

Christel Kumbruck

## **Digitale Signaturen und Vertrauen**

### **Abstract**

Der Beitrag befasst sich mit einem besonderen Aspekt elektronisch vernetzter Organisationen, nämlich der Materielosigkeit der Kooperation und der damit verbundenen zentralen Frage: Wie können wechselseitige Verbindlichkeiten in Organisationen abgesichert werden, wenn die zur Kommunikation und Kooperation benutzten elektronischen Medien die getauschten Informationen nur immateriell und dadurch flüchtig festhalten? Zum Zwecke rechtsverbindlicher Kooperation nutzen Menschen bisher eigenhändige Unterschriften. Es handelt sich dabei um einen psychosozialen Mechanismus, der Kooperationspartner moralisch verpflichtet und auf personalem Vertrauen basiert. In der elektronisch medierte Welt bedarf es technischer und organisatorischer Hilfsmittel, insbesondere der digitalen Signatur, die sich in vieler Hinsicht von der eigenhändigen Unterschrift unterscheidet. Die Autorin diskutiert die mit der digitalen Signatur einhergehenden Veränderungen in der Ausbildung von Vertrauen, nämlich der Ersetzung von personalem durch Systemvertrauen. Anhand empirischer Beispiele aus Simulationsstudien werden diesbezügliche Irritationen der Nutzer aufgezeigt und daraus abgeleitete technische und organisatorische Bedingungen, die es ermöglichen, das technische Mittel zum Aufbau von Systemvertrauen an den sozialen und personalen Vertrauensentwicklungsprozess rückzubinden.

### **1 Unsicherheiten in netzbasierten Organisationen**

Neue Organisationsformen zeichnen sich durch eine Auflösung der Ortsgebundenheit, der zeitlichen Bindung sowie der traditionellen organisatorischen Einbindung aus. Es gibt mehrere Entwicklungen (Bullinger/Brettreich-Teichmann/Fröschle 1995, 18 ff.; Goecke/Hesch 1997, 46ff.). Die klassische Telearbeit erfolgt mittels Heim-PCs, mobile Telearbeit mittels transportabler Computer, die den Nutzern per vorhandenen Anschluss jederzeit von quasi jedem Ort aus (Eisenbahn, Auto, Kommunikationspool) Zugang zu den Datenbanken ihrer Organisation ermöglichen. In Telearbeits- und Service-Centern arbeiten Mitarbeiter unterschiedlicher Organisationen mit direktem elektronischem Zugriff zu ihrer Organisation. Oftmals wird dabei „Desk-Sharing“ betrieben, d.h. es gibt keine personengebundenen Arbeitsplätze mehr, sondern die Arbeitsplätze werden von den jeweils anwesenden Personen temporär benutzt. Diese räumliche Entzerrung wird beispielsweise durch Groupware-Software kompensiert, die die Bildung virtueller Teams ermöglicht. Virtuelle Organisationen schließlich konstituieren sich als eine Vernetzung von mehreren autonomen Firmen. Sie greifen über die Grenzen der - weiterbestehenden - traditionellen Organisationen hinaus. Mitglieder unterschiedlicher Organisationen oder auch „organisationsfreie“ Personen stellen mittels der neuen Medien untereinander Kontakt her, falls und wann sie es w(s)ollen. Als

typische Beispiele sind zu nennen: Banken lassen in Fernost ihre Buchungen erledigen; Softwarehäuser lassen in Indien programmieren.

Diese verschiedenen neuen Organisationsformen, die sich dadurch auszeichnen, dass ihnen die Anwendung der modernen Informations- und Kommunikationstechnik ermöglicht, unabhängig von Raum und Zeit zusammenzuarbeiten, fasse ich unter dem Oberbegriff netzbasierte Organisationen zusammen. Sie können noch als Organisationen im klassischen Sinne angesehen werden, weil sie Ziele haben, die sie umsetzen, weil sie dauerhaft bestehen und einen festen Mitarbeiterstamm haben. Jedoch die Mitarbeiter kommen nicht mehr zwangsläufig an einem Ort zusammen, sondern erledigen ihre Aufgaben vor allem durch Telearbeit am PC, mit dem sie am personalen und elektronischen Organisationswissen teilhaben.

Ein damit einhergehendes Problem ist die Reduzierung der für den Zusammenhalt einer Organisation wichtigen vertrauensbildenden sozialen Kontakte. Eine besondere Ausprägung dieses Problems entsteht zusätzlich durch die Materiellosigkeit des elektronischen Austauschs. Elektronische Dokumente sind die Grundlage der Arbeitsweise in einer netzbasierten Organisation: Sie können ohne Medienbruch erstellt und verarbeitet, quasi ohne Zeitverlust um die ganze Erde transportiert und dann weiterverarbeitet werden, sie sind für viele Bearbeiter gleichzeitig im Original verfügbar und benötigen kaum Raum zur Aufbewahrung. Diesen der Materiellosigkeit der elektronischen Dokumente geschuldeten Vorteile stehen spezifische Nachteile gegenüber:

- Es besteht Unsicherheit bezüglich der Integrität eines elektronischen Dokumentes, weil eine Manipulation weder erkannt noch nachgewiesen werden kann.
- Die Vertraulichkeit elektronischer Dokumente ist nicht gewährleistet, weil alle Inhalte für alle am Transport beteiligten Instanzen (z.B. Betreiber) einsehbar sind.
- Der Verfasser eines elektronischen Dokumentes ist nicht erkennbar (auch nicht für einen Schriftgutsachverständigen), weil sich jeder mit geringem Aufwand als der Verfasser ausgeben kann, d.h. die Authentizität des Dokumentes ist nicht gesichert.

Diese Nachteile sind relevant für das Funktionieren einer Organisation, weil Dokumente die Grundlage des Arbeitsablaufs in Organisationen darstellen und ihre Struktur reproduzieren helfen. Die Mehrzahl aller in Unternehmensbüros und öffentlichen Verwaltungen erstellten Texte trägt darüber hinaus rechtsverbindlichen Charakter, beispielsweise Verträge, Bescheide, Mahnungen, Lieferungszusagen, Beschlüsse und Investitionsgewährungen. Daraus folgt, dass über die Zeit nachvollziehbar und nachweisbar sein muss, wer wann was bearbeitet oder genehmigt hat und somit dafür die Verantwortung trägt. Wenn beispielsweise an einem Dokument im Rahmen der arbeitsteiligen Textproduktion aus der Befürwortung der Einstellung eines potentiellen Mitarbeiters eine Ablehnung wird, ist dies für die Organisation und den Mitarbeiter eine relevante Entscheidungsänderung, die nachvollziehbar sein muss. Wenn die Speicherung solcher Texte ohne materiellen Träger erfolgt, bleiben auch keine materiellen Spuren zurück. (Bonin 1991)

## **2 Zur Bedeutung von Unterschriften und Signaturen**

*Eigenhändige Unterschriften* sind Willenserklärungen, bevor die erklärte Handlung ausgeführt wird. Mit der eigenhändigen Unterschrift setzen die Kooperationspartner ein auch vor Gericht anerkanntes Zeichen, dass sie für den unterzeichneten Inhalt nebst der sich daraus

ergebenden Konsequenzen eintreten wollen. Unterschriften sind wie der bekräftigende Händeschlag psychosoziale Mechanismen, welche die Kooperationspartner moralisch an ihre Vereinbarung binden. Sie sind im Gegensatz zum bekräftigenden Händeschlag eine wesentliche Voraussetzung dafür, dass im Falle der Nichterfüllung der Vereinbarungen durch einen Kooperationspartner der andere die Erfüllung vor Gericht einfordern kann. Dadurch wird das Risiko reduziert, dass der andere sich nicht kooperativ verhalten wird. Diese Mechanismen ermöglichen es den Kooperationspartnern, dass sie sich im Rahmen der unterzeichneten Vereinbarungen aufeinander verlassen können. Dieses Mittel wird auch im Mitzeichnungsverfahren in Organisationen genutzt. Jeder im Arbeitsablauf durch eine Person vollzogene Arbeitsschritt nebst impliziter Entscheidung wird durch eine Unterzeichnung gekennzeichnet. Die Reihenfolge der Unterschriften sowie handschriftliche Vermerke ermöglichen die Nachvollziehbarkeit des Entscheidungsganges und die Zuordnung zu den jeweils verantwortlichen Personen.

*Die digitale Signatur* ist die Telekooperationstechnik, die das Äquivalent zur eigenhändigen Unterschrift realisiert. Sie soll Integrität, d.h. Manipulationssicherheit, Vertraulichkeit und Authentizität der elektronischen Dokumente gewährleisten im Hinblick auf die Ausbildung von Handlungssicherheit. Angesichts der organisatorisch-räumlichen Komplexität von netzbasierten Organisationen kann nicht von geschlossenen, sondern von offenen Benutzergruppen ausgegangen werden. Die hierfür benötigten Sicherungsmaßnahmen beruhen auf dem Verfahren öffentlicher Schlüsselsysteme und des „vertrauenswürdigen Dritten“, so das RSA-Verfahren. (Rivest/Shamir/Adleman 1978)

Das Verfahren der digitalen Signatur arbeitet mit zwei asymmetrischen Schlüsseln, die zueinander passen wie Schlüssel und -loch; aus dem Einen kann jedoch nicht der andere ausgerechnet werden. Der Eine ist geheim in einer Chipkarte des Inhabers der digitalen Signatur, der Andere ist öffentlich und soll von jedem Kooperationspartner genutzt werden. Das Paar wird ausgeteilt und bestätigt durch eine Schlüsselzertifizierungsinstanz (der sogenannte vertrauenswürdige Dritte); diese ist vergleichbar mit einem Passamt. Die Anwendung des geheimen Schlüssels und die Überprüfung der Unversehrtheit einer Signatur erfolgt mittels einer Computersoftware.

Mit öffentlichen Schlüsselsystemen kann die Vertraulichkeit von Nachrichteninhalten gewährleistet werden. Der Absender verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des Empfängers und sichert damit, dass nur dieser die Nachricht mit seinem geheimen Schlüssel entziffern kann. Es ist dies die verbesserte Funktionalität eines Papier-Briefumschlages.

Im umgekehrten Verfahren können digitale Signaturen erzeugt und geprüft werden. Die digitale Signatur ist kein elektronisches Abbild der eigenhändigen Unterschrift, sondern eine verschlüsselte Kurzfassung des Dokumentes. Der Prüfende erhält nur dann identische Kurzfassungen, wenn das Kryptogramm mit dem geheimen Schlüssel, der zu dem öffentlichen Schlüssel passt, verschlüsselt worden ist; d.h. dann ist der Text nicht verändert worden. Solange nur der Berechtigte über den geheimen Schlüssel verfügt, kann durch dieses Verfahren auch nachgewiesen werden, dass die Nachricht von ihm stammt. Die Zuordnungsmöglichkeit zu einem Urheber basiert auf dem Besitz der Chipkarte und der Kenntnis der PIN (Personal Identity Number) in Verbindung mit der gesicherten Zuordnung des öffentlichen Schlüssels zu einer bestimmten Person. Um diese Zuordnung des öffentlichen Schlüssels zu einer bestimmten Person sicherzustellen und zu garantieren, bedarf es deshalb eines sogenannten „vertrauenswürdigen Dritten“. Dessen Bestätigung erfolgt ebenfalls durch eine

diesem eigene digitale Signatur und wird Zertifikat genannt. Wird dieses an die digitale Signatur des Senders angehängt, kann es automatisch auf die gleiche Weise wie das Dokument überprüft werden. (Hammer 1995; Provet/GMD 1993; Roßnagel u.a. 1994) Sowohl die Vergaben der digitalen Signatur als auch ihre Prüfung beim Empfang eines Dokumentes erfolgt als maschinelle Prozedur, die der Nutzer anstößt. Er unterschreibt nicht mit seiner Hand, sondern regt einen Verschlüsselungsmechanismus unter Hinzunahme seines persönlichen Codes in seiner Chipkarte an; er prüft nicht per Augenschein, sondern lässt die Maschine Kryptogramme vergleichen.

Die digitale Signatur unterscheidet sich somit in wesentlichen Punkten von der eigenhändigen Unterschrift, wodurch die kulturell eingespielten Mechanismen nicht mehr wirken können und sich für die telekooperative Gesellschaft die Frage der Schaffung von Vertrauen und Verbindlichkeit in Kooperationen neu stellt.

Dieser Problemkomplex wird in der Psychologie bisher unter dem Gesichtspunkt von Unsicherheit, Risikowahrnehmung und daraus abgeleitetem Umgang mit der Sicherheitstechnik (Stapf 1998, 45 ff.; Rudinger/Espey/Holte/Neuf 1998, 69 ff.; Neuf/Espey 1998, 199ff.; Espey u.a. 1998, 233ff.; Rudinger/Espey/Eßer 1998, 249 ff.; Dufft/Stapf 1998, 275 ff.) oder Kontrollverlust (Döring u.a. 1998, 159 ff.) diskutiert. Ich sehe demgegenüber – wie dies auch von Soziologen diskutiert wird – in diesem Zusammenhang ein Problem der „Vertrauensbildung“ (Braczyk u.a. 1998, 119ff.) Denn „Vertrauen in Technik ist immer auch Vertrauen in den sozialen Kontext, in den die jeweilige technische Anwendung eingebettet ist“. (Braczyk u.a. 1998, 120) Eigenhändige Unterschriften respektive die Technik der digitalen Signatur haben demnach eine wichtige sozialpsychologische Bedeutung für die Entstehung von Verbindlichkeit, d.h. für die Überbrückung von Unsicherheit zwischen Kooperationspartnern. Sie sind unter dem Gesichtspunkt von Vertrauen zu diskutieren.

### 3 Personales Vertrauen und Systemvertrauen

Vertrauen ist eine zentrale Determinante von Kooperation. Nach Petermann (1985, 7 ff.) *überbrückt Vertrauen die Kluft des Nichtwissens* darüber, wie sich der Kooperationspartner verhalten wird, wobei es gleichzeitig Ausdruck der Erwartung ist, dass etwas für den Vertrauenden Bedeutsames in Erfüllung geht. In Luhmanns (1973) soziologischer und systemtheoretischer Definition dient Vertrauen der Komplexitätsreduktion. In einer Situation der Ungewissheit müsse im Hinblick auf Handlungsfähigkeit ein *Vertrauensvorschuss* geleistet werden. Auch die Sozialpsychologen Bierhoff & Buck (1984) definierten Vertrauen ähnlich als *Bereitschaft zur Verwundbarkeit*. Vertrauen dient somit als psychosozialer Mechanismus der Überbrückung von Unsicherheit. Der Bedarf an Vertrauen entsteht aufgrund von grundlegenden Eigenarten sozialer Bezüge. Gegenseitige Leistungen können nur zeitlich verzögert und sequentiell ausgetauscht werden. Preisendörfer (1995, 264) nennt dies das „Zeitproblem“. Aus dem sequentiellen Charakter ergibt sich das „Informationsproblem“ (ebd.), nämlich die Unsicherheit, ob sich die Interaktionspartner an die impliziten oder expliziten Vereinbarungen halten werden. Vertrauen ist somit ein psychologischer und sozialer Mechanismus zur Lösung dieses Problems durch *einseitige Vorleistung*. Aufgrund der zeitlichen Verzögerung zwischen Vertrauensvorschuss und Gegenleistung besteht ein besonderes Risiko auf Seiten des Vertrauenden. (Vertragliche) Vereinbarungen sowie die Verantwortlichzeichnung im Rahmen organisatorischer Arbeitsabläufe sind Mechanismen

der Übernahme von Verantwortung durch einzelne Handlungsträger. Derjenige, der unterzeichnet, bringt damit eine einseitige Vorleistung. Damit verschafft er dem Kooperationspartner Handlungssicherheit, sei es ein geschäftliche Partner oder ein weitere Arbeitsschritte ausführender Mitarbeiter. Vertrauen verschafft einer Person sozusagen Handlungssicherheit in Situationen, die sie nicht bezüglich des Ergebnisses unter Kontrolle hat.

Vertrauen wird Winnicott (1974) zufolge zunächst über gegenseitige stabile Erfahrungen hergestellt. Hieraus erwächst einerseits auf Dauer eine soziale Kompetenz in Form von Menschenkenntnis, die es ermöglicht, auch einer unbekannt Person aufgrund gewisser Bedingungen, nämlich dem Wiedererkennen von als vertrauenswürdig erkannten Aspekten, Vertrauen zu schenken. Bei bekannten Personen wiederum wird das Vertrauen auch in weiteren Kooperationssituationen, die nicht von Angesicht zu Angesicht erfolgen, über wiederkehrende Spuren des Gegenüber reproduziert. Hierbei spielt die psychologische Bedingung der Objektpermanenz als Mittel der kognitiven und psychischen Orientierung eine wichtige Rolle. Die Möglichkeit zum *Wiedererkennen von Menschen oder Objekten* ist somit die erste konstitutive Bedingung für das Ausbilden von Vertrauen. Es wird dadurch plausibel, dass die Dauer einer Beziehung sowie dabei gemachte gute Erfahrungen mit dem Kooperationspartner Vertrauen stabilisieren.

*Komplement Verantwortung:* Es ist davon auszugehen, dass Vertrauen und Verantwortung in einem symmetrischen Verhältnis zueinander stehen. Die Vertrauensgewährung ist an die Erwartung gebunden, dass der Kooperationspartner die Verantwortung für den von ihm zugesicherten Part der Kooperation übernimmt. Verantwortung ist somit die „Antwort“ (Loh 1990, 77f.), die moralische Voraussetzung dafür, das in die Tat umzusetzen, wofür jemand sein Wort gegeben hat, also das „Eintreten, Einstehen eines Handlungssubjekts für Handlungsfolgen vor einer Instanz und gegenüber einem Adressaten“. (Lenk 1992) Verantwortung setzt immer einen Handlungsspielraum, zum Antwort-Geben, voraus. Sanktionen und Haftungsregelungen schränken die Möglichkeiten, Antwort zu geben, ein. Dagegen sind soziale Regelungsmechanismen wie Zeremonien und Gesten für die Verantwortungsübernahme besonders bedeutungsvoll.

Da Kooperation ein sozialer Prozess ist, wird er von Menschen getragen, die über vertragliche Verpflichtungen hinaus wechselseitige Vertrauensbeziehungen ausbilden. Ein wichtiger Faktor in diesem Prozess ist die Erfahrung, dass das in den Kooperationspartner gesetzte Vertrauen nicht enttäuscht wird. *Reziprozität* ist damit die zweite konstitutive Bedingung von Vertrauen. (Gouldner 1984)

Es wird hier deutlich, dass Vertrauen auch als ein sozialer Mechanismus des Austausches verstanden wird. Es deutet sich hier eine *symbolische oder rituelle Ebene* an, die dem Aufbau von Vertrauen dient. Diese hat ihre Verankerung in einem sogenannten normativen Konsens, wie Zündorf begründet ausführt:

„Die Risiken des Vertrauens bedürfen der Begrenzung und Abfederung durch Konventionen und Moral, durch Prinzipien von ‚Treu und Glauben‘, durch nicht- oder vorkontraktuelle, letztendlich lebensweltliche Elemente.“ (Zündorf 1986, 42)

*Feste soziale Bezüge und Regeln*, beispielsweise innerhalb von Organisationen, geben einen zusätzlichen Rahmen ab für die Entwicklung von Vertrauen, so dass ein Teil der individuellen Prüfung des Kooperationspartners überflüssig und das Ritual des Kennenlernens reduziert und verkürzt werden kann.

In den Vertrauensprozess geht nur zu einem geringen Teil explizites Wissen ein, zu einem größeren Teil jedoch Erkenntnisse aufgrund von Einfühlungsvermögen und der Erfahrung von Selbstwirksamkeit, die auf Feedback- und Lernprozessen beruhen. In diesem Sinne ist

der Prozess auf ein gewisses Maß an Intimität und Vertraulichkeit angewiesen. *Vertraulichkeit* ist damit eine weitere Bedingung von Vertrauen.

Zusammenfassend können folgende Anforderungen für personales Vertrauen benannt werden: Reziprozität, Kommunikation, Langfristigkeit von Beziehungen, Personenbezug der Handlungen, um gute Erfahrungen erkennen zu können, Möglichkeit zur Ausbildung und Nutzung von Riten, Symbolen und Zeichen für den sozialen Austausch und Rückbezug auf ein gemeinsames Normensystem, sowie Vertraulichkeit der Handlungen.

Nach diesen Ausführungen zum Vertrauensbegriff ist auf ein prinzipielles Problem des Vertrauensbegriffs hinzuweisen: Das Konstrukt Vertrauen wird in der Psychologie als personales Vertrauen verstanden. Vertrauen kann auch dazu genutzt werden, auf die physische Präsenz des Kooperationspartners zu verzichten, dessen Abwesenheit zu überbrücken, wie es ja in netzbasierten Organisationen notwendig ist. Nach Sydow und Loose (1995) muss dann aber in Anlehnung an Luhmann (1973) von Systemvertrauen gesprochen werden, wobei Vertrauen in Infrastruktur und äußere Bedingungen die Möglichkeit des direkten Vertrauens in eine Person ersetzt oder ergänzt. Dieser Vertrauentyp ist auf technische oder soziale Systeme ausgerichtet. Es ist dies ein Ansatz, der dem Problem von Ausbildung von Handlungssicherheit in einer durch I&K-Technik geprägten Organisation eher gerecht wird, weil er die Modifikation psychischer Qualitäten angesichts restriktiver Bedingungen verstehbar macht. D.h. auch wenn personales Vertrauen als grundlegend für kooperative Beziehungen angesehen wird, kann es doch unter modernen Bedingungen mit wenig oder gar keiner Kopräsenz zu einer Ersetzung und/oder Ergänzung in Form von Systemvertrauen kommen, eine Form von Vertrauen also, die nur in der Soziologie behandelt wird. Für die vorliegende Fragestellung ist die Verschränkung von Personen- und Systemvertrauen deshalb von grundlegender Bedeutung, weil es letztendlich um das Vertrauen in Personen geht, wenngleich die unmittelbare Auseinandersetzung mit technischen Hinweisen auf personale Vertrauenswürdigkeit erfolgt. Aus diesem Grund scheint die analytische Auftrennung in personales Vertrauen auf der einen und Risikobewusstsein auf der anderen Seite nicht sinnvoll.

Die Prozesse der Veränderung der personalen Vertrauensbildung durch den Einsatz von Informations- und Kommunikationstechnik und die damit verbundenen Verschränkungen von personalem und Systemvertrauen können mit den Ausführungen des Soziologen Giddens (1996) zum Verhältnis von schwacher und starker Kopräsenz und zur sogenannten Entbettung (*disembedding*) besser verstanden werden. Den Begriff Entbettung hat Giddens entwickelt zur Charakterisierung von Gesellschaften und Organisationen in der Moderne. Eine Entbettung ist das Herausheben sozialer Beziehungen aus ortsgebundenen Interaktionszusammenhängen und ihre unbegrenzte Raum-Zeit-Spannen übergreifende Umstrukturierung, wodurch das gesellschaftliche Tun nicht mehr in die Besonderheiten der Anwesenheitszusammenhänge, also in die spezifischen zeitlichen, räumlichen, assoziativen und ethischen Kontexte eingebettet ist. Es gibt keine Kopräsenz, die Erfahrungsmodalitäten auf der Ebene des Körpers ermöglicht. Vielmehr werden Verpflichtungen auf der Basis gemeinsam anerkannter Regeln organisiert. An die Stelle des personalen Vertrauens unter starker Kopräsenz („*facework commitments*“), also persönlich ausgehandelter Verpflichtungen, kann auch ein Handeln unter schwacher Kopräsenz („*faceless commitments*“) treten, das auf der Verpflichtung auf gemeinhin anerkannten Regeln beruht. Wenn jedoch die Vertrauensbasis des „*faceless commitments*“ nicht ausreicht, können unter der Bedingung physischer Anwesenheit neue Verbindlichkeiten und Verantwortlichkeiten ausgehandelt werden.

Eine solche Entbettung birgt jedoch Unsicherheiten, Risiken. Denn da eine Absicherung des Vertrauens nicht mehr (nur) über direkte interpersonale Beziehungen erfolgen kann, muss das abstrakte System (z.B. die netzbasierte Organisation) selbst Sicherheiten bereitstellen und/oder in seinem Umfeld müssen zusätzliche sicherheitsstiftende Mechanismen wirksam sein (z.B. Expertensysteme, z.B. technische Systeme), Entbettungsmechanismen, die die Entwicklung von Systemvertrauen unterstützen sollen. Systemvertrauen ist nicht unmittelbar an „facework“ bzw. Kopräsenz gebunden. Ein typischer Entbettungsmechanismus, der Systemvertrauen schaffen soll, ist bereits das Verfahren der eigenhändigen Unterschrift im Kontext der Papiernutzung zur Absicherung rechtsverbindlicher Kooperation. Es ist Ausdruck der Entbettung, dass sich Menschen nicht face-to-face begegnen müssen, und dient zugleich als Klammer der Abwesenden, also als Entbettungsmechanismus. Es hat sich über einen langen Zeitraum eingespielt und dient dem Erringen von Handlungssicherung. Die Praxis des Austauschs ungesicherter elektronischer Dokumente stellt demgegenüber eine immense Entbettung dar. Aber auch für den Austausch elektronischer Dokumente gibt es das Angebot zur Ausbildung von Systemvertrauen, nämlich durch das Verfahren der digitalen Signatur, das den Problemen, die auf der Materielosigkeit elektronischer Daten beruhen, entgegenwirkt und somit ebenfalls als „Entbettungsmechanismus“ fungiert.

Die Entbettungsmechanismen heben also die sozialen Beziehungen aus ihrer Situiertheit an spezifischen Orten heraus; sie dienen aber zugleich der Verklammerung von Abwesenden über den Weg der Vertrauensausbildung. Die Entbettung birgt Risiken, z.B. keine Möglichkeit zur direkten Kontrolle per Augenschein und kein Zurückbleiben materieller Spuren. Die Entbettungsmechanismen sollen diese Risiken abmildern durch die Gewährleistung von „Sicherheitsgarantien“.

In diesem Sinne beruhen alle Entbettungsmechanismen auf Vertrauen - nicht in Individuen, sondern in abstrakte Systeme. „Faceless commitments“ haben jedoch nur eine begrenzte Reichweite. Daraus ergibt sich nach Giddens (1996, 102) folgender Zusammenhang zwischen personalem und Systemvertrauen: „Alle Entbettungsmechanismen stehen in Wechselbeziehung zu rückbetteten Handlungskontexten.“ Was heißt dies? Prozesse des „disembedding“ bedürfen der Ergänzung durch solche des „reembedding“, d.h. des Wiederankoppelns von „faceless commitments“ durch „facework“ an die Akteure. Dieses Wiederankoppeln findet beispielsweise an sogenannten Begegnungspunkten statt. Ein typisches Beispiel ist der Versicherungsvertreter, der, indem er dem Versicherungsklienten im persönlichen Kontakt vertrauenswürdig erscheint, bei diesem (System-) Vertrauen in die abstrakte Institution Versicherung weckt. Dieses „reembedding“ ist deshalb wichtig, weil das Vertrauen in abstrakte Systeme zwar für die Sicherheit im Sinne tagtäglicher Zuverlässigkeit sorgt, es jedoch im innersten Wesen dieses Vertrauens liegt, dass es weder die Gegenseitigkeit noch die Intimität bieten kann, die, wie Erikson (1950) ausführt, von persönlichen Vertrauensbeziehungen ausgehen. Bei den abstrakten Systemen setzt das Vertrauen den Glauben an unpersönliche Prinzipien voraus, die nur in statistischer Weise „Widerworte geben“, wenn sie nicht die von den Betreffenden angestrebten Ergebnisse liefern. Hierin liegt eine Quelle für „Krisen“ im Aufbau von Systemvertrauen. Das Funktionieren von Systemvertrauen beruht somit auf einem ausgeglichenen - ausgependeltem - Verhältnis von „disembedding“ und „reembedding“. Der Akt der Rückbettung muss somit Anker bieten vergleichbar denen, die für den Aufbau von personalem Vertrauen notwendig sind.

## 4 Erprobung der digitalen Signatur

Im Folgenden werde ich einige meiner empirischen Ergebnisse aus den in der Projektgruppe Verfassungsverträgliche Technikgestaltung durchgeführten Simulations- und Langzeitstudien (Kumbruck 1995) in einer netzbasierten Büroorganisation - im Bereich der netzbasierten Rechtspflege sowie der vernetzten Gesundheitsversorgung - präsentieren, die sich auf die zentrale Anforderung für die Vertrauensausbildung bezieht, nämlich Personenbezug der Handlungen. (Kumbruck 1996; Roßnagel u.a. 1994; Bizer u.a. 1995; Ammenwerth u.a. 1999; Kumbruck 1999)

In Simulationsstudien wird der Alltag von morgen für einen befristeten Zeitraum durch berufliche Experten simuliert und erprobt. Beispielsweise arbeiteten in der Simulationsstudie telekooperative Rechtspflege echte Anwälte, Richter, Sekretariats- und Gerichtsangestellte in für die Studie mit modernster Telekooperationstechnik (inklusive digitaler Signaturtechnik) ausgestatteten Büros an vorbereiteten Rechtsfällen über einen Zeitraum von zweimal einer Woche. Die Fälle wurden schriftlich oder durch instruierte Mandanten in die Wege geleitet und endeten mit einer Gerichtsverhandlung. Die Teilnehmer wurden bei ihrer Arbeit wie in jeder Feldstudie beobachtet, und es wurden die Beobachtung betreffende offene Interviews durchgeführt. Zudem wurden nach jedem Arbeitstag Gruppengespräche geführt, in denen die Experten, die Entwickler und die Wissenschaftler einen Dialog über die Tageserfahrungen, ihre Bewertung sowie mögliche technische und organisatorische Gestaltungslösungen geführt wurde. Letztere gingen in die technische Neugestaltung für die zweite Erprobungsphase und in die Gestaltungsempfehlungen ein. Alle Interviews wurden hermeneutisch ausgewertet. Somit integriert die Methode der Simulationsstudie Elemente der Feldstudie, der Simulation und der partizipativen Systementwicklung. In der Untersuchung zur netzbasierten Büroorganisation war zusätzlich zur Simulationsstudie eine Langzeitstudie, in der die neue Technik erprobt wurde, möglich, so dass die Ergebnisse beider methodischer Ansätze verglichen werden konnten.

Aus psychologisch-arbeitswissenschaftlicher Sicht wurden Veränderungen in der Arbeitskultur untersucht, also Veränderungen in den kooperativen Handlungs- und Denkmustern aufgrund medialer Spezifika von Telekooperationstechnik wie Zeit- und Raumunabhängigkeit, Systemsteuerung des Arbeitsflusses, Papierlosigkeit und Virtualität der Dokumente. Ein Schwerpunkt lag dabei auf den Veränderungen im Absichern von Verbindlichkeiten mittels digitaler Signaturen.

Die eigenhändige Unterschrift ist eine persönliche Entäußerung ohne weitere Hilfsmittel und kann mittels eigener Wahrnehmung überprüft werden. Um zu signieren oder eine Signaturprüfung durchführen zu lassen, benötigt der Nutzer einen Rechner mit Sicherungssoftware und Zugriff auf einen Verzeichnungsdiens der Sicherungsinfrastrukturinstanz, ein daran angeschlossenes Kartenlesegerät, eine Chipkarte, in die von einer Sicherungsinfrastrukturinstanz ein geheimer Schlüssel geladen wurde sowie zur Aktivierung dieser Chipkarte eine Geheimnummer (PIN - personal identity number).

Es handelt sich hierbei um einen typischen Entbettungsmechanismus, wobei abstraktes Systemvertrauen personales Vertrauen ersetzen soll, gleichzeitig aber auch um Rückbettung gegenüber dem Zustand der frei beweglichen und manipulierbaren elektronischen Dokumente. Im Folgenden zwei Beispiele, an denen sich die Notwendigkeit des Personenbezug einer Handlung im Hinblick auf die Vertrauensbildung im Unterschriftverfahren manifestiert und diesbezügliche Schwächen des Verfahrens der digitalen Signatur offenbar werden.



#### 4.1 Das Problem mit der Entindividualisierung beim Signieren

Das Problem mit der Entindividualisierung beim Signieren zeigt sich im Umgang mit Chipkarte und PIN - d.h. der eigenen vergegenständlichten Identität:

Nutzer lassen die Chipkarte irgendwo liegen und können somit nicht signieren. In der Not lassen sie sich gegebenenfalls die Chipkarte von einem Kollegen oder Partner ausleihen. Es ist zwar möglich, mit der Chipkarte eines anderen, so man dessen PIN weiß, zu unterzeichnen, doch steht dann der Name des anderen in der Signatur.

Entsprechend kann die Chipkarte verloren gehen, im Chipkartenleser liegen bleiben oder entwendet werden. Auch den Zugriff auf ihre PIN machen viele Nutzer den Mitmenschen leicht. Sie nehmen beispielsweise ihr Geburtsdatum oder bewahren zusätzlich einen Zettel mit der Chipkarte auf, auf dem die Nummer steht. So kann die digitale Signatur von Unbefugten und von guten Freunden, die die Karte ausleihen, im Namen des Chipkarteninhabers benutzt werden. Kein Mensch kann feststellen, dass dieser nicht der Unterzeichner war.

Für die organisationsinterne Kommunikation wünschten sich unsere Probanden eine Büro-Signatur. Damit gäbe es aber keine individuelle Zuordnung der Signatur zu nur einer Person mehr.

Ein weiteres neues Handlungsmuster deutete sich darin an, dass die Anwender die Signaturfunktion freigaben und damit die Dokument-Authentikatoren gleich für mehrere Dokumente zugleich erzeugen ließen. Sie signierten also mehrere Dokumente zugleich, ohne diese für die Signaturerzeugung im Einzelnen zur Kenntnis zu nehmen. Sie nutzten somit den Rationalisierungsvorteil, den ein Computer auch für das Signieren bieten kann, nämlich die Tätigkeit des Signierens wie am Fließband durchzuführen: Für die Anwender bot dieses Verfahren Analogien zur Unterschriftenmappe, war sozusagen deren elektronische Variante. Die Sammel-Signatur ist jedoch gerade keine Unterschriftenmappe. Denn mittels der Sammel-Signatur wird im Gegensatz zur Unterschriftenmappe keine letzte Sichtkontrolle durchgeführt. Die Unterzeichnung der Dokumente einer Unterschriftenmappe erfolgt zwar auch im Schnelldurchgang, jedoch kann auch dann noch ein oberflächlicher Blick auf die Dokumente geworfen werden und bei dabei auftretendem Zweifel gezielt eine ausgiebige Dokumentenprüfung erfolgen.

Statt des gezielten Einsatzes der eigenhändigen Unterschrift wird die Signatur als Sammel-Signatur zu einer Routineangelegenheit umfunktioniert, die in gewisser Weise von einer Maschine übernommen wird. Dies bedeutet jedoch eine Entwertung der Funktion der Verantwortungsübernahme als einem bewussten Akt. Die Anwender gehen damit auch ein erhöhtes Risiko ein, dass ihnen ein Dokument untergeschoben wird, das sie nicht signieren wollen. (Pordesch/Schneider 1993; Pordesch 1993a; Pordesch 1999)

Was ist aus der Vorgehensweise der Nutzer zu schließen? Der Aufbau von Systemvertrauen, das indirekt personales Vertrauen beim Empfänger einer digitalen Signatur stärken soll, Abwesende verklammern soll, wird so durch das Verhalten der Nutzer unterminiert. Die Nachvollziehbarkeit von Verantwortlichkeiten an elektronischen Textversionen ist dadurch nicht gewährleistet. Ein Hintergrund für ein solches „verantwortungsloses“ Verhalten ist darin zu sehen, dass im elektronischen Verfahren die Involviertheit des Nutzers, sein aktives und an seine persönliche Entäußerung gebundenes Ja-Sagen zu einer Entscheidung im Rahmen eines Vorgangs oder zur Übernahme einer vertraglichen Verpflichtung nicht gefordert und nicht transparent ist. Die Handlung des Signierens erfolgt im Gegensatz zu der

des eigenhändigen Unterschreibens infolge der Hilfsmittel nicht unmittelbar. Diese „Unterbrechung“ der Entäußerung wird von den Anwendern aktiv dadurch fortgesetzt, dass sie die Signatur partiell auch nicht mehr als nur ihnen persönlich zukommend wahrnehmen, sondern sie als ihnen äußerlich u.a. an andere Personen, beispielsweise ihre Sekretärin, verleihen.

Die äußere Verobjektivierung, welche die Signierfunktion annehmen kann, birgt in sich Ambivalenz: Sie wird nicht immer verfügbar sein, weil sie an ein äußeres Objekt gebunden ist. Sie wird einer Person nicht unmittelbar „angewachsen“, sondern sozusagen zugeteilt sein und ist dann als Objekt benutzbar. Somit wird sie auch verleihbar. Damit kommen die Bemühungen um die Garantie der Urheberschaft an eine Grenze, die im Umgang der Anwender mit der Chipkarte liegen. Der Unterschied zur Fälschung der eigenhändigen Unterschrift besteht darin, dass diese ja wirklich eine Fälschung darstellt und als solche auch erkannt werden kann, im Gegensatz zum Missbrauch der Signaturutensilien. (Pordesch 1994, Pordesch 1993b.) Dem Handlungsbruch - das Verleihen der eigenen Signiermächtigkeit - muss zwangsläufig ein Bruch in der Bewertung des Signierens gegenüber dem der eigenhändigen Unterschrift folgen: Es stellt sich die Frage, wer im Falle der „Verleihung“ der Chipkarte und der „verteilten Verfügung“ über die Chipkarte die Verantwortung für die erteilte Signatur tragen wird und ob es für den Kooperationspartner noch angemessen ist, angesichts einer digitalen Signatur dem Namensträger derselben sein Vertrauen zu schenken?

Signaturen können nur insoweit einem Schlüsselinhaber zugerechnet werden, als sich die Anwender im Umgang mit ihrem geheimen Schlüssel beziehungsweise der Chipkarte und der PIN korrekt verhalten werden. Verantwortung im Kooperationsakt heißt deshalb ständiges Aufpassen auf diese Utensilien. Dies ist gegenüber der eigenhändigen Unterschrift ungewohnt, denn diese kann weder gestohlen noch liegengelassen werden. Hierfür muss sich erst noch Sensibilität in der Gesellschaft ausbilden. Auf der Handlungsebene stellt sich die Frage, ob sich dieses Aufpassen zu einem Routinevorgang entwickeln wird wie das Mitführen des Wohnungsschlüssels oder der Kreditkarte? Bezüglich der Bewertung der digitalen Signatur durch die handelnden Personen stellt sich die Frage, ob die Menschen möglicherweise auf andere Aspekte als bei der Prüfung der eigenhändigen Unterschrift achten werden. Wird ein Kooperierender beispielsweise einem Partner Vertrauen schenken, der seine Karte nicht dabei hat oder die PIN von einem Zettel ablesen muss?

Als Rückbettungsstrategie bietet sich folgendes gestalterisches Vorgehen an: Um die Personen, in die ja indirekt vertraut werden soll, stärker ins Spiel zu bringen (sie zu verpflichten), sind biometrische, d.h. individuumsbezogene Verfahren wie beispielsweise der digitale Daumenabdruck, um die Chipkarte zu aktivieren (nicht jedoch als Bestandteil der Signatur), in Erwägung zu ziehen.

## 4.2 Die unpersönliche Signatur

Der eigenhändige Unterschriftszug (Krakel) verweist aufgrund seines individuellen Musters eindeutig auf den Unterzeichner. Der Blick auf die eigenhändige Unterschrift reicht in der Regel als Prüfverfahren aus. Die Signatur auf dem elektronische Dokument ist Ausdruck des geheimen Schlüssels.

Die Individualität, die die Signatur ausdrücken soll, ist formaler Natur. Als Manko wird u.a. benannt: „Ich finde hier nicht die Physiognomie meines Kooperationspartners.“ D.h. eine optische Kontrolle über individuelle Spuren des Partners, wie sie das Prüfen des biometrischen Musters des Unterschriftszuges auszeichnet, hat der Prüfer einer digitalen

Signatur nicht. Nur der Computer kann die Unversehrtheit einer digitalen Signatur erkennen. Auf das Anstoßen dieser maschinellen Prüfung wird aber oft verzichtet und in Analogie zur eigenhändigen Unterschrift nur auf den Namen im Ausdruck der Signatur geschaut.

Das alleinige Lesen des Namens verweist darauf, dass das „Angebot“, das die Technik zum Aufbau von Systemvertrauen „macht“, nicht wahrgenommen wird, sondern sich die Menschen weiterhin an den traditionellen Mitteln zum Aufbau von personalem Vertrauen orientieren wollen.

Der Name findet sich auf Papierdokumenten im eigenhändigen Unterschriftszug. Auch wenn der Unterschriftszug meist kaum zu entziffern ist, hat er doch symbolischen Charakter für den Kooperationsakt, ist Zeichen der Vertrauenswürdigkeit und - beim Unterzeichnen - der Verantwortungsübernahme. Die Präsentation der eigenhändigen Unterschrift gilt als aussagekräftig und hat für den Unterschriftsprüfenden die Funktion, im Prozess des Erkennens eines konstanten Musters Vertrauen aufzubauen. Und in Analogie dazu schaut der Empfänger eines elektronischen Dokumentes vorrangig auf den einzigen ihm noch gebliebenen Hinweis auf das Individuum, (Name im Zertifikat) und fühlt sich damit auf der sicheren Seite. Der Name alleine ist im Zertifikat jedoch nicht aussagekräftig, denn er ist kein einmaliges materiell fixierbares Muster. Der eigenhändigen Unterschrift entsprechende individuelle Spuren wird es im elektronischen Verfahren zwar auch geben können, aber diese sind nicht mehr sicher; sie können in das Dokument hineinkopiert worden sein. Damit verlieren sie ihre praktische Funktion des Verweisens auf eine bestimmte Person.

Bei der Entgegennahme papierener Dokumente werden viele individuelle Spuren übermittelt, die sich auf dem Papier materiell vergegenständlichen in Form des Briefpapiers, Briefkopfs, der Schrift und vor allem des bekannten Unterschriftszuges. Sie zusammen bilden eine Gestalt. Ein Anwender bezeichnet sie deshalb als die „Physiognomie“ des Kooperationspartners, die er auf diese Weise „im übertragenen Sinne sehen“ könne.

Denn der Eindruck eines guten Briefpapiers mit Wasserzeichen oder eines Eselsohrs im Papier ist ebenso wie eine bestimmte Verwischtheit oder Akkuratess auf Grund der Nutzung einer bestimmten Tinte weiterhin an den physischen Träger gebunden. Diese materiellen Spuren lassen sich elektronisch nicht erfassen und nicht abbilden.

Individuumsspezifisch wäre nur die formal-organisatorische Zuordnung eines Zertifikats zu einer Person oder Organisation. Die äußere Erscheinung der digitalen Signatur, möglicherweise auch des elektronischen Dokuments, dürfte daher für den Empfänger an Aussagekraft verlieren. Er selbst wird den Gegenüber nicht persönlich erkennen und identifizieren können anhand seiner Spuren; was ihm bleibt, ist die Bestätigung der Identität durch die Sicherungsinfrastrukturinstanz als „vertrauenswürdigen Dritten“.

So beklagten sich die Anwender darüber, dass sie sich mangels der offensichtlichen individuellen Spuren kein Bild vom Kooperationspartner - „der Physiognomie“ - machen konnten, so dieser noch unbekannt war, und sich deshalb auch weniger verbindlich fühlten. Es handelt sich weniger um die Funktion objektiver Sicherheit, die das Erkennen der Physiognomie dienen kann, was bei Erstkontakt ja besonders deutlich wird, sondern eher um die Nutzung von Menschenkenntnis und die Aktivierung der Vertrauensbildung auf Grund des Wiedererkennens eines vertrauten Musters.. Auch wenn diese Fähigkeit, gerade wo sie sich nur auf einen Unterschriftszug nebst schriftlichem Kontext stützt, vielleicht von sehr rational denkenden Personen als „Kaffeleserlesen“ abgetan wird, so lässt sich doch nicht ihre Funktion, auf diese Weise „ein Gefühl von Sicherheit“ zu entwickeln, wegdiskutieren. Im elektronischen Prüfverfahren gibt es für dieses Gefühl keine entsprechenden Ansatzpunkte.

Die Ersetzung des eigenhändigen Unterschriftszugs als biometrisches Muster, das per einfache Sichtkontrolle zu erkennen und prüfen ist, durch das Zertifikat erfordert ein Umdenken und Änderungen im Handeln. Von der Vielfalt an individuellen Zügen wird bei der digitalen Signatur nur noch die im Zertifikat dokumentierte Zuordnung eines Schlüssels zu einer Person zurückbleiben. Diese Zuordnung jedoch wird nicht in Form eines typischen Musters dem Augenschein ersichtlich, wie es Menschen bisher gewohnt sind, Individualität zu definieren, sondern indirekt in Form einer Garantieerklärung durch eine dritte Instanz.

Die Möglichkeit, personenbezogene Muster erkennen zu können, scheint somit ein Rückbettungsmechanismus zu sein. Technisch realisierbar wäre beispielsweise die Präsentation eines Pixelmusters der eigenhändigen Unterschrift oder das Einblenden eines Fotos nach dem Signaturprüfen. Allerdings wird es den materiellen Grund für das „Sich-sicher-Fühlen“ nicht mehr geben, nämlich die Fixierung biometrischer Spuren. Jedoch wird solch ein Schein von Individualität das subjektive Risikoempfinden minimieren und Systemvertrauen erhöhen (ähnlich wie der nette Versicherungsvertreter).

## 5 Fazit

Die digitale Signatur ist somit zunächst ein technisches Verfahren zum Erkennen von Manipulationen, das mittels einer übergeordneten sichernden dritten Instanz zusätzlich auch die Urheberschaft belegen kann. Im Gegensatz dazu ist die eigenhändige Unterschrift eine individuelle Entäußerung im bilateralen Akt der Kooperationspartner und ein Symbol der wechselseitigen Vertrauensgewährung. Wenn die digitale Signatur korrekt verwendet würde, könnte sie mehr Handlungssicherheit bieten als die eigenhändige Unterschrift. Insofern ist sie gerade für die Fälle sehr geeignet, in denen Formulare getauscht werden und wenig Möglichkeiten für zwischenmenschliche Vertrauensbildung besteht.

Es sind eine Vielzahl von „Fehlhandlungen“ festgestellt worden, die jedoch zu einem großen Teil der Analogisierung zur eigenhändigen Unterschrift geschuldet sind. Sie sind Ausdruck des Versuchs, Systemvertrauen um persönliche Momente anzureichern oder, wie Giddens sagt, entbettete Verhältnisse rückzubetten. Für den Einsatz digitaler Signaturen gilt so die Frage, wie das Verhältnis von „disembedding“ und „reembedding“ ausgestaltet ist; wo und wie hier Prozesse des „reembedding“ wirken können. D.h. die technische, organisatorische und kulturelle Gestaltung dieses Instruments ist von weitreichender Bedeutung.

Kulturelle Gestaltung ist Umdefinition. So wird die digitale Signatur möglicherweise weniger Nähe zur eigenhändigen Unterschrift als zu einem Siegel haben. Ein Siegel dient der Sicherung des Inhaltes und schützt vor Einblick durch Dritte. Das Siegelzeichen verweist zwar auf eine Person, ist jedoch keine individuelle Entäußerung. Es steht im Gegensatz zur eigenhändigen Unterschrift nicht in der Tradition der Kopräsenz und dem damit verbundenen Prinzip des Erkennens und Wiedererkennens eines Musters, einer Gestalt. Es ist damit aber auch weniger ein symbolisches Mittel der Kooperation sondern der Koordination. Die digitale Signatur wäre deshalb auch nicht Zeichen für vertrauensvolles, sondern regelgeleitetes Miteinander-Handeln. Die Umdefinition ist Ausdruck der Vorstellung von Verbindlichkeit in der hoch arbeitsteiligen Gesellschaft. Dass die Siegelfunktion nicht per se diese Umdefinition erfordert, zeigt die japanische Variante der Unterschrift. Die japanische Gesellschaft kennt keine eigenhändige Unterschrift. Vielmehr hat jede Person einen Stempel, der aus den eigens für ihn aus Kanji geschnitzten Namenszeichen besteht. Die Missbrauchs-

quote ist dort geringer als in westlichen Ländern mit der eigenhändigen Unterschrift. Ein Grund hierfür könnte die Einbindung in den kulturellen Kontext der Ehre sein. Vertrauensbildung und Verantwortungsübernahme sind somit stark kulturell geprägt, wobei Symbole eine wichtige Rolle spielen.

## Literatur

- Ammenwerth, Elske u.a. (1998): Sicherer mobiler Informationsaustausch in Praxis und Klinik – Ergebnisse der Simulationsstudie; in: Günther Müller, Kurt-Hermann Stapf (Hg.): *Mehrseitige Sicherheit in der Kommunikationstechnik*. Band 2. Bonn, 381-396
- Ammenwerth, Elske, Christel Kumbruck, Ulrich Pordesch (1999): Folgerungen zur Methode der Simulationsstudie; in: Alexander Roßnagel, Reinhold Haux, Wolfgang Herzog: *Mobile und sichere Kommunikation im Gesundheitswesen*. Wiesbaden, 253-274
- Bierhoff, Hans Werner, Ernst Buck (1984): Vertrauen und soziale Interaktion; Bericht Nr. 83 aus dem Fachbereich Psychologie der Philipps-Universität Marburg/Lahn
- Bizer, Johann u.a. (1995): Rechtsverbindliche Telekooperation in der elektronischen Vorgangsbearbeitung. GMD-Studien Nr. 261. Bonn-St. Augustin
- Bonin, Hinrich (1991): Kooperative Texterstellung; in: *Verwaltungsführung – Organisation - Personal* 4, 205–212
- Braczyk, Hans-Joachim u.a. (1998): Vertrauensbildung aus soziologischer Sicht – das Beispiel Sicherheit in der Kommunikationstechnik; in: Günther Müller, Kurt-Hermann Stapf (Hg.): *Mehrseitige Sicherheit in der Kommunikationstechnik*. Band 2. Bonn, 119-150
- Bullinger, Hans-Joerg, W. Brettreich-Teichmann, Hans-Peter Fröschle (1995): Koordination zwischen Markt und Hierarchie; in: *Office Management* 12, 18-22
- Döring, Andreas u.a. (1998): Risiken und Chancen für einen selbstbestimmten Umgang mit neuen Kommunikationstechniken im Gesundheitswesen; in: Günther Müller, Kurt-Hermann Stapf (Hg.): *Mehrseitige Sicherheit in der Kommunikationstechnik*. Band 2. Bonn, 159-180
- Dufft, Cornelius, Kurt-Herrmann Stapf: Der Einfluss von Wissen auf das subjektive Bild von Sicherheit; in: Günther Müller, Kurt-Hermann Stapf (Hg.): *Mehrseitige Sicherheit in der Kommunikationstechnik*. Band 2. Bonn, 275-294
- Erikson, Erik Homburger (1950): *Childhood and society*. New York
- Espey, Jürgen u.a. (1998): Wie alarmiert sind die Nutzer?; in: Günther Müller, Kurt-Hermann Stapf (Hg.): *Mehrseitige Sicherheit in der Kommunikationstechnik*. Band 2. Bonn, 233-248
- Giddens, Anthony (1996): *Konsequenzen der Moderne*. Frankfurt
- Goecke, Robert, Gerhard Hesch (1997): Telearbeits- und Service-Center. Keimzellen virtueller Unternehmen; in: *Office Management* 3, 46-48
- Gouldner, Alvin W. (1984): Etwas gegen nichts. Reziprozität und Asymmetrie; in: Alvin W. Gouldner (Hg.): *Reziprozität und Autonomie*, Frankfurt/M. 1984
- Hammer, Volker (Hg.) (1995): *Sicherungsinfrastrukturen. Gestaltungsvorschläge für Technik, Organisation und Recht*. Berlin
- Kumbruck, Christel (1999): „Angemessenheit für situierte Kooperation“ ein Kriterium arbeitswissenschaftlicher Technikforschung und -gestaltung“. Münster
- Lenk, Hans (1992): *Zwischen Wissenschaft und Ethik*. Frankfurt /M. 1992
- Loh, Werner (1990): Unverantwortbarer Fortschritt oder Fortschritt der Verantwortung?; in: *Ethik und Sozialwissenschaften* 1, 77-79
- Luhmann, Niklas (1973): *Vertrauen - Ein Mechanismus der Reduktion sozialer Komplexität*. Stuttgart
- Neuf, Hartmut, Jürgen Espey, (1998): Gefahren der Telekommunikation: Welche Risiken beachtet der Verbraucher?; in: Günther Müller, Kurt-Hermann Stapf (Hg.): *Mehrseitige Sicherheit in der Kommunikationstechnik*, Band 2. Bonn, 199-218

- Petermann, Franz (1985): Psychologie des Vertrauens. Salzburg
- Pordesch, Ulrich, Michael Schneider (1993): Anwendungsrisiken elektronischer Signaturverfahren; in: GMD-Spiegel 2, 35-39
- Pordesch, Ulrich (1993a): Experimente zur Verletzlichkeit im Rahmen der Simulationsstudie formularorientierte Vorgangssysteme. Provet-Arbeitspapier 106. Darmstadt
- Pordesch, Ulrich (1993b): Risiken elektronischer Signaturverfahren; in: Datenschutz und Datensicherung 10, 561-569
- Pordesch, Ulrich (1994): Anwendungsrisiken digitaler Signaturverfahren. Provet-Arbeitspapier 144. Darmstadt
- Pordesch, Ulrich (1999): Nachweis der Präsentation signierter Daten. GMD Report 68. Darmstadt
- Preisendörfer, Peter (1995): Vertrauen als soziologische Kategorie; in: Zeitschrift für Soziologie 4, 263-272
- Provet, GMD (1993): Elektronische Signaturverfahren in der Simulationsstudie. Aufsatzsammlung als Schwerpunktthema im: GMD-Spiegel 2, 30-51
- Rivest, Ronald W., Adi Shamir, Leonard M. Adleman (1978): A method for obtaining digital signatures and public key cryptosystems; in: Communications of the ACM, 120 ff.
- Roßnagel, Alexander u.a. (1994): Die Simulationsstudie Rechtspflege - Eine neue Methode zur Technikgestaltung für Telekooperation. Berlin
- Rudinger, Georg, Jürgen Espey, Peter Eßer (1998): Mehrseitige Sicherheit in der Praxisbewertung des Nutzers; in: Günther Müller, Kurt-Hermann Stapf (Hg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Band 2. Bonn, 249-274
- Rudinger, Georg u.a. (1998): Der menschliche Umgang mit Unsicherheit, Ungewissheit und (technischen) Risiken aus psychologischer Sicht; in: Günther Müller, Kurt-Hermann Stapf (Hg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Band 2. Bonn, 69-98
- Stapf, Kurt-Hermann (1998): Psychologische Betrachtungen zum Sicherheitsbegriff; in: Günther Müller, Kurt-Hermann Stapf (Hg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Band 2. Bonn, 45-68
- Sydow, Jörg, Achim Loose (1994): Vertrauen und Ökonomie in Netzwerkbeziehungen - Strukturations-theoretische Betrachtungen; in: Jörg Sydow, Arnold Windeler (Hg.): Management interorganisationaler Beziehungen. Vertrauen, Kontrolle und Informationstechnik. Opladen. 160-193
- Winnicott, Donald W. (1974): Reifungsprozesse und fördernde Umwelt. München 1974
- Zündorf, Lutz (1986): Macht, Einfluss, Vertrauen und Verständigung. Zum Problem der Handlungskoordination in Arbeitsorganisationen; in: Rüdiger Seltz, Ulrich Mill, Eckardt Hildebrandt (Hg.): Organisation als soziales System. Berlin, 33-56

Anschrift der Verfasserin:

Dr. habil. Dipl. psych. Christel Kumbruck  
Technische Universität Hamburg-Harburg  
Arbeitswissenschaft/1  
Schwarzenbergstr. 95  
D-21073 Hamburg

**Schlagworte: digitale Signatur, Entbettungsmechanismen, netzbasierte Organisation, Vertrauen**

**Hinweis:** Die Zeitschrift ARBEIT hat einen Preis für den besten Aufsatz ausgeschrieben. Am Ende des Heftes sind die Bedingungen beschrieben.