Universität Konstanz

Fakultät für Verwaltungswissenschaft

Diplomarbeit

Institutionelle Aspekte der Vertrauensbildung bei Zahlungssystemen im Internet

Verfasser: Martin Schädler
Mangoldstr. 24
78462 Konstanz
martin.schaedler@sap.com

1. Gutachter: Prof. Dr. Rainer Kuhlen

2. Gutachter: Dr. Joachim Wolf

Konstanz, im Oktober 1999

„Business is built on trust.
Eye contact.
Firm handshakes.
Bold signatures on the dotted line.“

(Lee Bruno)

Abstract

Seit Anfang der 90er Jahre nimmt die Nutzung des Internets für kommerzielle Transaktionen stetig zu. Mittlerweile ist es möglich, Güter und Dienstleistungen über das Internet zu bezahlen. Weil das Internet ein offenes und damit unsicheres Netzwerk ist, sind potentielle Anwender aufgrund von Sicherheitsbedenken gerade im sensiblen Bereich finanzieller Transaktionen zögerlich, Internet-Zahlungssysteme einzusetzen. Selbst wenn diese Zahlungssysteme nach heutigen Erkenntnissen als sicher gelten können, fehlt dem Massenpublikum in der Regel das notwendige Wissen, um diese Sicherheit selbst zu beurteilen. Vertrauen kann hier mangelndes Wissen kompensieren und dadurch die Akzeptanz von Internet-Zahlungssystemen erhöhen. Internet-Zahlungssysteme sind jedoch eine neue Transaktionsform, die bislang nicht das Vertrauen des Massenpublikums gewinnen konnte. Institutionelle Vertrauensbildung kann durch zielgerichtete vertrauensbildende Maßnahmen Vertrauen in die Sicherheit von Internet-Zahlungssysteme aufbauen. Neben den vertrauenskritischen, technischen Aspekten, die hauptsächlich im Zusammenhang mit der Sicherheit der verwendeten kryptographischen Verfahren zu sehen sind, bestehen auch im organisatorischen und rechtlichen Bereich jeweils eigene, sehr spezielle Unsicherheitsmomente, die im Rahmen der institutionellen Vertrauensbildung berücksichtigt werden müssen. Als geeignetes Konstrukt für die Wahrnehmung dieser komplexen und interdisziplinären Aufgabe bietet sich die Idee des Vertrauensnetzwerks an, in dem verschiedene Institutionen, entsprechend ihrer jeweiligen Kompetenz und wahrgenommenen Neutralität, Vertrauen in den technischen, organisatorischen und rechtlichen Anwendungskontext der Internet-Zahlungssysteme vermitteln. Diese Idee geht davon aus, daß es keine singuläre Lösung der institutionellen Vertrauensbildung geben wird, sondern vielmehr die verschiedensten Institutionen in diesem Bereich tätig werden. Wer schließlich die Vertrauensvermittler sind und zukünftig sein könnten, die innerhalb des Vertrauensnetzwerks systematische Vertrauensarbeit erbringen, wird anhand von Beispielen dargestellt und kritisch beleuchtet.

Inhaltsverzeichnis

1 Kontext

1.1 Internet – vom wissenschaftlichen Austausch zum eCommerce

Der Gedanke, das Internet für die Anbahnung und Abwicklung kommerzieller Transaktionen zu nutzen, ist relativ neu. Bis Anfang der 90er Jahre wurde das Internet,[1] dessen Vorläufer ARPANET und MILNET ursprünglich aus einer militärischen Initiative konzipiert wurden, hauptsächlich für wissenschaftliche Zwecke genutzt. Zwei wichtige Innovationen öffneten schließlich die Tore zu einer Entwicklung, die wegen ihrer Bedeutung für Wirtschaft, Wissenschaft und Gesellschaft als ‚informationelle Revolution' bezeichnet werden kann.

Zum einen war es die Konzeption und Realisierung des World Wide Web (WWW) durch Tim Berners-Lee[2] während seiner Forschungsarbeiten am Europäischen Labor für Teilchenphysik (CERN) im Jahr 1991. Seither gewann das WWW immer mehr an Bedeutung für private und geschäftliche Transaktionen und wird von vielen Anwendern zu Unrecht mit dem Internet selbst identifiziert.[3] Zum anderen standen mit dem neuen Übertragungsprotokoll HTTP (Hypertext Transfer Protocol) und der entsprechenden Programmiersprache HTML (Hypertext Markup Language) einfach erlernbare und komfortable Werkzeuge zur Verfügung, die zur rasanten Ausbreitung und ungebrochenen Popularität des WWW führten.

Darüber hinaus wurde durch die Entwicklung und Verbreitung der Client Software für das WWW, der sogenannten Internet- oder HTML-Browser, eine komfortable und günstige Zugriffsmöglichkeit für die breite Masse geschaffen. HTML-Browser wie NSCA Mosaic, der Netscape Navigator oder Microsofts Internet Explorer ermöglichen Internetnutzern auf einfache Weise den Besuch jeder HTML-Seite im Internet. Über standardisierte Adressierungsverfahren können weltweit Verknüpfungen aufgebaut und angesprochen werden. Hilfreich für die Verbreitung von HTML-Browsern war die zuerst von Netscape verfolgte Lizenzpolitik, den Browser Netscape Navigator für nicht-kommerzielle Zwecke kostenlos zur Verfügung zu stellen. Die im Gegenzug von Microsoft gefahrene Strategie, den Internet Explorer als integralen Bestandteil des Windows 9x Betriebssystems an den Endkunden auszuliefern, führte zwar zu einer langwierigen juristischen Auseinandersetzung mit dem Erzkonkurrenten Netscape, erhöhte aber die Anzahl der installierten HTML-Browser beträchtlich.

---

[1] Kuhlen (1999), S.345: „Das Internet ist ein weltweites Computer-Netzwerk, das Computer aller Arten auf der Basis des Übertragungsprotokolls TCP/IP verbindet."

[2] Detaillierte Informationen zu Berners-Lee und seinen Arbeiten finden sich auf dem Server des W3 Consortium (http://www.w3.org).

[3] Neben dem WWW schließt das Internet noch eine Reihe weiterer Mehrwertdienste, z.B. eMail, FTP, WAIS, Gopher und proprietäre Mehrwertdienste wie AOL oder T-Online ein.

Es wurde für Organisationen aus allen Lebensbereichen dadurch einfacher und kostengünstiger, potentielle Interessenten auf einem breiten, sogar globalen Spielfeld zu erreichen. Produkte, Dienstleistungen und Information können ohne Rücksicht auf zeitliche und räumliche Barrieren mit minimalen Grenzkosten pro Nutzer angeboten werden. Damit war die technologische und ökonomische Basis für die Kommerzialisierung des Internet geschaffen. Das WWW hat sich inzwischen zum „universalen Präsentations- und Austauschinstrument für Forschung, Lehre und Technologietransfer bzw. Informationsvermittlung entwickelt“[4]. Was lag also für die Wirtschaft näher, als geschäftliche Transaktionen ebenfalls über dieses Medium abzuwickeln?

eCommerce (Electronic Commerce) umfaßt alle Formen der Unterstützung bzw. Automatisierung der wirtschaftlichen Leistungskoordination.[5] Der Begriff wird heute vor allem im Zusammenhang mit der elektronischen Abwicklung von Geschäftsprozessen zwischen Unternehmen und Kunden im Internet verwendet[6] und steht für „das Kaufen und Verkaufen von Produkten, Informationen und Dienstleistungen über elektronische Netze.“[7] eCommerce ist aus dieser Erkenntnis heraus zu einem aktuellen oder zumindest potentiellen Erfolgsfaktor für viele Unternehmen geworden. Wachstumsraten, die in anderen Bereichen kaum denkbar sind, machen deutlich, daß das Internet als globaler Markt nicht nur für Public Relation und Werbung genutzt werden kann, sondern auch für Folgeaktivitäten, wie Verkauf, Lieferung, Bezahlung und (After Sales) Service.

Der Deutsche Multimedia Verband (dmmv) schätzt, daß sich der eCommerce-Umsatz in Deutschland im Jahr 1998 auf ca. 2,7 Mrd. DM belaufen hat und damit im Vergleich zum Vorjahr dreimal so hoch ist.[8] Im Jahr 2002 – so die beeindruckende Schätzung der Unternehmensberatung Booz, Allen & Hamilton – werde der elektronische Handel via Internet in Deutschland einen Gesamtumsatz von ca. 40 Mrd. DM erwirtschaften.[9] Wollen Konsumenten und Anbieter alle Vorteile des elektronischen Handels genießen und ihre im Internet georderte Ware oder Dienstleistung auf dem gleichen Wege bezahlen, sind sie auf entsprechende Zahlungssysteme angewiesen. Innerhalb der Prozeßkette von Anbahnung, Bestellung, Lieferung und Bezahlung stellt die Möglichkeit der Internet-Zahlung einen weiteren Schritt zur Integration des gesamten Ablaufs ins Internet dar. Internet-Nutzer können alle notwendigen Transaktionen von der Bestellung bis zur Bezahlung ohne Medienbruch über das Internet abwickeln. Lediglich die Lieferung durch den

---

[4] Kuhlen (1996a), S.474
[5] Zbornik (1996), S.54
[6] Thome (1997), S.1
[7] Schuster/Färber/Eberl (1997), S.4
[8] DMMV (1999) – ein guter Überblick über Marktzahlen und Statistiken findet sich auch unter DMMV (1998).
[9] Vgl. Yahoo (1999)

Anbieter muß bei materiellen Gütern oder ortsgebundenen Dienstleistung auf konventionellem Wege erfolgen. Die Möglichkeit, Zahlungsvorgänge bequem und sicher via Internet durchzuführen ist, so Michael Waidner und Phil Janson vom IBM Forschungslabor Zürich, die Grundbedingung für die weitere Entwicklung des eCommerce.[10] Eine neuere, vom Bundesforschungsministerium in Auftrag gegebene Studie am Karlsruher Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) schließt sich dieser Aussage nicht an: „Die These, daß der Internet-Handel blockiert sei, weil keine angemessenen Zahlungsverfahren zur Verfügung ständen, ist zurückzuweisen."[11] Herkömmliche, durch den Versandhandel bereits bekannte Zahlungsformen wären, so die Studie, auch für den eCommerce tauglich. Allerdings bestünde im Klein- und vor allem im Kleinstpreisbereich durchaus ein bisher nicht gedeckter Bedarf an neuen Zahlungssystemen für das Internet.[12] Ob man die Existenz von sicheren Zahlungssystemen im Internet nun als Grundbedingung für die Ausweitung des eCommerce betrachtet oder nicht – sichere Zahlungssysteme stellen einen wichtigen Baustein für die weitere Entwicklung der kommerziellen Aktivitäten im Internet dar.

1.2 Sicherheit und Akzeptanz

Die Bereitstellung sicherer Zahlungssysteme im Internet durch die Hersteller und Betreiber ist eine Seite der Medaille. Auf der anderen Seite ist es das Massenpublikum, das durch seine Akzeptanz über den praktischen Einsatz dieser Zahlungssysteme bestimmt. Akzeptanz soll in diesem Zusammenhang in Anlehnung an die Definition von Reichwald „die Bereitschaft eines Anwenders, in einer konkreten Anwendungssituation das vom Techniksystem angebotene Nutzungspotential aufgabenbezogen abzurufen"[13] sein. Akzeptanz drückt sich sowohl in der potentiellen Nutzungsbereitschaft als auch in der praktischen Nutzung eines Internet-Zahlungssystems aus. Es ist anzunehmen, daß gerade bei finanziellen Transaktionen Sicherheit ein erhebliches Kriterium für Akzeptanz darstellt. Fast 40% der Konsumenten eröffnen u.a. deshalb kein Internet-Bankkonto, weil sie Sicherheitsbedenken haben.[14] Gar drei Viertel der Online Shopper halten es für unsicher und gefährlich, Kreditkartendaten über das Internet zu übertragen.[15] Und nur 15% vertrauen nach einer neuen, von IBM beauftragten Studie darauf, daß ihre Daten bei den eCommerce Unternehmen sicher aufgehoben sind.[16] Daß diese Skepsis nicht unbegründet ist, wurde durch die derzeit laufenden Ermittlungen gegen einen US-Unternehmer deutlich, der „möglicherweise der größte Kreditkartenbetrüger

---

[10] Vgl. Waidner/Janson (1995)
[11] Böhle/Riehm (1998), S.79
[12] Vgl. Böhle/Riehm (1998)
[13] Reichwald (o.J.), S.31; vgl. auch Reichswald/Bodem/Odemer/Schönecker/Sorg (o.J.), S.9f
[14] Vgl. Kristoferitsch (1998), S.52
[15] Vgl. Focus (1999), S.124
[16] Vgl. Südkurier (1999)

aller Zeiten“[17] ist. Er steht in dringendem Verdacht, mehr als 900.000 Kreditkartenbesitzer um 40 bis 50 Mio. US$ betrogen zu haben, indem er übers Internet deren Kreditkartennummern bei Banken und Händlern stahl.[18]

Gerade bei sensiblen, finanziellen Transaktionen wiegen Sicherheitsbedenken umso schwerer. Im Bereich der Internet-Zahlungssysteme kommt hinzu, daß das Internet ein offenes und unsicheres Medium ist. Die Akzeptanz elektronischer Zahlungsformen im Internet dürfte sich deshalb kaum durch ‚Trial and Error‘ durchsetzen. Fehlt das Vertrauen der Anwender, werden sie keine elektronischen Zahlungssysteme einsetzen.

1.3 Begriffsdefinition für Zahlungssysteme im Internet

Wenn heute von Zahlungssystemen im Internet gesprochen wird, hat das Massenpublikum nur eine vage Vorstellung, was genau sich hinter diesem Begriff verbirgt. Obwohl es mittlerweile eine Vielzahl funktionsfähiger Zahlungssysteme im Internet gibt, existiert in der deutschen Sprache keine allgemeingültige Definition für diese Systeme. Unterschiedliche Begriffe werden häufig undifferenziert verwendet, so daß sich die Bedeutung erst aus dem Verwendungskontext erschließen läßt.

Dieses begriffliche Defizit resultiert zum einen aus der Tatsache, daß die Entwicklung des Internets maßgeblich durch das Umfeld von Wissenschaft und Forschung geprägt wurde. Um Sprachbarrieren zu umgehen, findet Kommunikation im Internet hauptsächlich in englischer Sprache statt. Auch die dominante Stellung amerikanischer Unternehmen auf dem wissenschaftlichen Mehrwertemarkt des Internet[19] hat wesentlich zur Verbreitung der englischen Sprache beigetragen. Der wissenschaftlich-technische Austausch war nicht auf einen äquivalenten deutschen Begriff angewiesen. ‚Electronic Cash‘ bzw. ‚Digital Cash‘, ‚Digital Money‘ oder ‚E-Cash‘[20] waren und sind im englischen Sinne des Wortes die anerkannte Bezeichnung für Zahlungssysteme im Internet. Warum in dieser Arbeit dennoch von Zahlungssystemen im Internet gesprochen wird und nicht etwa von „Electronic Cash“, resultiert aus der Tatsache, daß „Electronic Cash“ bis Ende der 80er Jahre im deutschsprachigen Raum landläufig kartenbasierte Zahlungssysteme („ec-Karten“) bezeichnete. Diese Zahlungssysteme basieren auf geschlossenen Netzwerken; Transaktionen können nur von sicheren Orten (ec-Terminals oder Geldautomaten) und von Akteuren vorgenommen werden, die sich vorher (bspw. als Kunde einer Bank) authentifiziert haben. Diese Annahmen gelten für das anonyme, offene und damit unsichere Internet – von proprietären Netzwerken wie T-Online oder AOL einmal abgesehen - nicht.

---

[17] Vgl. c’t (1999)
[18] Vgl. Faughnan (1998)
[19] Kuhlen (1996a), S.115
[20] Der Begriff ‚E-Cash‘ ist nicht zu verwechseln mit dem ‚eCash‘ Zahlungssystem des US-

Der Begriff des elektronischen Zahlungssystems allein eignet sich noch weniger für die Beschreibung von internetbasierten Zahlungssystemen, da sich darunter sowohl das oben genannte ec-Karten System subsumieren läßt, als auch alle anderen Zahlungssysteme, bei denen keine materiellen Objekte, wie Bargeld, Schecks, Wechsel etc., transferiert werden. Clearing Systeme, wie sie von Finanzinstituten im Inter-Bankenhandel schon seit Jahrzehnten eingesetzt werden, sind ebenfalls zu den elektronischen Zahlungssystemen zu rechnen. Ein elektronisches Zahlungssystem kann sowohl in offenen, wie in geschlossenen (proprietären) Netzwerken realisiert werden. Eine Begriffseingrenzung, die sich nur auf die physikalischen Grundlagen des Zahlungssystems bezieht, bestimmt das Forschungsobjekt nicht eindeutig.

Kristoferitsch orientiert sich an der englischen Bedeutung des Begriffes und definiert Digital Cash (bezogen auf Internet Zahlungen) als „Summe aller Erscheinungsformen elektronischen Geldes“[21], dessen physikalische Existenz ausschließlich auf einer vereinbarten Abfolge von Bits und Bytes besteht. Obwohl Kristoferitsch „Chancen und Risiken des Zahlungsverkehrs via Internet“[22] behandelt, läßt seine Definition keinen direkten Bezug zum Internet und damit zu einer offenen Netzwerkstruktur erkennen.

Ebenso entwickelt die Definition von Lynch und Lundquist, die zwar richtig erkennen „Digital Money has no intrinsic value and the barest trace of physical value“[23] erst aus dem Kontext heraus ihre volle Aussagekraft.

Beide Definitionen sind ähnlich problematisch, wie die Bezeichnung ‚elektronische Zahlungssysteme‘. Sie schließen zwar Zahlungssysteme des Internet mit ein, können aber auch als adäquate Bezeichnungen für weitere Zahlungssysteme gelten, die außerhalb des Internets operieren. Spricht man von „Zahlungssystemen im Internet“, wird verdeutlicht, in welches spezifische Umfeld diese Zahlungssysteme eingebettet sind. Der Begriff der ‚Zahlungssysteme im Internet‘ oder kurz, der ‚Internet-Zahlungssysteme‘, erscheint deshalb als geeignete Bezeichnung.

1.4 Institutionelle Vertrauensbildung

Die weitere Entwicklung kommerzieller Aktivitäten im Internet wird maßgeblich dadurch bestimmt, inwieweit Kunden und Anbieter bereit sind, Zahlungssysteme im Internet als Äquivalent bzw. Substitut konventioneller Zahlungsmethoden zu akzeptieren und einzusetzen. Mit dem Einsatz konventioneller Zahlungsformen hat das Massenpublikum lange genug Erfahrung sammeln können, wiederholte positive Erfahrungen haben Vertrauen in die Kompetenz und Integrität des häufig persönlich bekannten Bankangestellten und des betreffenden Kreditinstitut aufgebaut. Das

---

Unternehmens DigiCash.

[21] Kristoferitsch (1998), S.41f

[22] Kristoferitsch (1998)

[23] Lynch/Lundquist (1996), S.100

alltägliche Bezahlen mit Kreditkarten oder die Benutzung des Geldautomaten bergen zwar gewisse Sicherheitsrisiken, jedoch zeigt die Erfahrung, daß diese bei korrekter Anwendung relativ gering sind.

Nur wenige Menschen – gemessen an der Gesamtheit der potentiellen Nutzer – haben bisher Erfahrungen mit Zahlungssytemen im Internet gemacht. „For many people, the Internet remains a mysterious and dangerous space, populated by computer viruses, teenage corporate hackers, and "get rich click" spam artists. People are understandably wary, and very slow to reach for their wallets.“[24] Im Gegensatz zu konventionellen Methoden fehlen persönliche Erfahrungen im Umgang mit Zahlungsformen im Internet. Wie sicher diese Zahlungsformen wirklich sind, hat das Massenpublikum weder aus Erfahrung gelernt, noch ist es in der Lage, diese Sicherheit zu beurteilen. Selbst engagierten Laien ist es kaum möglich, technische Konzepte und Funktionsweisen elektronischer Dienste und elektronischer Zahlungsformen nachzuvollziehen und einzuschätzen.

Das heißt jedoch nicht, daß potentielle Anwender erst im jahrelangen Umgang Schritt für Schritt Erfahrungen mit elektronischen Transaktionen sammeln müssen oder alternativ sich das Wissen aneignen müssen, um Ablauf und Sicherheit elektronischer Transaktionsformen zu beurteilen

Diese Arbeit will u.a. darlegen, daß Anwender trotz defizitären Wissens über Sicherheit und Ablauf elektronischer Transaktionen bereit sind, diese einzusetzen. Wenn das Massenpublikum Vertrauen aufbaut zu Institutionen oder deren persönlichen Mittlern, die ihnen diese Expertenfunktionen abnehmen und für die Sicherheit elektronischer Zahlungsformen auf Basis ihrer Kompetenz und Neutralität bürgen, werden sie auch ohne konkretes eigenes Wissen Internet-Zahlungssysteme akzeptieren. Wie im Verlauf der Arbeit noch dargelegt wird, gibt es triftige Gründe dafür, daß Institutionen und Organisationen (als Institutionen mit einer „greifbaren“ Organisationsstruktur) diese Vertrauensbildung wahrnehmen. Institutionen sollen hier nicht im weiten politikwissenschaftlichen Sinne einer regulativen sozialen Verhaltensordnung verstanden werden.

Im Kontext der Arbeit ist es treffend, eine Institution als die „einem bestimmten Bereich zugeordnete öffentliche Einrichtung, die dem Wohl oder Nutzen des einzelnen oder der Allgemeinheit dient“,[25] zu beschreiben. Eine öffentliche Einrichtung ist im Sinne dieser Arbeit nicht zwangsläufig eine staatliche Einrichtung, sondern kann genauso gut privaten oder kommerziellen Ursprungs sein.

---

[24] Needham (1999): Building Trust: Building Business
[25] Brockhaus (1997)

2 Zielsetzung und Aufbau der Arbeit

2.1 Zielsetzung der Arbeit

Bislang wurden die Zusammenhänge zwischen institutioneller Vertrauensbildung und der Akzeptanz von Zahlungssystemen im Internet skizziert. Ziel der Arbeit ist weiter, darzustellen, welche Ausprägung der institutionellen Vertrauensbildung bei Internet-Zahlungssystemen denkbar sind und welche Akteure diese Aufgabe übernehmen können. Dazu notwendig ist ein umfassendes Verständnis, warum Vertrauen gerade im Umgang mit (technisch abstrakten) Internet-Zahlungssystemen bedeutsam ist und welche vertrauenskritischen Bereiche davon betroffen sind. Nach einer detaillierten Darstellung der Grundlagen und Funktionen von Internet-Zahlungssystemen wird deutlich, daß die Anwendung von Internet-Zahlungssysteme in einem komplexen technischen, organisatorischen und rechtlichen Umfeld stattfindet. In diesem Umfeld werden alte und neue Akteure aktiv werden, die teilweise Vertrauen in spezifische technische, organisatorische oder rechtliche Bereiche vermitteln wollen und teilweise Vertrauen in Internet-Zahlungssysteme als Gesamtheit technischer, organisatorischer und rechtlicher Verfahren. Ein Vertrauensnetzwerk – so die hier vertretene Ansicht – kann als geeignete Form der Kompetenzsicherung, -bündelung und Kontrolle für diese Vertrauensarbeit angesehen werden.

2.2 Aufbau der Arbeit

Diesen Zielsetzungen entsprechend ist die vorliegende Arbeit gegliedert. Nach einem **ersten**, in die Thematik einführenden Kapitel und der Beschreibung von Zielsetzung und Aufbau der Arbeit in diesem **zweiten** Kapitel, soll im **dritten** Kapitel herausgearbeitet werden, wie Unsicherheit in der durch Technik geprägten Moderne entsteht und welche Kompensationsmechanismen Menschen entwickelt haben, um unter informationeller Unsicherheit mit technisch-abstrakten Systemen, zu denen Internet-Zahlungssysteme zweifellos gehören, umgehen zu können.

Bevor auf diesen Aspekt und seine Konsequenzen für die institutionelle Vertrauensbildung eingegangen wird, stellt das **vierte** Kapitel dar, was Vertrauen ausmacht, welche Einflußfaktoren vertrauensbildend oder –zerstörend wirken können. Die Berücksichtigung dieser Faktoren wird letztendlich über den Erfolg oder Mißerfolg der institutionellen Vertrauensbildung entscheiden. Dementsprechend werden sie auch als Grundlage für die Überlegungen zur praktischen Ausprägung der institutionellen Vertrauensbildung bei Internet-Zahlungssystemen herangezogen. Weiter wird erörtert, warum gerade im Kontext der Internet-Zahlungssysteme ein institutionelles Engagement in der Vertrauensbildung notwendig ist.

Das **fünfte** Kapitel widmet sich der Frage, welche Unsicherheitsmomente auf elektronischen Märkten bestehen und welche speziellen, vertrauenskritischen

Bereiche für Internet-Zahlungssystemen relevant sind. Ausgehend vom Grobmodell eines Internet-Zahlungsablaufs werden Sicherheitsanforderungen an Internet-Zahlungssysteme definiert. Nur wenn diese Sicherheitsanforderungen praktische Sicherheit garantieren, wird es möglich sein, diese innerhalb der institutionellen Vertrauensbildung über einen längeren Zeitraum erfolgreich zu vermitteln. Unter dieser Prämissen wird herausgearbeitet, daß Sicherheit im Kontext der Internet-Zahlungssysteme eben nicht nur technische, sondern genauso organisatorische und rechtliche Aspekte miteinschließt. Dieser Erkenntnis entspricht die Systematisierung der Vertrauensaspekte bei elektronischen Zahlungsformen in technische, organisatorische und rechtliche Aspekte. Vertrauensarbeit wird in jedem dieser Bereiche notwendig sein, um die jeweils sehr speziellen, aber dennoch interdependenten Unsicherheiten beseitigen zu können. Darüber hinaus werden Kontrollinstanzen notwendig sein, die auf Basis wahrgenommener Kompetenz und Neutralität für die Qualität der institutionellen Vertrauensbildung und die Bündelung der Expertise der Akteure zuständig sind.

Im **sechsten** Kapitel wird erläutert, auf welche Weise elektronische Zahlungssysteme sicherheitsrelevante Probleme lösen. Basierend auf einer Erläuterung kryptographischer Verfahren, die grundlegend für die Sicherung von Authentizität, Integrität und Vertraulichkeit elektronischer Transaktionen sind, wird die für den Bereich der elektronischen Zahlungssysteme relevante Anwendung von Verschlüsselungs- und Signaturtechnik dargestellt. Die Erläuterung zweier, derzeit im Internet verfügbarer Zahlungssysteme – SET (Secure Electronic Transaction) und eCash – gibt einen detaillierten Einblick in die praktische Anwendung dieser Technologien.

Wer nun die Institutionen sind und sein können, die Vertrauensbildung im Bereich der Internet-Zahlungssysteme betreiben, wird im **siebten** Kapitel diskutiert. Dazu werden exemplarisch die Aktivitäten einiger bereits tätiger Akteure beschrieben und auf neue, denkbare Akteure hingewiesen, die Vertrauensbildung in diesem Bereich ausüben können und hinsichtlich ihrer kommerziellen Ausrichtung sogar praktizieren müssen. Eingebettet sind diese Institutionen in ein Vertrauensnetzwerk, dessen Aufgabe neben der Bündelung fachspezifischer Kompetenzen die Kontrolle der vertrauensbildenden Maßnahmen sein wird. Da ein Vertrauensnetzwerk selbst keine Vertrauensbildung betreiben kann, wird es auf Institutionen und Organisationen angewiesen sein, die an den Kontaktpunkten mit den Anwendern vertrauensbildende Maßnahmen kommunizieren. Unter anderem verfügen Banken und Kreditinstitute über die notwendige Infrastruktur, um diese Arbeit flächendeckend zu erbringen.

Das **achte** und letzte Kapitel widmet sich nach einer kurzen Zusammenfassung der Erkenntnisse einem Ausblick über die zukünftige Entwicklung der institutionellen Vertrauensbildung bei Internet-Zahlungssystemen. Eine singuläre, institutionelle Lösung der Vertrauensbildung wird es bei Internet-Zahlungssysteme jedenfalls nicht

geben. Dieser Erkenntnis trägt das Konzept des Vertrauensnetzwerks Rechnung, in dem bestimmte Akteure – in erster Linie wahrscheinlich Banken und Kreditinstitute – eine zentrale Rolle spielen werden.

3 Unsicherheit und Vertrauen

3.1 Verunsicherung durch abstrakte Systeme

Technische Systeme sind aus dem Alltagleben nicht mehr wegzudenken. Häufig funktionieren diese Systeme jedoch nicht, wie beabsichtigt, weil sie falsch konstruiert sind, falsch bedient oder mißbraucht werden. Ob morgens der Wagen nicht anspringt, in Eschede der „Stolz der germanischen Ingenieurskunst“[26] - der ICE Konrad Röntgen - an einer Brücke zerschellt oder in Tschernobyl ein nie dagewesener Super GAU eintritt, das Versagen von technischen Systemen wird mit unterschiedlichen Härtegraden tagtäglich ins Bewußtsein des Massenpublikums gerufen. Je mysteriöser die Gründe und je schlimmer die Konsequenzen dieses Versagens sind, desto größer wird die dadurch erzeugte Verunsicherung. Obwohl unser Vertrauen in die Sicherheit der Technik ständig erschüttert wird, können wir ihr nicht entkommen, wir bewegen uns sozusagen in einer „Risikogesellschaft“.[27] Der Verzicht auf alle technischen Errungenschaften würde uns in der Entwicklung Jahrhunderte zurückwerfen. Vielleicht wird am Fortschritt festgehalten, weil die Hoffnung besteht, er würde mehr Nutzen als Gefahren bringen. Doch „im Modernisierungsprozeß werden mehr und mehr auch *Destruktivkräfte* freigesetzt, vor denen das menschliche Vorstellungsvermögen fassungslos steht.“[28] Das Wissen zur Absicherung des Modernisierungsprozesses wird immer abstrakter und komplexer. Schließlich kommt es zu einer paradoxen Spirale, die Beck als „Reflexivität der Moderne“[29] bezeichnet: Neue Systeme werden entwickelt, um sich gegen die negativen Folgen bestehender Systeme abzusichern. Diese neuen Systeme erzeugen aber wiederum einen Bedarf an informationeller Absicherung, der abermals durch neue Systeme befriedigt wird.

Wissenschaftler wie Anthony Giddens[30] und Ulrich Beck haben verdeutlicht, wie Unsicherheit in der durch Technik geprägten Moderne entsteht und welche Kompensationsmechanismen wir entwickelt haben, um trotzdem mit komplexen, abstrakten Systemen umgehen zu können. Moderne sind in diesem Sinne „modes of social life or organisation which emerged in Europe from about the 17th century onwards and which subsequently became more or less worldwide in their influence.“[31] Ohne den komplexen Ansatz von Giddens hier bis ins Detail zu diskutieren, ist Verunsicherung bzw. Unsicherheit in der Moderne auf defizitäres Wissen über die Funktion abstrakter Systeme zurückzuführen. Giddens identifiziert

---

[26] Spiegel (1999a)
[27] Beck (1986)
[28] Beck (1986), S.27
[29] Vgl. Beck/Giddens/Lash (1996)
[30] Giddens (1990)
[31] Giddens (1990), S.4

drei Eigenschaften der Moderne[32] – Trennung von Zeit und Raum, Loslösung des sozialen Lebens vom lokalen Kontext und die Anwendung komplexen Wissens – durch die „Disembedding“,[33] d.h. die ‚Entbettung‘ bzw. Entkontextualisierung des Menschen von seiner Lebenswelt entsteht. Diese ‚Entbettung‘ ist die Ursache der Verunsicherung, zum einen, weil sich die Organisationsform von Gesellschaft, Wirtschaft und Wissenschaft immer mehr dem Verständnis der Masse entziehen. Zum anderen ist es für das Massenpublikum immer weniger möglich, Funktionsweisen abstrakter technischer Systeme zu begreifen, da sie nicht in der Lage sind, die wissenschaftlich technischen Prinzipien, nach denen sie funktionieren, zu verstehen. Deshalb wird das Verständnis oder besser gesagt, die Kontrolle komplexer, technischer und organisatorischer Systeme an Experten delegiert, denen wir zutrauen, die Sicherheit dieser Systeme einschätzen zu können.[34] Die Moderne ist damit eine Zeit der Delegation von Verantwortung. Wir handeln „mit den abstrakten und technischen Systemen der Neuzeit in einem Zustand weitgehender informationeller Unsicherheit“.[35]

3.2 Kompensationsfunktion von Vertrauen

In Situationen, in denen der Gebrauch technisch abstrakter Systeme angebracht oder erforderlich ist, der Anwender jedoch nicht über eigenes Wissen verfügt, um die damit verbundenen Risiken einzuschätzen, wird er bereit sein, auf das Wissen Dritter zurückzugreifen, sofern diese als vertrauenswürdig betrachtet werden. Fehlendes Wissen wird durch Vertrauen in Personen oder Institutionen kompensiert. Hierin liegt die kompensatorische Funktion von Vertrauen.

Vertrauen, so Kuhlen, „ist ein ‚als ob‘ Ereignis.“[36] Vertrauen versetzt uns in die Lage, so zu handeln, als ob wir eigenes Wissen zur Verfügung hätten. Vertrauen ist jedoch kein Ersatz für Wissen. Es bildet sinnbildlich gesprochen die Brücke zwischen dem Wissen anderer und der eigenen informationellen Unbestimmtheit. Vertrauen ist deshalb weder unabhängig von Wissen, noch kann es Wissen vollkommen ersetzen. Durch Vertrauen ist es jedoch möglich, mit gleicher oder zumindest ähnlicher Zuversicht zu handeln, wie mit eigenem Wissen.[37] Vertrauen bedeutet damit, sich in einem bestimmten Kontext auf die Zuverlässigkeit einer Person oder eines Systems zu verlassen. Bei Personen läßt sich diese Verläßlichkeit durch psychologische Faktoren, wie z.B. den Glauben an die Aufrichtigkeit und Kompetenz einer Person

---

[32] Giddens (1990), S.53
[33] Giddens (1990)
[34] Vgl. Kuhlen (1999), S.70
[35] Kuhlen (1999), S.70
[36] Kuhlen (1998c), S.14
[37] Luhmann (1988), S.97ff unterscheidet situationsabhängig zwischen Vertrauen (Trust), das in sehr riskanten, indifferenten Situationen notwendig ist und Zuversicht (Confidence) in stabilen, bekannten oder zumindest überschaubaren Situationen. Je riskanter und indifferenter eine Situation ist, desto mehr Vertrauen ist notwendig, um das fehlende Wissen zu kompensieren.

begründen, bei abstrakten technischen Systemen auf den Glauben an die Korrektheit der ihnen zugrunde liegenden technischen Prinzipien:

„Trust may be defined as confidence in the reliability of a person or system, regarding a given set of outcomes or events, where that confidence expresses a faith in the probity or love of another, or in the correctness of abstract principles (technical knowledge).“[38]

Vertrauen kann sich damit nicht nur auf Personen aus Fleisch und Blut, sondern genauso auf abstrakte Systeme beziehen.

[38] Giddens, (1990), S.34

4 Vertrauensbildung

4.1 Einflußfaktoren der Vertrauensbildung

Um im späteren Verlauf der Arbeit die aktuelle und potentielle Ausprägungen der institutionellen Vertrauensbildung bei Internet-Zahlungssystemen erörtern zu können, müssen Einflußfaktoren und Eigenschaften, die den Prozeß der Vertrauensbildung beeinflussen, bekannt sein. Dabei soll nicht nur auf Faktoren eingegangen werden, die Vertrauen erzeugen, sondern auch auf die pragmatischen Eigenschaften von Vertrauen.

4.1.1 Spezifität

Giddens weißt in obigem Zitat bereits auf zwei dieser Faktoren hin. Zum einen ist Vertrauen spezifisch – es bezieht sich auf bestimmte Ergebnisse oder Ereignisse. Pauschalaussagen, wie ‚Ich vertraue der Bank' sind wenig aussagekräftig,[39] weil nicht erkennbar ist, wem und in welchem Kontext Vertrauen geschenkt wird. Welcher Bank wird vertraut? In welcher Angelegenheit? Kontoführung, Verrechnung der Kreditkartenausgaben, Abbuchung der Daueraufträge oder Vermögensanlagen? Unter Umständen kommen noch zeitliche Restriktionen hinzu, beispielsweise für die Dauer einer Mitgliedschaft oder Partnerschaft. Nur wenn Vertrauen ausreichend spezifiziert ist, kann zielgerichtete Vertrauensbildung stattfinden.

4.1.2 Subjektivität und Emotionalität

Zum anderen weißt Giddens explizit darauf hin, daß Vertrauen sich nicht nur auf Personen, sondern auch auf abstrakte Prinzipien beziehen kann. Das Massenpublikum ist jedoch aufgrund fehlenden Wissens meist nicht in der Lage, diese Prinzipien zu verstehen. Vertrauensbildung ist in diesem Fall kein direkter Prozeß zwischen Anwender und System. Vielmehr muß sich die Vertrauensbildung Zugangspunkte aufbauen, die Komplexität letztendlich durch emotionale Faktoren reduzieren. Vertrauensbildung ist zu allererst ein subjektives Ereignis. „All trust begins and ends with the self: Trust no one but yourself!"[40]

Vertrauen ist zwar auf Zuversicht in ein bestimmtes Personen- oder Systemverhalten begründet, begründet sich aber wiederum auf subjektiven Grundprinzipien, Einstellungen und Ansichten. Sie stellen die subjektiven, emotionalen Bewertungsmaßstäbe dar, anhand derer wir Vertrauen reklamierende Personen und vertrauenskritische Situationen einschätzen.

Somit ist Vertrauen nicht nur subjektiv, sondern auch gefühlsbetont. Kuhlen weißt darauf hin, daß Vertrauensarbeit im Bereich abstrakter, technischer Prinzipien und

---

[39] Kahre/Rifkin (1997), S.79f
[40] Kahre/Rifkin (1997), S.81

institutioneller Vertrauenssicherung eben auch auf emotionaler Ebene stattfinden muß: „Vertrauen in abstrakte Systeme und institutionelle Sicherung braucht ergänzend die emotionale Einstellung.“[41] Technischen Systemen und den darauf bezogenen Kontrollinstitutionen wird eher Vertrauen geschenkt, wenn die (vertrauenswürdigen) Personen bekannt sind, denen die Verantwortung für diese Systeme obliegt. Diese Erkenntnis hat sich die Werbung und Verkaufsförderung bereits zu Nutze gemacht. Treten die entsprechenden Personen nicht persönlich in Erscheinung oder sind nicht bekannt, muß eine weitere, vertrauenswürdige Mittlerinstanz eingeschaltet werden, die diese Personen repräsentiert. „Access points of abstract systems“[42] nennt Giddens diese Kontaktstellen zwischen Experten bzw. Repräsentanten einerseits und dem Massenpublikum andererseits. Genau an diesen Kontaktstellen findet Vertrauensvermittlung durch Personalisierung der Vertrauensbeziehung von Mensch zu Mensch oder um Giddens zu zitieren, durch ‚Facework Commitments‘,[43] statt: Vertrauenswürdige Personen als Experten oder Repräsentanten eines Systems fordern Vertrauen für sich. Vertrauen wir diesen Personen, vertrauen wir auch ihren Aussagen oder Handlungen, die Vertrauen in ein abstraktes System reklamieren und so letztendlich dem System selbst. Durch diesen ‚Vertrauenstransfer‘ schließt sich die Kette der Vertrauensbildung zwischen Laien und abstrakten Systemen.[44] ‚Facework Commitments‘ wirken dadurch, daß sie abstrakte Systeme durch Personalisierung wieder in einen zeitlich und räumlich bestimmbaren Kontext einbetten.[45] Wir erfahren Vertrauen zu einem Repräsentant eines Systems, den wir räumlich und zeitlich einordnen können.

4.1.3 Sensibilität und eigene Erfahrungen

Grundlegende Einsicht für erfolgreiche Vertrauensbildung ist, daß Vertrauen nicht enttäuscht werden darf. Negative Erfahrungen vor der eigentlichen Vertrauensbildung führen gar dazu, daß Vertrauen nicht oder nur durch aufwendige und langwierige Anstrengungen geschaffen werden kann: „The person whose reputation is at stake will obviously try to influence this processes, but that influence is only limited.“[46] Negative Erfahrungen in früher Kindheit sind ein gutes Beispiel dafür. Wichtig für die Vertrauensbildung in abstrakte Systeme ist deshalb, schon während der Sozialisations- und Lernphase ein grundlegendes Vertrauen zu vermitteln. Das kann aktiv durch Erziehung und Ausbildung geschehen oder in schwächerem Umfang durch die Vermeidung prägender, negativer Erlebnisse.

---

[41] Kuhlen (1998c), S.15
[42] Vgl. Giddens (1990), S.83
[43] Vgl. Giddens (1990), S.85
[44] Vgl. Kuhlen (1999), S.46f – Kuhlen illustriert dies sehr anschaulich anhand des Vertrauensmanagements von Mercedes z.Zt. der durch die ‚Elch-Test‘ Panne der A-Klasse hervorgerufenen Vertrauenskrise.
[45] Vgl. Giddens (1990), S.80
[46] Good (1988), S.38

Doch nicht nur in der primären Sozialisation und Ausbildung kann Vertrauensbildung erfolgen. Vertrauensbildung erfolgt im weiteren Sinne durch öffentliche Wertesysteme und dominante Einstellungen, die durch Medien und andere wirtschaftliche, gesellschaftliche und politische Akteure vermittelt werden.[47] Sie prägen Überzeugungen, indem sie das Publikum offener oder skeptischer für vertrauensbildende Maßnahmen machen. Wertesysteme und dominante Einstellungen wirken als Agenda-Setter und prädispositive Kräfte; sie bestimmen was und wie wir etwas wahrnehmen.

Vertrauen wird aus eigenen Erfahrungen gewonnen; die Erfahrung muß jedoch wieder und wieder bestätigt werden, um sich langsam als Vertrauen zu verfestigen. Je größer die Erfahrungsbasis ist, desto eher sind wir mit Situationen und Ereignissen vertraut, desto umfassender wird die Grundlage, auf die wir unser Vertrauen aufbauen können. „In der Regel sind die Quellen von Vertrauen also das Resultat eines zeitaufwendigen Prozesses."[48]

Ist Vertrauen einmal hergestellt, darf es nicht enttäuscht werden. Das gilt nicht nur für Vertrauen, das sich auf Erfahrungen begründet, sondern für jegliches Vertrauen: „Trust is hard to create but very easy to lose."[49] Wird man einmal von einem vertrauten Menschen hintergangen, ist man auch in Zukunft skeptischer. Ähnliches gilt für Vertrauen in technische Systeme, etwa, wenn wichtige Daten durch den Absturz eines Computersystems verloren gehen. Das vielleicht auf jahrelangen positiven Erfahrungen begründete Vertrauen in die Sicherheit des Systems wurde durch einen einmaligen Fehler zerstört oder zumindest schwer geschädigt. Die eigene Zuversicht in die Zuverlässigkeit der Person oder des Systems ist erschüttert worden – und Vertrauen ist nach Giddens eben Zuversicht in die Zuverlässigkeit von Personen oder Prinzipien.

4.1.4 Mißbrauch und Enttäuschung

Vertrauen kann eben deshalb mißbraucht werden, weil es nicht auf objektivem Wissen beruht.[50] Oben wurde dargestellt, daß Vertrauen auf subjektiven Grundprinzipien, Einstellungen und Ansichten fußt. Wissen hingegen ist objektiv, durch ‚harte Fakten' belegt und dadurch schwieriger zu manipulieren. Durch Wissen werden Handlungen informationell abgesichert. Verzichtet man darauf, sich durch eigenes Wissen abzusichern – etwa, weil dies aufgrund unzureichender Kompetenz oder fehlender Zeit und Motivation nicht möglich ist – können Informationsdefizite durch Vertrauen kompensiert werden. „Vertrauen haben bedeutet dann, auf objektive Informationen (bewußt) zu verzichten."[51] Weil es das Individuum selbst sind, das

---

[47] Vgl. Kuhlen (1998c), S.17
[48] Vogt (1996), S.69
[49] Kuhlen (1998c), S.48
[50] Vgl. Kuhlen (1999), S.72
[51] Kuhlen (1999), S.72, vgl. auch Giddens (1990), S.31

diesen Verzicht ausübt, trifft es der Mißbrauch von Vertrauen persönlich. Ein Teil der Schuld kann zwar auf diejenigen geschoben werden, die getäuscht und Vertrauen mißbraucht haben. Da dies durch den Verzicht auf eigenes Wissen erst ermöglicht wurde, liegt der anderen Teil der Schuld beim Individuum selbst.[52] Für falsches Wissen können andere verantwortlich gemacht werden[53] – z.B. falsche Berechnungen und Einschätzungen von Experten, mangelnde Kompetenz oder Genauigkeit von Wissenschaftlern oder Konstrukteuren. Falsches Wissen erschüttert dabei nur den Teilbereich, auf den es sich bezieht, enttäuschtes, falsches Vertrauen läßt den Menschen sofort an weiteren Vertrauensbereichen zweifeln. Vielleicht ist man generell zu vertrauensselig und bringt zu wenig eigene Skepsis gegenüber Vertrauenswürdigkeit reklamierenden Personen oder Institutionen auf? Auch wegen dieser Tatsachen ist Vertrauensbildung und –sicherung ein sensibler Prozeß.

4.1.5 Transparenz

Vertrauensbildung wird nicht zuletzt durch Transparenz ermöglicht, durch die „Offenlegung des dem System zugrunde liegenden technischen Wissens, auch wenn es nicht immer nachvollzogen werden kann."[54] Transparenz für sich alleine gesehen schafft vielleicht noch kein Vertrauen – aber sie ist die Grundlage dafür, daß vertrauensbildende Maßnahmen überhaupt als vertrauenswürdig erachtet werden. Transparenz schafft Vertrautheit und damit die Grundlage für Vertrauen. Durch Transparenz wird ein Gegengewicht zu der durch intransparente, abstrakte Systeme erzeugten Verunsicherung geschaffen. Das Internet als globaler elektronischer Markt ist kaum in der Lage, diese Transparenz herzustellen. Vermittlungsleistungen sind notwendig,[55] auch oder besonders, was die Vertrauensbildung betrifft. Die Schaffung von Transparenz und Offenheit ist, so wird anhand praktischer Beispiele im siebten Kapitel gezeigt, ein zentrales Instrument, dessen sich die institutionelle Vertrauensbildung bei Internet-Zahlungssystemen bedient.

4.2 Institutionelle Vertrauensbildung

Vertrauen wird also von einer Vielzahl unterschiedlicher Faktoren beeinflußt, die jeweils über Erfolg oder Mißerfolg der Vertrauensbildung und -sicherung entscheiden können. Vertrauensbildung ist, um es in Kuhlens Worte zu fassen, „gleichermaßen komplex und sensibel."[56] Glücklicherweise ist Vertrauen auch reparabel. Einmal enttäuschtes Vertrauen muß nicht unwiederbringlich verloren sein. Zielgerichtete Reparaturmaßnahmen, wie z.B. die Mercedes-Benz „Strategie des gläsernen Marketings"[57] im Fall der Vertrauenskrise der A-Klasse, kann begangene Fehler unter

---

[52] Vgl. Giddens (1990, S.31
[53] Vgl. Kuhlen (1999), S.72
[54] Kuhlen (1998c), S.17
[55] Vgl. Kuhlen (1996), S.6
[56] Kuhlen (1999), S.71
[57] Kuhlen (1999), S.44 zitiert hier Bernd Michael, Chef der düsseldorfer Werbeagentur ‚Grey'.

Umständen wieder ausbügeln. Auch für die ‚Vertrauensreparatur' gilt, was oben bereits für die Vertrauensbildung konstatiert wurde: Sie ist einerseits komplex, weil von einer Vielzahl unterschiedlicher Faktoren abhängig; sie ist zum anderen sensibel, weil bereits ein Fehler das ganze Unterfangen vereiteln kann.

Gerade weil Vertrauensbildung komplex ist, muß sie im Bereich der Internet-Zahlungssystem in großem Maße durch institutionelle Mittler kommuniziert werden. Daß der Bedarf nach institutioneller Vertrauenssicherung groß ist, sogar ständig ansteigt, zeigt sich an der Nachfrage und Existenz nach vertrauensbildenden Leistungen neutraler Dritter, sog. Trusted Third Parties. Sowohl Individuen als auch Unternehmen haben erkannt, daß sich Vertrauen im heute notwendigen Umfang nicht mehr allein durch persönliche Initiative aufbauen läßt. Privatleute bieten ihren Wagen gern mit dem Zusatz „TÜV neu" zum Verkauf an oder informieren sich vor Kaufentscheidungen in einschlägigen Fachzeitschriften über Qualitätseinschätzungen von Produkten und Dienstleistungen. Die Bedeutung von neutralen Urteilen zeigt sich nicht zuletzt daran, daß heute fast alle Fachzeitschriften Tests durchführen und veröffentlichen.[58] Auch Unternehmen haben erkannt, daß solche Referenzen und (positive) Qualitätseinschätzungen ein hochwertiges Verkaufsargument darstellen. Sie preisen ihre Produkte und Leistungen mit dem Verweis auf positive Testurteile oder Zertifikate vertrauenswürdiger Kontrollinstitutionen an. Ob es sich dabei um Institutionen handelt, die im staatlichen Auftrag Qualitätssicherung betreiben (z.B. der TÜV, Technischer Überwachungsverein), um Initiativen einzelner Unternehmen (SAP oder Microsoft Zertifizierungen), Einrichtungen, die allein der Qualitätssicherung dienen (Stiftung Warentest) oder von staatlicher oder wirtschaftlicher Seite beauftragte Unternehmen, die Qualitätssicherung als Erwerbszweck betreiben (z.B. ISO 9000 Zertifizierung durch Consulting-Unternehmen), ohne Qualitätssiegel, so möchte man bald meinen, läßt sich kaum mehr etwas verkaufen.

Qualitätssicherung wird instrumentalisiert, indem durch Verweis auf Kompetenz und Neutralität der Trusted Third Parties Vertrauen eingefordert wird. Auch hier findet ein Vertrauenstransfer statt – Trusted Third Parties fordern das Vertrauen aufgrund ihrer Expertise und übertragen durch ihre Urteile das Vertrauen der Verbraucher und Kunden auf Hersteller oder Produkte und Leistungen. Qualität ist zwar die Grundvoraussetzung, reicht aber allein nicht aus. Vertrauen in Qualität muß wiederum vermittelt werden. Dem zufolge müssen die Trusted Third Parties ihre Neutralität und Kompetenzen nach beiden Seiten ausspielen. Ansonsten werden sie für die Rezipienten unglaubwürdig und für die Beurteilten, die sich diese vertrauensbildende Leistung zu Nutze machen wollen, wertlos. Institutionelle Mittler, denen kein Vertrauen entgegengebracht wird, werden keine erfolgreiche

[58] Beispielsweise sind in fast allen Computerzeitschriften Hard-, Software und Dienstleistungstest zu finden.

Vertrauensbildung praktizieren können. Institutionelle Vertrauensbildung muß zuerst Vertrauen in sich selbst festigen, bevor dieses Vertrauen auf ein wie auch immer geartetes System übertragen werden kann.

Eingangs wurde bereits angesprochen, daß Vertrauen in Internet-Zahlungssysteme schon deshalb institutionell vermittelt werden muß, weil Objekt und Zielgruppe der Vertrauensbildung in einem globalen, auch zahlenmäßig kaum zu überblickenden Umfeld agieren. Durch Institutionen ist dieser Umfang erst zu handhaben. Wie unter 6.1.2 anhand der Verwendung asymmetrischer Verschlüsselungstechniken noch dargestellt wird, ist dieser Aspekt von großer Relevanz für die institutionelle Vertrauenssicherung bei Internet-Zahlungssystemen. Deutlich wird dies schon bei konventionellen Zahlungssystemen auf Kreditkartenbasis. Die Kreditkarte wird deshalb akzeptiert, weil sowohl Händler wie Kunde über Institutionen (Banken oder Kreditkartenunternehmen) in einen gemeinsamen Handlungskontext eingebunden sind, in dem die korrekte Abwicklung der Transaktion garantiert ist. Ansonsten müßten die Geschäftspartner erst eine persönliche Vertrauensbeziehung aufbauen. Für Internet-Zahlungssysteme kann die persönliche Vertrauensbeziehung nicht als realistische Alternative in Betracht gezogen werden. Institutionen können im Gegensatz zu Personen Garantien geben, die über das persönliche Umfeld hinausgehen.[59] Das ist einer der Gründe für die Notwendigkeit institutioneller Vertrauensbildung im Bereich der Internet-Zahlungssysteme.

Kuhlen schreibt vertrauensbildenden Institutionen eine Objektivierungsfunktion auf Basis von Expertenwissen zu.[60] Einzelne Experten, bzw. deren Einschätzungen müssen per se nicht objektiv sein. Indem Institutionen dieses Wissen bündeln und damit Einschätzungen und Urteile der Experten gegeneinander abwägen, erfüllen sie zweierlei Funktionen.

Zum einen sind Institutionen in der Lage, durch die Kombination von Expertenwissen einen wesentlich breiteren Bereich abzudecken als dies einzelne Experten vermögen. Gerade weil Vertrauen allgemein von vielen Faktoren abhängt und weil Vertrauensbildung bei Internet Zahlungssystemen sich auf verschiedene technische, organisatorische und rechtliche Bereiche beziehen muß, ist diese Funktion wichtig. Zum anderen schafft die Kombination von unterschiedlichen Expertenwissen innerhalb eines Vertrauensnetzwerks einen Interessenausgleich im Sinne der von Kuhlen angesprochenen Objektivierung. Subjektive Einschätzungen von Experten werden durch institutionelle Mechanismen konsolidiert, so daß die institutionelle Vertrauensbildung auf einer Grundlage aufbaut, die nicht nur der geforderten Expertise, sondern auch der geforderten Objektivität weitgehend entgegen kommt. Die Frage nach der (berechtigten) Vertrauenswürdigkeit von Vertrauen

---

[59] Vgl. Kahre/Rifkin (1997), S.86
[60] Kuhlen (1999), S.81

reklamierenden Institutionen ist in diesem Fall eher mit „Ja“ zu beantworten, wenn sich auch letzte Zweifel nie vollkommen ausräumen lassen: Auch Experten können irren, Objektivität kann geschickt vermittelte Subjektivität sein. Der Charakter einer öffentlichen Einrichtung erschwert jedoch die Durchsetzungschancen für Partikularinteressen. Zum einen bieten Institutionen Zugangspunkte für unterschiedliche Interessen; zum anderen wird ihr Verhalten durch Öffentlichkeit transparent und damit kontrollierbar.

Der Anspruch, daß Institutionen öffentlich zugängliche Einrichtungen sind, entspricht dieser Einsicht: Transparenz erleichtert die Vertrauensbildung. Transparenz wird jedoch nicht allein durch Öffentlichkeit erzielt, wenn diese auch konstitutiv für Transparenz ist. Im Bereich der Vertrauenssicherung bei Internet-Zahlungssystemen ist es üblich, daß die Träger der institutionellen Vertrauenssicherung ihre Ziele, Maßnahmen und sonstige Informationen offen zugänglich im Internet anbieten. Policy Papers oder Informationen über Zahlungssysteme und digitale Signaturen auf den Web Servern der Trust Center, Banken oder Kreditinstitute sind hierfür ein gutes Beispiel. Transparenz wird gebildet, indem Information frei zugänglich gemacht wird. Dadurch leisten solche Publikationen einen erheblichen Beitrag zu einem Zustand, den Kuhlen mit Referenz auf David Brin als informationelle Symmetrie bezeichnet.[61]

Nicht zuletzt ist gerade im Bereich der den gängigen Internet-Zahlungssystemen zugrunde liegenden digitalen Signaturen ein Bedarf an institutioneller Vertrauenssicherung festzustellen. Der Gesetzgeber reagierte in Deutschland mit einer weltweit bisher einmaligen gesetzlichen Regelung, dem Signaturgesetz (SigG) und der Signaturverordnung (SigV). Die Signaturgesetzgebung ist in dieser Hinsicht sicher die wichtigste, vertrauensbildende Maßnahme des Staates im Bereich der digitalen Signaturen und damit auch der Internet-Zahlungssysteme. Ziel der Siganturgesetzgebung ist die Schaffung einer sicheren Infrastruktur für digitale Signaturen. Damit das Konzept der digitalen Signatur[62] funktionieren kann, ist eine Infrastruktur erforderlich, die den freien Zugang zu den öffentlichen Schlüsseln (Public Keys) der Teilnehmer ermöglicht. Diese Public Key Infrastructure (PKI) muß institutionell eingebettet sein, um öffentliche Schlüssel wirklich öffentlich (d.h. allgemein zugänglich) zu halten. Nur so sind die öffentlichen Schlüssel der Teilnehmer mit wenig Aufwand bekannt zu machen, zu verifizieren und gegebenenfalls zu widerrufen. Diese Anforderung der asymmetrischen Verschlüsselung erklärt aus technischer Sicht die Forderung nach institutioneller Vertrauensbildung im Bereich digitaler Signaturen in Form von Trust Centern oder Webs of Trust.

---

[61] Vgl. Kuhlen (1999), S.82
[62] Vgl. 6.2.1 Digitale Signatur

Institutionelle Vertrauensbildung ist grundlegend für die Gewinnung von Vertrauen in Internet-Zahlungssysteme. Umfang, Interdisziplinarität, technische und organisatorische und rechtliche Faktoren gehen über den Bereich hinaus, der durch direkte und persönliche Vertrauensbildung abgedeckt werden kann. Dies gilt sowohl für die Bildung von Vertrauensbeziehungen zwischen Individuen, als auch zwischen Individuen und Institutionen und schon lange für Vertrauen zwischen den beteiligten Institutionen. Institutionelle Vertrauensbildung muß ergänzend Maßnahmen der persönlichen Vertrauensbildung durch ‚Facework Commitments' von Mitgliedern oder Repräsentanten einsetzen. Auch die Vertrauensbildung zwischen Organisationen oder allgemeiner zwischen Institutionen, die aufgrund der Vielzahl komplexer und komplex interagierenden Systeme notwendig wurde, ist letztendlich gesteuert durch das Vertrauen der Menschen, die diese Institutionen ausfüllen. Einer Institution wird eher Vertrauen entgegengebracht, wenn dieses Vertrauen durch Menschen aus Fleisch und Blut transportiert wird.

5 Kritische Vertrauensaspekte

Bei obigen Ausführungen zur institutionellen Vertrauensbildung wurden bereits einige, für Internet-Zahlungssysteme vertrauenskritische Faktoren angerissen. Um dieses Verständnis zu vertiefen, ist es wichtig, die elektronischen Märkte, auf denen Internet-Zahlungssysteme zum Einsatz kommen, als ein besonderes Umfeld zu erkennen, auf dem die Vertrauensfrage unter anderen Prämissen gestellt wird, wie bei konventionellen, physikalisch lokalisierbaren Transaktionen.

5.1 Vertrauen auf elektronischen Märkten

Elektronische Märkte, bzw. elektronische Marktplätze „als institutionelle Realisierung abstrakter elektronischer Märkte“[63] sind ein Beispiel für den giddens'schen Begriff des „Disembedding“ (‚Entbettung‘). Die von Kuhlen[64] geforderte Einrichtung von regionalen Marktplätzen kann als Gegenreaktion auf diese ‚Entbettung‘ verstanden werden. Anbieter und Kunden werden auf regionalen Marktplätzen wieder in einen lokalen, durch Nähe und Vertrautheit geprägten Kontext eingebunden. Insofern sind regionale Marktplätze sicherlich eine vertrauenschaffende Einrichtung auf elektronischen Märkten. Zahlungssysteme des Internet operieren zwar auch, aber eben nicht nur auf regionalen Marktplätzen, sie müssen funktionsfähig auf allen globalen, nationalen und regionalen Marktplätzen sein. Ansonsten handelt es sich nicht um Internet-Zahlungssysteme, sondern um Zahlungssysteme für bestimmte Marktplätze, für die wiederum andere Anforderungen gelten, als für Internet-Zahlungssysteme.

Wie stellen sich nun die Verunsicherungen auf elektronischen Marktplätzen aus Sicht des Massenpublikums dar? Wenn im virtuellen Sinne ein elektronischer Marktplatz betreten wird, steht steht zunächst keine finanzielle Transaktion im Vordergrund. Vor der Kaufentscheidung, die letztlich der Auslöser für die finanzielle Transaktion ist, steht die Information, bspw. über Produkte, Preise, Zahlungs- und Lieferbedingungen. Bei einem Einkauf in der ‚realen Welt‘ geschieht dies ‚Face-to-Face‘ zwischen Kunde und Verkäufer. Dieser gemeinsame (räumliche und zeitliche) Kontext fehlt im Internet. Kunde und Anbieter müssen sich nicht im selben zeitlichen und lokalen Kontext aufhalten, können eventuell ihre wahre Identität verschleiern. Ebenso sind Informationen oder Güter und Dienstleistungen nicht direkt einsehbar. Ob sich hinter dem elektronischen Abbild eines Unternehmens wirklich dieses Unternehmen verbirgt, ob Leistungen und Güter so erbracht oder geliefert werden, wie elektronisch angeboten, ob die Abrechnung wirklich den dargestellten Preisangaben entspricht und die Garantiezusagen eingehalten werden, ist für

---

[63] Kuhlen (1996b), S.1 – aufgrund des Themenstellung soll an dieser Stelle nur auf die kommerzielle Funktion von elektronischen Marktplätzen eingegangen werden.

[64] Vgl. Kuhlen (1996b)

potentielle Käufer ungewiß. Ebenso wissen Anbieter zunächst nicht, wer sich hinter dem elektronischen Pseudonym des Online Shoppers verbirgt und wie dessen Absichten aussehen. Die Anonymität im Internet macht Manipulation möglich, sowohl für Anbieter wie für potentielle Kunden. „Man ist sich nach wie vor unsicher über die Leistungen, über die Verläßlichkeit, über Schutz vor Mißbrauch."[65]

Diese Verunsicherung betrifft sämtliche Phasen der Transaktion:[66]

- ☞ Informations- (Anbahnungs-) Phase: Herkunft, Relevanz und Zugehörigkeit der für die Kaufentscheidung benötigten Information sind nicht verläßlich einzuschätzen.

- ☞ Abwicklungsphase: Es ist nicht ohne Weiteres sichergestellt, daß die finanziellen Transaktionen von den legitimierten Personen durchgeführt und nicht abgehört oder manipuliert werden und die bezahlten Leistungen wirklich elektronisch oder physikalisch im vereinbarten Umfang geliefert, abgerechnet und bezahlt werden.

- ☞ After-Sales Phase: Unsicherheit, ob Service- und Garantiezusagen wirklich eingehalten werden und Anbieter nicht bestreiten, jemals betreffende Zusagen gemacht zu haben oder sogar nach einem schnellen Geschäft spurlos vom elektronischen Marktplatz verschwunden sind.

- ☞ Gesamte Transaktion: Unsicherheit über die Verwendung der vom Kunden zurückgelassenen Interaktionsdaten, wie etwa der eMail Adresse, Präferenzen und andere persönliche Angaben.

Im Rahmen dieser Arbeit sind die Unsicherheitsmomente interessant, die sich während der Abwicklungsphase ergeben. Schon aus diesen Unsicherheitsmomenten läßt sich erahnen, daß Identitätssicherung, Verläßlichkeit im Sinne der zuverlässigen Durchführung der vom Anwender beabsichtigten Transaktion und Vertraulichkeit die Schlüsselbereiche sind, aus denen die Anforderungen an die Sicherheit von Internet-Zahlungssystemen abgeleitet werden können. „Unter Sicherheit ist im umfassenden Sinne das *Ziel* zu verstehen, informationsverarbeitende Systeme so zu entwerfen, herzustellen und einzusetzen, daß ein angemessenes Maß an Schutz gegenüber den relevanten Gefahren gegeben ist."[67] Die Frage ist nun, welches die relevanten Gefahren sind, oder besser, welches die vertrauenskritischen Bereiche bei Internet-Zahlungssystemen sind?

---

[65] Kuhlen (1998a)
[66] Natürlich lassen sich Kunden-Anbieter Beziehungen auch anders strukturieren, vgl. Schuster/Färber/Eberl (1997), S.6f
[67] Kersten (1993), S.X

5.2 Kritische Vertrauensaspekte bei Internet-Zahlungssystemen

5.2.1 Modell eines Internet-Zahlungsablaufs

Generell sind bei einem Zahlungsvorgang zumindest ein Käufer, dessen Pflicht die Leistung des Kaufpreises ist und ein Verkäufer, der gegen Erhalt des Kaufpreises eine entsprechende Leistung erbringt, involviert. Da bei Internet-Zahlungen (wie bei allen unbaren Zahlungsformen) kein physikalisches Geld transferiert werden kann, muß mindestens eine, meist jedoch zwei[68] weitere Parteien, in der Regel Banken, dafür sorgen, daß der Gegenwert der elektronischen Zahlung gedeckt wird.

Im einzelnen lassen sich folgende Vorgänge unterscheiden:

1. Der Kunde erhält von seiner Bank ein Medium, mit dem er Internet-Zahlungen durchführen kann.
2. Der Kunde wickelt den Zahlungsvorgang mit dem Händler ab.
3. Der Händler gibt die Zahlungsinformationen an seine Bank weiter.
4. Die Händlerbank belastet die Kundenbank mit dem zahlbaren Betrag.
5. Die Kundenbank schreibt den belasteten Betrag der Händlerbank gut.

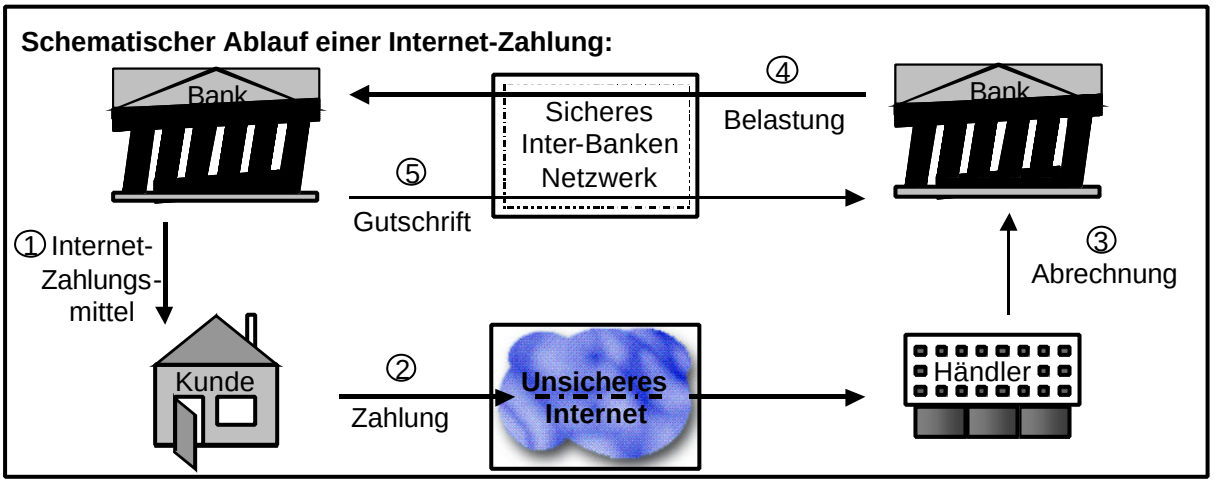

Abbildung 1: Schematischer Ablauf einer Internet-Zahlung[69]

Die Deckung der Internet-Zahlung verläuft genau umgekehrt. Der Kunde hat zuvor ein Konto bei einer Bank eröffnet, die Zahlungen mittels Internet-Zahlungssystemen anbietet. Beispielsweise überweist oder zahlt er Geld bar auf dieses Konto ein. Beim Belastungsvorgang wird vom Kundenkonto der belastete Betrag abgebucht und dem Konto des Händlers gutgeschrieben. Die elektronische Transaktion zwischen den Banken wird bisher (noch) über Inter-Bankennetzwerke, sog. Clearing-Netzwerke

[68] Z.B. wenn Kunde und Händler bei verschiedenen Kreditinstituten sind.
[69] Vgl. Waidner/Janson (1995)

abgewickelt.[70] Sicherheitsgründe sind dabei nicht vorrangig, denn es wäre heute technisch ohne weiteres möglich, durch kryptographische Verfahren ausreichende Sicherheit zu garantieren. In geschlossenen, d.h. proprietären Netzwerken – wozu Inter-Bankennetze zählen – ist dies jedoch mit weitaus geringerem Aufwand möglich.

Während des Zahlungsvorganges entstehen sowohl aus Händler- wie aus Kundensicht Unsicherheitsmomente[71] bezüglich

- ☞ der Identität von Kunde und Anbieter,
- ☞ der Ausspähung und mißbräuchlichen Verwendung der während dem Zahlungsvorgang übermittelten Informationen,
- ☞ der (intensional) korrekten Abwicklung des Zahlungsvorganges durch das Internet-Zahlungssystem,
- ☞ der Transaktionsnegierung, d.h. es wird abgestritten, daß eine Bestellung aufgegeben oder bestätigt wurde,
- ☞ der nachträglichen Verfälschung der Daten, bspw. indem Kreditkartennummer oder Zahlungsbetrag manipuliert werden,
- ☞ und letztendlich der juristischen Behandlung von digitalen Zahlungsvorgängen im Falle eines Zivilprozesses.

5.2.2 Sicherheitsanforderungen an Internet-Zahlungssysteme

Wollen Internet-Zahlungssysteme als *sicher,* bzw. im Kontext der Informationstechnik, als *vertrauenswürdig*[72] gelten, muß diesen Unsicherheiten durch Berücksichtigung folgender Faktoren Rechnung getragen werden:[73]

- ☞ Verläßlichkeit / Verbindlichkeit
  - Die Verfügbarkeit des Systems muß jederzeit gegeben sein.
  - Transaktionen müssen so durchgeführt werden, wie es der Benutzer beabsichtigt.
  - Der Status der Zahlung muß eindeutig sein – entweder die Transaktion wurde durchgeführt oder nicht. Elektronisch schwebende oder unvollendete

---

[70] Vgl. Waidner/Janson (1995)

[71] Vgl. Uebelacker / Kurz (1996), S.169 für allgemeine Risiken für Zahlungsverkehr im Internet und vgl. Schuster/Färber/Eberl (1997), S.6ff für ein deskriptives Beispiel der Sicherheitsrisiken eines Einkaufs via Internet. Vgl. Kristoferitsch (1998), S.62 für Anforderungen an Internet-Zahlungssysteme.

[72] Vgl. Kersten (1993), S. X

[73] Vgl. für ähnliche Gliederungen Kuhlen (1999), S.279 und S.339. Vgl. Schuster/Färber/Eberl (1997), S.9, vgl. Waidner/Janson (1995), vgl. Kristoferitsch (1998), S.64f, vgl. Garfinkel/Spafford (1997), S.113

Zahlungsvorgänge, bspw. durch einen Server- bzw. Netzwerkzusammenbruch, müssen ausgeschlossen sein.

☞ Integrität der Daten

- Die Daten dürfen während der Übertragung nicht durch Dritte ausgespäht oder manipuliert werden können.[74]
- Eventuelle Manipulationen müssen zuverlässig festgestellt werden können.

☞ Authentizität / Identität[75]

- Die Identität von Sender und Empfänger muß eindeutig zu bestimmen sein. Es muß sichergestellt sein, daß es sich bei den betroffenen Akteuren wirklich um diejenigen handelt, die sie vorgeben zu sein.
- Sender und Empfänger müssen bezüglich der ausgetauschten Information eindeutig referenzierbar sein, d.h. die ausgetauschten Informationen müssen den Akteuren eindeutig zuzuordnen sein.

☞ Vertraulichkeit

- Übertragene Informationen dürfen nur den Akteuren zugänglich sein, die diese tatsächlich für die Abwicklung der Internet-Zahlung benötigen.
- Im Idealfall besteht für den Anwender die Möglichkeit, Transaktionen anonym durchzuführen.

Die Verläßlichkeit und Verbindlichkeit der Transaktionen ist grundsätzlich abhängig von der verwendeten Hard- und Software, respektive ihrer fehlerfreien Funktionsfähigkeit. Der Authentizität, Integrität und Vertraulichkeit wird bei Internet-Zahlungssystemen in der Regel durch den Einsatz kryptographischer Verfahren entsprochen. Der Einsatz von asymmetrischen Verschlüsselungsverfahren (Public Key Verfahren), ihre Kombination mit symmetrischen Verfahren und Einweg-Funktionen (sog. Hash-Funktionen), kann bei korrektem Einsatz unter mathematischen Gesichtspunkten heute als sicher angesehen werden.[76]

Authentizität wird nach dem heutigen Stand der Technik durch digitale Signaturen gewährleistet. In Deutschland wurde im Rahmen des IuKDG (Informations- und Kommunikationsdienste-Gesetz) durch das SigG und die SigV – eine auf nationaler Ebene weltweit bisher einmalige Regelung – Rahmenbedingungen definiert, unter denen die Verwendung digitaler Signaturen als sicher gelten kann und Fälschungen

---

[74] Vgl. Kristoferitsch (1998), S.63 oder vgl. Schuster/Färber/Eberl (1997), S.4 für eine verständliche Erklärung des Packet Sniffing, dem Ausspähen der über TCP / IP versandten Datenpakete.

[75] Vgl. Waidner/Janson (1995), die Identität / Authentizität als Hauptsicherheitsproblem bei Internet-Zahlungssystemen sehen.

[76] Vgl. Sicherheit in der Informationsgesellschaft (1999b), vgl. Grossman (1997), S.61

zuverlässig aufgedeckt werden können.[77] Durch digitale Signaturen soll bei Zahlungsvorgängen im Internet sichergestellt werden, daß die Authentizität der beteiligten Parteien und der transferierten Information gewährleistet ist. Damit ist es möglich, sowohl den Zahlungsvorgang selbst bestimmten Person zuzuordnen, als auch die dabei übertragenen Informationen.

Integrität bedeutet, daß Zahlungsinformationen während der Übertragung durch das Internet nicht manipuliert wurden. Integrität wird z.B. bei SET basierten Internet-Zahlungsvorgängen[78] durch Erzeugung eines sog. Hash-Wertes gesichert. Dabei erzeugt der Absender einer Information mittels einer Hash-Funktion einen digitalen Fingerabdruck (Hash-Wert oder Message Authentication Code, MAC). Der Empfänger der Information kann diesen Prozeß wiederholen; sind die empfangene und die vom Empfänger neu berechnete Prüfsumme identisch, wurde das Dokument nicht verändert.

Vertraulichkeit steht für den Schutz der übertragenen Daten vor Ausspähung durch nicht autorisierte Dritte. Bestell- und Zahlungsinformationen dürfen nur den direkt beteiligten Akteuren zugänglich sein, bzw. nur den Akteuren, die einen bestimmten Informationsbestandteil zur Abwicklung der Transaktion benötigen. Eine beteiligte Bank muß für die Abrechnung lediglich wissen, welche Kreditkartennummer und in welcher Höhe welche Konten zu belasten sind, nicht jedoch, was konkret bestellt wurde. Umgekehrt benötigt der Händler zwar Bestellinformation und Zahlungsbedingungen, aber nicht die Kreditkartennummer des Kunden. Diesen Überlegungen trägt z.B. der SET-Standard Rechnung. Idealerweise besteht für Anwender sogar die Möglichkeit, wie bei Bargeschäften anonym zu bleiben. Das Internet-Zahlungssystem eCash löst das Problem der Vertraulichkeit, indem die Möglichkeit besteht, digitales Geld anonym zu generieren.[79] Durch Verwendung der asymmetrischen Kryptographie in Form digitaler Signaturen läßt sich nicht nur, wie oben angesprochen, Authentizität gewährleisten, sondern auch die Vertraulichkeit der Transaktion. Schließlich liegt der originäre Zweck kryptographischer Verfahren darin, Informationen vertraulich zu halten.

Die mathematische Sicherheit kryptographischer Verfahren ist nicht der einzige Faktor, der für die Sicherheit und Vertrauenswürdigkeit der Internet-Zahlungssysteme ausschlaggebend ist. Das Konzept der asymmetrischen Verschlüsselung besteht in der Verwendung öffentlicher und privater Schlüssel. Im Rahmen der Authentizitätssicherung muß zum einen die Identität des Schlüsselinhabers verifiziert werden und zum anderen eine Infrastruktur geschaffen werden, in der die sichere Verwaltung der Schlüssel gewährleistet ist. „Es muß sichergestellt werden, daß ein Schlüssel, der einem Kommunikationspartner zugesandt wird, garantiert dem

---

[77] Vgl. §1 I SigG
[78] Vgl. 6.3.1 SET Standard
[79] Vgl. 6.3.2 eCash

anderen zuzuordnen ist“[80] und seine Gültigkeit geprüft werden kann. Dieses Problem kann nicht durch das kryptographische Verfahren selbst gelöst werden. Die Authentifizierungsleistung, bei der Schlüssel und Identität ‚verknüpft‘ werden, muß durch einen neutralen Dritten erbracht werden. Demzufolge sind neben der Sicherheit der kryptographischen Verfahren die institutionelle Organisation und darüber hinaus die gesetzlichen und politischen Rahmenbedingungen, ohne die keine Rechssicherheit erzielt werden kann, ausschlaggebend für die Vertrauensbildung.

Diese Überlegungen haben bereits die vertrauenskritischen Bereiche angesprochen, die die institutionelle Vertrauensbildung bei Internet-Zahlungssystemen abdecken muß. Im folgenden Kapitel wird daraus eine Systematik vertrauenskritischer Bereiche erarbeitet.

5.2.3 Systematik vertrauenskritischer Bereiche

Angesichts der dargestellten Sicherheitsanforderungen müssen vertrauensbildende Institutionen in der Lage sein, Vertrauen in das technische, organisatorische und rechtliche (sicherlich auch politisch bestimmte) Umfeld der Internet-Zahlungssysteme herzustellen. Eine gewisse Vorleistung für die Systematisierung der vertrauenskritischen Bereiche läßt sich bei Kristoferitsch finden, der drei Sicherheitsbereiche bei Internet-Zahlungssystemen identifiziert:[81]

1. Verschlüsselungsmechanismen, d.h. die kryptographischen Verfahren, die den Zahlungssystemen im Internet zugrunde liegen.
2. Schutz vor Fehlfunktionen des Systems, aufgrund von Konzeptions- oder Programmierfehlern, die aufgrund einer Vielzahl von denkbaren Ausnahmesituationen kaum zu vermeiden sind.
3. Schutz vor internen Fehlerquellen, z.B. die Prävention von Sabotage und Fahrlässigkeit der Mitarbeiter von Trust Centern, unangemessene (Zugangs-) Berechtigungskonzepte etc.

Gerade durch den dritten Punkt wird deutlich, daß nicht alleine die technischen Komponenten der Hard-, Software einschließlich der kryptographischen Verfahren, die im ersten Punkt erwähnt werden, sondern auch deren konkrete Anwendung und Umsetzung durch organisatorische Maßnahmen bedeutsam für die Vertrauenswürdigkeit der Internet-Zahlungssysteme sind. Rechtliche Aspekte berücksichtigt Kristoferitsch allerdings nicht. Umfassender ist die Feststellung von Kuhlen: „Weiterhin [...] ist das gesamte Umfeld, in dem Kryptographie zum Einsatz kommt, der entscheidende vertrauensbestimmende Faktor. Das Umfeld ist nicht nur ein technisch bestimmtes, sondern in hohem Maße durch politische, rechtliche und

---

[80] Schuster/Färber/Eberl (1997), S.16
[81] Vgl. Kristoferitsch (1998), S.62f

soziale Aspekte beeinflußt."[82] Die hier eingeführte Systematisierung nach technischen, organisatorischen und rechtlichen Vertrauensbereichen berücksichtigt diesen Gedanken.

5.2.3.1 Technische Aspekte

5.2.3.1.1 Funktionsfähigkeit des Zahlungssystems

Die einwandfreie Funktionalität der eingesetzten Hard- und Software ist eine Grundbedingung für Internet-Zahlungssysteme. Die Existenz funktionsfähiger Internet-Zahlungssysteme zeigt, daß diese Anforderungen erfüllt werden (können).[83] Viele Internet-Zahlungssysteme sind nicht rein Software basiert. Zur Erhöhung der Sicherheit werden häufig Smartcards[84] verwendet. Auf diesen (konventionellen Kreditkarten optisch sehr ähnlichen) Karten mit eingebautem Microchip können Geldbeträge oder digitale Signaturen gespeichert und mit einer geheimen PIN (Personal Identification Number) geschützt werden.

Gängige Internet-Zahlungssysteme wie SET oder eCash bedienen sich einer Kombination verschiedener Verschlüsselungsmechanismen, um einen möglichst hohen Sicherheitsstandard zu gewährleisten. Einmal von den im nächsten Punkt angesprochenen Verfahren selbst abgesehen, muß diese Kombination sicher sein, d.h. es dürfen keine Sicherheitslücken entstehen. „Auch wenn die Sicherheit der mathematischen Verfahren und der verwendeten Chipkartentechnik unterstellt wird, führt die Implementation dieser Techniken in andere technische Systeme und in sogenannten Anwendungskontexten zu Schwachstellen."[85] Selbst bei Programmen, die gleiche Verfahren einsetzen, kann es deshalb zu großen Unterschieden im Sicherheitsniveau kommen.[86] Eine große Gefahr besteht in der unsachgemäßen Implementierung der RSA Verschlüsselungsverfahrens (benannt nach seinen Erfindern Rivest, Shamir und Adleman) in Internet-Zahlungssysteme.[87]

Das Zahlungssystem muß nicht nur gegen Mißbrauch durch Dritte gesichert sein, sondern auch gegen Fehlbedienungen des Benutzers. Es muß bedienungsfreundlich, einfach erlernbar, robust und funktional adäquat sein. Zahlungsvorgänge dürfen nur initiiert werden, wenn eine absichtliche Handlung des Benutzers vorliegt.

5.2.3.1.2 Sicherheit kryptographischer Verfahren

Kryptographische Verfahren, die bspw. in Form der Verschlüsselung, der digitalen Signatur und als Hash-Funktionen bei Internet-Zahlungssystemen zum Einsatz

---

[82] Kuhlen (1999), S.284
[83] Vgl. Kristoferitsch (1998), S.134f: Natürlich gibt es auch negative Beispiele, wie das umständliche und für Internet-Händler sehr teure System NetCash.
[84] Vgl. Utimaco (1999) für eine Einführung in die Technologie der Smart Cards.
[85] Roßnagel (1998), S.3315
[86] Vgl. Kristoferitsch (1998), S.75
[87] Vgl. Kristoferitsch (1998), S.76

kommen, sind unter mathematischen Gesichtspunkten als sicher einzustufen.[88] Die Sicherheit eines kryptographischen Verfahrens ist abhängig vom Aufwand, den ein nicht autorisierter Dritter (Angreifer) hat, um den Schlüssel zu berechnen und damit die Information zu dechiffrieren. Ist dieser Aufwand größer, als der Nutzen des Angreifers, dann gilt das Verfahren als sicher.[89] Dies ist z.B. der Fall, wenn die Geheimhaltungszeit einer Information unter der Rechenzeit liegt, die für ihre Dechiffrierung notwendig ist. Ausschlaggebend ist dabei die Länge der verwendeten Schlüssel. Je länger diese Schlüssel sind, desto größer ist der Aufwand, sie zu errechnen. Eine Verdoppelung der Schlüssellänge von 64 Bit auf 128 Bit verdoppelt beispielsweise die möglichen Kombinationen und damit den Aufwand für den Angreifer nicht, sondern steigert ihn exponentiell.

Aus diesem Grund kann davon ausgegangen werden, daß steigende Rechenkapazität wie häufig vermutet wird, gerade nicht dazu führt, daß kryptographische Verfahren unsicherer werden, sondern, daß sie im Gegenzug die Verwendung fast beliebig langer Schlüssel ermöglichen, die einen exponentiell höheren Dechiffrierungsaufwand bedeuten. Die Frage, wie lange ein sicherer Schlüssel sein muß, ist nicht ohne weiteres zu beantworten. Das US Unternehmen RSA Data Security sucht die Anwort, indem es Wettbewerbe für das erfolgreiche Brechen von Schlüsseln veranstaltet.[90] Wegen der erforderlichen Rechenleistung schließen sich dabei weltweit bis zu einige tausend Computern zu einem sog. ‚Code Cracking Ring'[91] zusammen, der durch eine rechenintensive Primzahlfaktorzerlegung versucht, den betreffenden Schlüssel zu errechnen. Bei diesem Verfahren wird eine Zahl (der öffentliche und damit bekannte RSA Schlüssel) in zwei Primzahlen zerlegt, aus deren Multiplikation sich der gesuchte geheime Schlüssel errechnen läßt. Diese Faktorisierung ist bei langen Primzahlen in angemessener Zeit nicht mit einem einzelnen Computer zu schaffen: „As with several other recent large scale factoring projects, we propose to attack this number with a very large number of workstations independently operating at dozens of research and corporate networks around the world. We are soliciting volunteers to provide compute cycles to help us towards our goal."[92] Bereits 1994 gelang es auf diese Weise, im Rahmen des von RSA Data Security gesponsorten „RSA 129 Factoring Challenge Project", eine 129-stellige Zahl in ihre beiden Primzahlfaktoren zu zerlegen. Mehr als 600 Freiwillige waren damit 8 Monate in einem ‚Key Cracking Ring' beschäftigt. Inzwischen gelang bereits die Zerlegung einer 140-stelligen Zahl in ihre Primzahlfaktoren.[93] Ein solcher Ring, in dem mehrere tausend Computer insgesamt fünf Monate parallel rechneten, konnte

---

[88] Vgl. Sicherheit in der Informationsgesellschaft (1999b), vgl. Grossman (1997), S.61
[89] Schuster/Färber/Eberl (1997), S.10
[90] Vgl. RSA (1999e)
[91] Vgl. Cypherpunks (1999), vgl. Distributed.net (1999)
[92] Wright (1994)
[93] Vgl. RSA (1999i)

im Juni 1997 einen 56 Bit DES (Data Encryption Standard) Schlüssel brechen. Auch Netscapes 40 Bit RC4 Algorithmus konnte bereits mittels mehrerer Hochleistungscomputer gebrochen werden. Wie hieraus deutlich wird, gestaltet sich bereits das Brechen dieser relativ ‚kurzen' Schlüssel als äußerst aufwendig. Ein Angreifer alleine hätte mit Hilfe eines Standard PCs statistisch gesehen kaum eine Chance, den richtigen Schlüssel durch Zufall zu finden. Experten gehen davon aus, daß Schlüssellängen größer 75 Bit durch Brute Force Attacks[94] wie oben beschrieben, in angemessener Zeit nicht zu brechen sind.[95] M. Blaze von den Bell Labs geht gar davon aus, daß Schlüssel mit einer Länge um die 90 Bit bei der prognostizierten Entwicklung der Informationstechnologie mindestens weitere 20 Jahre als sicher gelten dürften.[96] Darüber hinaus besteht allenfalls die Möglichkeit, daß neue Algorithmen, die auf teilweise noch zu erfindenden mathematischen Verfahren beruhen müßten, auch bei geringerer Rechenleistung das Brechen längerer Schlüssel ermöglichen. Allerdings ist es, wie im Falle gesteigerter Rechenleistung, auch hier denkbar, daß neue mathematische Verfahren die Entwicklung von noch stärkeren kryptographischen Verfahren stimulieren.

Egal welches Kryptoverfahren eingesetzt wird, Mathematik spielt bei der Beurteilung der Sicherheit eine entscheidende Rolle. Mathematik benötigt kein Vertrauen – sie schafft Zuversicht durch konkretes Wissen.[97] Warum ist institutionelle Vertrauenssicherung im Bereich technisch-abstrakter kryptographischer Verfahren dann notwendig? Kuhlen stellt fest, daß es beim derzeitigen Stand des Wissens über die Sicherheit kryptographischer Verfahren eigentlich nicht nötig ist, Vertrauen zu haben.[98] Eigentlich nicht – doch wer garantiert, daß die Experteneinschätzungen korrekt sind und richtig interpretiert werden? Kryptographische Verfahren sind abstrakt, komplex und damit für Laien kaum nachzuvollziehen. Dementsprechend ist auch die Bewertung der mathematischen Sicherheit dieser Verfahren durch das Massenpublikum nicht möglich. Kaum ein Anwender wird in der Lage sein, die für die Beurteilung der Sicherheit von Kryptoverfahren notwendige Wahrscheinlichkeitsrechnung durchzuführen und zu interpretieren. Dies gilt schon lange, wenn eine Kombination verschiedener Verfahren eingesetzt wird. Doch selbst wenn das Wissen um die Sicherheiit vorhanden ist, wird oftmals auf intuitiver Basis gehandelt. Unsicherheiten entstehen, wenn die eigene Intuition dem objektiv vorhandenen Wissen widerspricht. Selbst wenn es Milliarden von Faktorkombinationen gibt – niemand kann garantieren, daß ein Angreifer nicht bereits nach wenigen Minuten zufällig auf das richtige Primzahlenpaar stößt.

---

[94] Vgl. Kristoferitsch (1998), S.73ff: Ein Verfahren, um Schlüssel durch simples Ausprobieren aller möglichen Kombinationen zu brechen.
[95] Vgl. Kuhlen (1999), S.282
[96] Vgl. Grossman (1997), S.61
[97] Vgl. Kuhlen (1999), S.282
[98] Vgl. Kuhlen (1999), S.283

„Technische Realität, technische *Wahrheit* und soziale Realität, intuitive Welterfahrung können durchaus auseinanderklaffen und lassen selbst in an sich unberechtigten Situationen Unsicherheiten entstehen, die nicht durch bewiesene Sicherheit, sondern durch Vertrauen [...] kompensiert werden müssen."[99] Sicherheit muß – das gilt nicht nur für kryptographische, sondern auch für organisatorische und rechtliche Verfahren – wiederum durch Vertrauen versichert werden.[100]

5.2.3.2 Organisatorische Aspekte

Die Abwicklung von Internet-Zahlungen benötigt ein komplexes institutionelles und organisatorisches Umfeld, das den Erfordernissen der Identitätssicherung, des Key-Managements (Verwaltung der Teilnehmerschlüssel) und letztendlich auch der finanziellen Deckung der Transaktion Rechnung trägt.

5.2.3.2.1 Transaktionsabwickung

Letztendlich erfolgt die reale Deckung einer Internet-Zahlung durch Belastung oder Gutschrift über Kreditinstitute oder Banken. Transaktionen über Internet-Zahlungssysteme, bei denen nur Bits und Bytes und kein reales Geld transportiert wird, stoßen diese Vorgänge bei den entsprechenden Institutionen an. Anwender müssen deshalb nicht nur der korrekten Funktion des Zahlungssystems vertrauen, sondern auch darauf, daß Banken und Kreditinstitute den Prozeß, der durch die Internet-Transaktion ausgelöst wird, auch wirklich durchführen. Grundsätzlich gilt dieses Problem für alle unbaren Zahlungsformen. Aus der gängigen Verwendung konventioneller, unbarer Zahlungssysteme kann geschlossen werden, daß sich im Laufe der Zeit in diesem Bereich Vertrauen etabliert hat. Banken werden gemeinhin als vertrauenswürdige Dritte für die Abwicklung elektronischer Finanztransaktionen betrachtet, wie die hohe Akzeptanz von Kreditkarten beweist.

5.2.3.2.2 Authentizitätssicherung und Key-Management

Asymmetrische Kryptographieverfahren, die bei Internet-Zahlungssystemen eingesetzt werden, verlangen eine Identitätsfeststellung und ein verläßliches Key-Management. Eine Institution muß damit beauftragt werden, die Identität eines Schlüsselinhabers festzustellen, in Form eines digitalen Zertifikates mit seinem öffentlichen Schlüssel zu verknüpfen und zu verwalten. Weniger kritisch ist in der Praxis die korrekte Identitätssicherung durch Institutionen,[101] kritischer hingegen, wie vertrauenswürdig diese Institutionen hinsichtlich ihres Umgangs mit den Schlüsseln der Teilnehmer sind. Wird der Staat als vertrauenswürdiger Partner für Identitätssicherung und Key-Management erachtet, übernimmt er diese Funktion, bzw. delegiert an entsprechend zertifizierte und damit aus staatlicher Sicht

---

[99] Kuhlen (1999), S.284
[100] Kuhlen (1999), S.284
[101] Natürlich besteht immer ein gewisses Risiko, daß Trust Center bzw. deren Mitarbeiter falsche Zertifikate ausstellen; doch dieses Risiko ist auch bei konventionellen Identitätssicherungsleistungen gegeben: vgl. CCC (1984).

kompetente, vertrauenswürdige und sicherlich auch kontrollierbare Akteure. Das deutsche IuKDG geht von dieser Annahme aus und überträgt die Aufsicht über Key-Management Institutionen, sog. Zertifizierungsstellen (engl. Trust Center), an eine staatliche Einrichtung, die RegTP (Regulierungsbehörde für Telekommunikation und Post). Dagegen ist nichts einzuwenden, solange staatlichen Einrichtungen in dieser Hinsicht vertraut wird.

Die in den letzten Jahren heftig geführte Kryptographiekontroverse[102] könnte jedoch Zweifel aufkommen lassen, ob der Staat wirklich ein vertrauenswürdiger und somit unparteiischer Dritter ist und zukünftig sein wird. Weil starke Kryptoverfahren nicht nur zur Sicherung von Identität, Integrität und Vertraulichkeit legaler Kommunikation eingesetzt werden können, sondern auch für kriminelle Aktivitäten, wurden Forderungen laut, die Anwendung starker kryptographischer Verfahren ganz oder teilweise zu beschränken. In die gleiche Richtung geht der Vorschlag, den Trust Centern die Pflicht aufzuerlegen, Kopien von den privaten Schlüsseln der Teilnehmer zu speichern (sog. Key-Escrow Verfahren) oder ‚Generalschlüssel' zu implementieren (sog. Key-Recovery Verfahren), die im ‚Ernstfall' den Strafverfolgungsbehörden erlauben, verschlüsselte Nachrichten zu dechiffrieren. Wenn aus Furcht vor staatlichem Mißbrauch der Staat nicht als vertrauenswürdig eingeschätz wird, wer soll dann für die Identitätssicherung und das Key-Managment zuständig sein? Auch an der Neutralität und Vertrauenswürdigkeit von Banken oder Kreditinstituten kann gezweifelt werden, solange sie kommerzielle Aktivitäten und damit subjektive Interessen verfolgen, einmal ganz abgesehen davon, daß sie im möglichen Fall einer Regulierung kryptographischer Verfahren für staatliche Interessen instrumentalisiert werden können. Aus der Cyberpunk-Szene dürfte die Idee der sog. Webs of Trust entstammen, womit ursprünglich anonyme Remailer Systeme bezeichnet wurden,[103] die geprägt vom Mißtrauen gegenüber staatlicher Autorität die Sicherung von Authentizität und Vertraulichkeit der privaten Kommunikation im Internet auf eine unabhängige, private Grundlage stellen sollen. Diese Idee liegt dem PGP[104] (Pretty Good Privacy) Web of Trust, einem privat organisierten, selbstreferenzierenden Netzwerk, zugrunde. Die Realität zeigt, daß selbst große Webs of Trust funktionieren, eine globale Gestaltung aber relativ große Probleme mit sich bringt. „But PGP [Web of Trust (Anm. d. Verf.)] did demonstrate that for relatively regional communities [...], you can built up a quite secure communication path."[105] Für Zahlungssysteme des Internet ist diese privat organisierte Identitätssicherung kaum geeignet.

---

[102] Vgl. Möller (1997) für eine umfassende Darstellung der Kryptokontroverse in Deutschland.
[103] Vgl. Kuhlen (1999), S.312
[104] PGP ist eine asymmetrische Verschlüsselungssoftware, die von Phil Zimmermann im Internet publiziert wurde.
[105] Galvin (1997), S.19

5.2.3.3 Rechtliche Aspekte

Das Internet als globales, immaterielles und von rapidem technischen Fortschritt geprägtes Medium stellt die nationalstaatliche Gesetzgebung vor große Probleme. „Eine juristische Absicherung für Vertragsabschlüsse und Bezahlung über das Internet besteht so gut wie nicht.“[106] Dieses Defizit konnte auch durch das Signaturgesetz nicht beseitigt werden. Für den Einsatz von Internet-Zahlungssystemen ist nicht nur Vertrauen in ihre technischen und organisatorischen Aktionsbereiche notwendig, sondern auch in die rechtliche Verbindlichkeit des Zahlungsvorganges und die Verfügbarkeit starker Kryptographieverfahren.

5.2.3.3.1 Rechtliche Verbindlichkeit von Internet-Zahlungen

Mit der Frage der rechtlichen Verbindlichkeit des Zahlungsvorganges ist grundsätzlich das Problem des rechtlichen Stellenwerts digitaler Signaturen angesprochen, die im elektronischen Rechtsverkehr eine eigenhändige Unterschrift ersetzen sollen. Kann die Fälschung einer eigenhändigen Unterschrift von Experten (Graphologen) aufgedeckt werden, ist dies bei einer digitalen Unterschrift nicht möglich. Die Kopie einer digitalen Signatur ist vom Original nicht mehr zu unterscheiden. Gelingt es einem Angreifer durch Diebstahl oder kryptoanalytische Verfahren in den Besitz einer digitalen Signatur zu kommen, kann er sich damit im Namen des Inhabers authentifizieren, ohne daß dies durch Expertenbeweise festzustellen ist. Für Juristen und letztendlich auch für Anwender ist deshalb die kritische Frage, wie vertrauenswürdig eine derartige digitale ‚Unterschrift‘ ist und welche Beweiskraft sie im Vergleich zur eigenhändigen Unterschrift, die in weit über 3800 Rechtsvorschriften als verbindlich vorgeschrieben wird, besitzt.[107]

Rechtsgrundlage für digitale Signaturen ist in Deutschland das SigG, das am 1. August 1997 in Kraft trat und die entsprechende SigV. Die Signaturgesetzgebung soll eine Sicherheitsinfrastruktur schaffen, in der die Anwendung digitaler Signaturen als sicher gelten kann.[108] Das SigG geht dabei von einer Sicherheitsvermutung aus; digitale Signaturen, die den Rahmenbedingungen des SigG entsprechen, können als sicher gelten. Inwieweit diese Sicherheitsvermutung gerechtfertigt ist, wird seit Inkrafttreten des SigG diskutiert.[109] Unabhängig von der Sicherheitsvermutung ist problematisch, daß digitale Signaturen nicht den Formvorschriften des §126 I BGB entsprechen, die festlegen, daß eine „Urkunde von dem Aussteller eigenhändig oder mittels notariell beglaubigten Handzeichens unterzeichnet werden“[110] muß. Das Bundesjustizministerium reagierte bereits im Januar 1997, also knapp 7 Monate vor in Kraft treten der Signaturgesetzgebung, mit einem Gesetzesentwurf, der die

---

[106] Schuster/Färber/Eberl (1997), S.22; vgl. auch Informationweek (1998b)
[107] Vgl. Kuhlen (1999), S.286
[108] Vgl. §1 I SigG
[109] Vgl. 7.3.1.3.1 Rechtliche Basis digitaler Signaturen: Darstellung der Kontroverse zwischen Roßnagel und Hoeren.
[110] §126 I BGB

Änderung von Formvorschriften, die die eigenhändige Unterschrift vorsehen, einleiten soll. „Dieser Entwurf sieht in einem neu zu schaffenden §126 a BGB die Ersetzung der Schriftform durch eine ‚Textform' bei den zivilrechtlichen Bestimmungen vor, bei denen die strenge Schriftform entbehrlich ist. Nach Art. 1 Nr. 1 des Entwurfes zu §126 a Abs. 1 S. 1 BGB soll der Textform dabei bereits Genüge geleistet sein, wenn der Text in Schriftzeichen lesbar und die Person des Erklärenden erkennbar ist."[111] Die Textform soll dann als gewahrt gelten, wenn die elektronischen Daten jederzeit durch entsprechende Hilfsmittel, wie Computerprogramme, in Schriftzeichen umgewandelt und damit lesbar gemacht werden können. Dieser Gesetzesentwurf ist jedoch gescheitert, da Experten die Manipulationsrisiken einer solchen Textform (die im entsprechenden Gesetzesentwurf keinerlei Bezug zur Verwendung der digitalen Signatur erkennen ließen) als sehr hoch einschätzten. Die Anforderung an einen neuen Entwurf liegt darin, die entsprechenden Rechtsvorschriften des SigG stärker zu berücksichtigen.[112]

5.2.3.3.2 Staatliche Kryptoregulierung

Ein grundlegendes Problem für die Vertrauenswürdigkeit von Internet-Zahlungssystemen entsteht durch die Forderung nach staatlicher Kryptoregulierung, bspw. ein Importverbot für starke Kryptographiesysteme. In Deutschland besteht eine solche Regulierung (derzeit) nicht, wird allerdings hinsichtlich der Verbrechensbekämpfung kontrovers diskutiert.[113] Sieht man einmal von der kaum durchsetzbaren Lösung eines generellen Verschlüsselungsverbotes ab, bestehen zwei weitere Möglichkeiten der Kryptoregulierung.[114] Wie schon angedeutet besteht eine Überlegung darin, die Hinterlegung der geheimen, privaten Schlüssel der Teilnehmer in Key-Escrow oder Key-Recovery Systemen gesetzlich vorzuschreiben, auf die staatliche Einrichtungen im Bedarfsfall zugreifen können.[115] Andere Forderungen zielen darauf ab, nur staatlich genehmigte Verschlüsselungsverfahren zuzulassen.[116] Durch Begrenzung der maximal zulässigen Schlüssellänge der zugelassenen Verfahren soll die Entschlüsselung von Nachrichten mit potentiell kriminellen Inhalten durch staatliche Instanzen in angemessener Zeit möglich sein. Dieser Überlegung entspricht auch das US-amerikanische Vorgehen, den Export von kryptographischen Systemen, die Schlüssel mit mehr als 56 Bit verwenden, aus militärischen Sicherheitsgründen zu verbieten.[117] Diese Beschränkung ist mittlerweile

---

[111] Vgl. Brisch (1999)
[112] Vgl. Hillebrand/Büllingen (1998), S.43
[113] Vgl. Möller (1997)
[114] Vgl. Kristoferitsch (1998), S.86f für die möglichen Ausprägungen einer Kryptoregulierung
[115] Vgl. Kristoferitsch (1998), S.96 und vgl. Welt (1996): Eine enge Mitarbeiterin des Bundesdatenschutzbeauftragten favorisierte eine Key-Escrow Lösung
[116] Vgl. Möller (1997)
[117] Vgl. Kristoferitsch (1998), S.97f – 56 Bit Systeme dürfen nur dann exportiert werden, wenn ein Key-Recovery Modus implementiert ist, mit dem sich die geheimen Schlüssel nachbilden lassen. Ausnahmegenehmigungen bis 128 Bit können für Internet-Zahlungssysteme beantragt werden.

in einem Präzedenzfall als verfassungswidrig eingestuft worden.[118] Natürlich können solche Restriktionen nicht nur staatlichen Stellen die Verbrechensbekämpfung erleichtern, sondern es auch potentiellen Angreifern, die über das notwendige Wissen und eine entsprechende Ausstattung verfügen erleichtern, Internet-Zahlungen zu manipulieren Gelänge es einem Angreifer gar, in ein Key-Escrow System einzudringen und Zugriff auf die privaten Schlüssel der Teilnehmer zu bekommen, würde auf einen Schlag die gesamte vertrauliche Kommunikation und Identitätssicherung der Teilnehmer zerstört, was nicht zuletzt auch von der Wirtschaft als immenses Risiko betrachtet wird. Die Authentizität, Integrität und Vertraulichkeit von finanziellen Transaktionen im Internet wäre nicht mehr gewährleistet. Über das Für und Wider einer staatlichen Kryptoregulierung wird im Rahmen dieser Arbeit noch diskutiert; festzuhalten bleibt an dieser Stelle, daß eine staatliche Kryptoregulierung, die negative Auswirkungen auf den Sicherheitsstandard kryptographischer Verfahren hat, die Vertrauensbildung in Internet-Zahlungssysteme erheblich erschweren, wenn nicht unmöglich machen kann.

5.2.3.4 Kontrollinstanzen

Organisationen und Institutionen, die Vertrauen in technische, organisatorische und rechtliche Bereiche der Internet-Zahlungssysteme aufbauen, sind letztendlich Vertrauensvermittler. Diese Mittler müssen selbst ein Vertrauensverhältnis mit dem Massenpublikum aufbauen, um erfolgreiche Vertrauensbildung betreiben zu können. Vertrauensbildende Maßnahmen einer Institution, deren Kompetenz und Neutralität fraglich ist, werden kaum als vertrauenswürdig betrachtet.

In besonderem Maße gilt dies für Organisationen und Institutionen, die die Bündelung und Kontrolle der technischen, organisatorischen und rechtlichen Aspekte wahrnehmen. Diesen Kontrollinstanzen wird die Aufgabe zufallen, vertrauensbildende Aussagen anderer Institutionen zu bündeln und zu kontrollieren. Kontrollinstitutionen im Bereich der Internet-Zahlungssysteme sollen damit Anworten auf die Fragen geben, welche Hard- und Softwareprodukte und Anbieter, welche Kryptographieverfahren, welche Key-Management Institutionen und Finanzinstitute vertrauenswürdig sind und welche rechtliche Geltung finanziellen Transaktionen im Internet zukommt. Kontrollinstitutionen können sich aufgrund staatlicher, kommerzieller oder nicht-kommerzieller Initiativen organisieren. Für all diese Institutionen gilt jedoch, daß sie zuerst einmal selbst Vertrauen in ihre eigene Kompetenz und Neutralität aufbauen müssen. Vertrauensbildung selbst benötigt schon Vertrauen. Ob und wie Kompetenz und Neutralität von staatlichen, kommerziellen oder Non-Profit Institutionen gewährleistet werden können, wird nach der nun folgenden Einführung in die kryptographischen Grundlagen diskutiert.

---

[118] Vgl. c't (1999), S.20

6 Grundlagen der Internet-Zahlungssysteme

6.1 Kryptographische Verfahren

Bereits die Regierung des griechischen Stadtstaates Sparta benutzte vor ca. 2500 Jahren sog. Skytale, um vertrauliche Nachrichten zu verschlüsseln.[119] Dabei wurde ein streifenförmiges Papier um die Skytale – einen Zylinder oder Kegel – gewickelt und die Botschaft der Länge nach auf den Streifen geschrieben. Waren Sender und Empfänger im Besitz einer identischen Skytale, konnte der Empfänger die Nachricht damit dechiffrieren.

Heute ist die Verschlüsselung vertraulicher Nachrichten mindestens genauso wichtig, wie in der Antike. Allerdings haben sich die Verfahren – nicht zuletzt durch den Einsatz der Informationstechnologie – wesentlich weiter entwickelt. Kryptographische Verfahren kommen immer dort zum Einsatz, wo Information vor ungewollter Einsichtnahme durch Verschlüsselung geschützt wird. Ein weiterer Anwendungsbereich für moderne Kryptoverfahren ist die Sicherung von Authentizität und Integrität[120] - alles Sicherheitsaspekte, die bei Internet-Zahlungssystemen von höchster Relevanz sind.

Kryptologie ist die Bezeichnung für die Lehre der geheimen Nachrichtenübertragung.[121] Sie umfaßt sowohl Kryptographie als Wissenschaft, die sich mit der Entwicklung von Verschlüsselungssystemen beschäftigt, als auch die Kryptoanalyse, die auf das Brechen dieser Systeme abzielt.

Kryptographische Verfahren beinhalten einen Klartext, der dem unchiffrierten Original entspricht, einem Schlüssel und einem chiffrierten Text. Mit Hilfe des Schlüssels wird der Klartext verschlüsselt und kann durch eine unsichere Umgebung wie das Internet transportiert werden, ohne daß Personen, die nicht im Besitz eines passenden Schlüssels sind, ihn einsehen oder verändern können. Der Empfänger, der sich im Besitz des passenden Schlüssels befindet, kann aus dem chiffrierten Text das Original zurückgewinnen. Je nach Verfahren werden zum Ver- und Entschlüsseln zwei identische Schlüssel oder zwei unterschiedliche, aber dennoch aufeinander bezogene Schlüssel verwendet. Verwenden Empfänger und Sender identische Schlüssel, spricht man von symmetrischer Verschlüsselung, verwenden sie unterschiedliche Schlüssel, handelt es sich um ein asymmetrisches Verschlüsselungsverfahren. „Derzeit wird eine Kombination beider Verfahren – in Verbindung mit der Einbindung sogenannter Einweg-Hashfunktionen – als der beste Schutz vor Mißbrauch angesehen.“[122]

---

[119] Vgl. Beutelspacher (1991), S.11
[120] Vgl. Beutelspacher (1991), S.1f
[121] altgriech: ‚???pt?s‘ (geheim) und ‚????s‘ (Wort, Sinn)
[122] Kristoferitsch (1998), S.65

6.1.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung (auch Secret Key Verfahren) verwenden Sender und Empfänger den gleichen Schlüssel. Ein solches Verfahren ist die oben beschriebene Verschlüsselung mittels einer Skytale, die dem symmetrischen Schlüssel entspricht, den Sender und Empfänger besitzen müssen. Ein moderneres Beispiel ist die monoalphabetische Verschlüsselung, bei der ein Text chiffriert wird, indem seine Buchstaben um eine bestimmte Anzahl Zeichen im Alphabet verschoben werden. Aus den Begriffen ‚ZAHLUNGSSYSTEME DES INTERNET' wird durch Verschiebung um drei Zeichen (Schlüssel) im Alphabet der chiffrierte Text ‚CDKOXQJVVBVWHPH GHV LQWHUQHW'. Dieses Verfahren ist nicht besonders sicher, da ein Angreifer (der weiß, daß mit dieser Methode verschlüsselt wurde) maximal 25 Möglichkeiten[123] ausprobieren müßte, um den Schlüssel zu brechen.[124] Ein Verfahren der Kryptoanalyse besteht bspw. darin, aus der statistischen Häufigkeit bestimmter Buchstaben oder Buchstabenkombinationen auf den Schlüssel zurückzuschließen. In der deutschen Sprache ist das ‚E' der meistverwendete Buchstabe. Im obigen Chiffretext würde somit der Buchstabe ‚H' ins Auge springen, was einer Verschiebung um drei Buchstaben nach rechts entspricht. Die Verschlüsselung über natürliche Sprachen ist wegen dieser statistischen Auffälligkeiten sehr unsicher. Um diese Auffälligkeiten zu verschleiern, werden heute nicht-natürliche Sprachen oder polyalphabetische Schlüsselsysteme benutzt.[125]

Für die Verschlüsselung digitaler Daten wird häufig das von IBM entwickelte und vom amerikanischen National Bureau of Standards 1977 als offizielles Standardverfahren anerkannte DES Verfahren benutzt. Bei diesem monoalphabetischen, symmetrischen Verfahren werden die binären Abbilder natürlichsprachiger Texte – also Folgen von 0 und 1 – jeweils in ‚Paketen' zu 64 Zeichen (64 Bit) verschlüsselt. Der Schlüssel ist in einer 64-stelligen Zahl enthalten, von der 56 Bit für den Schlüssel zur Verfügung stehen und 8 Bit für die Paritätsprüfung. Bei einem 56 Bit Schlüssel bestehen $2^{56} = 7 \times 10^{16}$ Kombinationsmöglichkeiten. Auch nachdem im Juni 1997 ein ‚Key Cracking Ring' einen DES Schlüssel erfolgreich entschlüsseln konnte, gilt der DES Algorithmus als relativ sicher. Allerdings wurde durch die Entschlüsselung deutlich, daß eine größere Schlüssellänge, etwa mit 112 oder 168 Bit zumindest mittelfristig zwingend erforderlich ist.[126] Unabhängig von der verwendeten Schlüssellänge haben symmetrische Verfahren erhebliche Nachteile.

---

[123] Das dt. Alphabet besteht aus 26 Zeichen – es bestehen also 25 Möglichkeiten einen Buchstaben zu verschieben.

[124] Ein solches Verfahren wird im Usenet unter dem Namen ROT benutzt.

[125] Vgl. Beutelspacher, S.26

[126] Vgl. Sicherheit in der Informationsgesellschaft (1999b): „IBM schlug seinerzeit sogar einen Schlüssel von 112 Bit Länge vor. Dies wurde auf Anraten der US-Sicherheitsbehörde NSA nicht realisiert. Ein möglicher Grund dafür ist die in den neunziger Jahren bekanntgewordene differentielle Kryptoanalyse. (...) Dementsprechend halten sich hartnäckig Gerüchte, das die NSA Maschinen besitzt, die in weniger als einer Viertelstunde zum Ziel kommen."

Zum einen muß der Schlüssel vor dem Senden der verschlüsselten Nachricht ausgetauscht werden und zwar auf sicherem Wege, damit er nicht von einem potentiellen Angreifer abgefangen werden kann. Dies kann bspw. durch persönlichen Kontakt oder vertrauenswürdige Boten geschehen. „Für einige exklusive Kommunikationspartner kann dies eine praktikable Lösung sein, für eine beliebige Händler-Kunden Beziehung ist dieses Verfahren zu aufwendig.“[127] Symmetrische Verfahren werden hauptsächlich beim gesicherten Datenaustausch im Bankenbereich verwendet.[128]

Zum anderen muß mit jedem Kommunikationspartner ein Schlüssel ausgetauscht werden. Bei Internet-Zahlungssystemen müßten bspw. ein Anbieter mit jedem seiner Kunden einen individuellen Schlüssel vereinbaren. In einem Netzwerk wie dem Internet nimmt dieses Unterfangen gigantische Ausmaße an, wenn jeder Teilnehmer mit allen anderen einen jeweils individuellen Schlüssel vereinbaren will.[129]

Der Vorteil der symmetrischen Verschlüsselung ist, daß sie relativ wenig Rechenleistung erfordert, was eine entsprechende Transaktionsgeschwindigkeit, die auch für Internet-Zahlungssysteme wichtig ist, ermöglicht. Insgesamt eignet sich die symmetrische Verschlüsselung eher für die Geheimhaltung, als für die Authentifizierung. Da Sender und Empfänger im Besitz des symmetrischen Schlüssels sind, ist im Nachhinein anhand der Verschlüsselung nicht mehr festzustellen, wer der Sender und wer der Empfänder der Nachricht war.

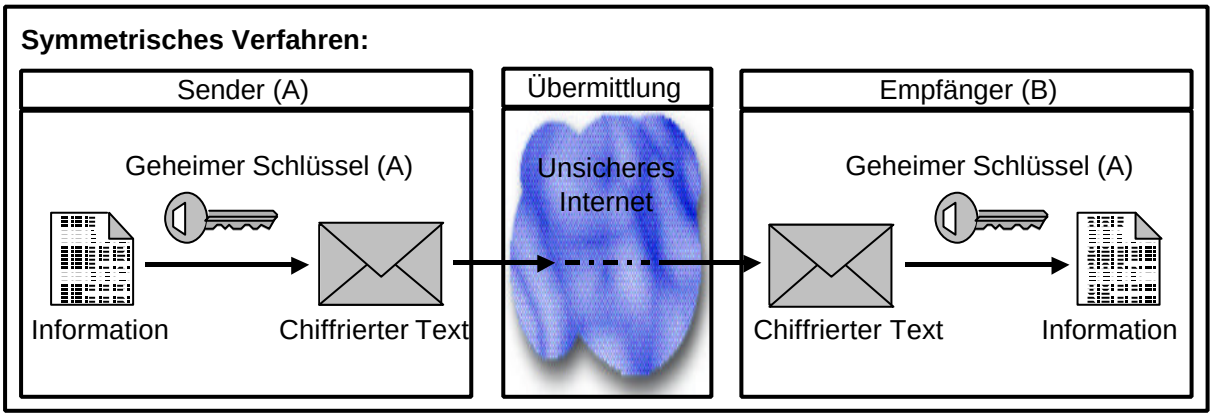

Abbildung 2: Symmetrisches Verfahren

6.1.2 Asymmetrische Verschlüsselung

Bei asymmetrischen Verfahren werden vom Sender und Empfänger jeweils verschiedene Schlüssel zum chiffrieren und dechiffrieren der Nachricht verwendet. Eine Nachricht, die mit dem einen Schlüssel chiffriert wurde, kann ausschließlich mit dem zugehörigen zweiten Schlüssel dechiffriert werden. Ein solches asymmetrisches

---

[127] Schuster/Färber/Eberl (1997), S.11
[128] Vgl. Beutelspacher (1991), S.26
[129] Insgesamt müssen bei n Teilnehmern n(n-1)/2 Schlüssel generiert und sicher getauscht werden.

Verfahren ist das Public Key Verfahren. Dabei wird einer der beiden Schlüssel, der private Schlüssel, geheim gehalten, der öffentliche Schlüssel hingegen wird publik gemacht, beispielsweise durch Veröffentlichung in einer Datenbank. Möchte jemand eine verschlüsselte Nachricht an einen Empfänger senden, benutzt er dessen öffentlichen Schlüssel zur Chiffrierung. Die Nachricht kann allein vom Empfänger mit seinem privaten Schlüssel dechiffriert werden, nicht jedoch mit dem öffentlichen Schlüssel. Das Prinzip der digitalen Signatur geht von der umgekehrten Vorstellung aus. Wenn eine Nachricht mit dem öffentlichen Schlüssel einer Person oder Organisation dechiffriert werden kann, muß sie mit dem zugehörigen privaten Schlüssel, den nur der Sender besitzt, chiffriert worden sein. Dadurch läßt sich die Authentizität des Absenders verifizieren.

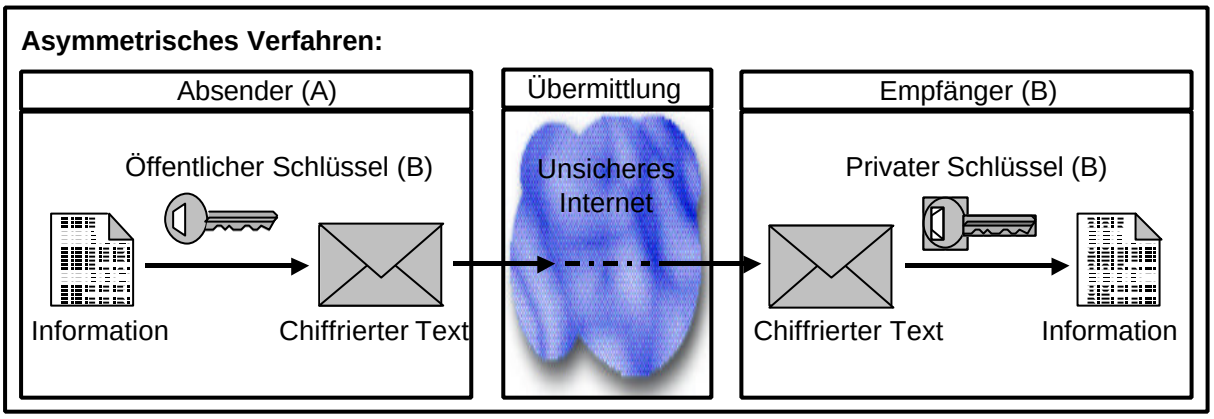

Abbildung 3: Asymmetrisches Verfahren

1977 wurde dieses Verfahren im RSA Algorithmus durch Rivest, Shamir und Adleman realisiert. Der RSA Algorithmus basiert, wie viele kryptographische Algorithmen, die heute verwendet werden, auf frühen mathematischen Theoremen, hier auf dem Satz von Euler. Kurz gesagt, werden öffentlicher und privater Schlüssel erzeugt, indem zwei hinreichend große Primzahlen multipliziert werden und aus dieser dritten Zahl die beiden Schlüssel berechnet werden. Es ist sehr schwierig, aus dem öffentlichen den privaten Schlüssel zu errechnen oder die Nachricht ohne den privaten Schlüssel zu dechiffrieren. Ein Angreifer müßte versuchen, diese dritte Zahl wieder in die beiden Primzahlen zu zerlegen. Dieses Vorgehen, Primzahlenfaktorisierung genannt, „gehört aber zu den schwierigsten Problemen der Mathematik“,[130] vor allem, wenn man bedenkt, daß die verwendeten Primzahlen mehrere hundert Stellen lang sind. Deshalb gilt der RSA Algorithmus gemeinhin als sicher, zumindest, wenn man Schlüssellängen von 512 oder gar 1024 Bit zugrunde legt.[131]

Der RSA Algorithmus trägt den Problemen der Schlüsselverwaltung, die bei symmetrischen Verfahren aufkommen, Rechnung. Die öffentlichen Schlüssel können

---

[130] Vgl. Beutelspacher (1991), S.133
[131] Vgl. RSA (1999g): RSA schlägt vor, Schlüssellängen von 768 bzw. 1024 Bit zu verwenden.

frei zugänglich gemacht werden, während die privaten Schlüssel nicht veröffentlicht werden müssen. Es brauchen keine geheimen Schlüssel ausgetauscht zu werden. Darüber hinaus sind weniger Schlüssel notwendig als bei symmetrischen Verfahren.[132] Ebenfalls problemlos ist die Aufnahme neuer Teilnehmer. Bei symmetrischen Verfahren müßten neue Teilnehmer mit allen Beteiligten jeweils einen individuellen Schlüssel austauschen. Beim asymmetrischen Verfahren brauchen die Teilnehmer nicht alle ihre Schlüsselbestände ‚upzudaten'. Außerdem eignet sich das asymmetrische Verfahren hervorragend für digitale Signaturen. Bei diesem Aspekt darf allerdings nicht vergessen werden, daß auch asymmetrische Verfahren – besonders wenn sie zur Authentizitätssicherung benützt werden – ein Key-Management benötigen. Ein schwerwiegender Nachteil des asymmetrischen Verfahrens ist, daß es eine wesentlich höhere Rechenleistung erfordert, als das symmetrische Verfahren. Aus diesem Grunde kommt bei vielen Internet-Zahlungssystemen eine Kombination beider Verfahren zum Einsatz.

6.1.3 Kombination symmetrischer und asymmetrischer Verfahren

Symmetrische und asymmetrische Verfahren haben beide spezifische Nachteile. Symmetrische Verfahren benötigen relativ wenig Rechenleistung, bringen aber den schwerwiegenden Nachteil mit sich, daß mit jedem Teilnehmer ein individueller Schlüssel vereinbart und auf sicherem Wege ausgetauscht werden muß. Asymmetrische Verfahren lösen dieses Problem elegant durch die Verwendung privater und öffentlicher Schlüssel, verursachen aber einen wesentlich höheren Rechenaufwand. Werden beide Verfahren kombiniert, lassen sich die jeweiligen Vorteile nutzen, die Nachteile weitgehend ausschließen. Eine Nachricht wird mit einem symmetrischen Schlüssel, der extra für diese Übermittlung erzeugt wurde (Session Key) verschlüsselt. Dieser Session Key wird mit dem asymmetrischen öffentlichen Schlüssel des Empfängers chiffriert und zusammen mit der bereits symmetrisch chiffrierten Nachricht an den Empfänger gesendet. Dieser kann mit seinem privaten Schlüssel den asymmetrisch verschlüsselten Session Key dechiffrieren und mit diesem die Nachricht entschlüsseln.

---

[132] Vgl. Beutelspacher (1991), S.116: Die Schlüsselanzahl ist beim asymmetrischen Verfahren genau 2n, also doppelt so groß, wie die Teilnehmerzahl n. Bei 1001 Teilnehmern sind es bei einem symmetrischen Verfahren n(n-1)/2 = 500.500 Schlüssel, bei einem asymmetrischen nur 2002.

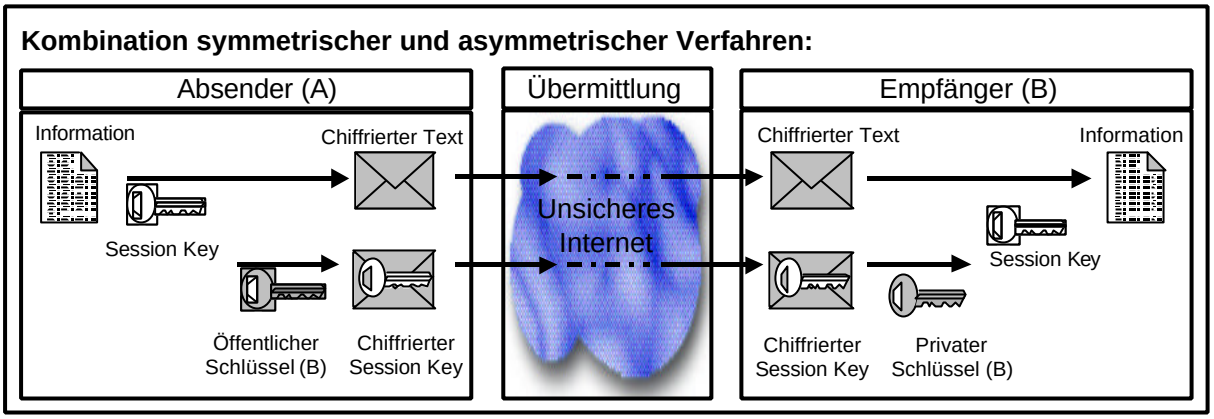

Abbildung 4: Kombination symmetrischer und asymmetrischer Verfahren

Da lediglich der Session Key mit dem asymmetrischen Verfahren ver- und entschlüsselt werden muß und die Nachricht selbst symmetrisch verschlüsselt ist, kann die notwendige Rechenleistung drastisch reduziert werden. Dennoch lassen sich die Vorteile des asymmetrischen Verfahrens nutzen.

6.1.4 Hash-Funktionen

Hash-Funktionen berechnen aus einem Text eine Zeichenkette fixer Länge, den sogenannten MAC (Message Authentication Code). Der MAC ist quasi eine Prüfsumme des Textes. Bei Hash-Funktionen sollte gewährleistet sein, daß der verwendete Algorithmus kollisionsfrei arbeitet und es damit sehr unwahrscheinlich ist, daß aus zwei verschiedenen Texten die gleiche Prüfsumme generiert wird. Bereits die Änderung eines einzigen Zeichens im Originaltext führt zu deutlichen, nicht direkt nachvollziehbaren Änderungen des MAC. Hash-Funktionen sind Einweg-Funktionen, d.h. die Operation kann nicht rückgängig gemacht werden. Wenn die Hash-Funktion zur Integritätsprüfung verwendet wird, ist dies auch gar nicht nötig. Um die Integrität einer Nachricht zu prüfen, wird vor und nach der Übermittlung jeweils ein MAC errechnet. Stimmen beide MACs überein, kann man sehr sicher sein, daß die Nachricht nicht während der Übertragung manipuliert wurde. Hash-Funktionen werden in Form der digitalen Signatur zusammen mit Verschlüsselungsverfahren angewendet, um authentische Nachrichtenübertragung zu gewährleisten. Gängige Funktionen sind SHA-1 (Secure Hash Algorithm 1), die 160 Bit MACs erzeugt oder MD5 (Message Digest 5) mit einer Länge von 128 Bit.

6.1.5 Steganographie

Bevor die praktische Anwendung der im vorherigen Abschnitt erläuterten Techniken dargestellt wird, soll hier noch auf eine vollkommen andere Methode zur sicheren Nachrichtenübertragung eingegangen werden. Bisher wurden Verfahren dargestellt, die den vertraulichen Inhalt einer Nachricht schützen. Steganographische Verfahren hingegen wollen gänzlich verschleiern, daß eine vertrauliche Nachricht übermittelt wird. Dazu wird die geheime Nachricht in einer zweiten, scheinbar unverfänglichen Information, bspw. einem digitalen Bild, ‚versteckt' und gemeinsam übermittelt.

Dieses Verfahren gilt als sehr sicher, besonders, wenn die vertrauliche Nachricht zusätzlich mit dem öffentlichen Schlüssel des Empfängers chiffriert wurde, bevor sie in der unverfänglichen Information untergebracht wird. Der „Nachteil [steganographischer Verfahren (Anm. d. Verfassers)] liegt derzeit im damit verbundenen Arbeitsaufwand und darin, daß ihre Anwendung nicht immer möglich sein wird – beispielsweise im Zuge einer Zahlungsanweisung an eine Bank.“[133] Weil mit diesem Verfahren eine staatliche Kryptoregulierung relativ einfach umgangen werden kann, wird es in der Diskussion um das Für und Wider einer Regulierung[134] nochmals erwähnt.

6.2 Anwendungsbereiche

Bisher wurde dargestellt, wie kryptographische Verfahren zur Sicherung von Vertraulichkeit und Integrität verwendet werden können. Ein bedeutender Vorteil asymmetrischer Verfahren liegt darin, daß sie darüber hinaus zur Authetizitätssicherung eingesetzt werden können. Die digitale Signatur ist quasi ein digitaler Personalausweis, mit dessen Hilfe die Identität eines Teilnehmers einwandfrei identifiziert werden kann.[135] „Sie ist das elektronische Äquivalent zur handschriftlichen Unterschrift und soll für elektronische Dokumente [zu denen auch finanzielle Transaktionen gehören (Anm. d. Verf.)] deren Aufgaben übernehmen.“[136] Diese bestehen in der[137]

- ☞ Echtheitsfunktion: Das unterzeichnete Dokument wurde in der vorliegenden Form unterzeichnet.
- ☞ Abschlußfunktion: Die Unterschrift schließt die Bearbeitung eines Dokumentes ab.
- ☞ Warnfunktion: Durch die Unterschrift wird die Bedeutung der so bezeugten Willenserklärung bewußt.
- ☞ Identitätsfunktion: Die Unterschrift wurde durch den Unterzeichnenden selbst geleistet.

In Deutschland hat der Gesetzgeber durch das SigG und die SigV die Rahmenbedingungen geschaffen, um diese Funktionen auch digitalen Signaturen zukommen zu lassen. Echtheits-, Abschluß- und Identitätsfunktion können durch digitale Signaturen erbracht werden. Für die Warnfunktion ist es unerläßlich, daß ein Internet-Zahlungssystem die digitale Signatur eines Zahlungsvorganges nur dann

---

[133] Kristoferitsch (1998), S.71
[134] Vgl. 7.3.1.3.2 Staatliche Kryptoregulierung
[135] Vgl. Kristoferitsch (1998), S.78 für eine detaillierte Bestimmung.
[136] Schuster/Färber/Eberl (1997), S.14
[137] Vgl. Schuster/Färber/Eberl (1997), S.25

erzeugt, wenn definitiv eine intensionale Handlung des Benutzers – bspw. durch wiederholte Bestätigung – vorliegt. Dieser Punkt wurde bereits als Vertrauensaspekt in die Funktionsfähigkeit der Hard- und Software des Zahlungssystems angesprochen. Wie digitale Signaturen realisiert werden, zeigt das nächste Kapitel.

6.2.1 Digitale Signatur

Die digitale Signatur ermöglicht im wesentlichen die Identifikation des Absenders einer Nachricht und sichert die Integrität der übertragenen Information. Geheimhaltung und Vertraulichkeit sind zunächst zweitrangig.

Technisch realisiert wird die digitale Signatur durch asymmetrische Kryptographie und Hash-Funktionen. Ein Absender erzeugt einen MAC der Nachricht, verschlüsselt diesen mit seinem privaten Schlüssel und sendet den chiffrierten MAC an den Empfänger. Parallel sendet er die Information unverschlüsselt an den Empfänger. Dieser entschlüsselt den chiffrierten MAC mit dem öffentlichen Schlüssel des Absenders. Gelingt dies, weiß er, daß der MAC mit dem privaten Schlüssel des Absenders chiffriert wurde. Die Authentizität des Absenders ist gewährleistet. Erhält der Empfänger die unverschlüsselte Information, kann er ebenfalls einen MAC davon erzeugen und diesem mit dem MAC vergleichen, den er verschlüsselt vom Absender erhalten hat. Sind die beiden MACs identisch, wurde die Nachricht während der Übermittlung nicht verändert. Somit sind Authentizität und Integrität der Transaktion gewährleistet.

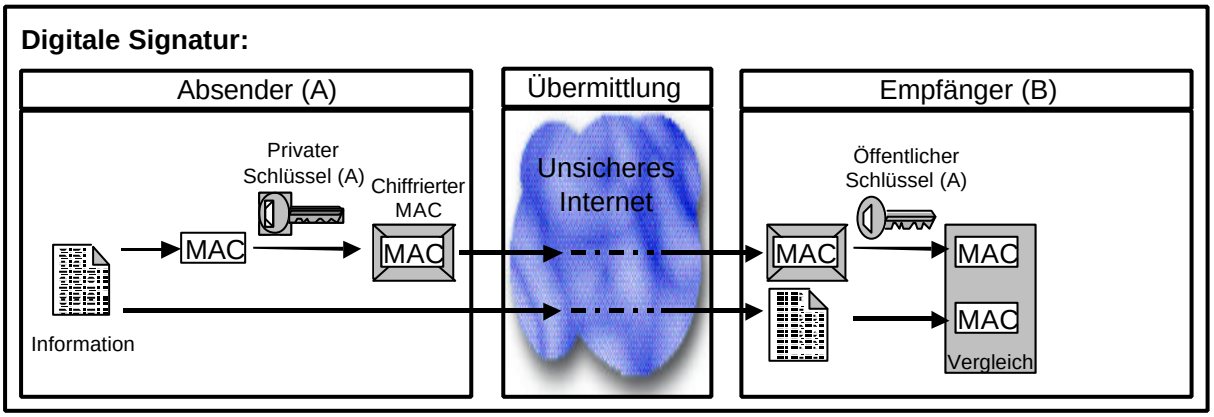

Abbildung 5: Digitale Signatur

Bisher wurde einfach angenommen, daß die Identität der Schlüsselinhaber gewährleistet ist. Wieso sollte jedoch in der Realität davon ausgegangen werden, daß ein bestimmter Schlüssel wirklich derjenigen Person zuzuordnen ist, die sie vorgibt zu sein? Schließlich könnte jemand anderer einen solchen Schlüssel erzeugen und publizieren. Die Lösung dieses Problems wurde bereits angesprochen: Eine Institution oder Organisation muß damit beauftragt werden, zu verifizieren, daß ein Schlüssel wirklich einer bestimmten Person gehört. Dazu erzeugt die Institution oder Organisation nach einer Identitätsprüfung, wie sie bspw. durch persönliches Erscheinen oder notarielle Beglaubigung erfolgen kann, ein digitales Zertifikat, das

die Identität der betreffenden Person mit ihrem öffentlichen Schlüssel untrennbar verbindet.[138] Nach dem SigG muß dieses Zertifikat neben Informationen, die auf die Identität des Teilnehmers schließen lassen, seinen öffentlichen Schlüssel und einen Gültigkeitszeitraum enthalten.[139] Ein „klassisches Anwendungsbeispiel“[140] für diese Zertifikate sind Internet-Zahlungssysteme.

6.2.2 Duale Signatur

Die duale Signatur ist eine Variante der digitalen Signatur, die bei der im folgenden Kapitel dargestellten sicheren Kreditkartenzahlung mittels SET eingesetzt wird. Mit der dualen Signatur können zwei oder mehr Nachrichten so verbunden werden, daß ihre Zusammengehörigkeit sichergestellt ist. Dennoch ist es möglich, diese Nachrichten getrennt zu verschlüsseln. So kann ein Teil der Zahlungsinformation (bspw. die Kreditkarteninformation) vor dem Händler geheimgehalten werden, während er zugleich die für ihn bestimmte Bestellinformation einsehen kann. Für die Bank gilt umgekehrt, daß sie zwar Kreditkarteninformation einsehen kann, nicht jedoch die Bestellung. Trotzdem ist es möglich, nachzuweisen, daß Kreditkarten- und Bestellinformation zusammengehören.

Im graphischen Beispiel könnte der Empfänger B die Bank sein, die Kreditkarteninformationen (Dokument 2) mit ihrem privaten Schlüssel dechiffrieren kann. Die Bestellung kann sie nicht einsehen. Dennoch kann sie verifizieren, daß die Dokumente zusammengehören, indem sie den MAC für Dokument 2 neu generiert und zusammen mit dem bekannten MAC1 einen MAC4 erzeugt. Ist dieser identisch mit dem MAC3, den sie erwiesenermaßen von A erhalten hat, weiß die Bank, daß es sich um die authentischen, zusammengehörigen Dokumente des Absenders A handelt.

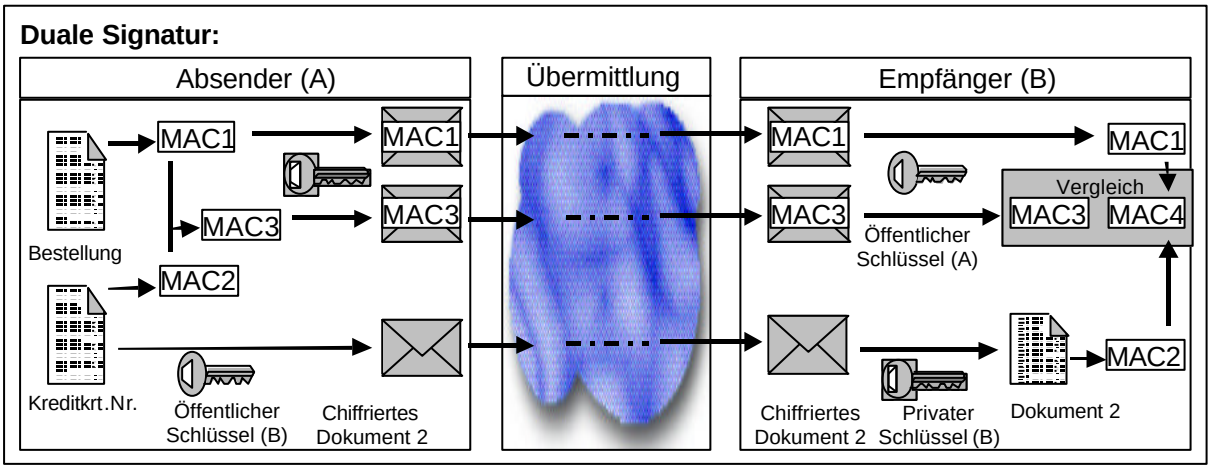

Abbildung 6: Duale Signatur

---

[138] Vgl. Schuster/Färber/Eberl (1997), S.105
[139] Vgl. §7 I, SigG: daneben müssen noch weitere Informationen enthalten sein, wie lfd. Nr. des Zertifikates, Name der Zertifizierungsstelle, Algorithmus und Hinweise auf ev. Einsatzrestriktionen.
[140] Kuhlen (1999), S.288

6.3 Realisierung und Praxis der Zahlungssysteme im Internet

6.3.1 Der Sonderfall proprietärer Netzwerke

Immer wieder wurde betont, daß das Internet ein offenes Netzwerk ist. Dennoch existieren innerhalb des Internets geschlossene Benutzergruppen, wie sie in proprietären Netzwerken von T-Online oder AOL zu finden sind. Diese geschlossenen Online-Dienste sind Teil des Internets und verfügen über ein Gateway, durch das ihre Mitglieder Zugang zum Internet erhalten. Umgekehrt ist das nicht der Fall. T-Online und AOL bspw. sind nur für Mitglieder zugänglich, die sich während der Einwahl über ihre Benutzernamen und Paßwörter authentifizieren. Sie sind „also dem Anbieter bekannt, so daß sich dann [...] ein Abrechnungssystem problemlos integrieren läßt.“[141] Beim Zugriff auf das WWW hingegen ist eine Authentifizierung nicht erforderlich. Zahlungssysteme im Internet können deshalb nicht auf einer bestehenden Authentifizierung aufsetzen, sondern müssen die notwendigen Voraussetzungen selbst schaffen.

Auf den nächsten Seiten werden zwei praktisch erprobte Internet-Zahlungssysteme vorgestellt, die den grundsätzlichen Paradigmen in diesem Bereich entsprechen.[142] Der SET Standard setzt auf dem bereits bestehenden Kreditkartensystem auf und ermöglicht die Abwicklung von Internet-Zahlungsvorgängen über das sichere Übertragungsprotokoll SET. eCash hingegen arbeitet mit einer virtuellen Währung, die es ermöglicht, Zahlungsvorgänge mit einem hohen Grade an Anonymität ‚bargeldnah‘ im Internet abzuwickeln.[143]

6.3.2 SET Standard

SET ist eine gemeinsame Entwicklung der Kreditkartenanbieter Visa und MasterCard,[144] die sich natürlich erhoffen, dadurch die Verwendung von Kreditkarten im Internet zu forcieren. SET wird mittlerweile von allen großen Kreditkartenunternehmen und Softwarefirmen unterstützt und hat somit gute Chancen, im Bereich der Internet-Zahlungssysteme der de-facto Standard zu werden.[145] Im Gegensatz zu anderen sicheren Protokollen wie SSL oder S-HTTP ist SET speziell für Internet-Zahlungen entwickelt worden und kann trotz seiner Verbindung zu konventionellen Kreditkartensystemen als eigenes Zahlungssystem betrachtet werden. Wie sieht der praktische Ablauf einer SET-Zahlung aus?

---

[141] Zahlungssysteme im Internet (1998) und vgl. Schuster/Färber/Eberl (1997), S.48
[142] Vgl. Kristoferitsch (1998), S.125ff; vgl. Schuster/Färber/Eberl (1997), S.32ff
[143] Vgl. Böhle/Riehm (1998), S.60
[144] Vgl. MasterCard (1999b); vgl. Visa (1999f)
[145] Vgl. Böhle/Riehm (1998), S.111

„Der Purchase Request beinhaltet die Bestellung des Kunden und die Quittung des Händlers. Der Kunde sendet als erstes die Initialisierungsnachricht, auf die der Händler eine unterschriebene Antwort mit seinem Signaturzertifikat und dem zertifizierten Schlüssel seines Finanzinstitutes sendet.

Anschließend kontrolliert der Kunde ob die Zertifikate von einer gültigen Zertifizierungsstelle ausgegeben wurden und vergleicht die Unterschrift mit einem selbst erstellten Fingerabdruck [der Unterschrift (Anm. d. Verf.)].

Der Kunde versieht Bestellung und Zahlungsinformationen mit einer dualen Signatur. Die Zahlungsanweisung wird nun mit dem DES Verfahren chiffriert. Der DES-Schlüssel wird gemeinsam mit den Kreditkarteninformationen RSA verschlüsselt (mit dem Schlüssel des Finanzinstitutes). Bestellung und Zahlungsanweisung werden jetzt an den Händler geschickt (evtl. mit Kundenzertifikat). Nachdem der Händler Kundenzertifikat und duale Signatur geprüft hat, sendet er dem Kunden eine Quittung. Der Kunde prüft wieder das Zertifikat und speichert die Quittung ab.

Jetzt folgt die Payment Authorisation Message. Bei dieser leitet der Händler die Zahlungsanweisung zusammen mit einer Zahlungsfähigkeitsanfrage an das Finanzinstitut weiter. Dieses prüft wiederum sämtliche Zertifikate und vergleicht die Zahlungsanweisung des Kunden mit den Angaben des Händlers. Sind diese Tests erfolgreich abgelaufen, fragt das Finanzinstitut bei der Kundenbank nach, ob die Zahlung in Ordnung geht und sendet die Antwort zusammen mit einem ‚Capture Token' an den Händler. Der Händler entschlüsselt diese Daten wieder und speichert sich das Token, das er zur späteren Abrechnung mit seiner Bank benötigt, ab und liefert seinem Kunden die Ware.

Wenn der Händler zu einem späteren Zeitpunkt mit seinem Finanzinstitut abrechnet, sendet er das erhaltene Capture Token mit dem zu zahlenden Betrag, einem Transaction Identifier und seinen beiden Zertifikate in der Payment Capture Message an das Finanzinstitut. Über das Bankennetz wird dann die Zahlung veranlaßt und der Händler erhält eine Antwort, die er sichert."

Das folgende Schaubild soll diesen Ablauf verdeutlichen.

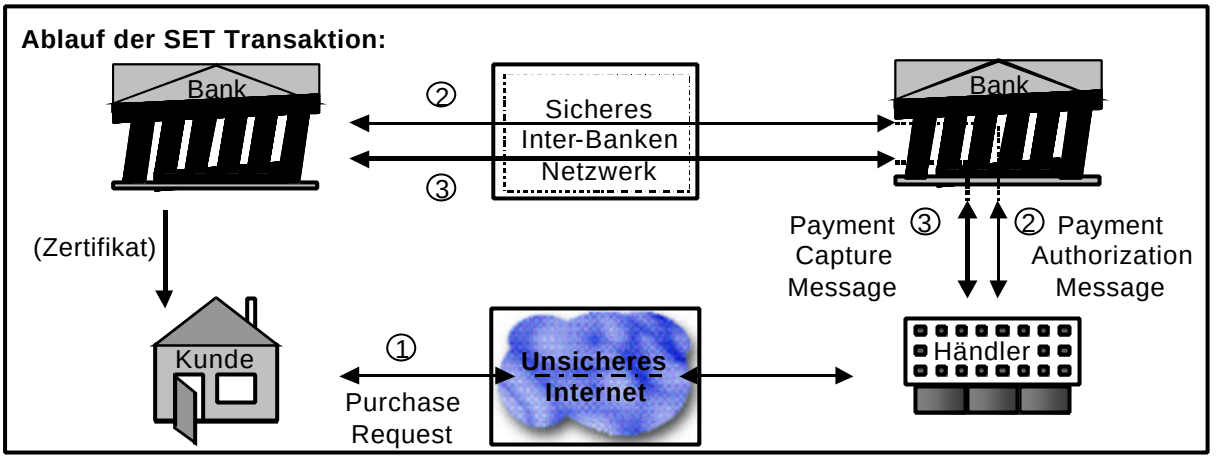

Abbildung 7: Ablauf der SET Transaktion[146]

SET verwendet die gesamte Bandbreite kryptographischer Verfahren, wie digitale und duale Signaturen, Zertifikate und SHA-1 Hash-Funktionen. Um einen optimalen Ausgleich zwischen Sicherheit und Transaktionsgeschwindigkeit zu schaffen, wird eine Kombination von symmetrischer 56 Bit DES- und asymmetrischer 1024 Bit RSA-Verschlüsselung eingesetzt. Wichtig ist, daß der Händler aufgrund der dualen Signatur nur die Bestellinformationen und das Kreditinstitut nur die Kreditkarteninformationen einsehen kann. Dadurch wird ein gewisses Maß an Anonymität gewährleistet. Die Bank weiß zwar, wieviel und auf welche Kreditkarte belastet werden muß, nicht aber, was bestellt worden ist. Umgekehrt kennt der Anbieter zwar die Bestellung, nicht aber die Kreditkartennummer des Kunden. Die Authentizität der Parteien wird durch digitale Signaturen und Zertifikate gewährleistet.

Insgesamt kann SET als relativ sicheres Zahlungssystem angesehen werden. Dennoch weist das Verfahren bislang Nachteile auf.[147] Zum einen unterstützt SET nur die oben erwähnten Verfahren DES und RSA. Auch die Länge des DES Schlüssels ist mit 56 Bit aufgrund der US-amerikanischen Exportrestriktionen (die mittlerweile als verfassungswidrig eingestuft worden sind) relativ kurz ausgefallen. Zum anderen ist SET bisher eine reine Softwarelösung. Die Auslagerung der privaten Schlüssel auf eine Hardwarekomponente – sog. Smartcards – wird jedoch in Kürze mit C-SET (Chip-Secured Electronic Transactions) möglich sein. C-SET wird derzeit noch in Frankreich und Belgien getestet[148] und soll voraussichtlich bis Ende 1999 verfügbar sein. Schlüssel und Zertifikate sind bis dahin als Software auf dem lokalen Computer installiert, was zum einen unsicher ist, zum anderen die Mobilität der Anwender stark einschränkt. Hinzu kommt, daß SET aufgrund der aufwendigen Zahlungsabwicklung

---

[146] Vgl. Schuster/Färber/Eberl (1997), S.25 - Hier sind nur die drei wichtigsten Transaktionen dargestellt. Vgl. Visa (1999b): Visa selbst unterscheidet sechs Schritte zu denen auch die Lieferung zählt.

[147] Vgl. Kristoferitsch (1998), S.118f

[148] Vgl. Kristoferitsch (1989), S.119 und vgl. Visa (1997b)

kaum für Mikro- und Kleinzahlungen[149] geeignet ist. Dennoch handelt es sich bei SET um „einen großen Schritt in Richtung sicherer Kreditkartentransaktionen“.[150]

Doch nicht nur aufgrund seiner Sicherheit werden diesem Zahlungssystem große Durchsetzungschancen eingeräumt. Sicherheit ist – so wurde bereits ausführlich dargestellt – notwendige aber nicht ausreichende Bedingung für die Akzeptanz von Internet-Zahlungssystemen. Auch Sicherheit muß über Vertrauen vermittelt werden. SET basiert auf einer bestehenden und damit vertrauten Kreditkarteninfrastruktur. Kreditkarten sind in der heutigen Gesellschaft von der Öffentlichkeit weitgehend akzeptierte Zahlungsmittel. Diese Akzeptanz durch dominante öffentliche Einstellungen ist ein weiterer vertrauensbildender Faktor,[151] der sich potentiell auf SET übertragen läßt. Darüber hinaus stehen Institutionen hinter SET, die bereits das Vertrauen der Anwender im konventionellen Zahlungsverkehr genießen. Es ist anzunehmen, daß sich dieser Vertrauensbonus auch bei SET erfolgreich plazieren läßt.

6.3.3 eCash

Das Internet-Zahlungssystem eCash des holländischen Unternehmens DigiCash („Numbers that are money“) baut nicht auf konventionellen Zahlungssystemen auf, sondern geht einen neuen Weg. eCash arbeitet mit virtuellem Geld. Da virtuelles Geld real gedeckt werden muß, ist es notwendig, daß der Anwender ein Konto bei einer Institution unterhält, die eCash ausgibt. Dazu gehören derzeit nur wenige Kreditinstitute, in Deutschland lediglich die Deutsche Bank.[152]

Den Ablauf einer eCash Zahlung muß man sich folgendermaßen vorstellen. Nachdem der Kunde bei einem autorisierten Kreditinstitut ein Konto eröffnet hat, erhält er die Software und eine PIN. Der Anwender generiert mit dieser Software digitales Geld,[153] läßt es von seiner Bank signieren und speichert es in der eCash Geldbörse (Wallet) auf der Festplatte seines PCs. Das sog. ‚Blinding Verfahren‘ stellt dabei sicher, daß die Bank die virtuellen Münzen durch eine digitale Signatur validieren kann, ohne deren Seriennummer zu kennen.[154] Die Kundenbank kann keine Verbindung zwischen ihrem eCash Kunden und den Seriennummern der digitalen Münzen herstellen. Wenn der Anwender mit eCash bezahlen will, transferiert er den virtuellen Geldbetrag an den Händler, der ihn an seine Bank weiterleitet. Die Bank verifiziert die Signatur der Münzen und prüft in einer

---

[149] Vgl. Inf-Wiss (1998) für eine Klassifizierung von Zahlungsbeträgen – Mikrobeträge < 5$ < Kleinbeträge < 10$ < Makrobeträge < 500$.
[150] Kristoferitsch (1998), S.119
[151] Vgl. Kuhlen (1999), S.84
[152] Vgl. DigiCash (1999a)
[153] Damit auf diesem Wege nicht künstliche Liquidität geschaffen wird, erwägt man, nur Kreditinstituten die Genehmigung für die ‚Prägung‘ von eCash Münzen zu erteilen.
[154] Vgl. Inf-Wiss (1998): Falls Anonymität erwünscht ist, kann der Kunde die Münze auch selbst generieren, und durch Einsatz eines Blendungsfaktors von der Bank anonym signieren lassen.

Datenbank, in der die Seriennummern aller bereits eingelösten eCash Münzen gespeichert sind, ob die entsprechende Münze schon einmal eingelöst wurde. Der letztere Vorgang ist notwendig, um ein ‚Double Spending' – also das mehrfache Einlösen einer digitalen Münze – zu verhindern. Da die Bank des Händlers die eCash Münzen von diesem erhält, weiß sie bei dieser Überprüfung nichts über die Identität des Kunden – Anonymität ist sowohl bei der Erzeugung wie bei der Einlösung der Münzen gewährleistet. Wenn die Signatur gültig ist und die Münze noch nicht als bereits eingelöst klassifiziert ist, veranlaßt die Händlerbank das Clearing und gibt eine positive Bestätigung an den Händler, der nun die Ware versenden kann.

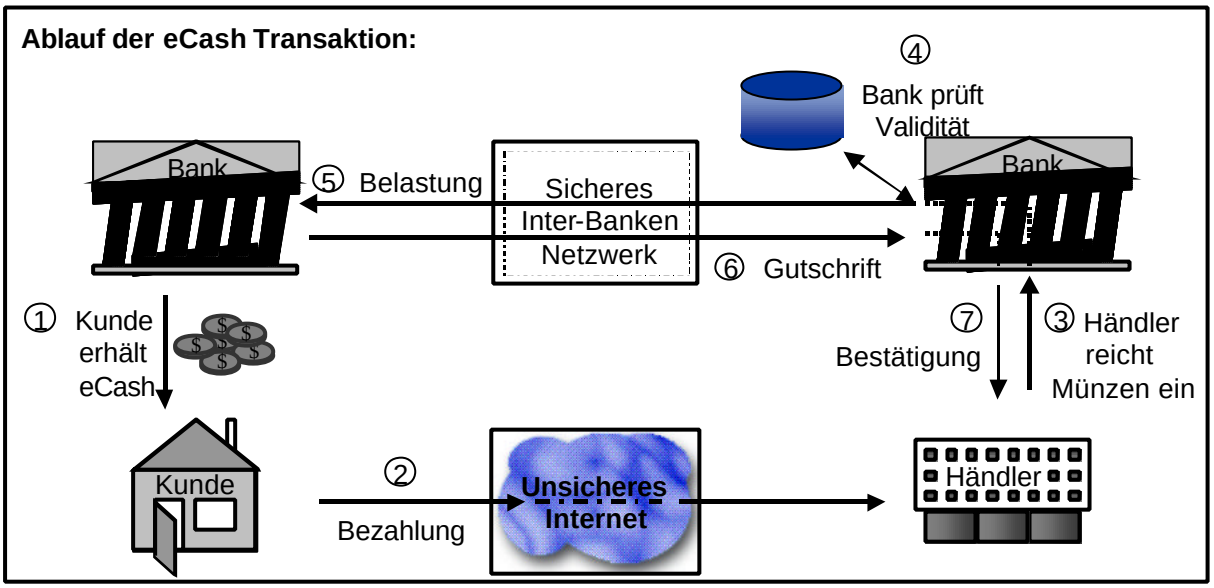

Abbildung 8: Ablauf der eCash Transaktion

Wie SET verwendet auch eCash digitale Signaturen, Zertifikate und SHA-1 Hash-Funktionen. Gleichsam werden symmetrische 3-DES (Triple DES)[155] Schlüssel mit einer Länge von 128 Bit und der asymmetrische 1024 Bit RSA Schlüssel eingesetzt.[156] Vorteilhaft hinsichtlich der Schlüssellänge ist sicherlich, daß DigiCash kein US-Unternehmen ist und damit nicht den (noch) bestehenden US Exportbestimmungen für kryptographische Verfahren unterliegt.[157]

Dadurch kann auch das eCash Verfahren als relativ sicher angesehen werden und bietet gegenüber SET erhebliche Vorteile, wie die Eignung zur Zahlung von Mikro- und Kleinbeträgen. Mit eCash können darüber hinaus nicht nur Zahlungen zwischen Anbietern und Kunden, sondern auch zwischen privaten eCash Nutzern getätigt werden. [158]

---

[155] Vgl. Garfinkel/Spafford (1997), S.116: Beim Triple-DES Verfahren wird der DES Algorithmus insgesamt 3 Mal angewendet, wodurch sich die Sicherheit mindestens verdoppeln läßt.
[156] Vgl. Schoemaker (1998)
[157] Vgl. Kristoferitsch (1998), S.134
[158] Vgl. Kristoferitsch, S.131 und vgl. DigiCash (1999b) für eine Demonstration der eMail Zahlung mit eCash.

Bei allen Zahlungen bietet eCash dem Käufer echte Anonymität. Einnahmen können vor der Bank jedoch nicht verheimlicht werden, was illegale Geldwäsche im selben Maße erschwert, wie bei anderen Zahlungssystemen auch. Hat die Bank die eCash Münzen im ‚Blinding Verfahren' signiert „ist eCash, grob gesprochen, wie Bargeld anzusehen und befindet sich nicht mehr im geschützten Einflußbereich der Bank."[159] Die benutzerfreundliche Menüsteuerung der Zahlung ist ein weiterer Vorteil.[160] Selbst im Falle eines Festplattenzusammenbruches ist es bei korrekt installierter Software möglich, die noch nicht verbrauchten Münzen zu identifizieren und sich von der Bank gutschreiben zu lassen.

Dementsprechend bemerkt Kristoferitsch, daß es wirklich schwer ist, effektive Schwächen des Systems auszumachen.[161] Nachteilig könnte die zu geringe Schlüssellänge sein – doch andere Verfahren (z.B. SET) benutzen noch kürzere symmetrische Schlüssel. Praktische Beschränkungen werden dem Anwender dadurch auferlegt, daß bisher nur wenige Banken und Kreditinstitute eCash Zahlungen ermöglichen. Als Nachteil könnte sich erweisen, daß die Seriennummern aller bereits eingelösten Münzen gespeichert werden müssen. Um diesen Aufwand möglichst gering zu halten, werden eCash Münzen bei der Signatur durch die Bank mit einem elektronischen ‚Haltbarkeitsdatum' versehen. Abgelaufene und nicht eingelöste Münzen können jederzeit bei der entsprechenden Bank rückgetauscht werden und gehen so nicht verloren. Ein bedeutender Nachteil im Kontext des globalen Marktplatzes Internet ergibt sich aus der Tatsache, daß eCash an die jeweilige nationale Währung gebunden ist. Zahlungen in US-$ lassen sich z.B. mit einem (D-Mark) eCash Konto bei der Deutschen Bank nicht durchführen. Hinsichtlich der Einführung des EURO ist aber zu erwarten, daß dieses Problem in Kürze gelöst wird. Eine Multi-Currency Version von eCash befindet sich derzeit in Entwicklung.[162]

„Trotz dieser derzeitigen Einschränkungen präsentiert sich eCash als ein System, das vor allem im Klein- bis Mikrobetragsbereich gute Chancen besitzt, in naher Zukunft weite Verbreitung zu finden."[163] Sowohl Sicherheit wie Leistungsfähigkeit dieses Zahlungssystems sind nach heutigen Bewertungskriterien sehr hoch einzustufen. Wie bei SET ist bei eCash eine bestehende Vertrauensstruktur in Form der eCash emittierenden Banken vorhanden. Allerdings ist eCash nicht nur ein Zahlungssystem wie SET, sondern eine virtuelle Währung. Bei SET Transaktionen ist dem Anwender zumindest der gedankliche Rückgriff auf seine vertraute Kreditkarte möglich. Eine Transformationsleistung durch Übertragung von Vertrauen in das Kreditkartensystem auf Vertrauen in das SET Verfahren, erscheint bei eCash

---

[159] Kristoferitsch (1998), S.129
[160] Vgl. DigiCash (1999b): Das sehr gute eCash Demoprogramm simuliert verschiedene Transaktionen (einschließlich Peer-to-Peer).
[161] Vgl. Kristoferitsch (1998), S.133
[162] Vgl. Kristoferitsch (1998), S.133
[163] Kristoferitsch, (1998), S.132

wesentlich schwieriger. Bedenken gehen dahin, daß eCash als reine Softwarelösung emotional als unsicher eingestuft wird.[164] Äquivalente Erfahrungen, die Vertrauen in virtuelles Geld bilden könnten, sind bei den wenigsten Anwendern vorhanden. Es sind aber „auch die praktischen Erfahrungen mit den Systemen selber, die Vertrauen begründen.“[165] Dieser Nachteil muß durch vermehrte Anstrengungen der institutionellen Vertrauensbildung wettgemacht werden. Die Frage, welche Ausprägung institutionelle Vertrauensbildung annehmen kann, soll nun behandelt werden.

[164] Vgl. Böhle/Riehm (1998), S.
[165] Kuhlen (1999), S.85

7 Praxis institutioneller Vertrauensbildung

Vertrauensbildung in Internet-Zahlungssysteme ist ein äußerst komplexer Vorgang. Nicht nur deshalb, weil Vertrauen von einer Vielzahl Faktoren abhängig ist, sondern gerade, weil Vertrauensbildung bei Internet-Zahlungssystemen sich nicht nur – wie man auf den ersten Blick annehmen könnte – auf den technischen Aspekt beschränken darf. Mindestens genau so wichtig sind vertrauensbildende Maßnahmen in den vertrauenskritischen rechtlichen und organisatorischen Bereichen. Auch in diesen Bereichen besteht auf Seite der Anwender Verunsicherung hinsichtlich der organisatorischen und rechtlichen Aspekte, die im Bereich der Internet-Zahlungssysteme von Bedeutung sind.

Deshalb muß die institutionelle Vertrauensbildung eine interdisziplinäre Ausrichtung haben und in allen vertrauenskritischen Bereichen hinreichend erfolgreich sein. Diese Erkenntnis soll die Grundlage sein, auf der Ausprägung und Akteure der institutionellen Vertrauensbildung bei Internet-Zahlungssystemen skizziert werden. Mitbestimmend für die Erfolgschancen der institutionellen Vertrauensbildung sind die in Kapitel 4.1 identifizierten Einflußfaktoren der Vertrauensbildung.

7.1 Erfolgreiche institutionelle Vertrauensbildung

Die Berücksichtigung dieser Einflußfaktoren ist von großer Bedeutung für den Erfolg oder Mißerfolg der institutionellen Vertrauensbildung bei Internet-Zahlungssystemen. Sie setzen sozusagen die Rahmenbedingungen, die von den Akteuren berücksichtigt werden müssen. Im folgenden werden die erarbeiteten Einflußfaktoren der Vertrauensbildung mit ihrer Implikation auf die institutionelle Vertrauensbildung bei Internet-Zahlungssystemen dargestellt. Im nächsten Kapitel wird schließlich erörtert, welche Institutionen die systematisierten, vertrauenskritischen Bereiche bei Internet-Zahlungssystemen abdecken bzw. abdecken könnten. Zunächst sollen die in Kapitel 4.1 identifizierten Einflußfaktoren in den Kontext der Vertrauensbildung bei Internet-Zahlungssystemen gerückt werden.

☞ Vertrauen ist eine spezifische Erscheinung, die in einem bestimmten Kontext gebildet und gegebenenfalls verloren wird. Vertrauensbildung bei Internet-Zahlungssystemen ist deshalb eine interdisziplinäre Angelegenheit, die technische, organisatorische und rechtliche Vertrauensaspekte gleichermaßen abdecken muß. Vertrauen in sichere Kryptoverfahren, vertrauenswürdiges Key-Management oder die rechtliche Geltung sind unabdingbar, wenn Vertrauen in Internet-Zahlungssysteme geschaffen werden soll. Weil diese Aspekte in den Folgen ihrer Interaktion für das Massenpublikum kaum zu durchschauen sind, müssen weitere Institutionen auftreten, die Vertrauen in Internet-Zahlungssysteme als Kombination technischer, organisatorischer und rechtlicher Faktoren vermitteln.

☞ Weil Vertrauen immer auch eine emotionale Entscheidung ist, sind persönliche Mittler notwendig, die Komplexität auf emotionaler Ebene reduzieren können. Institutionen, die erfolgreiche Vertrauensbildung praktizieren wollen, müssen – bspw. über die giddens'schen ‚Access Points' – Vertrauen in die Internet-Zahlungssysteme auf operativer Ebene persönlich vermitteln, indem sie z.B. Experten wie Programmierer, Mathematiker und Juristen oder designierte Repräsentanten als personale Mittler einsetzen.

☞ Vertrauen darf nicht enttäuscht werden. Bei Internet-Zahlungssystemen betrifft dies sowohl technische, als auch organisatorische und rechtliche Vertrauensbereiche. Wird das Vertrauen in einen spezifischen Teilbereich der Vertrauensbildung enttäuscht, wie bspw. wenn das Key-Management System eines Trust Centers von Hackern gebrochen wird oder Kreditkartennummern gestohlen werden, zerstört dies Vertrauen in eben diesen organisationellen Bereich der Internet-Zahlungssysteme. Fraglich ist, ob dadurch das ganze Vertrauensgebäude zusammenbricht. In dieser Hinsicht ist sicherlich die Arbeit der Kontrollinstanzen, die innerhalb des Vertrauensnetzwerks die Bündelung und Kontrolle vertrauensbildender Maßnahmen wahrnehmen, von großer Bedeutung für die Verhinderung von Vertrauenskrisen.

☞ Transparenz kann Vertrauen schaffen. Informationen, die für die Bewertung der Sicherheit von Internet-Zahlungssystemen wichtig sind, müssen zugänglich und publik gemacht werden. Auch wenn Laien nicht in der Lage sind, diese Informationen kontextbezogen zu bewerten, schafft diese Transparenz ein Klima der Vertrautheit und damit eine Vertrauensbasis. Im technischen Bereich der kryptographischen Verfahren hat die von Anfang an erfolgte öffentliche Publikation des DES Algorithmus nicht unwesentlich dazu beigetragen, Vertrauen in seine Sicherheit zu bilden.[166] Ebenso sind die. ‚RSA Challenges' – Wettbewerbe um das Brechen von Schlüsseln – des US Unternehmens RSA Data Security eine solche vertrauensbildende Maßnahme. Auch im organisatorischen und rechtlichen Vertrauensbereich ist Transparenz eine geeignete Maßnahme zur Vertrauensbildung. So verweisen Trust Center auf ihre Policy Papers, auf Sicherheitsmaßnahmen und Qualitätsurteile neutraler Dritter, um Vertrauen in das komplexe System zu bilden, daß die vertrauensvolle Aufgabe des Key-Managements wahrnehmen soll. Im rechtlichen Bereich kann Transparenz bspw. durch öffentliche Publikation der Rechtsfolgen, der juristischen und politischen Diskurse[167] und Rechtsurteile erfolgen. Kontrollinstitutionen müssen erkennen lassen, auf welcher Legitimationsbasis und anhand welcher Verfahren sie ihre Kontrollfunktionen ausüben.

---

[166] Vgl. Beutelspacher (1991), S.26f
[167] Vgl. Hoeren (1998) und vgl. Roßnagel (1998)

☞ Eigene Erfahrungen sind ein wichtiger, wenn auch zeitintensiver Faktor für die Vertrauensbildung. Positive Erfahrungen müssen über einen längeren Zeitraum hinweg gemacht werden, bis sich Vertrauen verfestigen kann. Ob dieser Zeitraum bei Internet-Zahlungssystemen schon erreicht wurde ist zweifelhaft, weil die ersten Internet-Zahlungssysteme vor ungefähr vier bis fünf Jahren auf den Markt kamen.[168] Einen Vertrauensbonus genießen sicherlich Internet-Zahlungssysteme, die auf konventionellen, als vertrauenswürdig erfahrenen Verfahren aufsetzen, wie SET, das auf dem Kreditkartenverfahren beruht. Bei eCash stellt sich die Situation ganz anders dar. Virtuelles Geld ist eine neuartige Erscheinung, bei der eigene Erfahrungen und die öffentliche Einstellung noch keine Rolle spielen. Gerade bei diesem System müssen vertrauensbildende Maßnahmen vermutlich stärker eingesetzt werden, um das Massenpublikum zu aktivieren.

Bevor die Praxis der institutionellen Vertrauensbildung bei Internet-Zahlungssystemen beleuchtet wird, soll nun das Vertrauensnetz als Rahmenkonstrukt der Vertrauensbildung dargestellt werden.

7.2 Vertrauensnetzwerk

Ein Vertrauensnetzwerk ist nicht zu verwechseln mit einem Web of Trust, wie es bei der populären Public Key Verschlüsselungssoftware PGP zur Identitätssicherung verwendet wird. Auf dieses spezielle, selbstorganisierende Modell wird in diesem Kapitel noch ausführlich eingegangen. „Die Idee der Vertrauensnetzwerke kann aber auch losgelöst von der spezielleren Aufgabe der Anonymitäts- / Schlüsselsicherung auf Verfahren zur Vertrauenssicherung auf elektronischen Märkten allgemein übertragen werden.“[169] Die Diskussion ist dann nicht nur auf die alternativen Identitätssicherungsmethoden hierarchischer oder selbstorganisierender Art beschränkt. Vertrauensnetzwerke im hier verwendeten Sinne sollen eben nicht nur Vertrauen herstellen in den organisatorischen Bereich des Key-Managements und der Identitätssicherung, sondern in sämtliche vertrauenskritischen Bereiche, d.h. in Internet-Zahlungssysteme als Kombination technischer, organisatorischer und juristischer Aspekte.

Die wissenschaftliche Theorie sozialer Netzwerke betrachtet Menschen als Netzwerkknoten, die Verbindungen zu anderen Menschen unterhalten, die wiederum als Knoten dargestellt werden.[170] Diesem Konstrukt entsprechend sind Institutionen und Organisationen der institutionellen Vertrauensbildung als Knoten im Vertrauensnetzwerk verbunden. Durch das Vertrauensnetzwerk formiert sich eine

---

[168] Vgl. Kristoferitsch (1998), S.125
[169] Kuhlen (1999), S.313
[170] Vgl. Keupp/Röhrle (1987), S.12

‚Community' von Akteuren mit gleichen oder zumindest ähnlichen Zielen hinsichtlich der Vertrauensbildung.

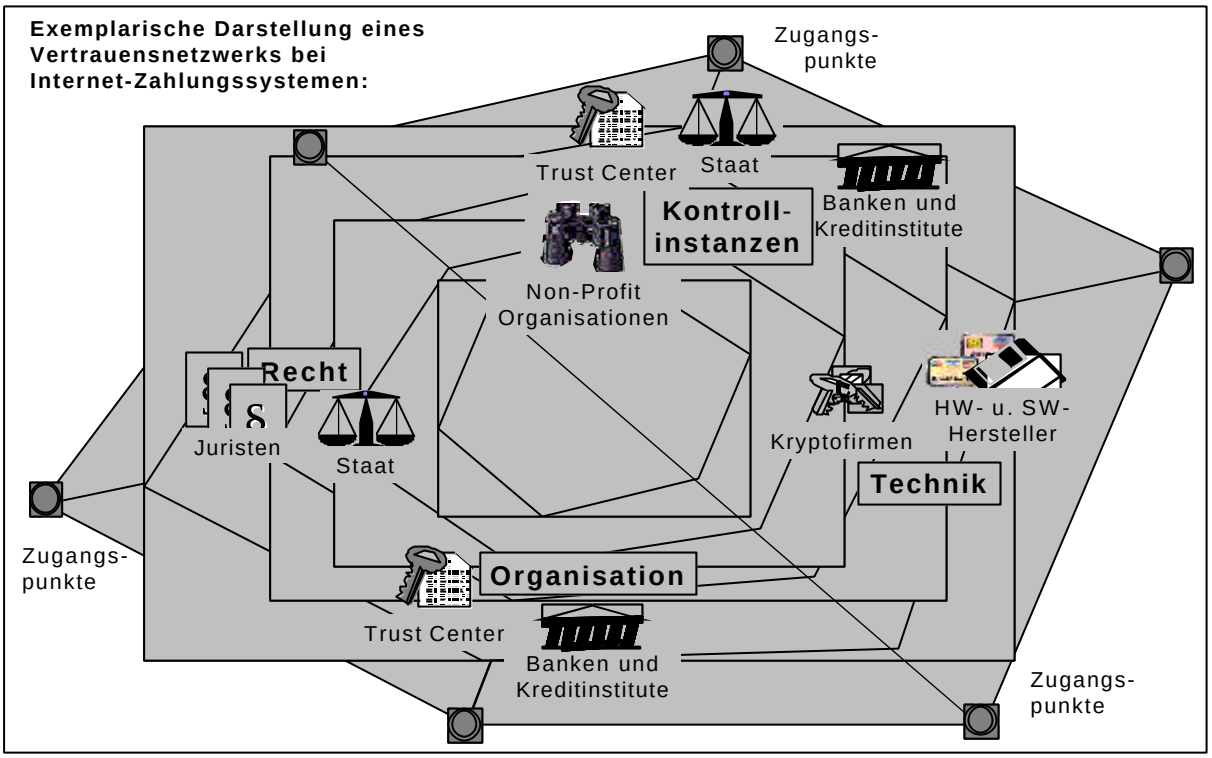

Abbildung 9: Exemplarische Darstellung eines Vertrauensnetzwerks bei Internet-Zahlungssystemen

In der Graphik zeigt sich deutlich, daß es bei der institutionellen Vertrauensbildung keine singuläre, institutionelle Lösung geben kann. [171] Vertrauensbildung kann auf der einen Seite spezifisch erfolgen – bspw. hinsichtlich der Sicherheit eines kryptographischen Verfahrens – auf der anderen Seite ermöglicht die Verknüpfung in einem Vertrauensnetzwerk die Bündelung der fachspezifischen Kompetenzen[172] und die Wahrnehmung von Kontrollfunktionen. Somit werden im Vertrauensnetzwerk sowohl Akteure tätig sein, die Vertrauen auf Basis ihrer fachspezifischen Kompetenz vermitteln, als auch Institutionen und Organisationen, die hier als Kontrollinstanzen bezeichnen werden sollen. Sie praktizieren Vertrauensbildung auf einer höheren Aggregationsstufe, indem sie spezifische vertrauensbildende Maßnahmen in den Kontext der Internet-Zahlungssysteme einordnen. Sie können damit verläßliche Antworten auf die Frage nach der Vertrauenswürdigkeit der Zahlungssysteme geben und nicht nur auf die Vertrauenswürdigkeit hinsichtlich einzelner technischer, organisatorischer und rechtlicher Aspekte. Durch diese Bewertung üben sie gleichzeitig eine Kontrollfunktion über diejenigen Institutionen und Organisationen aus, die Vertrauensarbeit in den spezifischen Bereichen leisten.

---

[171] Vgl. Kuhlen (1999), S.307
[172] Vgl. Kuhlen (1999), S.315

Bereits in der Vertrauensbildung bewährte Institutionen, wie bspw. Banken und Kreditinstitute, oder neutrale Kontrollinstanzen gemeinnütziger, kommerzieller oder staatlicher Natur, wie Verbraucherschutzverbände, Bürgerinitiativen, wissenschaftliche Vereinigungen, Vereine, Unternehmensberatungen, oder staatliche Einrichtungen wie die RegTP oder das BSI (Bundesamt für Sicherheit in der Informationstechnik), werden ihre Arbeit auch auf vertrauensbildende Maßnahmen im Bereich der Internet-Zahlungssystemen bzw. der elektronischen Transaktionen generell, ausdehnen, soweit dies nicht, wie beim BSI oder etlichen Banken, schon geschehen ist. In Folge entstehen auch neue Organisationen und Institutionen, die vertrauenskritische Bereiche der Internet-Zahlungssysteme ganz oder partiell mit vertrauensbildenden Leistungen abdecken wollen, wie Trust Center oder Zertifizierungsinstanzen. Neue Kontrollinstanzen werden entstehen, die Kompetenz bündeln, bewerten und auf dieser Basis als neutrale Vertrauensmittler im Bereich der Internet-Zahlungssysteme gegenüber dem Massenpublikum auftreten.

Weil Vertrauen auch zwischen Organisationen eine Rolle spielt, wird Vertrauen nicht nur an den Zugangspunkten vermittelt werden müssen, sondern auch zwischen den Organisationen, etwa zwischen Anbietern kryptographischer Verfahren und Herstellern oder Betreibern von Zahlungssystemen, zwischen staatlichen Instanzen, die die gesetzlichen Rahmenbedingungen schaffen und Herstellern kryptographischer Techniken oder Systembetreibern. Hersteller von kryptographischen Verfahren und Internet-Zahlungssystemen, staatliche Akteure, wie das BSI oder politische Fachausschüsse im Bereich des eCommerce, Trust Center – sie alle werden Vertrauensbildung betreiben, werden sich genauso neutraler Kontrollinstanzen bedienen, die ihre Vertrauensarbeit bündeln, kontextualisieren und mit dem Massenpublikum kommunizieren. Wer diese vertrauensbildenden Kontrollinstanzen sind und zukünftig sein werden, ist im Detail noch nicht abzusehen.

„Wenn es auch noch nicht durchgängige Praxis ist, so spricht einiges dafür, daß Kontrollinstanzen unter dem Gesichtspunkt der Vertrauensbildung in erster Linie in die Hände *neutraler* Dritter (Trusted Third Parties) gelegt werden sollen.“[173] Problematisch ist allerdings, wie das Kriterium der Neutralität spezifiziert werden soll. Wann ist eine Institution neutral und in welcher Hinsicht? Inwieweit kommerzielle Unternehmungen überhaupt diesem Kriterium entsprechen können, muß hinterfragt werden. Unternehmen, die selbst im Bereich der Internet-Zahlungssysteme aktiv sind, wie etwa Unternehmen der kryptographischen Branche, Hersteller von Internet-Zahlungssystemen oder Banken können auch ein kommerzielles Interesse daran haben, Vertrauen dort zu reklamieren, wo dies nicht unbedingt angebracht ist. „Auch die Delegation dieser Aufgaben an neutrale Instanzen, die aber diese Aufgabe selbst wieder in der Regel in kommerzieller Absicht betreiben, löst das Problem der

---

[173] Kuhlen (1999), S.305 und vgl. Grossman (1997), S.182ff

ökonomischen Interessenverflechtung nicht."[174] Dennoch gibt es auch einige Punkte, die für eine kommerzielle Organisation vertrauensbildender Maßnahmen sprechen, bspw. im vertrauenskritischen Bereich des Key-Managements. Wenn nicht nur kommerziellen, sondern auch staatlichen Instanzen kein uneingeschränktes Vertrauen entgegengebracht wird, wie das v.a. in totalitären politischen Systemen, aber häufig auch in Demokratien westlicher Prägung der Fall ist, können nur interessenfreie, nicht-kommerzielle Institutionen effektive Vertrauensbildung erwirken. Diese Idee liegt auch der Identitätssicherung durch Webs of Trust zugrunde. Als Kontrollinstanzen für Internet-Zahlungssysteme können Webs of Trust kaum fungieren, da sie zum einen auf private und weniger auf kommerzielle Transaktionen ausgerichtet sind und eher eine spezielle Erscheinungsform des Key-Managements sind, als Institutionen, die eine aktive Kontrollfunktion wahrnehmen wollen.

Vertrauensbildende Kontrollaufgaben können erfolgversprechend auf Basis erwiesener Kompetenz und Neutralität erbracht werden. Die entsprechende fachspezifische Kompetenz ist in einer Vielzahl von Institutionen vorhanden, von denen viele sicherlich dem oben geschilderten Problem der ökonomischen Interessenverflechtung unterliegen. Vertrauensnetzwerke können hier einen wertvollen Beitrag leisten, indem sie ökonomische Partialinteressen, wie etwa die Bevorzugung bestimmter Verschlüsselungsverfahren oder Zahlungssysteme, zunächst bündeln und dann neutralisieren. Dabei sind Vertrauensnetzwerke nicht auf spezielle Akteure angewiesen. „Vertrauensnetzwerke wollen sich unabhängig von institutionalisierter Kompetenz und institutionalisierten Interessen machen."[175] Kompetenz einmal vorausgesetzt, ist Neutralität die entscheidende Legitimationsbasis für Vertrauensnetzwerke. Reputation wird sicherlich ein Faktor sein, der nicht nur bei der Vertrauensvermittlung gegenüber dem Massenpublikum eine wichtige Rolle spielt. Auch bei der Sicherung von Kompetenz und Neutralität innerhalb des Vertrauensnetzwerks werden die beteiligten Institutionen und Organisationen die höchste Akzeptanz für ihre vertrauensbildenden Maßnahmen erfahren, die eine positive (d.h. kompetente und objektive) Reputation aufbauen können. Ein Akteur, der sein Vertrauen verspielt hat, wird es in einem Vertrauensnetzwerk ungleich schwerer haben, dieses Vertrauen wieder herzustellen. Mit diesem Sanktionsmechanismus garantieren Vertrauensnetzwerke eine Einhaltung der ‚Spielregeln' und können die Qualität und Reliabilität der vertrauensbildenden Maßnahmen verbessern.

Allerdings besteht auch in einem Vertrauensnetzwerk die grundsätzliche Frage, wem in welcher Angelegenheit vertraut werden kann. Sowohl hinsichtlich der Akteure, die in den einzelnen vertrauenskritischen Bereichen Vertrauensbildung betreiben, als

---

[174] Kuhlen (1999), S.314
[175] Kuhlen (1999), S.314

auch in noch viel höherem Maße hinsichtlich der Kontrollinstanzen. Kann keinem der Akteure im Vertrauensnetzwerk ausreichende Neutralität unterstellt werden, wird die Legitimation letztendlich durch das Vertrauensnetzwerk selbst erbracht werden müssen. Welches sind die Kriterien und Verfahren, die eine Bewertung der Neutralität und Kompetenz und damit der Vertrauenswürdigkeit von vertrauensbildenden Institutionen zulassen? Kuhlen nennt in diesem Zusammenhang einerseits objektive Bewertungskriterien, unter die sicherlich die Publikationshäufigkeit oder Referenzen anderer Experten fallen und andererseits die Mitgliedschaft in angesehenen Institutionen als mögliche Indikatoren.[176]

Wenn Vertrauensnetzwerke auch per se keine Kontrollinstanzen sein können, so tragen sie durch ihre Objektivierungs- und Bündelungsfunktion zur Ausbildung und Verläßlichkeit von Kontrollinstanzen bei. Sie setzen damit den Rahmen für die Arbeit dieser Instanzen. Ohne Vertrauensnetzwerke ist sowohl die Bündelung als auch die Objektivierung von vertrauensbildenden Maßnahmen und fachlicher Kompetenz nur schwer möglich. Und genau deshalb wird einem Vertrauensnetzwerk im Bereich der institutionellen Vertrauensbildung in Internet-Zahlungssysteme eine entscheidende Rolle zugebilligt.

In welcher Form dieses Netzwerk realisiert wird und wer letztendlich die Initiative übernimmt, ein Vertrauensnetz aufzubauen, darüber kann derzeit nur spekuliert werden. Von Kuhlen werden Vertrauensnetzwerke genannt, die aus privatem oder institutionellem Engagement aufgebaut werden.[177] Privat initiierte und betriebene Vertrauensnetzwerke, die sich einzelne Personen zur informationellen Absicherung ihrer Handlungen einrichten, sind für den Bereich der Internet-Zahlungssysteme mit umfassender technischer, organisatorischer, rechtlicher Komplexität und globaler Reichweite wahrscheinlich weniger geeignet, als institutionelle Ansätze durch Akteure, die im Bereich der Vertrauensbildung schon über eine wahrgenommene Kompetenz und Neutralität verfügen und sich durch Vertrauensnetzwerke absichern möchten. Privat organisierte Vertrauensnetzwerke setzen gerade im komplexen Bereich der Internet-Zahlungssysteme einen hohen Grad an informationeller Kompetenz und persönlicher Initiative voraus. Dafür sind solche Netzwerke wesentlich unabhängiger von organisierten – in gewissem Maße auch subjektiven – Interessen, als Vertrauensnetzwerke, die durch institutionelles Engagement aufgebaut werden. Allerdings ist auch hier zu berücksichtigen, daß gerade die Bewertung von Kompetenz und Neutralität Privatpersonen – zumal wenn sie nicht über entsprechende informationelle Kompetenz verfügen – vor große Probleme stellen, die allerdings durch elektronische Expertendatenbanken[178] gemildert werden können. Wer diese Expertendatenbanken auf Basis welcher Kriterien aufbauen soll,

---

[176] Vgl. Kuhlen (1999), S.315
[177] Vgl. Kuhlen (1999), S.315
[178] Vgl. Kuhlen (1999), S.315

wird zur Zeit im Rahmen eines Forschungsprojektes am informationswissenschaftlichen Lehrstuhl der Universität Konstanz untersucht. Augenscheinlich wird auch der Aufbau persönlicher Vertrauensnetzwerke – sofern es sich bei den betreffenden Personen nicht selbst um Experten handelt – auf bereits vorhandenen Bündelungs- und Kontrolleistungen aufsetzen müssen. Unter diesem Aspekt ist es fraglich, ob speziell im Bereich der Internet-Zahlungssysteme nicht schon professionelle Vertrauensnetzwerke bzw. ein wie auch immer geartetes Äquivalent, notwendig sind, um diese Vorleistung zu erbringen. In jedem Fall können persönliche Vertrauensnetzwerke als persönliche, emotionale Ergänzung der institutionell arrangierten Vertrauensnetzwerke fungieren.

Im nun folgenden Teil der Arbeit wird anhand praktischer Beispiele verdeutlicht, welche vorhandenen und neuen Institutionen und Organisationen in den einzelnen vertrauenskritischen Bereichen bereits tätig sind oder tätig werden können und welchen Institutionen die Kontrolle dieser vertrauensbildenden Maßnahmen am ehesten zufallen könnte.

7.3 Akteure und Formen der institutionellen Vertrauensbildung

7.3.1 Spezifische Vertrauensbildung

Spezifische Vertrauensbildung bei Internet-Zahlungssystemen konzentriert sich auf die technischen, organisatorischen und rechtlichen, vertrauenskritischen Bereiche. Wie für die Kontrollinstanzen bereits konstatiert wurde, sind wahrgenommene Kompetenz und Neutralität auch hier entscheidende Erfolgsfaktoren. Institutionen, die dem Massenpublikum Kompetenz und Unvoreingenommenheit vermitteln können, werden am ehesten in der Lage sein, Vertrauen in ihren spezifischen technischen, organisatorischen oder rechtlichen Bereich aufzubauen.

7.3.1.1 Technische Aspekte

Im technischen Bereich wurden zwei vertrauenskritische Aspekte identifiziert, die sich auf die Verläßlichkeit der Hard- und Software des Internet-Zahlungssystems und auf die Verläßlichkeit der dem System zugrunde liegenden kryptographischen Verfahren beziehen. Welche Institutionen sind nun auf Basis ihrer Kompetenz überhaupt in der Lage, Vertrauen in diese spezifischen Bereiche zu vermitteln?

7.3.1.1.1 Funktionsfähigkeit des Zahlungssystems

Gerade die Hersteller von Internet-Zahlungssystemen sind bemüht, Vertrauen in die korrekte Funktionsweise der Hard- und Software zu schaffen. Sie besitzen das notwendige Wissen über Einsatz und Funktionalität der technischen Komponenten und haben natürlich ein kommerzielles Interesse an der Diffusion ihrer Produkte.

Die vertrauensbildenden Maßnahmen des niederländischen eCash Herstellers DigiCash sind gezielt auf das Massenpublikum ausgerichtet. Zu diesen Maßnahmen

zählt z.B. die Möglichkeit, verschiedene Arten von eCash Zahlungen in einer simulierten Transaktion mit realistischen Benutzermenüs im WWW nachzuvollziehen. Durch diese Maßnahme wird nicht nur Transparenz bezüglich des Ablaufs einer eCash Zahlung geschaffen. Die Demonstration legt auch den Grundstein für die auf eigenen Erfahrungen basierende Ausbildung von Vertrauen. Natürlich wird eine einmalige Demonstration noch kein Vertrauen schaffen – sie ist jedoch eine grundlegende Erfahrung, auf der sich Vertrauen aufbauen läßt. Potentielle Anwender sind nicht gezwungen, ein Konto bei einer eCash Partnerbank zu eröffnen um dann im realen Selbstversuch zu erfahren, was sich hinter eCash überhaupt verbirgt, sondern können ohne größere Anstrengungen eine (simulierte) eCash Transaktion durchführen. Auch bezüglich der technischen Realisierung von eCash betreibt DigiCash eine transparente Informationspolitik. Die eingesetzten kryptographischen Verfahren, Sicherheitsaspekte und Protokolle werden mit ihren sicherheitsrelevanten Auswirkungen laienverständlich dargestellt.[179]

Ähnlich stellen sich die vertrauensbildenden Maßnahmen der SET Hersteller Visa und MasterCard dar. Visa stellt umfangreiche Informationen über die Funktionsweise und den Ablauf von SET Transaktionen zur Verfügung.[180] Wie DigiCash ermöglicht auch Visa ein ‚Look and Feel' mit einer realistisch animierten Online Demonstration einer SET Transaktion.[181] Spezifische Fragen, die mögliche Unsicherheitsmomente bei SET Anwendern betreffen, werden in einem FAQ-Forum (Frequently Asked Questions) behandelt.[182] Wer tiefer in die technische Materie einsteigen will, kann sich die Spezifikation des SET Protokolls aus dem Internet herunterladen.[183] Die vertrauensbildenden Maßnahmen von Visa richten sich bezüglich des technischen Detaillierungsgrads an Interessenten mit unterschiedlichem Hintergrundwissen. Für die Vertrauensbildung mit dem Massenpublikum sind die formalen Protokollspezifikationen kaum geeignet. Dennoch ist die transparente Darstellung der technischen Grundlagen, selbst wenn sie vom Massenpublikum nicht immer interpretiert werden können, eine Maßnahme, die vielleicht noch kein Vertrauen, aber zumindest Vertrautheit schafft. Um die fehlerfreie Funktion der Software zu dokumentieren, können diverse Pressemitteilungen eingesehen werden, die von erfolgreichen Tests durch Banken zeugen.[184] Positive Einschätzungen neutraler Dritter, die bereits das Vertrauen des Massenpublikums genießen, sind sicher eine geeignete Maßnahme, um dessen Vertrauen zu gewinnen. Interessant ist, daß Visa sich auch des eigenen Vertrauensbonuses, den es bereits im konventionellen Bereich der Kreditkartenzahlungen besitzt, sehr wohl bewußt ist: „You can trust Visa

---

[179] Vgl. Schoemaker (1998)
[180] Vgl. Visa (1999b)
[181] Vgl. Visa (1999e)
[182] Vgl. Visa (1999a) und vgl. SETCo (1999a)
[183] Vgl. SETCo (1999b)
[184] Vgl. Visa (1997a)

and your bank to work for you in the virtual world – just as you know they do in the physical world.“ [185] Das Vertrauen, das dem Kreditkartenunternehmen Visa entgegengebrachte wird, soll so auf das Zahlungssystem SET transferiert werden. Daß Visa auch zukünftig wachsenden Sicherheitsanforderungen gerecht werden will und die Weiterentwicklung von SET aktiv vorantreibt, wird durch eine Reihe von weiteren Pressemitteilungen dokumentiert.[186] MasterCard verweist auf seiner Web Site auf den National Fraud Information Center, eine Non-Profit Verbraucherschutzorganisation, die zur Vermeidung von Internet-Betrügereien jeglicher Art beitragen will. Auch diese Referenz auf eine ‚neutrale'[187] Kontrollinstanz ist geeignet, Vertrauen in die Sicherheit des Zahlungssystems SET zu bilden.

Das vom Information Sciences Institute der University of Southern California entwickelte Internet-Zahlungssystem NetCash ist ein Beispiel für mangelnde Transparenz. Von diesem Zahlungssystem ist nicht bekannt, welche technischen Verfahren bzw. kryptographischen Algorithmen zum Einsatz kommen[188], was eine Vertrauensbildung in die Sicherheit dieses Systems zwangsläufig erschweren muß.[189]

Diese Beispiele zeigen, daß DigiCash und Visa / MasterCard, aber auch andere Hersteller von Internet-Zahlungssystemen[190] größtenteils auf Transparenz und ‚Look and Feel' Erlebnisse setzen, um Vertrauen in ihre Zahlungssysteme aufzubauen. Da diese Unternehmen ein starkes, kommerzielles Interesse an der Verbreitung ihrer Zahlungssysteme haben, werden sie vom Massenpublikum nicht zwangsläufig als neutrale Institutionen betrachtet. Sie sind deshalb auch auf vertrauensbildende Leistungen von Dritten angewiesen, was sich deutlich an den Referenzen auf Banken und Non-Profit Institution, wie den National Fraud Information Center, erkennen läßt. Diese Feststellung gilt auch für die Hersteller kryptographischer Verfahren, die im nächsten Abschnitt behandelt werden.

7.3.1.1.2 Sicherheit kryptographischer Verfahren

Bedeutendster Anbieter im Bereich kryptographischer Verfahren ist das US-amerikanische Unternehmen RSA Data Security. Mehr als 400 Millionen Mal sind Verschlüsselungs- und Authentifizierungstechniken von RSA Data Security in Applikationen wie Netscapes Navigator, Microsoft Windows und Internet-Zahlungssystemen, wie SET und eCash integriert.[191]

---

[185] Vgl. Visa (1999d)
[186] Vgl. Visa (1999c)
[187] Vgl. National Fraud Information Center (1999): Der National Fraud Information Center wird durch eine Reihe von Unternehmen finanziell unterstützt, z.B. MasterCard, MCI, Bell Atlantic u.a., was auf gewisse Abhängigkeiten schließen lassen kann.
[188] Vgl. Kristoferitsch (1998), S.133
[189] Allerdings bringt dies auch den Vorteil, daß ein Angreifer nicht weiß, welche Verschlüsselungsmethode verwendet wird.
[190] Vgl. Millicent (1999), CyberCash (1999), NetBill (1999)
[191] Vgl. RSA (1999a)

Vertrauensbildende Maßnahmen von RSA Data Security sind hauptsächlich auf Experten ausgerichtet. Dies erstaunt nicht, denn die Bewertung von kryptographischen Verfahren setzt eine hohe Fachkompetenz voraus. Dennoch finden sich auch bei RSA Informationen, die auf das Massenpublikum ausgerichtet sind. Erwähnenswert sind ein FAQ Bereich,[192] der unter anderem über Tätigkeitsbereiche des Unternehmens, Notwendigkeit der Kryptographie, den RSA Algorithmus und die Sicherheit der heutigen kryptographischen Verfahren informiert. Darüber hinaus werden ein Glossar mit kryptographischen Fachbegriffen,[193] Informationen über die gängigen Internet-Sicherheitsprotokolle[194] und Referenzen auf Systeme und Anbieter, die RSA einsetzen,[195] angeboten.

An Experten richten sich die von den RSA Labs[196] ausgeschriebenen Wettbewerbe, sog. RSA Challenges, für das Brechen verschiedener kryptographischer Algorithmen und Schlüssel.[197] Wenn eine bestimmte ‚Challenge' gemeistert wurde (d.h. ein Schlüssel oder Algorithmus gebrochen ist), benachrichtigt RSA per eMail die Mitglieder einer Mailing-Liste.[198] Durch die rasche elektronische Publikation der Ergebnisse wird ein hoher Grad an Transparenz bezüglich der Sicherheit von kryptographischen Verfahren erzeugt. RSA Data Security publiziert damit auch negative Meldungen über die Sicherheit der eigenen Verschlüsselungsverfahren und wird so eine neutrale Reputation aufbauen können.

Darüber hinaus richtet RSA Data Security die „RSA Data Security Conference and Expo"[199] aus, die sich mit der gesamten Bandbreite technischer, organisatorischer und rechtlicher Aspekte der Kryptographie beschäftigt und ein breites Diskussionsforum für wissenschaftliche, staatliche und kommerzielle Akteure bietet. Ziel dieser Anstrengungen sind weniger das Massenpublikum, das sich über die Sicherheit von Internet-Zahlungssystemen informieren will, als eher die fachkompetenten, kommerziellen Betreiber der Systeme oder Kontrollinstanzen. Dennoch wird durch diese Transparenz auch beim Massenpublikum eine Vertrauensbasis geschaffen, auf die weitere vertrauensbildende Maßnahmen oder Institutionen aufsetzen können.

Ähnliche vertrauensbildende Maßnahmen wie Expertenseminare, differenzierte Informationsbereitstellung oder Presseveröffentlichungen finden sich bei anderen

---

[192] Vgl. RSA (1999d)
[193] Vgl. RSA (1999f)
[194] Vgl. RSA (1999b)
[195] RSA (1999h)
[196] Die RSA Labs sind eine von RSA Data Security finanzierte Forschungseinrichtung.
[197] Vgl. RSA (1999e)
[198] Vgl. RSA (1999e): Um sich in diese Liste einzutragen, ist lediglich eine eMail an majordomo@rsa.com mit dem Text „subscribe curious-about-secret-key-challenges" zu senden.
[199] Vgl. RSA (1999c)

Herstellern kryptographischer Verfahren, etwa bei GDS,[200] ASCOM[201] oder Security Dynamics.[202]

7.3.1.2 Organisatorische Aspekte

Bezüglich der organisatorischen Infrastruktur stellt sich für das Massenpublikum die Frage, welche Institutionen Identitätssicherung und Key-Management bei digitalen Signaturen vertrauensvoll wahrnehmen und wie vertrauenswürdig Banken und Kreditinstitute hinsichtlich der korrekten Abwicklung der Internet-Zahlungen sind.

7.3.1.2.1 Transaktionsabwicklung

Die vertrauensvolle Abwicklung von finanziellen Transaktionen ist schon seit jeher wichtige Geschäftsgrundlage von Banken und Kreditinstituten. Diese Institutionen haben bei konventionellen Zahlungssystemen wiederholt bewiesen, daß ihnen in diesem Bereich nicht zu unrecht großes Vertrauen entgegengebracht wird. Da Daten über konventionelle Zahlungen (z.B. EC- und Kreditkartentransaktionen) schon heute weitestgehend elektronisch verarbeitet werden, dürfte auch im Bereich der Internet-Zahlungssysteme[203] zu erwarten sein, daß Banken und Kreditinstitute kompetent und vertrauenswürdig handeln.

Vertrauen in die korrekte Abwicklung der Internet-Zahlung sollte damit nicht das vordergründige Problem sein, auf das sich vertrauensbildende Maßnahmen dieser Institutionen konzentrieren. Dieser Einsicht entspricht die öffentliche Positionierung von Banken und Kreditinstituten, die weniger darauf abzielt, Vertrauen in ihre Abwicklungskompetenz zu bilden, als vielmehr in spezifische Zusatzleistungen des Anlagen- und Kreditgeschäfts oder eben in Internet-Zahlungssysteme.

Daß absolutes Vertrauen in die Abwicklungskompetenz von Banken und Kreditinstituten nicht ohne weiteres vorausgesetzt werden kann, zeigt der eingangs beschriebene Fall des wohl größten Kreditkartenbetrugs aller Zeiten.[204] Experten gehen davon aus, daß die Kreditkarteninformationen nicht beim Zahlungsverkehr via Internet abgefangen worden sind, sondern in großer Anzahl bei Banken und Kreditinstituten gestohlen wurden. Banken und Kreditinstituten[205] ist darüber hinaus Fahrlässigkeit vorzuwerfen, da sie unverschlüsselte Zahlungsvorgänge anstandslos abgewickelt haben, bzw. die Bezahlung mittels unverschlüsselter Transaktionen überhaupt zulassen. Ob und wie dieser Betrugsfall durch vertrauensbildende oder besser, durch vertrauensreparierende Maßnahmen kommuniziert werden wird, bleibt abzuwarten.

---

[200] Vgl. GDS (1999)
[201] Vgl. Ascom (1999)
[202] Vgl. Security Dynamics (1999)
[203] Vgl. Bussiek (1998)
[204] Vgl. 1.2 Sicherheit und Akzeptanz
[205] Vgl. Faughnan (1998): John Faughnan erwähnt, daß deutsche Banken (z.B. die Hypo-Bank) relativ strenge Sicherheitsvorkehrungen haben, so daß in Deutschland nur wenige Fälle bekannt wurden.

Da aller Wahrscheinlichkeit nach Banken und Kreditinstituten innerhalb des Vertrauensnetzwerks eine wichtige Stellung als Kontrollinstanzen zukommen wird, soll die praktische Ausprägung der institutionellen Vertrauensbildung dieser Akteure im entsprechenden Teil weiter unten erläutert werden.[206]

7.3.1.2.2 Authentizitätssicherung und Key-Management

Gängige Internet-Zahlungssysteme setzen digitale Signaturen für die Sicherung der Authentizität der an einer Transaktion beteiligten Objekte und Personen ein. Der Einsatz dieses Verfahrens bedingt zwangsläufig eine Einrichtung, die zumindest die Identität der Signaturinhaber verifiziert und ihre öffentlichen Schlüssel verwaltet. Zur Lösung dieser Aufgabe existieren zwei grundsätzlich verschiedene Verfahren, einerseits hierarchische, professionell organisierte Verfahren, wie die im SigG festgelegte Idee der Trust Center und andererseits privat organisierte Modelle, die sog. Webs of Trust. „Für beide Formen ist das Ziel letztendlich gleich. Irgend jemand muß damit beauftragt werden, daß das, was geschehen soll, tatsächlich von den Personen geschieht, die dafür vorgesehen sind und daß die durchgeführten Transaktionen vertraulich bleiben und nicht manipuliert werden können.

7.3.1.2.2.1 Trust Center

Im deutschen SigG wird ein hierarchisches Modell als adäquate Sicherheitsinfrastruktur für digitale Signaturen festgelegt.

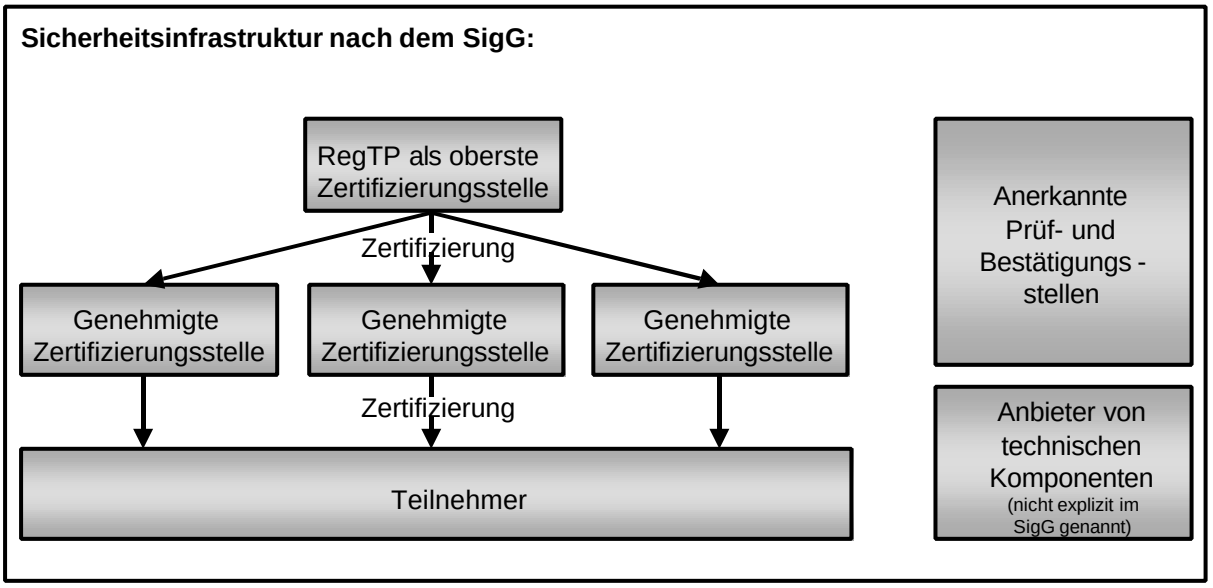

Abbildung 10: Sicherheitsinfrastruktur nach dem SigG[207]

Eine zentrale staatliche Behörde, die RegTP, fungiert als nationale Wurzelinstanz[208] und zertifiziert bei Vorliegen bestimmter Eigenschaften, wie Zuverlässigkeit und

---

[206] Vgl. 7.3.2 Kontrollinstanzen
[207] Vgl. Deutsche Telekom (1998), S.2
[208] Vgl. SigG §4 I

Fachkompetenz,[209] sogenannte Trust Center, die im Wortlaut des SigG als „Zertifizierungsstellen“ bezeichnet werden. Die Prüfung, ob Zertifizierungsstellen oder einzelne technische Komponenten mit dem SigG konform sind, übernehmen sog. Prüf- und Bestätigungsstellen. Anbieter technischer Komponenten sind im SigG zwar nicht explizit genannt; durch die Prüf- und Bestätigungsstellen zertifizierte technische Komponenten werden jedoch durch die RegTP im Bundesanzeiger veröffentlicht und den Zertifizierungsstellen bekanntgemacht. Um nachgeordnete Zertifizierungsstellen zu zertifizieren, muß die RegTP zunächst selbst ein gesetzeskonformes Trust Center aufbauen, da die RegTP mit ihrem ‚Wurzelschlüssel‘ Zertifikate für die Signaturschlüsselpaare der Zertifizierungsstellen signieren und in einem Verzeichnis öffentlich zugänglich machen muß.[210] Nach einer Identitätsprüfung signiert die Zertifizierungsstelle mit ihrem privaten Schlüssel die digitalen Zertifikate[211] der Teilnehmer, die in der Hauptsache Name bzw. Pseudonym eines Teilnehmers und den ihm zugeordneten öffentlichen Schlüssel enthalten. Der private Schlüssel des Teilnehmers wird auf einer PIN-geschützten Chipkarte so gespeichert, daß die Zertifizierungsstelle keine Kenntnis von diesem Schlüssel erlangt.[212] Die PIN und die entsprechende Chipkarte erhält der Teilnehmer auf getrenntem Wege. Der öffentliche Schlüssel des Teilnehmers wird in einem öffentlich zugänglichen Verzeichnis aufgeführt.[213] Unter bestimmten Umständen hat der Trust Center von ihm ausgegebene Zertifikate zu sperren.[214] Bis hierher besteht die vertrauenskritische Aufgabe der Trust Center hauptsächlich in der korrekten Identifikation der Teilnehmer und der korrekten Erzeugung und sicheren Verwaltung der Teilnehmerschlüssel. Auf die hierzu erforderlichen Sicherheitsmaßnahmen organisatorischer, baulicher und technischer Art wird im SigG verwiesen.[215] Da der private Schlüssel der Teilnehmer der Zertifizierungsstelle nicht bekannt ist, besteht keine Gefahr des Mißbrauchs, es sei denn, der Teilnehmer selbst handelt fahrlässig, z.B. indem er seine Chipkarte mit PIN verliert, daß unbefugte Dritte in den Besitz seines Zertifikats gelangen. Dieser ‚menschliche Faktor‘ kann nie völlig ausgeschlossen werden. Ein Mißbrauch durch staatliche oder private Akteure ist im Rahmen der heute gültigen gesetzlichen Regelungen und bei sorgfältigem Umgang mit den privaten Schlüsseln unwahrscheinlich.[216]

Wesentlich heikler wäre die Situation, wenn Trust Center Kopien der privaten Teilnehmerschlüssel besitzen würden, etwa wenn eine derartige Key-Escrow

---

[209] Vgl. SigG §4 II
[210] Vgl. SigG §4 V
[211] Vgl. 6.2.1 Digitale Signatur
[212] Vgl. SigV §5 II
[213] Vgl. SigG §5 I
[214] Vgl. SigG §8
[215] Vgl. §12 SigG
[216] Vgl. Kristoferitsch (1998), S.75: Kristoferitsch verweist auf ein neues Verfahren, bei dem die Karten mit Salpetersäure oder flüssigem Helium behandelt werden, um an den Schlüssel zu gelangen.

Regelung erlassen würde oder Teilnehmer freiwillig Kopien ihrer privaten Schlüssel bei Trust Centern hinterlegen, um bei Verlust ihrer Chipkarte oder PIN noch auf ihre verschlüsselten Daten zugreifen zu können. Um Sicherungskopien ihrer privaten Schlüssel zu speichern, können die Teilnehmer andere Akteure, bspw. Freunde oder ihren Rechtsanwalt, einsetzen. Im Fall einer gesetzlichen Regelung, die staatlichen Stellen in bestimmten Situationen den Zugriff auf private Teilnehmerschlüssel erlaubt, erhält die Vertrauensfrage eine neue Dimension. Einmal vom notwendigen Vertrauen in die sichere Aufbewahrung der Schlüssel und dem potentiellen Mißbrauchsrisiko durch Kriminelle abgesehen, ist fraglich, inwieweit die Teilnehmer staatlichen Instanzen bezüglich des Gebrauchs oder Mißbrauchs der hinterlegten, privaten Schlüsseln vertrauen. Überlegungen, die Hinterlegung der privaten Schlüssel zwingend vorzuschreiben, sind alles andere als utopisch und werden auch in Deutschland kontrovers diskutiert.[217]

Welche Akteure sind nun bemüht, Vertrauen in die organisatorische Infrastruktur der Internet-Zahlungssysteme zu vermitteln? Zu den aktiven staatlichen Akteuren sind sowohl die RegTP, als auch das BSI und eine gemeinschaftliche Initiative ‚Sicherheit in der Informationsgesellschaft' des Bundesministeriums für Wirtschaft und Technologie, des Bundesministeriums des Innern und des BSI zu zählen.

Die Internet-Präsenz der RegTP bietet, neben dem auch für die Wurzelinstanz obligatorischen Verzeichnisdienst der öffentlichen Schlüssel[218], Informationen, die als vertrauensbildende Maßnahmen im Bereich der Kryptographie und digitalen Signatur anzusehen sind.

Von der betreffenden Startseite[219] aus werden neben allgemeinen Informationen über Funktionsweise und Ablauf der Digitalen Signatur (als Datei oder Videoclip erhältlich) die entsprechenden Rechtsgrundlagen (IuKDG, SigG, SigV, Maßnahmenkataloge), amtliche Veröffentlichungen (bspw. über die erteilten Lizenzen zum Betrieb einer Zertifizierungsstelle), eine Zusammenstellung von FAQs und eine informative Sammlung von Links zum Thema digitale Signatur aufgeführt. Darüber hinaus besteht die Möglichkeit, direkt (per Telefon, Fax oder eMail) mit dem verantwortlichen Mitarbeiter der RegTP in Kontakt zu treten. Die Policy Seite der RegTP, die hinsichtlich der Vertrauensbildung sehr interessant gewesen wäre, befindet sich z.Zt. leider noch im Aufbau.

Wesentlich knapper gefaßt sind die Informationen, die auf dem Server des BSI enthalten sind. Im Kontext der digitalen Signaturen ist das ‚Projektbüro Digitale Signatur'[220] interessant, dessen primäres Ziel nach Aussage des BSI „die Information

---

[217] Möller (1997)
[218] Vgl. RegTP (1999c)
[219] Vgl. RegTP (1999b) und auf die von dort aus verwiesenen Links.
[220] Vgl. BSI (1999c)

der Öffentlichkeit rund um das Thema ‚Digitale Signatur'"[221] ist. Dieser Zielsetzung entsprechen die angebotenen Informationen kaum. Sie bestehen hauptsächlich in Querverweisen zu anderen Ressourcen – etwa der RegTP oder der gemeinsamen Initiative ‚Sicherheit in der Informationsgesellschaft'. Positiv fallen die vom BSI angebotenen Dienstleistungen[222] (Hotline, Beratungsleistungen etc.) auf, die jedoch weniger für das Massenpublikum, als eher für kommerzielle Anwender und potentielle Zertifizierungsstellenbetreiber gedacht sind. Ebenso sind auf dieser Seite Kontaktmöglichkeiten (per Telefon, Fax und eMail) zu den entsprechenden Experten des BSI erwähnt. Insgesamt wird das Projektbüro Digitale Signatur seinem selbstgesteckten Ziel – Information der Öffentlichkeit – somit nur unzureichend gerecht.

Umfassender stellen sich die Informationen und Kontaktmöglichkeiten der oben genannten. Initiative ‚Sicherheit in der Informationsgesellschaft' dar. Auf der Homepage[223] werden neben ausgesprochen (laien-) verständlichen Informationen über kryptographische Grundlagen, Anwendung und rechtliche Stellung digitaler Signaturen, ein Glossar der wichtigen Fachbegriffe, eine Sammlung häufig gestellter Fragen (FAQs) und Kontaktmöglichkeiten zu Experten angeboten. Darüber hinaus besteht die Möglichkeit, einen News-Letter zu abonnieren und eigene Themen und Webseiten vorzuschlagen, die redaktionell bearbeitet werden. Das News-Archiv, auf das ebenfalls auf der Homepage verwiesen wird, enthält neueste sicherheitsrelevante Informationen. Insgesamt präsentiert diese Initiative ein umfassendes, sehr verständliches und - nicht zuletzt durch die redaktionelle Kontrolle und Offenlegung vertrauenskritischer Informationen - vertrauenswürdiges Klima.

Derzeit liegen der RegTP insgesamt 33 Anträge auf Zulassung einer Zertifizierungsstelle vor; diese Zahl ist jedoch nicht aussagekräftig, weil zum einen viele dieser Anträge keine Erfolgsaussichten besitzen und zum anderen viele aussichtsreiche Bewerber noch keinen Antrag eingereicht haben.[224] Die derzeit einzige, von der RegTP zugelassene Zertifizierungsstelle in Deutschland ist der Trust Center der Deutschen Telekom, Telesec. „Pikanterie am Rande: Telesec ist eine Tochter der Telekom AG und die liefert die technische Ausrüstung für das Basis-Trustcenter bei der Regulierungsbehörde."[225]

Vertrauensbildende Maßnahmen der Telesec im Bereich der digitalen Signaturen sind hauptsächlich aufs Massenpublikum und damit auf potentielle Kunden ausgerichtet. Wie bei den bereits genannten Institutionen wird eine Fülle von Informationen über kryptographische Verfahren, über die Sicherheit der digitalen

---

[221] Vgl. BSI (1999b)
[222] Vgl. BSI (1999a)
[223] Vgl. Sicherheit in der Informationsgesellschaft (1999a)
[224] Vgl. Kontaktinformationen (1999)
[225] Seeger (1998)

Signatur[226] und der rechtlichen Situation[227] zur Verfügung gestellt. Eine interaktive Präsentation über Einsatz und Funktion digitaler Signaturen steht online zur Verfügung.[228] Bauliche und organisatorische Sicherheitsmaßnahmen werden ebenfalls dargestellt.[229] Auch die Telesec setzt somit hauptsächlich auf Transparenz und elektronisch simulierte, persönliche Erfahrungen. Allerdings ist zu erwarten, daß ein gewichtiger Teil der Vertrauensbildung nicht über das WWW, sondern im persönlichen Kontakt, also durch die Angestellten der Telekom in den T-Punkt Niederlassungen, erbracht werden muß. Für die meisten Anwender werden diese Personen die Zugangspunkte sein, an denen personale Vertrauensvermittlung stattfindet. In dieser Infrastruktur liegt der offensichtliche Vorteil, den Telesec gegenüber zukünftigen Mitkonkurrenten haben dürfte.[230] Vorausgesetzt, das Personal in den T-Punkten hat die notwendige Kompetenz, um diesen Anforderungen gerecht zu werden. Derzeit scheint diese Kompetenz nicht vorhanden zu sein. Auf eine persönliche Anfrage in T-Punkte in Konstanz[231] und Heidelberg[232] hin wurden zwar Anträge und Informationsmaterialien zur digitalen Signatur ausgehändigt, Auskünfte über das Signaturverfahren und Sicherheitsaspekte konnte das Personal jedoch nicht geben. Nach Auskunft eines T-Punkt Mitarbeiters[233] verstehen sich die T-Punkte nicht als Auskunftsstelle für potentielle Anwender digitaler Signaturen, sondern lediglich als Ausgabestelle für Anträge und Informationsmaterialien der Telesec. Angesichts des derzeit noch hohen Beratungsbedarfs[234] bei digitalen Signaturen besteht hier zweifelsohne ein erhebliches Defizit. Geplante Schulungen und Weiterbildungsmaßnahmen – so teilte die Telesec auf eine Anfrage hin mit – sind für T-Punkt Mitarbeiter nicht geplant, allerdings bestünde die Möglichkeit, sich über eine kostenlose PKS Support Hotline zu informieren: „Im Interesse einer bezahlbaren Dienstleistung müssen wir das Kern-know-how konzentrieren." Darüber hinaus – so die widersinnige Argumentation der Telesec – besteht bei digitalen Signaturen ein hoher Beratungsbedarf, der das übrige Tagesgeschäft stark behindern würde.[235] Die Telesec sieht ihren Konkurrenzvorteil nicht in der Möglichkeit, an personalen Zugangspunkten Vertrauen in digitale Zertifikate zu vermitteln, sondern lediglich im logistischen Vorteil einer vorhandenen Registrierungsinfrastruktur. Offensichtlich geht das Unternehmen davon aus, daß potentielle Kunden entweder ein hohes Maß an Eigeninitiative bzw. an informationeller Kompetenz oder schon ein hohes Maß an

---

[226] Vgl. Deutsche Telekom (1999d) und vgl. Deutsche Telekom (1999c)
[227] Vgl. Deutsche Telekom (1999b)
[228] Vgl. Deutsche Telekom (1999a)
[229] Vgl. Deutsche Telekom (1999e)
[230] Vgl. RegTP (1999a): 1999 wird mit der Zulassung von drei bis sieben weiteren Zertifizierungsstellen gerechnet.
[231] Am 23.7.99, T-Punkt, Rosgartenstraße 10, 78462 Konstanz.
[232] Am 28.7.99, T-Punkt, Hauptstraße 55, 69117 Heidelberg
[233] Am 23.07.1999, T-Punkt Konstanz, Rosgartenstraße
[234] Vgl. Hillebrand/Büllingen (1998), S.43
[235] Vgl. eMail der Telesec – Kontaktstelle ‚T-Teleseccrypt@telekom.de', 01.07.1999

Vertrauen mitbringen. Ob sich diese Annahmen als haltbar erweisen, erscheint zweifelhaft. Schließlich ist, wie die Telekom richtig erkannt hat, ein großer Beratungsbedarf bei digitalen Signaturen zu beobachten.

Auf eine ähnliche Infrastruktur können sich staatliche Einrichtungen, sowie Finanzinstitute stützen. Gerade letztere sind aufgrund ihrer langjährigen Erfahrung und vertrauenswürdigen Reputation prädestiniert, auch im neuen Bereich des Key-Managements als vertrauenswürdige Dritte aktiv zu werden: „Placing large numbers of cryptographic keys – which in a digital world will be our identities – in the hands of trusted third parties is going to create a new set of institutions with the kind of power and responsibilities currently associated with banks.“[236] Da Banken und Kreditinstitute allem Anschein nach nicht nur eine zentrale Rolle als Key-Management Institutionen spielen können, sondern im eigenen ökonomischen Interesse umfassende Kontroll- und Vertrauensarbeit im Bereich der Internet-Zahlungssysteme wahrnehmen müssen, werden diese Akteure weiter unten gesondert behandelt.[237]

Festzuhalten bleibt, daß staatliche und kommerzielle Institutionen, die heute im Bereich der Identitätssicherung und im Key-Management aktiv sind, in der Vertrauensbildung auf ähnliche Maßnahmen setzen, wie die Hersteller von kryptographischen Verfahren und Internet-Zahlungssystemen. Transparenz im Sinne einer offenen Informationspolitik und die Vermittlung erster eigener Erfahrungen durch elektronische Simulationen werden derzeit als geeignetes oder vielleicht besser als ausreichendes Instrument zur institutionellen Vertrauensbildung betrachtet. Für Institutionen mit breiter Infrastruktur dürfte darüber hinaus die Qualität der an den Geschäftsstellen erbrachten Vertrauensarbeit ein wichtiger, bisher jedoch vernachlässigter Erfolgsfaktor sein.

7.3.1.2.2.2 Webs of Trust

Das Web of Trust, wie es im Rahmen der Verschlüsselungssoftware PGP zum Einsatz kommt, ist ein privat organisierter Ansatz, der Identitätssicherung losgelöst von staatlicher und institutioneller Kontrolle verwirklichen will.

Identitätssicherung in einem Web of Trust läuft folgendermaßen ab:[238] Jeder Teilnehmer erzeugt für sich selbst ein Schlüsselpaar, wobei er die Länge der Schlüssel (und damit den Sicherheitsgrad) selbst bestimmen kann. Den öffentlichen Schlüssel übermittelt der Teilnehmer an eine Person seines Vertrauens, von der er eine Bestätigung in Form eines digitalen Zertifikats erhält, das besagt, daß der Schlüssel auch wirklich ihm zuzuordnen ist. Dieses Zertifikat kann der Teilnehmer benutzen, um sich gegenüber weiteren Teilnehmern zu authentifizieren. Schwieriger wird es, wenn zwei Personen Informationen austauschen wollen, die sich nicht

---

[236] Grossman (1997), S.185
[237] Vgl. 7.3.2 Kontrollinstanzen
[238] Vgl. Telstra (1999) für eine große Sammlung von PGP-Handbüchern und -Dokumentationen.

persönlich kennen. Sie müssen versuchen, über andere Personen eine Vertrauenskette aufzubauen. Praktisch sieht das so aus: A will mit C vertrauliche Informationen austauschen, die beiden kennen sich jedoch nicht persönlich. Weder A noch C weiß sicher, daß hinter dem öffentlichen Schlüssel des anderen auch wirklich die Person steht, die sie vorgibt zu sein. Wenn A und C einen gemeinsamen Bekannten B haben, dem sie vertrauen, ist das Problem gelöst. B bestätigt gegenüber A die Identität von C und umgekehrt. Wenn A und C keinen gemeinsamen Bekannten haben, der für ihre Identität bürgt, müssen sie versuchen, eine Vertrauenskette über weitere Personen zu konstruieren. Diese Vertrauenskette kann u.U. sehr lang werden.[239] Lange Vertrauensketten bringen erhebliche Probleme mit sich, für die eine Lösung in einem Web of Trust, das auf institutionelle Komponenten (z.B. Trust Center) verzichtet, aussteht:

- ☞ Je länger Vertrauensketten werden, desto höher ist ihre Fehleranfälligkeit; wenn nur ein Glied in der Kette die Anforderungen nicht versteht oder nicht erfüllt, bricht die gesamte Kette zusammen.[240]

- ☞ Die Vertrauenswürdigkeit der Teilnehmer sinkt, je größer der Abstand in der Vertrauenskette ist.[241]

- ☞ Umgekehrt steigt der Aufwand für die Überprüfung der Vertrauenswürdigkeit eines Zertifikates mit der Länge der Vertrauenskette.[242]

- ☞ Die Ungültigkeit eines Zertifikats ist in akzeptabler Zeit nicht mit allen Mitgliedern des Web of Trust zu kommunizieren.

Um diese Probleme klein zu halten, sollten Vertrauensketten so kurz wie möglich konstruiert werden. Für den universellen Einsatz digitaler Zertifikate bei Internet-Zahlungssystemen ist diese Forderung jedoch nicht zu erfüllen. Als Alternative zur institutionelle Vertrauensbildung und –sicherung durch Trust Center können Webs of Trust deshalb nicht fungieren: „Von seiten der Wirtschaft wird dieses (außerstaatliche, außerinstitutionelle, private) Modell der Vertrauenssicherung durch ein Web of Trust wegen seines Aufwandes und der Fehleranfälligkeit nicht als mögliche Alternative zur institutionalisierten Kryptographiesicherung bzw. zu Signaturverfahren angesehen.“[243]

---

[239] Vgl. Parkins (1997) für die exemplarische Darstellung einer umfangreichen Vertrauenskette.
[240] Vgl. Kuhlen (1999), S.313
[241] Vgl. Galvin (1997), S.18f
[242] Vgl. Galvin (1997), S.18f
[243] Kuhlen (1999), S.313

7.3.1.2.2.3 Bewertung

Die Praxis der Webs of Trust, Vertrauen an persönlich bekannte Personen zu delegieren, kommt der gewohnten Vertrauenspraxis sehr entgegen. Ein solches Web of Trust auf globaler Basis zu organisieren ist nicht möglich. Infolge dessen werden institutionelle Komponenten notwendig sein, die Identitätssicherung und Key-Management im entsprechenden Umfang wahrnehmen können. Dabei wird sich eine hierarchische Struktur aufbauen müssen, in der sich nationale Wurzelinstanzen – wie in Deutschland die RegTP – gegenseitig zertifizieren und damit für die von ihnen ausgestellten Zertifikate auf supranationaler Ebene bürgen. Eine sehr interessante und durchaus praktikable Lösung, die auf einer staatlichen Organisation aufsetzt, schlägt Jim Galvin im World Wide Web Journal vor: „Well, one way is for local governments to issue a digital as well as a birth certificate. This gives us a nice hierarchical infrastructure that, in fact, applies for all practical purposes worldwide."[244]

7.3.1.3 Rechtliche Aspekte

7.3.1.3.1 Rechtliche Verbindlichkeit von Internet-Zahlungen

Rechtliche Unsicherheiten, die im Zusammenhang mit Internet-Zahlungssystemen bestehen, werden in Deutschland durch das SigG vermindert. Das SigG bildet in Deutschland die rechtliche Basis für die Anwendung digitaler Signaturen.

Kontrovers diskutiert wird zum einen die Grundsatzfrage, ob die Sicherheitsvermutung des SigG, die davon ausgeht, daß die Sicherheit digitaler Signaturen durch die Bestimmungen des SigG garantiert wird, gerechtfertigt ist. Auf der anderen Seite besteht nach dem Scheitern der Gesetzesnovelle[245] des §126 I BGB immer noch das Problem, daß elektronische Signaturen nicht den gesetzlichen Formvorschriften genügen.

Die Grundsatzfrage, ob die Sicherheitsvermutung gerechtfertigt ist, läuft nicht ausschließlich auf eine technische oder mathematische, sondern im Zuge einer einheitlichen europäischen Gesetzgebung auf eine politische Diskussion hinaus. Roßnagel, der an der Formulierung des SigG maßgeblich beteiligt war, sieht die Sicherheit digitaler Signaturen unter den im SigG festgelegten Maßnahmen als realisiert an: „Signaturgesetz und Signaturverordnung enthalten für alle Sicherheitsaspekte entsprechende Sicherheitsanforderungen und Mechanismen, [um (Anm. d. Verf.)] ihre Erfüllung sicherzustellen."[246] Hoeren weißt in diesem Zusammenhang darauf hin, daß es im Rahmen der europäischen Nivellierung zu einer Absenkung des im SigG festgeschriebenen Sicherheitsstandards kommen wird, weil die deutschen Standards auf EU-Ebene als übertrieben, wenn nicht wettbewerbsfeindlich angesehen werden. Ungeachtet einer zukünftigen

---

[244] Galvin (1997), S.19
[245] Vgl. 5.2.3.3.1 Rechtliche Verbindlichkeit von Internet-Zahlungen
[246] Roßnagel (1998), S.3314

europäischen Gesetzgebung – hier liegt der eigentliche Widerspruch zu Roßnagel – sieht Hoeren die den digitalen Signaturen zugrundeliegende Sicherheit der asymmetrischen Verschlüsselung lediglich als zeitabhängige Tatsache an: „Sobald sich die Technik weiterentwickelt, wird das Vertrauen in bestehende Verschlüsselungstechniken hinfällig. (...) Eine digitale Signatur hat keinen Beweiswert; dieser variiert intertemporal.“[247]

Das BSI geht allerdings davon aus, daß Schlüssel mit 1024 Bit innerhalb der nächsten fünf Jahre als sicher angesehen werden können. Und für die Zeit danach stehen Pläne für die Verdoppelung der Schlüssellänge bereit; allerdings können Schlüssel mit 2048 Bit derzeit noch nicht auf Smartcards untergebracht werden, was die Flexibilität der Anwender erheblich einschränkt und darüber hinaus den Transport der Zertifikate vom Trust Center zum Inhaber erheblich komplizierter gestaltet.[248]

Wenn digitale Signaturen keinen juristischen Beweiswert haben, hat das für alle mittels dieser Signaturen abgewickelten Vorgänge und damit auch für finanzielle Transaktionen im Internet entscheidende Konsequenzen. Haben digitale Signaturen keine eindeutige Beweiskraft, wie ist dann in einem Zivilprozeß zweifelsfrei nachzuweisen, daß Transaktionen in der elektronisch dokumentierten Form von den Inhabern der digitalen Zertifikate zu einem bestimmten Zeitpunkt vorgenommen wurden? Ist jeweils ein elektronischer Dokumentenbeweis notwendig, um diese Fakten einwandfrei festzustellen? Roßnagel verneint aufgrund der Sicherheitsvermutung die Notwendigkeit eines solchen Beweises,[249] Hoeren sieht ihn im Einzelfall als unverzichtbar an.[250]

Letztlich soll der Beweiswert der digitalen Signatur durch die technische Sicherheit gerechtfertigt werden. Den Gerichten steht es im Rahmen der freien Beweiswürdigung dann frei, digitale Signaturen als rechtskräftiges Beweismittel zu akzeptieren. Würde die Sicherheitsvermutung jedoch widerlegt, wird diese Tatsache höchstwahrscheinlich in die entsprechenden Gerichtsurteile einfließen.

Unabhängig vom Beweiswert digitaler Signaturen erscheint hinsichtlich ihres praktischen Einsatzes problematisch, daß sie nach wie vor nicht den Formvorschriften des §126 I BGB entsprechen. Es besteht zwar die Möglichkeit, daß Akteure, die regelmäßig digitale Signaturen in ihrem Geschäftsverkehr verwenden, bis zu einer entsprechenden Gesetzesnovelle einen Vertrag vereinbaren, der festlegt, wie sie digital signierte Dokumente behandeln wollen.[251] Für beliebige Händler-Kunden-Beziehungen, die bei Internet-Zahlungen die Regel sein werden, scheint eine solche Individualregelung ungeeignet. Schließlich wäre es inakzeptabel,

---

[247] Hoeren (1998), S.2854
[248] Vgl. Seeger, H. (1998)
[249] Vgl. Roßnagel (1998), S.3320
[250] Vgl. Hoeren (1998), S.2854
[251] Vgl. Hillebrand/Büllingen (1998), S.43

wenn Händler und Kunde jeweils erst einen Vertrag unterzeichnen müßten, bevor die finanzielle Transaktion rechtssicher abgewickelt werden kann. Dieser Vertrag müßte aufgrund derzeit gültiger Formvorschriften des §126 I BGB handschriftlich unterzeichnet werden. Um dieser Problematik zu begegnen, ist eine Anpassung der gesetzlichen Formvorschriften notwendig. Nach dem gescheiterten Gesetzesentwurf für einen neu zu schaffenden §126 a BGB bleibt derzeit allerdings offen, ob ein neuer Anlauf den von Experten geforderten Bezug zum Signaturgesetz in der gewünschten Form herstellen kann.

Für Anwender ist und bleibt deshalb die kritische Frage, welche Beweiskraft mittels digitaler Signaturen vorgenommene Zahlungsvorgänge haben. Wenn sich die Rechtsprechung an der Sicherheitsvermutung orientiert und digitalen Signaturen im Rahmen der freien Beweiswürdigung eine umfassende Beweiskraft zugesteht, wird das sicherlich Vertrauen in digitale Signaturen und damit auch in Internet-Zahlungssysteme bilden. Ähnliches würde für die Ausdehnung der gesetzlichen Formvorschriften auf digitale Signaturen gelten. Doch auch wenn diese Probleme überwunden werden, muß die gewährte Rechtssicherheit dem Massenpublikum vermittelt werden. Dementsprechend hat die Bundesnotarkammer einen umfassenden rechtlichen Beratungsbedarf in diesem Bereich diagnostiziert, der u.a. von Notaren, Rechtsanwälten oder Zertifizierungsstellen befriedigt werden kann.[252]

Gerade Notare und Anwälte bzw. entsprechende Vereinigungen dieser Berufsgruppen, denen schon in anderen Bereichen ein hohes Maß an Vertrauen entgegengebracht wird, könnten als die personalen Zugangspunkte für die Vertrauensbildung in die rechtlichen Aspekte der Internet-Zahlungssysteme fungieren. Daß diese Vertrauensbildung notwendig ist, daran besteht kein Zweifel. Noch hat sich in der Rechts- und Alltagspraxis kein auf Erfahrung begründetes Vertrauen in die Gültigkeit von digitalen Signaturen und Internet-Zahlungsvorgängen etablieren können.

Letztlich sei noch ein Punkt angesprochen, der den Zusammenhang zwischen der ökonomischen Dimension und Vertrauensbildung bezeichnet und hinsichtlich der praktischen Umsetzung der im Signaturgesetz formulierten Maßnahmen nicht vernachläßigt werden darf. Wie am Beispiel der Zertifizierungsleistungen von Telesec ersichtlich ist, sind mit dem SigG konforme digitale Zertifikate derzeit (noch) eine relativ teure Angelegenheit.[253] Digitale Zertifikate werden auf Smartcards gespeichert, für deren Benutzung wiederum ein Kartenlesegerät am PC installiert sein muß. Die Kostenfrage trifft nicht nur das Massenpublikum, sondern in noch größerem Ausmaß die Händler, die sich – ähnlich wie die Zertifizierungsstellen – von der RegTP

---

[252] Vgl. Hillebrand/Büllingen (1998), S.43

[253] In den T-Punkten bietet die Telekom derzeit ein Set bestehend aus Chipkarte, Lesegerät und Software zum Preis von 159.- DM an.

zertifizieren lassen müssen. „Der Vorgang dauert sehr lange und ist viel zu teuer“, [254] so Lutz Becker vom Bundesverband für Informations- und Kommunikationssysteme, die Kosten liegen in sechsstelliger Größenordnung. Noch viel teurer ist der Aufbau einer gesetzeskonformen Zertifizierungsstelle. Bis zu 20 Mio. DM Aufwand veranschlagen Experten hierfür.[255] Es scheint, daß paradoxerweise gerade die Vertrauen schaffenden Sicherheitsmaßnahmen des SigG den Aufbau einer vertrauenswürdigen Infrastruktur hemmen. Neben der institutionellen Vertrauensbildung wird deshalb ein Beitrag zur Akzeptanz von Internet-Zahlungssystemen darin bestehen müssen, die damit verbundenen Leistungen zu einem konkurrenzfähigen Preis anzubieten.

Da die Beweiskraft digitaler Signaturen von ihrer technischen Sicherheit abhängt und diese wiederum auf der Sicherheit der zugrunde liegenden kryptographischen Verfahren aufbaut, ist der unreglementierte Zugriff auf starke Kryptographie eine grundlegende Bedingung für die Bereitstellung sicherer und damit vertrauenswürdiger Internet-Zahlungssysteme. In dieser Hinsicht wird seit geraumer Zeit eine dogmatisch anmutende Diskussion um das Für und Wider staatlicher Kryptoregulierung geführt.

7.3.1.3.2 Staatliche Kryptoregulierung

Die Verfügbarkeit starker und damit sicherer kryptographischer Verfahren ist eine entscheidende Voraussetzung für die Vertrauenswürdigkeit von Internet-Zahlungssystemen. In Deutschland ist eine rege Diskussion über Sinn und Zweck bzw. Ausprägung einer eventuellen Kryptoregulierung entbrannt.[256] Eine zukünftige, gesetzliche Regulierung des bislang freien Zugriffs auf kryptographische Verfahren kann somit nicht ausgeschlossen werden.[257]

Befürworter einer staatlichen Kryptoregulierung stützen sich dabei auf das u.a. vom früheren Innenminister Kanther ins Feld geführte Argument, eine Kryptoregulierung wäre erforderlich, um die Arbeit der Strafverfolgungsbehörden zu gewährleisten.[258] Bei genauer Betrachtung scheint dieses Argument kaum haltbar. Es ist unwahrscheinlich, daß gerade Kriminelle eine entsprechende Kryptobeschränkung respektieren und nur legale Verschlüsselungsverfahren einsetzen. Eventuell kriminalisierte kryptographische Verfahren sind aber für jedermann im Internet zugänglich.[259] Kristoferitsch weißt in diesem Zusammenhang auf zwei Möglichkeiten

---

[254] Vgl. Informationweek (1998d)
[255] Vgl. Seeger, H. (1998)
[256] Vgl. Möller (1997) für einen hervorragenden Überblick über die Kryptokontroverse bis 1997 in Deutschland.
[257] Vgl. Kristoferitsch (1998), S.96
[258] Vgl. Möller (1997)
[259] Vgl. bspw. Passport Online (1999) oder vgl. Stealth Encryption (1999) – Internet Suchmaschinen liefern für Begriffe wie 'steganography' oder 'encryption' unzählige Treffer zu Download-Seiten.

hin, wie selbst der Einsatz unerlaubter Verschlüsselungsverfahren verschleiert werden kann:[260]

- ☞ Die Anwendung steganographischer Verfahren, die gänzlich verschleiern, daß eine geheime Nachrichtenübermittlung stattfindet.
- ☞ Eine mittels unerlaubtem Verfahren verschlüsselte Nachricht wird ein zweites Mal mit einem legalen Verfahren verschlüsselt.

Wird eine dieser Möglichkeiten genutzt, haben Strafverfolgungsbehörden kaum eine Chance, Nachrichten mit ungesetzlichem Inhalt aufzuspüren, geschweige denn, zu entschlüsseln. Im ersten Fall entgeht ihnen vollkommen, daß eine Nachricht mit kriminellem Inhalt übermittelt wird, im zweiten Fall müßten sie zuerst die legale Verschlüsselung dechiffrieren, um überhaupt erkennen zu können, daß eine illegale Verschlüsselungstechnik eingesetzt wird. Unter welcher Rechtfertigung diese Dechiffrierung erfolgen soll, wenn der Inhalt der Nachricht unbekannt ist, vermag niemand zu sagen.

Darüber hinaus ist zweifelhaft, ob eine staatliche Kryptoregulierung hinsichtlich der absoluten Zahl von Verbrechen, bei denen Kryptoverfahren benutzt werden, überhaupt zu vertreten ist. Amerikanische Studien gehen von derzeit ca. 500 Fällen im Jahr weltweit aus. In den meisten dieser Fälle war es den Strafverfolgungsbehörden auch ohne staatliche Kryptoregulierung gelungen, die entsprechenden Daten zu entschlüsseln.[261] Ob sich angesichts dieser Fakten eine generelle Beschränkung des Rechts auf private und sichere Kommunikation vertreten läßt, ist mehr als fraglich. Weiterhin ist es fragwürdig, ob eine wie auch immer geartete Kryptoregulierung verfassungskonform zu realisieren ist. Bedenken bestehen hauptsächlich bezüglich der Verträglichkeit mit Art. 10 GG (Brief-, Post- und Fernmeldegeheimnis).[262] Wie auch immer die politische Entscheidung ausfallen wird, vertrauensfördernd ist diese Diskussion nicht. Noch ist das Thema Kryptoregulierung nicht vom Tisch – die restriktive Haltung der USA, die eine Kryptoregulierung nach dem Key-Escrow Verfahren favorisiert, gibt auch den Befürwortern regulativer Maßnahmen hierzulande Auftrieb.[263] In einer aktuellen Vorlage ‚Eckpunkte der deutschen Kryptopolitik' sprechen sich Innen- und Wirtschaftsministerium allerdings gegen eine Regulierung der Kryptographie, einschließlich der Key-Escrow- und Key-Recovery Verfahren, aus. Realistisch

---

[260] Vgl. Kristoferitsch (1998), S.91f
[261] Vgl. Kuhlen (1998b)
[262] Vgl. Hingst (1998) und vgl. GFI (1997); vgl. Kuhlen (1999), S.299 der auf eine Kollision mit weiteren Grundrechten der wirtschaftliche Entfaltungsfreiheit (Art. 12 Abs.1 und Art. 2 Abs.1 GG) und der informationellen Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) hinweist.
[263] Vgl. Hingst (1998)

betrachtet „stellt der Mißbrauch von Verschlüsselung in Deutschland für die Strafverfolgung kein ernsthaftes Problem dar.“[264]

Soweit zum Sinn und Zweck einer Beschränkung kryptographischer Verfahren. Auch eine gesetzlich vorgeschriebene Hinterlegung der privaten Schlüssel beim entsprechenden Trust Center (Key-Escrow Verfahren) oder die Implementation eines ‚Generalschlüssels‘, der im Einzelfall die Dechiffrierung einer Nachricht ohne den privaten Schlüssel erlaubt (Key-Recovery Verfahren), würde sich darauf stützen, daß Kriminelle die Schlüsselgenerierung von einem (staatlich kontrollierten) Trust Center durchführen lassen. Auch das ist eine höchst unrealistische Annahme. Starke Verschlüsselungssoftware, wie das im Internet frei erhältliche PGP,[265] erlauben eine selbständige Generierung der Teilnehmerschlüssel. Die Beschränkung kryptographischer Verfahren oder Schlüsselverwahrung ist nicht nur unter pragmatischen Gesichtspunkten unsinnig, sondern auch kontraproduktiv:

- ☞ Die Vertrauensbildung in digitale Signaturen und Trust Center würde erheblich erschwert, wenn eine gesetzliche Regelung den Einsatz von Key-Escrow oder Key-Recovery Verfahren vorschreibt. In diesem Fall kann sich die institutionelle Vertrauensbildung nicht darauf beschränken, das Vertrauen des Massenpublikums in die korrekte Identitätssicherung und Schlüsselverwaltung zu gewinnen. Vertrauensbildende Maßnahmen müßten darüber hinaus Vertrauen in die gesetzeskonforme Handhabung und sichere Aufbewahrung der privaten Schlüssel durch Staat und Zertifizierungsstellen aufbauen. Diese zusätzliche Aufgabe wird die Vertrauensbildung zwangsläufig erschweren. Kristoferitsch geht noch weiter und stellt fest: „Damit [d.h. mit Key-Escrow oder Key-Recovery Verfahren (Anm. d. Verf.)] wird die Grundidee der Identitätssicherung ad absurdum geführt“,[266] weil die Vertraulichkeit des privaten Schlüssels nicht mehr durch den Schlüsselinhaber alleine zu garantieren ist.

- ☞ Die meisten Internet-Zahlungssysteme sind im Fall einer gesetzlichen Beschränkung auf schwache Kryptoverfahren gar nicht oder nur auf deutlich niedererem Sicherheitsniveau zu realisieren. Dadurch sinkt die Sicherheit und Vertrauenswürdigkeit dieser Zahlungssysteme erheblich.[267]

- ☞ Überwachung und Ausübung der Kryptoregulierung kostet Geld, ohne daß der Nutzen für die Strafverfolgung ersichtlich ist; dazu der frühere Wirtschaftsminister Rexrodt: „Verbote würden wenig bringen, aber viel kosten.“[268]

---

[264] Spiegel (1999b)
[265] Vgl. z.B. PGP (1999) zum Herunterladen der neuesten Version von PGP.
[266] Vgl. Kristoferitsch (1998), S.90
[267] Vgl. Kristoferitsch (1998), S.88
[268] Frankfurter Rundschau (1997)

☞ Experten befürchten, eine Kryptoregulierung werde den Wirtschafts- und Informationsstandort Deutschland im internationalen Vergleich erheblich benachteiligen.[269]

Letztendlich ist die langwierige Diskussion um das Für und Wider einer wie auch immer gearteten Kryptoregulierung nicht geeignet, Vertrauen in die Sicherheit von Internet-Zahlungssystemen aufzubauen. Zum einen weil gerade starke Kryptoverfahren notwendig sind, um eine nach heutigem Stand sichere Authentifizierung, Datenintegrität und Vertraulichkeit zu gewährleisten. Zum anderen, weil Key-Escrow und Key-Recovery Verfahren die Gefahr mit sich bringen, daß Angreifer in den Trust Center eindringen und die privaten Schlüssel in ihren Besitz bringen.

7.3.2 Kontrollinstanzen

Vertrauensbildung bei Internet-Zahlungssystemen ist eine spezifische und gleichzeitig interdependente Aufgabenstellung. Sie ist spezifisch, weil im technischen, organisatorischen und rechtlichen Bereich jeweils besondere, vertrauenskritische Aspekte relevant sind, die die institutionelle Vertrauensbildung berücksichtigen muß. Vertrauensbildung bei Internet-Zahlungssystemen ist interdependent, weil Vertrauen nur dann aufgebaut werden kann, wenn das Zusammenwirken sämtlicher Faktoren letztendlich dazu führt, daß ein Internet-Zahlungssystem vertrauenswürdig ist. So ergibt sich die Notwendigkeit einer sicheren Organisation der Schlüsselverwaltung aus der zugrunde liegenden Technologie der asymmetrischen Kryptographie, die wiederum durch rechtliche Vorgaben beeinflußt wird. Das folgende Gedankenspiel verdeutlicht dies.

Auf der Eurocrypt 99 stellte Adi Shamir am 4. Mai 1999 das opto-elektronische Design seiner Entschlüsselungsmaschine TWINKLE (The Weizman INstitute Key Location Enginge)[270] vor, die „so schnell im Schlüssel knacken wie 1000 PCs in Serie“ [271] sein soll und nach Abschluß der Produktentwicklung nicht mehr als 5000$ kosten dürfte. Die Sicherheit des 512 Bit RSA Algorithmus, so Shamir, sei dadurch ernsthaft bedroht. Wenn es nun möglich wäre, diese Maschinen zu koppeln oder parallel zu schalten, sind dann auch längere Schlüssel in kurzer Zeit zu knacken? Sind gängige Internet-Zahlungssysteme, die derzeit mit höchstens 1024 Bit verschlüsseln, dann mit einer verhältnismäßig geringen Investition serienweise zu knacken? Welche Auswirkungen wird dieser Sachverhalt auf die Beweiswürdigung der bei Internet-Zahlungssystemen eingesetzten digitalen Signaturen in Zivilprozessen haben? Müssen neue gesetzlichen Anforderungen an die Schlüsselerzeugung und Administration der Trust Center erlassen werden?

---

[269] Vgl. Möller (1997) oder vgl. Kuhlen (1999), S.300f
[270] Vgl. Shamir (1999) und vgl. c't (1999), S.21
[271] Vgl. ORF (1999)

Um solche oder ähnliche Fragen zu beantworten, sind Kontrollinstanzen notwendig, die zum einen durch ihre Kontrollfunktion die Qualität der institutionellen Vertrauensbildung verbessern und zum anderen die bereichsübergreifenden Folgen dieser Entwicklungen bündeln und kontextualisieren. Dadurch sind sie nicht nur in der Lage, sehr spezielle Aussagen zur Sicherheit von Kryptoverfahren, zur Vertrauenswürdigkeit von Zertifizierungsstellen oder zu rechtlichen Fragestellungen zu geben, sondern können dem Massenpublikum die Vertrauenswürdigkeit eines Internet-Zahlungssystems als Kombination technischer, organisatorischer und rechtlicher Elemente zu vermitteln. Manche Kontrollinstanzen werden nur einen spezifischen Teilbereich der Vertrauensbildung abdecken können, andere werden im eigenen Interesse eine umfassende Vertrauensarbeit leisten müssen, die sich nicht auf technische, organisatorische oder rechtliche Details, sondern auf das Zahlungssystem als Ganzes konzentriert.

7.3.2.1 Partikularinteressen und Neutralität

Vertrauensnetzwerke legen die Basis für die Bündelung und Objektivierung von Wissen. Per se erbringt ein Vertrauensnetzwerk jedoch keine Vertrauensarbeit. Vertrauensbildung bei Internet-Zahlungssystemen – dies war eine Annahme zu Beginn der Arbeit – muß institutionell vermittelt werden. Wenn Vertrauensnetzwerke auch helfen, Kompetenz zu bündeln und zu objektivieren, Vertrauen können sie deshalb nicht vermitteln, weil ein Vertrauensnetzwerk ein abstraktes Gebilde ist, das nicht über die zur Vertrauensbildung notwendigen personalen und institutionellen Kontaktpunkte verfügt. Diese Zugangspunkte stellen institutionelle Mittler bereit. Sie werden an den Zugangspunkten aktiv und vermitteln die vertrauensbildenden Aussagen, die sich innerhalb des Vertrauensnetzwerks formieren.

Grundsätzlich kommen als institutionelle Kontrollinstanzen staatliche, kommerzielle und gemeinnützige Institutionen in Frage. Vertrauensarbeit, so Kuhlen, sollte „interessenneutral und unter Vermeidung von Einseitigkeit geleistet werden.“[272] Die Frage ist nun, inwiefern gerade kommerzielle Einrichtungen einen Spagat zwischen ihrer kommerziell fundierten Kompetenz und der notwendigen Neutralität machen können. Und wenn es nicht die kommerziellen Akteure sind, kann dem Staat im Hinblick auf eine mögliche Kryptoregulierung die notwendige Vertrauenswürdigkeit unterstellt werden? Bezüglich der juristischen Realisierung einer staatlichen Kryptoregulierung wäre es durchaus denkbar, daß dem Bundesverfassungsgericht, das letztendlich über die Verfassungskonformität einer Krpytoregulierung zu entscheiden hätte, eine wichtige Rolle als vertrauensbildende Kontrollinstanz zufällt.

Wenn Staat und Wirtschaft nicht als vertrauenswürdige Partner betrachtet werden, bleiben nur nicht-kommerzielle, nicht-staatliche Akteure. Forschungsinstitute, wissenschaftliche und gemeinnützige Vereinigungen oder Fachkongresse können

---

[272] Kuhlen (1999), S.314

genauso in der institutionellen Vertrauensbildung aktiv werden. Aber auch hier darf nicht übersehen werden, daß diese Akteure häufig aus staatlichen und kommerziellen Quellen durch Spenden oder Fördermittel finanziert werden. Ob aus dieser Perspektive generell Neutralität unterstellt werden kann, ist im Einzelfall vielleicht weniger zweifelhaft, als bei staatlichen oder kommerziellen Akteuren selbst, letzte Verdachtsmomente lassen sich jedoch häufig nicht ausräumen.

7.3.2.2 Pragmatische Überlegungen

Die Frage, wer die notwendige Vertrauensarbeit im Bereich der Internet-Zahlungssysteme leisten soll, muß auch von einer ganz pragmatischen Seite betrachtet werden. Dann stellt sich die Frage, wer die Aufgabe überhaupt wahrnehmen kann. Vertrauensnetzwerke selbst können es wie gesagt nicht, sie schaffen lediglich die Rahmenbedingungen. Wahrscheinlich sind es in diesem Fall doch wieder staatliche oder kommerzielle Akteure, die als Kontrollinstanzen auftreten und auf dieser Basis Vertrauensarbeit leisten! Schon häufiger wurde in dieser Arbeit auf den Vertrauensbonus hingewiesen, den gerade Banken und Kreditinstitute im Bereich finanzieller Transaktionen genießen.[273] International tätige Banken und Kreditinstitute sind vielleicht besser als die meisten anderen Akteure dazu in der Lage, über multiple personale Zugangspunkte – d.h. durch die Mitarbeiter in den weltweiten Filialen und Niederlassungen – vertrauensbildende Maßnahmen erfolgreich und mit der notwendigen internationalen Tragweite zu plazieren. Schuster, Färber und Eberl weisen ihnen sogar explizit die umfassende Aufgabe zu, „das Vertrauen der Öffentlichkeit in das Zahlungsmittel zu gewährleisten."[274] Exemplarisch sei hier die Deutsche Bank („eCommerce is our trade"[275]), nach der Fusion mit Bankers Trust das größte Kreditinstitut der Welt, genannt. In den größeren Filialen der Deutschen Bank finden sich designierte ‚Electronic-Service Berater', die fundierte Kenntnisse im Bereich der Internet-Zahlungssysteme verfügen und somit als personale Kontaktpunkte der Vertrauensbildung fungieren können.[276] Darüber hinaus steht eine Hotline zur Verfügung, deren Mitarbeiter jedoch nach eigenen Angaben nur über das Know-how verfügen, das in den Filialen in Form des oben genannten Informationsmaterials bereits verfügbar ist.[277] Diese Hotline stellt quasi einen ‚First Level Support' dar, der aus den Anfragen diejenigen ausfiltert, die sofort beantwortet werden können. Die übrigen Problemstellungen werden an Experten im

---

[273] Vgl. Grossman (1997), S.185, vgl. Kuhlen (1999), S.304, vgl. Gavin (1997), S.20
[274] Schuster/Färber/Eberl (1997), S.29
[275] Vgl. Deutsche Bank (1999b)
[276] Z.B. am 12.08.1999, Deutsche Bank Filiale Konstanz, Bahnhofsstr. 1, 78462 Konstanz und am 09.08.1999, Deutsche Bank Filiale Mannheim, Hausanschrift P 7, 10-15, 68161 Mannheim.
[277] Vgl. Tel. 069/01805 / 22 42 00, Telefoninterview vom 09.08.1999 mit einem Mitarbeiter der (First Level Support) eCash-Hotline der Deutschen Bank.

‚Second Level Support' weitergeleitet und von diesen umgehend per eMail oder Telefonanruf beantwortet.[278]

Im Gegensatz zur Deutschen Telekom scheint sich die Deutsche Bank bewußt zu sein, daß die Akzeptanz von Internet-Zahlungssystemen maßgeblich vom Vertrauen des Massenpublikums abhängt, „denn zur Marktdurchdringung und Akzeptanz solch fortschrittlicher Zahlungsmittel wie eCash oder auch Kreditkartenzahlungen im Internet nach SET-Standard ist das Thema Vertrauen in der Tat sehr entscheidend für deren Erfolg."[279] ‚Electronic-Service-Berater' in den größeren Filialen in Kombination mit Informationsbereitstellung und Remote-Support Leistungen zeugen zumindest von der verhaltenen Umsetzung dieser Erkenntnis. Da die Deutsche Bank den Einsatz von eCash derzeit (noch) als ‚Pilotversuch' betrachtet, werden – so Nicole Schütz von der Gesellschaft für Finanzmarketing mbH, die den ‚Second Level Support' für die Deutsche Bank wahrnimmt – keine weiteren, vertrauensbildenden Maßnahmen ergriffen. Zumindest solange sich die Akzeptanz von Internet-Zahlungssystemen nicht auf breiter Ebene zeigt.[280] Doch warum soll das Massenpublikum Internet-Zahlungssysteme akzeptieren, wenn es ihnen nicht das nötige Vertrauen, das nach eigener Aussage der Deutschen Bank bzw. der Gesellschaft für Finanzmarketing mbH entscheidend für Akzeptanz und Erfolg dieser Zahlungsform ist, entgegenbringt? Die Deutsche Bank scheut angesichts der noch geringen Verbreitung der Internet-Zahlungssysteme vor größeren Start-Up Investitionen zurück und geht eher davon aus, daß durch den Bedeutungszuwachs des eCommerce eine ausreichend große Nachfrage nach Internet-Zahlungssystemen auch ohne weitere vertrauensbildende Maßnahmen erzeugt wird.[281] Die Aussage, daß „Filialmitarbeiter der Deutschen Bank in erster Linie Banker und nicht vordringlich Techniker (...) sind",[282] ist zwar richtig, aber angesichts der Relevanz der Vertrauensbildung zu kurzsichtig.

Insgesamt lassen sich aus diesen Fakten Parallelen zur Haltung der Deutschen Telekom erkennen. Zum einen scheint der ökonomische Nutzen vertrauensbildender Maßnahmen von der Deutschen Bank zwar erkannt worden zu sein. Allerdings gehen beide Unternehmen davon aus, daß sich eine Ausweitung dieser Aktivitäten derzeit nicht rechnet. Zum anderen erwarten beide Unternehmen, daß sich die Akzeptanz von Internet-Zahlungssystemen bzw. digitalen Signaturen auch ohne größere vertrauensbildende Anstrengungen einstellen wird. Hierin zeigt sich der Widerspruch zwischen Erkenntnis und Umsetzung deutlich: Wo liegt die Bedeutung der institutionellen Vertrauensbildung, wenn sich der Erfolg auch ohne diese

---

[278] Diese Beratungsleistungen wurden von der Deutschen Bank 'outgesourct' (!); vgl. eMail der Gesellschaft für Finanzmarketing mbH ‚nicole.schuetz@gefm.com', 13.08.1999.
[279] eMail der Gesellschaft für Finanzmarketing mbH ‚nicole.schuetz@gefm.com', 13.08.1999
[280] Tel. 069/910-64545, Telefoninterview vom 19.08.1999
[281] Vgl. Tel. 069/910-64545, Telefoninterview vom 19.08.1999
[282] eMail der Gesellschaft für Finanzmarketing mbH ‚nicole.schuetz@gefm.com', 13.08.1999

einstellen wird? Offensichtlich wird in beiden Fällen von einer starken Eigeninitiative bzw. einem großen Vertrauensvorschuß der Anwender ausgegangen.

Wie Banken, Kreditinstitute und andere kundennahe Unternehmen könnten auch staatliche Einrichtungen, Ämter und Behörden ihre lokale und personale Präsenz erfolgreich ins Spiel bringen. Gerade staatliche Einrichtungen, wie etwa Landrats- oder Rechts- und Ordnungsämter, die bereits im Bereich der Identitätssicherung aktiv und akzeptiert sind, können ihre Tätigkeit auf das elektronische Terrain ausweiten. Genauso können Notare und Anwälte die personale Ergänzung der institutionellen Vertrauensbildung sein und neben ihrer lokalen Nähe auf tradierte Vertrauensbeziehungen aus ihrer bisherigen Tätigkeit zurückgreifen, die dem Vertrauensbonus der Banken und Kreditinstitute sehr nahe kommen.

Akteure aus dem Non-Profit Bereich, z.B. wissenschaftliche Expertenvereinigungen, Verbraucherschutzverbände und Forschungseinrichtungen oder gemeinnützige Vereine wie der Chaos Computer Club, dessen Arbeit bereits zur Aufdeckung von Sicherheitslücken bei EC- und Telefonkartensystemen beigetragen hat, werden wahrscheinlich ein höheres ‚Neutralitäts-Rating' erhalten, als kommerzielle oder staatliche Einrichtungen. Daß eine Koordination staatlicher, kommerzieller und nicht-kommerzieller Aktivitäten ein vielversprechender Ansatz sein kann, zeigt sich an der Initiative des EuroHandelsinstitut e.V. (EHI).[283] Das EHI – eine Interessenvereinigung des Handels – entwickelt auf Druck von Verbraucherschutzverbänden z.Zt. „ein Zertifikat für Online-Shops, das das Vertrauen der Kunden im Internet genießt."[284] Wie weitere, hier dargestellte Akteure der institutionellen Vertrauensbildung, setzt das EHI explizit auf Transparenz: „Dabei basiert Vertrauen auf Transparenz. Dem Kunden soll Transparenz hinsichtlich der Anbieterkennzeichnung, der Preisstellung, der Lieferzeiten, der Zahlung, des Datenschutzes und –sicherheit sowie der Allgemeinen Geschäftsbedingungen des Shops gewährt werden."[285] Online Shops, die dieses Logo tragen, verpflichten sich unter anderem zur Verwendung sicherer Zahlungssysteme, sowie zur transparenten Darstellung der Preisangaben, der Lieferfristen und der Verwendung der Kundendaten. Große Handelsunternehmen wie Kaufhof und Karstadt, Verbände des Einzelhandels, die Hard- und Softwarehersteller Compaq und Oracle sind bereits beteiligt. Der für die Zertifizierung zuständige „Beirat wird sich aus Vertretern des Handels, der Verbraucherverbände, Bundes- und Länderbehörden und aus bekannten Unternehmen der IT-Industrie mit einschlägigen Kompetenzbereichen zusammensetzen."[286] In dieser Form der Interessenrepräsentation drückt sich ein weiteres Potential der institutionellen Vertrauensbildung aus. Durch die Integration verschiedener Interessengruppen und

---

[283] Vgl. EHI (1999)
[284] Jansen (1999)
[285] EHI (1999)
[286] Jansen (1999)

Fachkompetenzen wird, analog zur Idee des Vertrauensnetzwerks, Neutralität, Kompetenz und Kontrolle innerhalb der Institution gefördert. Auch solche Institutionen müssen Zugangspunkte bereitstellen, an denen eben nicht nur ihre Neutralität und Kompetenz, sondern in ebenso großem Maße ihre Vermittlungsleistung gefragt ist. Das EHI will das Vertrauen des Massenpublikums „durch Online- und Print-Publikationen, mit Unterstützung der entsprechenden wirtschaftlichen und politischen Institutionen“ gewinnen. Damit ist das EHI auf die Vermittlungsleistung kommerzieller und / oder staatlicher Akteure angewiesen, die diese Leistungen aus kommerziellem bzw. öffentlichem Interesse flächendeckend erbringen können und wollen - genauso, wie kommerzielle und staatliche Akteure sich die Leistungen von Non-Profit Institutionen, denen meist eine größere Interessenfreiheit zugestanden wird, zunutze machen.

8 Zusammenfassung und Ausblick

Vertrauen in die Sicherheit von Internet-Zahlungssystemen ist grundlegend für die Akzeptanz durch das Massenpublikum. Weil Internet-Zahlungssysteme und das ihnen zugrunde liegende Wissen abstrakt und komplex sind, wird das Massenpublikum kaum in der Lage sein, aufgrund eigenen Wissens oder eigener Erfahrungen Urteile über deren Sicherheit zu bilden. Daraus resultieren erhebliche Unsicherheiten im Umgang mit Internet-Zahlungssystemen. Fehlt das eigene Wissen, kann Vertrauen diese Unsicherheiten kompensieren. Dann ist das Massenpublikum auf Institutionen angewiesen, die ihm die Vertrauenswürdigkeit der Internet-Zahlungssysteme vermitteln. Die Vertrauenswürdigkeit von Internet-Zahlungssystemen ist dabei keine absolute Gegebenheit, die sich allein mit technischen Maßgrößen, etwa der Stärke der eingesetzten kryptographischen Verfahren, beurteilen läßt. Internet-Zahlungssysteme beinhalten darüber hinaus organisatorische und rechtliche Aspekte, mit jeweils eigenen, sehr speziellen Fragestellungen und Unsicherheiten, die in ihren Auswirkungen aufeinander von Experten nur schwer und vom Massenpublikum gar nicht abzuschätzen sind. Dementsprechend müssen vertrauensbildende Institutionen in genau diesen Bereichen bestrebt sein, die Vertrauenswürdigkeit bestimmter Verfahren, Leistungen oder rechtlicher Regelungen mit dem Massenpublikum und anderen Organisationen zu kommunizieren. Ebenso werden Institutionen aktiv, die aus kommerziellem oder öffentlichem Interesse heraus Vertrauen in die Internet-Zahlungssysteme als Zusammenspiel technischer, organisatorischer und rechtlicher Mechanismen vermitteln müssen. Besonders Banken und Kreditinstituten, aber auch staatlichen Einrichtungen wie dem BSI und der RegTP oder nicht-kommerziellen Institutionen, wie Verbraucherschutzverbänden, wird hier eine entscheidende Rolle zukommen.

Damit wird Vertrauensarbeit auf verschiedenen Wegen von verschiedenen Institutionen erbracht. Eine singuläre, institutionelle Lösung für die Vertrauensbildung bei Internet-Zahlungssystemen wird es somit nicht geben. Dieser Einsicht entspricht das Konzept des Vertrauensnetzwerks, in dem die verschiedensten Institutionen aktiv werden, sich gegenseitig ergänzen, kontrollieren und an den Kontaktstellen zum Massenpublikum vertrauensbildende Maßnahmen kommunizieren. Weil gerade im technischen und rechtlichen Bereich und demzufolge auch hisichtlich der organisatorischen Umsetzung der Authentifikation und des Key-Managements, weitere Veränderungen anstehen, wird diese Arbeit kontinuierlich und konsequent erbracht werden müssen.

Derzeit – so scheint es zumindest – ist Vertrauen noch eine ‚Holschuld' der Anwender. Eine aktive institutionelle Vertrauensbildung, wie die bereits angesprochenen Maßnahmen von Daimler-Benz anläßlich der Vertrauenskrise nach dem ‚Elch-Test', ist im Bereich der Internet-Zahlungssysteme bisher nicht zu

beobachten – vielleicht deshalb, weil es im Bereich dieser Zahlungssysteme noch zu keiner ernsthaften Vertrauenskrise gekommen ist. Neben Eigeninitiative ist ein hohes Maß an informationeller Kompetenz notwendig, um überhaupt die vertrauenswürdigen, nach Möglichkeit gleichermaßen kompetenten und neutralen Institutionen zu kontaktieren und sich die Vertrauen schaffenden Maßnahmen zu erschließen. Anhand der Beispiele wurde ersichtlich, daß die institutionelle Vertrauensbildung heute hauptsächlich auf informationelle Transparenz setzt. Ergänzend sind aber sicherlich personale Maßnahmen der Vertrauensvermittlung notwendig. Gerade in diesem Bereich werden Institutionen, die über eine vorhandene Personalinfrastruktur verfügen, z.B. Finanzinstitute, Telekommunikationsunternehmen, Behörden und öffentliche Anstalten, einen gewichtigen Teil der Vertrauensarbeit leisten können. Für diese Institutionen wird es demnach immens wichtig sein, fachliche Kompetenz und Vertrauenswürdigkeit durch Mitarbeiter oder Repräsentanten vermitteln zu können. Die bereits dargestellte Position der Telekom und der Deutschen Bank, die davon ausgehen, daß sich weitere vertrauensbildende Maßnahmen noch nicht rechnen, ist einer erfolgreichen Vertrauensbildung wenig dienlich, wenn nicht sogar abträglich. Mitarbeiter dieser Institutionen, die am personalen Zugangspunkt nicht das erforderliche Know-how vermitteln können, erwecken eventuell den Anschein, daß die Bank als Institution selbst über keine ausreichende Kompetenz im Bereich der Internet-Zahlungssysteme verfügt. Vielleicht müssen sich Banken, Kreditinstitute und Telekommunikationsunternehmen, denen schon seit jeher ein sehr konservatives Image anhaftet, erst damit anfreunden, daß zum einen die Vertrauensfrage im Internet eine vollkommen andere Dimension annimmt, als bei konventionellen Transaktionen. Zum anderen müssen diese Institutionen erkennen, daß im neuen Bereich der Vertrauensbildung bei Internet-Zahlungssystemen erst einmal Start-Up Kosten entstehen, die nicht schon zu Beginn durch Einsparungen in der Transaktionsabwicklung oder durch zusätzliche Einnahmen gedeckt werden. Die notwendige Break-Even Menge von tatsächlichen Anwendern, ab der sich vertrauensbildende Maßnahmen auch unter kalkulatorischen Gesichtspunkten auszahlen, kann jedenfalls nur dann erreicht werden, wenn Internet-Zahlungssysteme vom Massenpublikum als sichere und damit vertrauenswürdige Zahlungsform akzeptiert werden. Um dies zu erreichen, werden diese Institutionen kaum umhin kommen, ihre vertrauensbildenden Maßnahmen auszuweiten und durch qualifizierte Mitarbeiter auf personaler Ebene zu kommunizieren.

Doch nicht nur aus diesem Grunde wird die physische Infrastruktur dieser Institutionen eine bedeutsame Rolle spielen. Finanzielle Transaktionen sind besonders sensible Vorgänge. Komplexe (Internet-Zahlungs-) Systeme - so wurde mit Bezug auf Anthony Giddens erläutert – führen zu einer ‚Entbettung' aus dem lokalen und zeitlichen Kontext. Dieser ‚Entbettung' können Institutionen mit einer umfassenden Infrastruktur durch physikalische Präsenz gegensteuern und

sozusagen einen lokalen Bezugspunkt bieten, der sensible Finanztransaktionen vielleicht erst als vertrauenswürdig vermittelbar macht. Großmann sieht diese physikalische Präsenz eher als Notwendigkeit, denn als Chance: „Would you buy digital cash for more than a trivial amount of real money from a company whose physical address you didn't know?"[287] Durch ihre Reputation als neutraler Broker im Bereich finanzieller Transaktionen ist es sehr wahrscheinlich, daß Banken auch im Bereich der Internet-Zahlungssysteme als vertrauenswürdige und gleichzeitig kompetente Partner angesehen werden. Wahrscheinlich wird ihnen solange ein hohes Maß an Vertrauen entgegengebracht, wie dieses Vertrauen nicht enttäuscht wird. Vorteile für große Organisationen, zu denen die meisten Finanzinstitute zählen, sind sicherlich auch in ihren finanziellen Ressourcen und in ihrem Bekanntheitsgrad zu sehen – „This [trustworthiness (Anm. d. Verf.)] is an area where familiar names have a big advantage."[288]

Auch deshalb ist zu erwarten, daß Finanzinstitute im Bereich der Zertifizierungsleistungen aktiv werden, soweit sie es nicht schon sind. Sie verfügen über die finanziellen und personellen Ressourcen, die erforderlich sind,[289] um die Sicherheitsanforderungen des Signaturgesetzes (bzw. der Maßnahmenkataloge) umzusetzen. Darüber hinaus, so Grosman, werden Key-Management Institutionen ähnliche Macht und ähnliche Verantwortung haben, wie derzeit Banken und Kreditinstitute.[290]

Um das Problem fehlender, international gültiger, gesetzlicher Rahmenbedingungen zu umgehen, bereitet ein Konsortium von acht Banken,[291] darunter auch die Deutsche Bank, den Aufbau einer kommerziellen, weltweiten Zertifizierungslösung in Form des ‚Global Trust Enterprise' vor. Dieses Unternehmen soll digitale Zertifikate mit weltweiter Gültigkeit unabhängig von nationalen oder regionalen Rechtsvorschriften ausgeben.[292]

Am Erfolg dieses Unterfangens wird sich vielleicht am deutlichsten zeigen, inwieweit das Massenpublikum dem Engagement kommerzieller Akteure in der institutionellen Vertrauensbildung bei Internet-Zahlungssystemen Vertrauen schenkt. Es wird sich darüber hinaus zeigen, ob diese Akteure ihre Vertrauensstellung gewissenhaft ausfüllen oder aus wirtschaftlichen Interessen dort Vertrauen reklamieren, wo es eigentlich gar nicht angebracht ist. Hierin liegt sicherlich das größte Risiko der institutionellen Vertrauensbildung und die größte Herausforderung für die Kontrollfunktion des Vertrauensnetzwerks.

---

[287] Grossman (1997), S.183
[288] Grossman (1997), S.183
[289] Vgl. Informationweek (1998d) und vgl. Seeger, H. (1998)
[290] Vgl. Grossman (1997), S.185
[291] Deutsche Bank, Hypo Vereinsbank, ABN Amro, Bank of Amerika, Bankers Trust, Barclays Bank, Chase Manhattan Bank, Citibank.
[292] Vgl. Informationweek (1998a)

Weil es letztendlich der Anwender ist, der darüber zu entscheiden hat, wem er im Bereich der Internet-Zahlungssysteme Vertrauen schenkt, kann ein ausreichendes Maß an informationeller Kompetenz, oder noch besser, an Hintergrundwissen über die Chancen und Risiken im Umgang mit Internet-Zahlungssystemen nicht schaden.

Denn was für den gewöhnlichen Wochenmarkt gilt, ist mit bestimmten Einschränkungen auch auf den globalen elektronischen Marktplatz zu übertragen: Nicht unbedingt die, die das beste Angebot unterbreiten, machen das Rennen - häufig sind es einfach diejenigen, die am lautesten schreien...

Abbildungsverzeichnis

Literaturverzeichnis

Agre/Rotenberg (1997): P.E. Agre, M. Rotenberg: Technology and Privacy – The New Landscape; MIT Press; Cambridge (MA) 1997

Ascom (1999): Ascom Information Security: Welcome to ASCOM Information Security. http://www.ascom.ch/infosec (verifiziert 30.08.1999)

Beck (1986): U. Beck: Risikogesellschaft: Auf dem Weg in eine andere Moderne. Suhrkamp Verlag. Frankfurt 1986

Beck/Giddens/Lash (1996): U. Beck, A. Giddens, S. Lash: Reflexive Modernisierung: Eine Kontroverse. Suhrkamp Verlag. Frankfurt 1996

Belotti (1997): V. Belotti: Design for Privacy in Multimedia Computing and Communications Enviroments. In: Agre/Rotenberg (1997), S.63 – 98

Beutelspacher (1991): A. Beutelspacher: Kryptologie (2. Aufl.). Verlag Vieweg. Braunschweig 1991

Böhle/Riehm (1998): K. Böhle, U. Riehm: Wissenschaftliche Berichte FZKA 6161. Forschungszentrum Karlsruhe GmbH, Technik und Umwelt. Karlsruhe 1998. Oder: http://www.itas.fzk.de/deu/ITASLIT/bori98a.pdf (verifiziert 30.08.1999)

Brisch (1999): K. Brisch: Rechtssicherheit im Internet. http://www.sicherheit-im-internet.de/cgi-bin/showdoc.pl?doc=sii1999020405.html (verifiziert 05.09.1999)

Brockhaus (1997): Bibliographisches Institut F.A. Brockhaus AG (Hrsg.): Fremdwörter-Duden auf CD-ROM.1997

BSI (1999a): Bundesamt für Sicherheit in der Informationstechnik: BSI Projektbüro ‚Digitale Signatur' – Dienstleistungen. http://www.bsi.de/aufgaben/projekte/pbdigsig/main/dienstl.htm (verifiziert 19.08.1999)

BSI (1999b): Bundesamt für Sicherheit in der Informationstechnik: BSI Projektbüro ‚Digitale Signatur' – Ziele. http://www.bsi.de/aufgaben/projekte/pbdigsig/main/ziele.htm (verifiziert 19.08.1999)

BSI (1999c): Bundesamt für Sicherheit in der Informationstechnik: Projektbüro Digitale Signatur. http://www.bsi.de/aufgaben/projekte/pbdigsig/index.htm (verifiziert 19.08.1999)

Business Week (1998): Business Week: A Little Net Privacy Please. Businessweek, 16.03.1998. Oder: http://www.businessweek.com/@@4WZJy4cASJ*2SwAA/1998/11/b3569104.htm (verifiziert 19.08.1999)

Bussiek (1998): T. Bussiek: Diffusion of Payment System Technology - Old and New Factors of Influence. http://www.iig.uni-freiburg.de/~bussiek/dynmod_e.html (verifiziert 19.08.1999)

C't (1999): c't – Magazin für Computertechnik: Aktuell – Datenschutz und –sicherheit, 11/1999, S.20f

CCC (1984): Chaos Computer Club: Die Datenschleuder Nr. 2, 1984. Falsche Namen, echte Ausweise. http://www.ccc.de/Archive/ds02/jackpot.d02.html (verifiziert 19.08.1999)

CyberCash (1999): CyberCash, Inc: Home. http://www.cybercash.com/ (verifiziert 22.09.1999)

Cypherpunks (1999): Cypherpunks: Cypherpunks ‚brute' key cracking ring. http://www.brute.cl.cam.ac.uk/brute/ (verifiziert 19.08.1999)

Deutsche Bank (1999a): Deutsche Bank: eCommerce mit der Deutschen Bank. http://public.deutsche-bank.de/deuba/ui/ec/ecommerce.nsf/doc/ITEZ-45Z6PQ/$file/ec_start4.htm (verifiziert 28.08.1999)

Deutsche Bank (1999b): Deutsche Bank: Deutsche Bank – Die Bank für Europa. http://public.deutsche-bank.de/index.htm (verifiziert 28.08.1999)

Deutsche Telekom (1998): Deutsche Telekom: Informationen zur Teilnahme am Publik Key Service. Deutsche Telekom. PKS_SigG_9/98V1

Deutsche Telekom (1999a): Deutsche Telekom – TELESEC: Ernst B. Droht in Gefahr. http://www.telekom.de/angebot/telesec/inter/index.htm (verifiziert 22.08.1999)

Deutsche Telekom (1999b): Deutsche Telekom – TELESEC: Referenzen. http://www.telekom.de/angebot/telesec/ref/index.htm (verifiziert 22.08.1999)

Deutsche Telekom (1999c): Deutsche Telekom – TELESEC: Vertrauliche Kommunikation. http://www.telekom.de/angebot/telesec/vertrau/index.htm (verifiziert 22.08.1999)

Deutsche Telekom (1999d): Deutsche Telekom: Telekom Zertifikate. http://www.telekom.de/zertifikate/index.htm (verifiziert 24.08.1999)

Deutsche Telekom (1999e): Telekom Zertifikate – Einführung Zertifikate - Trust Center. http://www.telekom.de/zertifikate/html/einf_zert/trust_center/index.htm (verifiziert 24.08.1999)

DMMV (1998): Deutscher Multimedia Verband: Pressemitteilung. ‚Electronic Commerce' - eine Bestandsaufnahme zur aktuellen Situation in Deutschland. http://www.dmmv.de/presse/ec05-98.htm (verifiziert 22.08.1999)

DMMV (1999): Deutscher Multimedia Verband: Überblick. Marktzahlen. http://www.dmmv.de/multi/index.html (verifiziert 22.08.1999)

Digicash (1999a): Digicash: Current eCash™ Issuers. http://www.ecashtechnologies.com/ecash/issuers/index.html (verifiziert 29.08.1999)

Digicash (1999b): Digicash: eCash™ Demonstration. http://www.ecashtechnologies.com/ecash/demo/index.html (verifiziert 29.08.1999)

Distributed.net (1999): Distributed.net: Node Zero. http://www.distributed.net/index.html.de (verifiziert 22.08.1999)

EHI (1999): EuroHandelsinstitut e.V.: EHI. AboutUs. Ziel des Vertrauenslogo. http://www.ehi.org/logo/ziele.htm (verifiziert 24.08.1999)

Fauhnan (1998): J. Fauhnan: International Credit Card/Check Card Fraud with Small Charges. http://www.labmed.umn.edu/~john/ccfraud.html (verifiziert 22.08.1999)

Feisthammel (1999): P. Feisthammel: Das Web of Trust (Vertrauensnetz). http://www.rubin.ch/pgp/weboftrust.de.html (verifiziert 09.09.1999)

Focus (1999): Focus: Internet-Buchhandel. Focus 25/1999, S. 124f

Frankfurter Rundschau (1997): Frankfurter Rundschau: Vertrauen ist der Schlüssel zum Geschäft im Netz. Nr. 61/11, 13.3.97, S.13. Oder: http://www.iks-jena.de/mitarb/lutz/security/cryptoban/rexrodt. cebit.fr.html (verifiziert 22.08.1999)

Galvin (1997): J. Galvin: Building Trust from the Ground up. In: The World Wide Web Journal: Web Security – A Matter of Trust. Volume 2, Issue 3, Summer 1997. O'Reilly & Associates. Sebastopol (CA) 1997, S.15 – 21

Gambetta (1988): D. Gambetta: Trust: Making and breaking cooperative relations. Blackwell. New York (NY) 1988

Garfinkel/Spafford (1997): S. Garfinkel, G. Spafford:Cryptography and the Web. In: The World Wide Web Journal: Web Security – A Matter of Trust. Volume 2, Issue 3, Summer 1997. O'Reilly & Associates. Sebastopol (CA) 1997, S.113 – 126

Garwin (1988): D.A. Garwin: Managing Quality, Harvard Business School, New York (NY) 1988

GDS (1999): GRETACODER Data Systems AG): Encryption, Authentication, Transaction Security. http://www.gds.ch/ (verifiziert 22.08.1999)

GfI (1997): Gesellschaft für Informatik: Gesellschaft für Informatik zur Krypto-Debatte. http://www.david-datenschutz.de/gizucrypto.html (verifiziert 22.08.1999)

Giddens (1990): A. Giddens: The Consequences of Modernity. Stanford University Press. Stanford (MA) 1990

GOST (1999): Global Operating Systems Technology Group – GOST: The USC NetCash anonymous network payment research prototype. http://gost.isi.edu/info/netcash/ (verifiziert 24.08.1999)

Good (1988): D. Good: Individuals, Impersonal Relations, Trust. In: Gambetta (1988), S. 31-48

Grossmann (1997): W.M. Grossmann: net.wars. New York University Press, New York (NY) 1997

Hillebrand/Büllingen (1998): A. Hillebrand, F. Büllingen: Durch Sicherungsinfrastruktur zur Vertrauenskultur: Kritische Erfolgsfaktoren und regulatorische Aspekte der digitalen Signatur – Diskussionsbeitrag 1888. Wissenschaftliches Institut für Kommunikationsdienste. Bad Honnef 1998

Hingst (1998): W.-C. Hingst: Die deutsche Krypto-Kontroverse. http://www.heise.de/tp/deutsch/inhalt/te/1416/1.html (verifiziert 22.08.1999)

Hoeren (1998): T. Hoeren: Internet und Recht – neue Paradigmen des Informationsrechts. In: Neue Juristische Wochenschrift Nr.51, 1998, S.2849 – 2854

Individual Network (1997): Individual Network e.V.: Certification Policy. http://www.in-ca.individual.net/policy.html (verifiziert 09.09.1999)

Informationweek (1998a): Informationweek: Channel E-Commerce: Banken übertrumpfen Staat beim Web-Handel http://www.informationweek.de/channels/channel6/982206b.htm (verifiziert 19.08.1999)

Informationweek (1998b): Informationweek: Channel E-Commerce: E-Commerce erhöht Preisdruck massiv http://www.informationweek.de/channels/channel6/981029.htm (verifiziert 19.08.1999)

Informationweek (1998c): Informationweek: Channel E-Commerce: EU will die digitale Signatur regeln http://www.informationweek.de/channels/channel6/980811a.htm (verifiziert 19.08.1999)

Informationweek (1998d): Informationweek: Das Signaturgesetz kommt zu teuer. http://www.informationweek.de/topthemen/982108b.htm (verifiziert 19.08.1999)

Inf-Wiss (1998): Lehrstuhl Informationswissenschaft, Universität Konstanz: Zahlungssysteme im WWW. http://www.inf-wiss.uni-konstanz.de/CURR/summer98/imk/Internet-Zahlungssysteme/zahlungssysteme.html (verifiziert 24.08.1999)

Jansen (1999): H. Jansen: EuroHandelsinstitut e.V. Zertifikate für Online Shops. http://www.ehi.org/aktuell/30/199905/05_002.html (verifiziert 24.08.1999)

Kahre/Rifkin (1997): R. Kahre, A. Rifkin: Weaving a Web of Trust. In: The World Wide Web Journal: Web Security – A Matter of Trust. Volume 2, Issue 3, Summer 1997. O'Reilly & Associates. Sebastopol (CA) 1997, S.77 – 112

Keupp/Röhrle (1987): H. Keupp, B. Roehrle (Hrsg.): Soziale Netzwerke. Campus: Frankfurt/M. 1987.

Kristoferitsch (1998): G. Kristoferitsch: Digital Money – electronic cash – smart cards: Chancen und Risiken des Zahlungsverkehrs via Internet. Wirtschaftsverlag Ueberreuter. Wien 1998

Kuhlen (1996a): R. Kuhlen: Informationsmarkt: Chancen und Risiken der Kommerzialisierung von Wissen. 2. Auflage. Universitätsverlag Konstanz (UVK), Konstanz 1996

Kuhlen (1996b): R. Kuhlen: Zur Virtualisierung von Regionen durch elektronische Marktplätze (Bericht 79-96). Universität Konstanz – Informationswissenschaft. Konstanz 1996

Kuhlen (1998a): R. Kuhlen: Und wenn's schiefgeht? Vertrauen ist ein Erfolgsfaktor für die elektronischen Märkte. http://www.spiegel-online.de/netzweltarc/kolumnen/kuhlen1.html (verifiziert 22.08.1999)

Kuhlen (1998b): R. Kuhlen: Nur ein bißchen Verschlüsseln ist schwierig. http://www.inf-wiss.uni-konstanz.de/CURR/summer98/imk/sicherheit2.html (verifiziert 22.08.1999)

Kuhlen (1998c): R. Kuhlen: Trust – Vertrauen. Informationsethische Basis elektronischen Marktgeschehens (Bericht 86-98). Universität Konstanz – Informationswissenschaft. Konstanz 1998

Kuhlen (1999): R. Kuhlen: Die Konsequenzen von Informationsassistenten (Vorabdruck). Suhrkamp Verlag. Frankfurt 1999

Lethi (1999): I. Lethi, Certifying Trust. http://www.tcm.hut.fi/Research/TeSSA/Papers/Lehti-Nikander/lehti-nikander-98.html (verifiziert 22.08.1999)

Luhmann (1988): N. Luhmann: Familiarity, confidence, trust: Problems and Alternatives. In: Gambetta (1988), S.94 – 107

Lynch/Lundqist (1996): D. Lynch, L. Lundqist: Digital money: The New Era of Internet Commerce. J. Wiley and Sons. Chichester 1996

MasterCard (1999a): MasterCard: MasterCard SET. http://www.mastercard.com/shoponline/set/index.html (verifiziert 22.08.1999)

MasterCard (1999b): MasterCard: Shop Online SET. http://www.mastercard.com/shoponline/set/conclusion.html (verifiziert 10.09.1999)

Millicent (1999): Millicent: Millicent MicroCommerce System. http://www.millicent.com/ (verifiziert 22.08.1999)

Miville/Gustke (1994): F.P. Miville, R. von Gustke: Was ist Qualität, und wie sollte man Qualität verstehen, um erfolgreiches Qualitätsmanagement zu betreiben. In: Theorie und Praxis der Wirtschaftsinformatik, Heft 175, Januar 1994, S.8-19.

Möller (1997): U. Möller: Kryptographie: Rechtliche Situation, politische Diskussion. http://www.thur.de/ulf/krypto/verbot (verifiziert 22.08.1999)

National Fraud Information Center (1999): National Fraud Information Center: Supporters of the Internet Fraud Watch. http://www.fraud.org/info/thanks/ifwdono.htm (verifiziert 24.08.1999)

Needham (1999): K. Needham: Building Trust: Building Business. http://www.profitcorner.com/free_report_AIM7.htm (verifiziert 22.08.1999)

NetBill (1999): NetBill: NetBill Central. http://www.netbill.com/ (verifiziert 22.08.1999)

ORF (1999): ORF ON Futurezone: 512-bit Schlüssel ernsthaft gefährdet. http://futurezone.orf.at/futurezone.orf?read=detail&id=846&tmp=68663 (verifiziert 24.08.1999)

Parkins (1997): K. Parkins: PGP – The Web of Trust. http://www.heureka.clara.net/sunrise/pgpweb.htm (verifiziert 22.08.1999)

Passport Online (1999): Passport: Steganography. http://www.passport.ca/~shields/natlang/stegano.html (verifiziert 24.08.1999)

PC World (1999): PC World: PC World News – Code Cracked in Record Time. http://www2.pcworld.com/pcwtoday/article/0,1510,9413,00.html (verifiziert 22.08.1999)

Petrasch (1998): R. Petrasch: Einführung in das Software Qualitätsmanagement. Logos Verlag. Berlin 1998

PGP (1999): Pretty Good Privacy: The International PGP Homepage. http://www.pgpi.com/ (verifiziert 24.08.1999)

RegTP (1999a): Regulierungsbehörde für Telekommunikation und Post: Kontaktinformationen. Digitale Signatur – Fragen und Antworten (FAQs). http://www.regtp.de/Fachinfo/Digitalsign/neu/kontakti.htm (verifiziert 22.08.1999)

RegTP (1999b): Regulierungsbehörde für Telekommunikation und Post: NRCA Aktuell. Digitale Signatur. http://www.regtp.de/Fachinfo/Digitalsign/neu/index.htm (verifiziert 05.09.1999)

RegTP (1999c): Regulierungsbehörde für Telekommunikation und Post: Verzeigung zu den abrufbaren Verzeichnissen des VD. http://www.nrca-ds.de/abrufbar.htm (verifiziert 24.08.1999)

RegTP (1999d): Regulierungsbehörde für Telekommunikation und Post: Amtliche Veröffentlichungen. Digitale Signatur. Anerkannte Prüf- und Bestätigungsstellen für Sicherheitskonzepte. http://www.nrca-ds.de/abrufbar.htm (verifiziert 24.08.1999)

Reichswald (o.J.): R. Reichswald: Zur Notwendigkeit der Akzeptanzforschung bei der Entwicklung neuer Systeme der Bürotechnik. Hochschule der Bundeswehr – Fachbereich Wirtschafts- und Organisationswissenschaften. München o.J.

Reichswald/Bodem/Odemer/Schönecker/Sorg (o.J.): R. Reichswald, H. Bodem, W. Odemer, H. Schönecker, S. Sorg: Bedingungen der Bedienerakzeptanz eines Textverarbeitungssystems. Hochschule der Bundeswehr – Fachbereich Wirtschafts- und Organisationswissenschaften. München o.J.

Roßnagel (1998): A. Roßnagel: Die Sicherheitsvermutung des Signaturgesetzes. In: Neue Juristische Wochenschrift Nr.51, 1998, S. 3312 – 3320

RSA (1999a): RSA Data Security: RSA – About RSA Data Security. http://www.rsa.com/about/ (verifiziert 22.08.1999)

RSA (1999b): RSA Data Security: RSA – Security Protocol Overview. http://www.rsa.com/standards/protocols/ (verifiziert 22.08.1999)

RSA (1999c): RSA Data Security: RSA `99. http://www.rsa.com/conf99/overview.html (verifiziert 22.08.1999)

RSA (1999d): RSA Data Security: RSA Laboratories – Cryptography FAQ. http://www.rsa.com/rsalabs/faq/ (verifiziert 22.08.1999)

RSA (1999e): RSA Data Security: RSA Laboratories Challenges. http://www.rsa.com/rsalabs/html/challenges.html (verifiziert 22.08.1999)

RSA (1999f): RSA Data Security: RSA Labs FAQ – Glossary. http://www.rsa.com/rsalabs/faq/html/glossary.html (verifiziert 22.08.1999)

RSA (1999g): RSA Data Security: RSA Press Release. RSA Laboratories Key-Size Directive Reaffirmed at Technical Conference. http://www.rsa.com/pressbox/html/990504.html (verifiziert 22.08.1999)

RSA (1999h): RSA Data Security: RSA Secure solutions directory. http://www.rsa.com/solutions/ (verifiziert 22.08.1999)

RSA (1999i): RSA Data Security: Factoring Challenge. Status. http://www.rsa.com/rsalabs/html/status.html (verifiziert 10.09.1999)

Schuster/Färber/Eberl (1997): R. Schuster, J. Färber, M. Eberl: Digital Cash → Zahlungssysteme im Internet. Springer Verlag. Berlin, Heidelberg, New York 1997

Schwarz (1998): T. Schwarz: Zahlungssysteme im Internet. http://www.absolit.de/Finanz/Zahlungssystem.htm (verifiziert 22.08.1999)

Security Dynamics (1999): Security Dynamics – Homepage. http://www.securitydynamics.com/index.html (verifiziert 24.08.1999)

Seeger (1998): H. Seeger: Trust Center – Teure Sicherheit. http://www.spiegel.de/netzweltarc/themen/trustcenter.html (verifiziert 22.08.1999)

SETCo (1999a): SETCo: SETCo Frequently Asked Questions. http://www.setco.org/faq.html (verifiziert 24.08.1999)

SETCo (1999b): SETCo: The SET™ Standard Specification. http://www.setco.org/set_specifications.html/ (verifiziert 24.08.1999)

Shamir (1999): A. Shamir: Factoring large numbers with the TWINKLE device. Department of applied Math. The Weizman Institute. Revohot. http://www.sicherheit-im-internet.de/download/TWINKLE.PDF (verifiziert 24.08.1999)

Shoemaker (1998): B. Shoemaker: Basic Security of the eCash Payment System. http://www.digicash.com/ecash/docs/cosic.pdf (verifiziert 24.08.1999)

Sicherheit in der Informationsgesellschaft (1999a): Initiative Sicherheit in der Informationsgesellschaft: Homepage. Sicherheit, Gefahren und Schutz im Internet. http://www.sicherheit-im-internet.de/home.html (verifiziert 24.08.1999)

Sicherheit in der Informationsgesellschaft (1999b): Initiative Sicherheit in der Informationsgesellschaft: Einbahnstraßen, Falltüren und Euklid. http://www.sicherheit-im-internet.de/cgi-bin/showdoc.pl?doc=sii1999020401.html (verifiziert 24.08.1999)

Sietmann (1997): R. Sietmann: Electronic Cash – Der Zahlungsverkehr im Internet. Verlag Schäffer-Poeschel. Stuttgart 1997

Spiegel (1999a): Der Spiegel: Verkehr – Die deutsche Titanic. Nr. 21/1999, S.36ff

Spiegel (1999b): Der Spiegel: Datenverschlüsselung – Geheimnis gewahrt. Nr. 21/1999, S.20

Stealth Encryption (1999): Stealth Encryption: Stealth Encryption FREE Page. http://www.stealthencrypt.com/free.html (verifiziert 24.08.1999)

Südkurier (1999): Südkurier: Wenig Vertrauen in Sicherheit. Nr. 233, 8.10.1999, S.13

Telstra (1999): Telstra: PGP documentation. http://www.software.com.pl/newarchive/authancd/pgp/doc.shtml (verifiziert 22.08.1999)

Thome (1997): R. Thome (Hrsg.): Electronic Commerce: Anwendungsbereiche und Potentiale der digitale Geschäftsabwicklung. Verlag Vahlen. München 1997

Trustcenter (1999): Trustcenter: Zertifizierungsrichtlinien. http://www.trustcenter.de/html/Zertifikate/308.htm (verifiziert 24.08.1999)

TRUSTe (1999): TRUSTe: How Does Online Privacy Impact Your Bottom Line?. http://www.truste.org/webpublishers/pub_bottom.html (verifiziert 09.09.1999)

Turkle (1998): S. Turkle: Leben im Netz. Identität in Zeiten des Internet. Rowohlt Verlag. Reinbek 1998

Utimaco (1999): Utimaco Safeware AG: Technologien – Sicherheit durch Smartcards. Einsatz von Smartcards im IT-Sicherheitsbereich. http://www.utimaco.com/technik/smartcrd.htm (verifiziert 24.08.1999)

Visa (1997a): Visa: Visa Pressetexte. Sicheres Bezahlen im Internet: Visa startet weltweit größten SET-Pilotversuch. http://www.visa.de/df/presse/pressetexte/970602_001.htm (verifiziert 24.08.1999)

Visa (1997b): Visa: Visa Pressetexte. Der Secure Electronic Transaction-Standard wird ‚tragbar'. http://www.visa.de/df/presse/pressetexte/970627_001.htm (verifiziert 24.08.1999)

Visa (1999a): Visa: SEC/SEC-FAQ. Fragen und Antworten zu SET und SEC. http://www.visa.de/ks/service/setfaq.htm (verifiziert 22.08.1999)

Visa (1999b): Visa: SET. http://www.visa.de/ks/service/set.htm (verifiziert 24.08.1999)

Visa (1999c): Visa: Visa Pressetexte Technologie. http://www.visa.de/df/presse/pressetexte/technologie.htm (verifiziert 24.08.1999)

Visa (1999d): Visa: Visa-Electonic Commerce-SEC-Intro. http://www.visa.com/nt/sec/no_shock/intro_L.html (verifiziert 24.08.1999)

Visa (1999e): Visa: Visa-Electonic Commerce-SET-Shopping Experience. http://www.visa.com/nt/sec/no_shock/toy_entry_L.html (verifiziert 24.08.1999)

Visa (1999f): Visa: Visa-Electronic Commerce-SET. http://www.visa.com/nt/ecomm/security/set.html (verifiziert 10.09.1999)

Vogt (1996): J. Vogt: Vertrauen und Kontrolle in Transaktionen. Verlag Gabler. Wiesbaden 1996

Waidner/Janson (1995): M. Waidner, P. Janson: IBM Zurich Research Laboratory. Electronic Payment over open networks. http://www.zurich.ibm.com/Technology/Security/publications/1995/JaWa95.dir/JaWa95e.html (verifiziert 24.08.1999)

Welt (1996): Die Welt: Mona Lisa als verschlüsselte Nachricht. Sicherheitsexperten warnen vor Terroristen im Internet. Nr.277-48, 26.11.1996, S.2

Wright (1994): D. J. Wright: A Discussion of RSA-129 Activity. http://www.math.okstate.edu/~wrightd/numthry/rsa129.html (verifiziert 19.08.1999)

Yahoo (1999): Yahoo: Studie - Elektronischer Handel in Deutschland boomt. http://finanzen.de.yahoo.com/schlagzeilen/19990702/finance/0930903612-0000005330.html (verifiziert 19.08.1999)

Zbornik (1996): S. Zbornik: Elektronische Märkte, elektronische Hierarchien und elektronische Netzwerke. Universitätsverlag Konstanz. Konstanz 1996