussenhandel und Territorialität des Rechts. Grundlegung einer Neuen Institutionenökonomik des Aussenhandels. Baden-Baden: Nomos.

SMEDINGHOFF, THOMAS J. (1998): ABA/ACCA Survey of Electronic Commerce Practices. Summary of Results. American Bar Association, Science and Technology Section, (http://www.abanet.org/scitech/abbaacca.html).

STRAUSS, RALF & SCHODER, DETLEF (2000): e-Reality 2000 - Electronic Commerce von der Vision zur Realität. Status, Entwicklung, Erfolgsfaktoren und Management-Implikationen des Electronic Commerce. Consulting Partner Group GmbH, Frankfurt.

SWISSKEY (1999): Certification Practice Statement. (http://www.swisskey.ch/pdf/cps2.1_d.pdf).

VANBERG, VIKTOR J. (1996): Ökonomische Rationalität und politische Opportunität. Zur praktischen Relevanz der Ordnungsökonomie. Lectiones Jenenses. Heft 8. Jena: Max-Plank-Institut zur Erforschung von Wirtschaftssystemen.

VANBERG, VIKTOR J. (1997): "Die normativen Grundlagen von Ordnungspolitik." ORDO, Vol. 48, 707 - 726.

VERISIGN (1999): Certification Practice Statement. (https://www.verisign.com/repository/CPS1.2/CPS1.2.pdf).

Gesetzestexte

Deutschland:

GESETZ ZUR DIGITALEN SIGNATUR (SIGG) vom 22. Juli 1997

VERORDNUNG ZUR DIGITALEN SIGNATUR (SIGV) vom 22. Oktober 1997

ENTWURF EINES GESETZES ÜBER DIE RAHMENBEDINGUNGEN FÜR ELEKTRONISCHE SIGNATUREN UND ZUR ÄNDERUNG WEITERER VORSCHRIFTEN in der Fassung des Kabinettsbeschlusses vom 16. August 2000.

EU

RICHTLINIE ÜBER GEMEINSCHAFTLICHE RAHMENBEDINGUNGEN FÜR ELEKTRONISCHE SIGNATUREN vom 13. DEZEMBER 1999.

Schweiz

VERORDNUNG ÜBER DIENSTE DER ELEKTRONISCHEN ZERTIFIZIERUNG vom 12. April 2000.

USA

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT vom 30. Juni 2000.

FREIBURGER DISKUSSIONSPAPIERE ZUR ORDNUNGSÖKONOMIK
FREIBURG DISCUSSION PAPERS ON CONSTITUTIONAL ECONOMICS

98/1 **Vanberg, Viktor J.**: Markets and Regulation – On the Contrast Between Free-Market Liberalism and Constitutional Liberalism. Published in: Constitutional Political Economy Vol. 10 No. 3, October 1999, p. 219 - 243.

98/2 **Pejovich, Svetozar**: Toward a Theory of the Effects of the Interaction of Formal and Informal Institutions on Social Stability and Economic Development.

99/1 **Vanberg, Viktor J.**: Standortwettbewerb und Demokratie.

99/1A **Vanberg, Viktor J.**: Globalization, Democracy and Citizens' Sovereignty: Can Competition Among Governments Enhance Democracy? Published in: Constitutional Political Economy, Vol. 11, No. 1, March 2000, p. 87-112.

99/2 **Vanberg, Viktor J.**: Ordnungsökonomik und Ethik. Zur Interessenbegründung von Moral. Veröffentlicht in: B. Külp, V. J. Vanberg (Hrsg.): Freiheit und wettbewerbliche Ordnung, Haufe Verlagsgruppe: Freiburg, Berlin, München, 2000, S. 579-605.

99/2A **Vanberg, Viktor J.**: Constitutional Economics and Ethics – On the Relation Between Self-Interest and Morality.

99/3 **Cassel, Susanne**: Die Rolle von Think Tanks im US-amerikanischen Politikberatungs-prozess.

00/1 **Sideras, Jörn**: Systems Competition and Public Goods Provision. Published in: Jahrbuch für Neue Politische Ökonomie, Band 19, Tübingen: Mohr Siebeck, 2000, S. 157 - 178.

00/2 **Vanberg, Viktor J.**: Markets and the Law.

00/3 **Vanberg, Viktor J.**: F.A. von Hayek.

00/4 **Vanberg, Viktor J.**: Der konsensorientierte Ansatz der konstitutionellen Ökonomik. Veröffentlicht in: H. Leipold, I. Pies (Hrsg.): Ordnungstheorie und Ordnungspolitik - Konzeptionen und Entwicklungsperspektiven, Schriften zu Ordnungsfragen der Wirtschaft, Band 64, Stuttgart, 2000, S. 251-276

00/5 **Vanberg, Viktor J.**: Functional Federalism: Communal or Individual Rights? On B. S. Frey's and R. Eichenberger's Proposal for a "New Federalism". Published in: KYKLOS, Vol. 53, 2000, p. 363-386

00/6 **Zoll, Ingrid:** Zwischen öffentlicher Meinung und ökonomischer Vernunft: Individuelle Meinungen über Globalisierung und Wettbewerb.

01/1 **Sideras, Jörn:** Konstitutionelle Äquivalenz und Ordnungswahl.

01/2 **Märkt, Jörg:** Knut Wicksell: Begründer einer kritischen Vertragstheorie?

01/3 **Hansueli Stamm:** Institutioneller Rahmen des Electronic Commerce: Eine ordnungs-ökonomische Analyse am Beispiel der digitalen Signatur.