Rechtssicherheit trotz Anonymität in offenen digitalen Systemen*, *Teil 1*

Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann

Zusammenfassung: *Ausgehend von der zunehmenden Bedeutung der Abwicklung von Rechtsgeschäften über offene digitale Systeme wird die Forderung abgeleitet, diese Systeme so zu gestalten, daß ihre Benutzung unbeobachtbar durch Unbeteiligte und anonym vor Beteiligten stattfinden, aber dennoch die notwendige Rechtssicherheit garantiert werden kann. Es wird gezeigt, daß juristische Regelungen alleine nicht ausreichen, um dies überprüfbar garantieren zu können (Kap. 1).*

Als Ergänzung der juristischen Regelungen werden daher die bekannten technischen, d.h. informatischen Methoden und Vorschläge dargestellt, um einerseits die Unbeobachtbarkeit und Anonymität der Systembenutzung garantieren (Kap. 2) und andererseits unter Erhaltung der Anonymität über das offene System mit ausreichender Rechtssicherheit die typischerweise anfallenden Geschäfte abwickeln zu können (Kap. 3). Aufgrund der besonderen Wichtigkeit werden zwei Möglichkeiten zum betrugssicheren Werteaustausch (z.B. Informationsdienstleistung gegen Geld) zwischen anonymen Parteien (Kap. 4) und ein anonymes digitales Zahlungssystem und dessen Abwandlungen ausführlicher dargestellt (Kap. 5). Ein Ausblick auf offene Probleme und ein Fazit aus praktischer Sicht beschließen die Arbeit (Kap. 6).

Das Papier erscheint in zwei Teilen: der erste Teil enthält die Kapitel 1 bis 3, der zweite Teil die Kapitel 4 bis 6 sowie das Literaturverzeichnis für beide Teile.

1 Einführung

Mit der Einführung eines neuen Kommunikationssystems durch die Deutsche Bundespost, des ISDN (integrated services digital network), das zunächst nur alle schmalbandigen Kommunikationsdienste wie Telefon, Telex, Teletex etc. und später auch alle breitbandigen Kommunikationsdienste wie Fernsehen und Bildfernsprechen in sich vereinigen und den Benutzern durch wenige, „multifunktionale" Endgeräte anbieten wird [ScSc_84, ScSc1_84, ScSc_86], wird zugleich die Grundlage für die Einführung *offener digitaler Systeme* gelegt. Ein solches System soll potentiell allen Benutzern des ISDN zugänglich sein und spezielle Dienste anbieten. Möglichkeiten wären reine Informationsdienste, etwa in der Nachfolge von Bildschirmtext, die ihren Benutzern spezielle Datenbanken zugänglich machen, die Verbreitung von POS-Terminals oder „elektronische Marktplätze" [Riha_85, TuCh_85], die den Benutzern das Anbieten und Bestellen von Waren, das Überweisen von Geld, kurz das *Abwickeln von Rechtsgeschäften* verschiedenster Art erlauben.

Diese Verlagerung von Alltagsgeschäften in eine digitale Umgebung wird im wesentlichen zwei Probleme aufwerfen:

Zum einen gehen die heutigen Vorschriften über Rechtsgeschäfte meist von Willenserklärungen aus, die von Menschen aus Fleisch und Blut in unverfälschbarer Weise, etwa durch unterschriebene Dokumente, abgegeben werden, und deren Abgabe notfalls durch ebensolche Menschen bestätigt werden kann. In einem offenen digitalen System tritt an die Stelle des Menschen sein Rechner, der zudem keine materiellen unterschriebenen Dokumente erzeugt, sondern nur digital codierte Information, die beliebig kopiert werden kann. Das Erzeugen einer solchen Information, die z.B. die verbindliche Bestellung einer Ware darstellen kann, ist zudem auch weniger durch einen Menschen bezeugbar als wiederum durch eine Maschine, etwa einen Rechner der Post, die die Information über das ISDN dem Empfänger übermittelte.

Offensichtlich erfassen die hergebrachten Normen, insbesondere Formvorschriften und Konventionen darüber, was als Beweismittel betrachtet wird, nicht die neuen Bedingungen und müssen, damit Rechtssicherheit herrschen kann, angepaßt werden. Dabei muß darauf geachtet werden, daß die neuen Systeme und Normen dieselben Zwecke wie bisher erfüllen. Zum Beispiel erfüllt ein Verzicht auf Unterschriften wie etwa bei Bildschirmtext diese Forderung natürlich nicht, denn das technische System muß ein Äquivalent für Unterschriften anbieten, das es erlaubt, eine Erklärung in unverfälschbarer Weise einem Benutzer als Urheber zuzuordnen [Rede_84].

Zum anderen wird durch die Nutzung offener digitaler Systeme der Benutzer wesentlich durchschaubarer, als das bisher der Fall war.

So erfährt der Geschäftspartner zumeist viel genauer als bisher, was den Kunden interessiert, etwa beim Anbieten eines Lexikondienstes anstelle des Verkaufs des ganzen Lexikons oder bei Pay-TV anstelle pauschaler Verteilung von Fernsehprogrammen. In ähnlicher Weise können auch einige völlig neue Geschäftspartner, z.B. spezielle Auskunftssysteme, Rückschlüsse über ihre Kunden ziehen.

Des weiteren werden an vielen Geschäften mehr Partner als bisher beteiligt sein, so etwa die Banken bei Verwendung gewisser digitaler Zahlungssysteme (vgl. Kap. 5) an jedem Geldtransfer über das ISDN und bei Verwendung von POS-Terminals an fast jedem Einkauf, auch wenn die Ware nicht über das ISDN bestellt wird. Dies gilt insbesondere für Part-

* Dies ist eine in den Abschnitten 2.2.1.1, 3.1.2.1, 3.1.2.2, 5.3 und 7 überarbeitete und um den Abschnitt 5.6 ergänzte Fassung eines in „Computer und Recht" (Dr. Otto Schmidt, Köln) 3/10-12 (1987) erschienenen Artikels.

ner wie etwa die Post als Betreiber von Bildschirmtext, die aufgrund einer Vermittlerfunktion an mehreren verschiedenartigen Geschäften desselben Benutzers beteiligt sind.

Neben den Geschäftspartnern, die zwangsläufig gewisse Informationen erhalten müssen, können aber auch völlig Unbeteiligte durch Beobachten des offenen Systems oder des zur Kommunikation verwendeten ISDN Informationen über die Benutzer gewinnen. Beobachter könnten dabei die Betreiber sein, z.B. die Post oder Anbieter von Mehrwertdiensten, über sogenannte Trojanische Pferde (siehe 2.1) die Hersteller der verwendeten Soft- oder Hardware oder auch durch Abhören der Leitungen andere Interessierte.

Alle können zudem das erhaltene Wissen, da es bereits digital codiert vorliegt, beliebig speichern, besser auswerten als früher und mit den Informationen anderer vergleichen.

Die genannten Möglichkeiten der Informationsgewinnung betreffen natürlich nicht nur ausgewählte einzelne Benutzer, deren Persönlichkeitsrechte etwa durch das G10-Gesetz legal eingeschränkt werden, sondern viele der genannten möglichen Beobachter haben Gelegenheit, über sehr viele oder gar alle Benutzer eines Systems Daten zu sammeln, so daß hier die Möglichkeit zur Massenüberwachung gegeben ist (anders als bei den weiter bestehenden konventionellen Überwachungstechniken wie etwa Abhören, die aus Aufwandsgründen nur Individualüberwachung erlauben).

Insbesondere unter dem Gesichtspunkt des im Volkszählungsurteil des Bundesverfassungsgerichtes formulierten Rechtes auf informationelle Selbstbestimmung [Bund_83] ist zu bedenken, ob ein die Persönlichkeitsrechte aller stark gefährdendes System mit unserer Verfassung vereinbar ist.

Beide genannten Probleme, einerseits die Anpassung gültiger Normen an die neue Umgebung und die Gestaltung der Systeme in einer die Rechtssicherheit gewährenden Art, andererseits die Wahrung der Persönlichkeitsrechte, sind zu lösen, bevor ein System in Betrieb genommen werden darf. Zu zeigen, daß beide zusammen für offene digitale Systeme lösbar sind, und mögliche für die Praxis geeignete Ansätze hierzu darzustellen, ist das Ziel dieses Beitrags.

2 Anonymität

2.1 Anonymität per Gesetz

Der erste Ansatz, offene Systeme zu realisieren, die die Persönlichkeitsrechte ihrer Benutzer nicht gefährden und nicht zu Massenüberwachungen mißbraucht werden können, ist, die zur Überwachung notwendigen Handlungen per Gesetz zu verbieten, wie dies, wenn auch nicht in ausreichendem Umfang, in den Datenschutzgesetzen, durch das Fernmeldegeheimnis u.ä. geschieht.

Diese Handlungen bestehen im wesentlichen aus dem Erfassen von Daten durch Unbeteiligte, z.B. die Post, und dem unerwünschten Verarbeiten oder Weitergeben von erhaltenen Daten durch Beteiligte.

Sind solche Handlungen möglich, so stößt ihr gesetzliches Verbot an zwei prinzipielle Grenzen:

Die Einhaltung eines solchen Verbotes ist aufgrund der beliebigen Kopierbarkeit und Verarbeitbarkeit von Daten nicht kontrollierbar. Daten, selbst legal erhaltene, werden durch eine Verarbeitung nicht verändert, so daß eine Kontrolle der Daten permanent erfolgen müßte. Bereits eine Lücke in dieser Kontrolle könnte zum unbemerkbaren Weitergeben führen, und einmal erstellte Kopien außerhalb des legalen Bereiches sind praktisch jeder Kontrolle entzogen.

Selbst wenn doch einmal die unerlaubte Weitergabe bemerkt wird (bzw. gerade dann), kann bereits irreparabler Schaden entstanden sein, z.B. wenn personenbezogene Daten eines Benutzers veröffentlicht wurden.

An dieser Stelle kann man einwenden, daß doch zumindest in manche an einem Geschäft Unbeteiligte und Beteiligte ein gewisses Vertrauen gerechtfertigt erscheine: die Post als Betreiber des ISDN werde sicher ihre Kunden nicht beobachten, und auch Banken könne man zumindest den Willen zum vertraulichen Umgang mit Kundendaten nicht absprechen.

Leider lassen sich die möglichen interessierten Beobachter und Geschäftspartner nicht auf diesen Kreis beschränken. So kann zur Zeit weder die Post garantieren, daß die von ihr verwendete ISDN-Hardware und Software keine versteckten Systemteile enthält, die z.B. an den Hersteller, etwa im Zuge der bei Systemen dieser Größe häufigen Wartungsarbeiten, vertrauliche Informationen weitergeben (sogenannte Trojanische Pferde, vgl. [PoKl_78, Thom_84]), noch kann dies eine Bank für ihr Rechenzentrum tun. Ebensowenig kann eine Garantie für die Nichtanwendung normaler Abhörmechanismen oder die Verschwiegenheit von Angestellten gegeben werden, wobei jedoch für die Massenüberwachung ersteres generell und letzteres bei geeigneten Organisationsstrukturen weniger kritisch ist.

Eine rein juristische Lösung des Problems ist also unmöglich, so daß man zusätzlich versuchen muß, durch technische Maßnahmen die unerwünschte Erfassung und Verarbeitung von Daten zu verhindern. Dies ergibt sich auch durch eine sinngemäße Anwendung von § 6 BDSG (und Anlage, [GGSS_78]) auf offene digitale Systeme.

2.2 Technische Datenschutzmaßnahmen

Wollte man versuchen, die technischen Datenschutzmaßnahmen zentral durchzuführen, also durch den Systembetreiber selbst oder indem dieser unter öffentliche Kontrolle gestellt wird, so hieße dies, die Systemverwaltung sogenannten sicheren Geräten anzuvertrauen, die gewisse Daten gar nicht nach außen geben. Wegen der Komplexität solcher zentraler Geräte ist aber eine vollständige Untersuchung auf Trojanische Pferde mit den heute bekannten Methoden nicht möglich, auch müßte diese nach jeder Wartungsmaßnahme wiederholt werden, und nicht zuletzt dürfte die technische Zuverlässigkeit eines zentralen Gerätes, das auf wirkliche wie vermeintliche Angriffe auf seine Unausforschbarkeit mit einer Zerstörung zumindest seiner vertraulichen Daten reagieren muß, äußerst gering sein.

Auch technische Maßnahmen können das oben genannte Problem der beliebigen Kopierbarkeit und Verarbeitbarkeit bereits erfaßter Daten also nicht vollständig lösen. Wohl aber kann technisch garantiert werden, daß keine Daten über das notwendige Maß hinaus erfaßt werden können. Dies erzwingt, daß die technischen Datenschutzmaßnahmen im wesentlichen durch die Benutzer selbst durchgeführt werden müssen.

Letzteres wäre sogar dann vorzuziehen, wenn alle oben genannten technischen Probleme gelöst wären, weil nur dies den einzelnen Bürgern erlaubt, die Maßnahmen selbst zu überprüfen. Letzteres ist wichtig, da gemäß den Regeln des gesunden Menschenverstandes und der Begründung des Urteils des Bundesverfassungsgerichts zur Volkszählung vom Dezember 1983 [Bund_83 Seite 272] die Bürger nicht nur sicher und unbeobachtet sein, sondern sich auch so fühlen sollen. Außerdem erschwert eine dezentrale Realisierung

eine schnelle und heimliche Änderung der Datenschutzvorschriften durch den Staat.

Aus etwa denselben Gründen wie die folgenden Datenschutzmaßnahmen müssen auch die späteren Maßnahmen zum Erzielen von Rechtssicherheit im wesentlichen durch die Benutzer selbst, nicht etwa einen Systembetreiber, durchgeführt werden.

Bei der Durchführung all dieser Maßnahmen können die Benutzer sich aber der Unterstützung von Rechnern bedienen. Für diese Zwecke gibt es hinreichend kleine und billige Rechner, z.B. PCs, die kaum teurer sind als Terminals, die für die Teilnahme am offenen System ohnehin nötig sind. Diese können auch so zuverlässig und unter öffentlicher Kontrolle gebaut werden, daß sich jeder Benutzer zumindest darauf verlassen kann, daß sein eigener Rechner nicht gegen seinen Willen handelt, insbesondere keine Trojanischen Pferde enthält, die Daten über ihn ohne seinen Willen preisgeben. Im folgenden wird meist nicht mehr explizit unterschieden zwischen dem, was der Benutzer selbst tut, und dem, was er seinen Rechner tun läßt.

2.2.1 Unbeobachtbarkeit durch Unbeteiligte

Ein völlig unbeteiligter Beobachter eines Geschäftes, z.B. ein Abhörer oder die Post, muß und sollte keinerlei Information erhalten; das Geschäft sollte für ihn *unbeobachtbar* sein. Er sollte im Idealfall nicht einmal die Tatsache feststellen können, daß ein Geschäft abgewickelt wurde, zumindest aber nicht, zwischen welchen Partnern.

Wird ein Geschäft nur durch den Austausch von Nachrichten über ein Kommunikationssystem, z.B. das ISDN, abgewikkelt - wie wir es hier meist annehmen werden - so genügt hierfür die Anwendung eines geeigneten *Kryptosystems* und die Verwendung eines *Datenschutz garantierenden Kommunikationssystems*.

2.2.1.1 Kryptosysteme

Verschlüsselung der Daten mittels eines Kryptosystems soll garantieren, daß der Inhalt einer gesendeten Nachricht nur den Besitzern eines bestimmten Schlüssels zugänglich ist. (Gute und fundierte Einführungen in das Thema Kryptosysteme findet man z.B. in [Denn_82, Hors_85, Bras_88, DaPr_89].)

Hinsichtlich der erlaubten und möglichen Verteilungen dieser Schlüssel unterscheidet man zwischen *symmetrischen* und *asymmetrischen* Kryptosystemen. Erstere werden oftmals auch konventionelle Kryptosysteme, letztere Kryptosysteme mit öffentlichen Schlüsseln genannt.

In einem symmetrischen Kryptosystem (Bild 1), wozu alle klassischen Kryptosysteme gehören, wird die Kommunikation zwischen zwei Partnern dadurch gesichert, daß beide einen gemeinsamen geheimen Schlüssel kennen, der sowohl zur Ver- als auch zur Entschlüsselung dient.

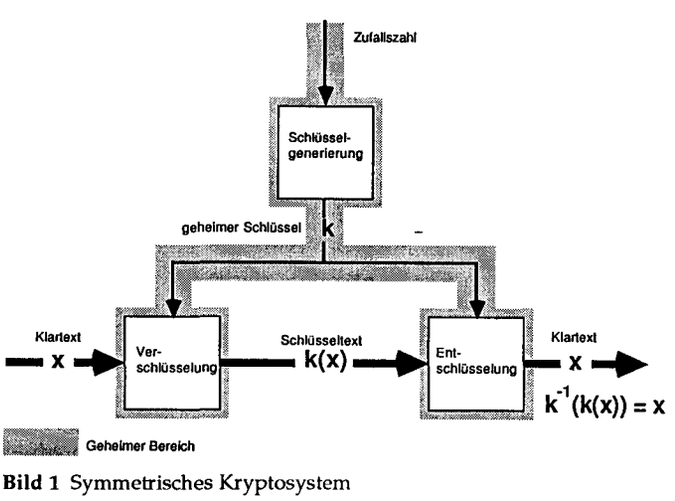

Bild 1 Symmetrisches Kryptosystem

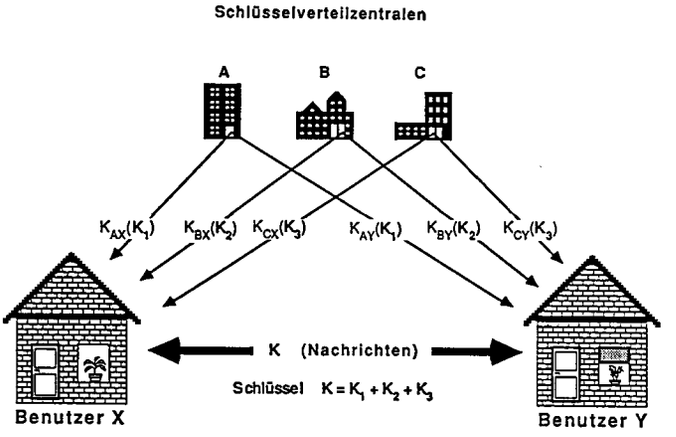

Bild 2 Schlüsselverteilung bei symmetrischem Kryptosystem

Damit wird ein Schlüssel nicht einem bestimmten Benutzer, sondern einer bestimmten Kommunikationsbeziehung zugeordnet. Um eine Kommunikationsbeziehung gesichert beginnen zu können, müssen sich beide Partner zuvor auf einen gemeinsamen Schlüssel einigen. Bei offenen digitalen Systemen muß dies innerhalb des Systems selbst erfolgen, da man nicht davon ausgehen kann, daß die Partner vorher schon in direktem Kontakt miteinander standen. Für dieses Schlüsselverteilproblem existieren im wesentlichen zwei Lösungsansätze.

Der klassische sieht die Verwendung einer Schlüsselverteilzentrale vor, mit der jeder Benutzer vor Beginn seiner Teilnahme am Systemgeschehen außerhalb des Systems einen Schlüssel vereinbart hat. Auf Anfrage generiert sie einen Schlüssel für eine Kommunikationsbeziehung und teilt ihn den künftigen Kommunikationspartnern unter Verwendung der mit den jeweiligen Benutzern vereinbarten Schlüssel vertraulich und authentisiert mit [DaPr_89].

Da eine solche Zentrale durch Kenntnis aller verwendeten Schlüssel potentiell alle gesendeten Nachrichten entschlüsseln kann, ist aus Datenschutzgründen diese einfache Lösung zumindest für offene Systeme nicht akzeptabel. Ein Ausweg ist die Verwendung vieler unabhängiger Schlüsselverteilzentralen, die je einen Schlüssel generieren und beiden Kommunikationspartnern mitteilen (Bild 2). Die Kommunikationspartner verwenden als Schlüssel die Summe aller mitgeteilten Schlüssel, so daß alle Schlüsselverteilzentralen zusammenarbeiten müßten, um die Summe zu errechnen und die Kommunikation zu überwachen.

Der zweite Ansatz verwendet zur Schlüsselverteilung ein asymmetrisches Kryptosystem, wie es unten beschrieben wird.

Das bekannteste moderne symmetrische Kryptosystem ist DES (data encryption standard [DES_77]), das vom NBS (der amerikanischen Normungsbehörde für den öffentlichen Bereich) als Zwischenlösung (bis zur Normung eines besseren) definiert und veröffentlicht wurde. Seine Sicherheit ist zwar nicht bewiesen, es hat aber bis heute allen (bekanntgegebenen) Versuchen standgehalten, es zu brechen. Schnelle Hard- und Softwareimplementierungen sind vorhanden (bis 20 Mbit/s [Abbr_84, AT&T_86, VHVD_88] auf einem Chip bzw. 715 kbit/s mit einem Apple Macintosh IIci (MC 68030, 25 MHz) [Aßma_89, PfAß_90]), so daß in Kombination mit einem asymmetrischen Kryptosystem zur Verteilung geheimer Schlüssel (hybride Verschlüsselung) ein standardmäßiger Einsatz im ISDN möglich wäre.

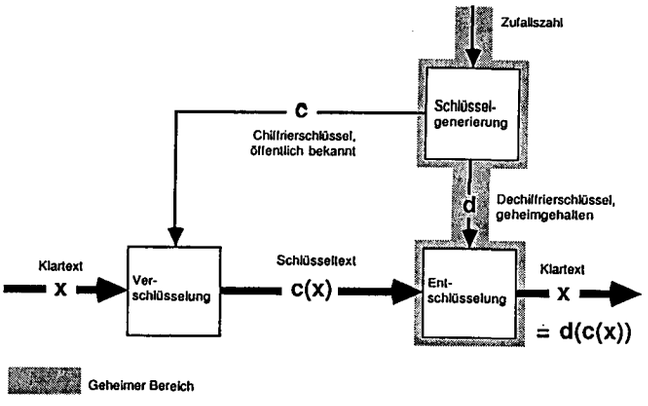

Bild 3 Asymmetrisches Kryptosystem

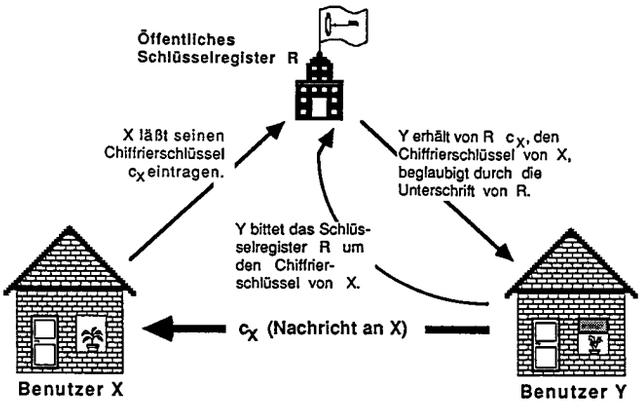

Bild 4 Schlüsselverteilung bei asymmetrischem Kryptosystem

Mit dem bei DES verwendeten Prinzip lassen sich durch Änderung von Teilfunktionen und Verwendung längerer Schlüssel viele weitere gut implementierbare symmetrische Kryptosysteme konstruieren, deren Sicherheit zwar auch nicht bewiesen, aber wesentlich weniger zweifelhaft ist als bei DES [Aßma_89, PfAß_90].

Daneben gibt es auch symmetrische Kryptosysteme, deren Sicherheit bewiesen wurde:

Die Vernam-Chiffre (one-time pad) verbirgt den Nachrichteninhalt perfekt, d.h. ein Angreifer erhält überhaupt keine Information, ist aufgrund ihres hohen Schlüsselverteilaufwandes (man benötigt für jedes Nachrichtenbit ein „neues" Schlüsselbit) jedoch nur für Spezialanwendungen geeignet [Shan_49].

Einige symmetrische Systeme sind „kryptographisch" sicher, d.h. ihr Brechen ist als ebenso schwer wie die Lösung eines wohluntersuchten und allgemein als schwer erachteten Grundproblems bewiesen [VaVa_85, LuRa_88]. Ein typisches solches Grundproblem ist die Berechnung der Primfaktoren einer gegebenen Zahl. Eine Faktorisierung beliebiger Zahlen, die aus sehr großen Primfaktoren zusammengesetzt sind, ist bisher, obwohl sich Mathematiker seit langer Zeit damit beschäftigen, praktisch unmöglich [LeMa_89]. Die „Unlösbarkeit" dieses Grundproblems (wie auch die der anderen verwendeten) konnte bislang selbst jedoch nicht bewiesen werden. Die Verschlüsselungsgeschwindigkeit kryptographisch sicherer symmetrischer Systeme ist der der folgenden asymmetrischen vergleichbar.

Die Idee der asymmetrischen Kryptosysteme (Bild 3) wurde erst 1976 veröffentlicht [DiHe_76] und löst das Schlüsselverteilproblem auf überraschend einfache Art: Statt einen einzigen Schlüssel zum Ver- und Entschlüsseln zu verwenden, verteilt man diese Funktion auf zwei zusammengehörige Schlüssel c und d. Der Schlüssel d soll nur zum Entschlüsseln (dechiffrieren) dienen und muß natürlich geheimgehalten werden, weshalb er auch privater Schlüssel genannt wird. Der Schlüssel c hingegen soll nur das Verschlüsseln (chiffrieren), nicht jedoch das Entschlüsseln ermöglichen, weshalb er veröffentlicht werden kann und daher auch öffentlicher Schlüssel genannt wird. Insbesondere darf man also keine realistische Möglichkeit haben, ein unbekanntes d aus dem zugehörigen c herzuleiten.

Rein theoretisch könnte man d aus c natürlich immer durch Durchprobieren aller möglichen Schlüssel bestimmen, denn nur das richtige d entschlüsselt alle mit c verschlüsselten Nachrichten richtig. Es muß daher so viele Möglichkeiten geben, daß dies praktisch keinerlei Erfolg verspricht.

Außerdem müssen, damit niemand kurze Standardnachrichten erraten und mit dem öffentlichen Schlüssel testen kann, Nachrichten mehrere Verschlüsselungen besitzen. Dies kann man erreichen, indem man die Nachrichten vor der Verschlüsselung mit zufällig gewählten Zeichenfolgen verlängert oder indem man ein bereits indeterministisch verschlüsselndes Kryptosystem (probabilistic encryption, [GoMi_84, BlGo_85]) verwendet.

Einfacher als das Herleiten von d aus c muß hingegen das Generieren eines beliebigen Paares von zueinander passenden c und d sein, da dies der Schlüsselbesitzer am Anfang selbst durchführen muß.

Durch ein asymmetrisches Kryptosystem entsteht die Möglichkeit, einen Schlüssel oder genauer ein Schlüsselpaar (c, d) statt einer Kommunikationsbeziehung einem einzelnen Benutzer zuzuordnen, der sich zudem diesen Schlüssel selbst generieren kann. Möchte jemand mit diesem Benutzer gesichert kommunizieren, so muß er sich lediglich dessen öffentlichen Chiffrierschlüssel c besorgen. Dies kann entweder durch eine offene Anfrage an den gewünschten Benutzer geschehen, wodurch allerdings Authentikationsprobleme entstehen [Inge_84, RiSh_84], oder unter Verwendung zentraler, gegen Manipulation gesicherter Register (Bild 4), deren Verwalter jetzt durch die Kenntnis der öffentlichen Schlüssel keine Möglichkeit zum Mithören verschlüsselter Nachrichten mehr erhalten.

1978 wurde mit RSA das erste und nach wie vor bekannteste asymmetrische Kryptosystem (Ver- und Entschlüsselungsfunktion sowie Schlüsselgenerierungsfunktion entsprechend obigen Anforderungen) veröffentlicht [RSA_78].

Die Sicherheit von RSA konnte bislang nicht bewiesen werden. Es wird allgemein vermutet, daß das Entschlüsseln nur mit Kenntnis des öffentlichen Schlüssels so schwer ist wie die Gewinnung der Primfaktoren einer gegebenen Zahl. Einzelne Nachrichten können jedoch durch aktive Angriffe entschlüsselt werden [Davi_82]. Durch Kombination mit einem passenden Redundanzprädikat (z.B. [PfPf_89]) kann die Gefahr aktiver Angriffe praktisch ausgeschlossen werden. Auch die Sicherheit dieser Kombinationen ist bislang allerdings unbewiesen. Hardwareimplementierungen von RSA erreichen Verschlüsselungsraten von 200 kbit/s (bei einem Modulus von 660 bit, [Sedl_88]), Softwareimplementierungen sind deutlich langsamer (z.B. 57 bit/s auf einem IBM PC (intel 80 88, 4,77 MHz) [Bras_88 Seite 31]).

Es sei angemerkt, daß es asymmetrische Kryptosysteme gibt, deren Sicherheit gegen passive Angriffe als so schwer wie Faktorisieren bewiesen wurde [GoMi_84, BlGo_85]. Es gibt allerdings (noch) keine asymmetrischen Kryptosysteme, die als gegen aktive Angriffe sicher bewiesen werden konnten. (Für das in [BlFM_88] skizzierte angeblich beweisbare System konnte noch kein Sicherheitsbeweis gefunden werden [BeMi_89].)

Die Verwendung eines asymmetrischen Kryptosystems wie RSA+Redundanzprädikat, entweder zum Verschlüsseln selbst oder nur am Anfang einer Geschäftsbeziehung zum Austausch eines geheimen Schlüssels eines schnelleren symmetrischen Kryptosystems, kann die geforderte Geheimhaltung des Inhalts von Nachrichten vor Unbeteiligten unserer Meinung nach hinreichend sicher garantieren.

Daher ist eine Normung eines asymmetrischen Kryptosystems zum Schlüsselaustausch sowie eines schnellen symmetrischen Kryptosystems zur Ver- und Entschlüsselung der Nutzdaten dringend notwendig, soll das ISDN ein *offenes* System bilden. Andernfalls ist Datenschutz (ebenso wie Datensicherheit) nur innerhalb *geschlossener* Benutzergruppen, die sich jeweils auf ein Kryptosystem geeinigt haben, erreichbar.

Dies ist ein zwar altbekanntes, aber dennoch ungelöstes organisatorisches Problem: international und national wurde zwar versucht, RSA und DES zu normen, doch sind diese Versuche abgebrochen worden [WaPP_87]. Statt dessen wurde durch die ISO lediglich eine Möglichkeit geschaffen, beliebige Kryptosysteme (durch Beschreibung der Schnittstellen) zu registrieren. Eine Bewertung der registrierten Kryptosysteme ist nicht vorgesehen [DaPr_89 Seite 347].

Es ist zu hoffen, daß der fortdauernde Mangel an Normen wenigstens die Deutsche Bundespost als Betreiber des ISDN anspornt, geeignete öffentlich validierte Kryptosysteme zu standardisieren.

2.2.1.2 Datenschutz garantierende Kommunikationssysteme

Ein Datenschutz garantierendes Kommunikationssystem garantiert seinen Benutzern, daß der Sender bzw. Empfänger einer Nachricht ohne dessen Mitwirkung nicht festgestellt werden kann, insbesondere auch nicht durch den Betreiber des Kommunikationssystems (was die Hauptschwierigkeit ist) oder den Kommunikationspartner. Da die bekannten Konzepte für Datenschutz garantierende Kommunikationssysteme und ihre Realisierbarkeit an anderer Stelle [PfPW_88, Pfit_90] eingehend diskutiert sind und für das Verständnis des folgenden nur das Wissen um ihre Existenz wichtig ist, wird hier auf eine genauere Beschreibung verzichtet.

2.2.2 Anonymität vor Beteiligten

Unbeobachtbarkeit eines Geschäftes auch vor einem Beteiligten zu fordern ist offenbar sinnlos. Um die Erfassungsmöglichkeit unnötiger personenbezogener Daten zu verhindern, ist hier vielmehr das Ziel, die Identität eines Benutzers so weit wie möglich vor seinen Partnern zu verbergen, ihn also *anonym* zu halten.

Für die Stärke von Anonymität gibt es drei Kriterien.

Das erste ist das verwendete *Angreifermodell*, das beschreibt, vor welchen Partnern Anonymität herrschen soll und ob diese bestehen bleibt, wenn mehrere Partner oder auch Unbeteiligte ihre Informationen zusammentragen. Hierzu gehört insbesondere die Frage, ob es speziell vorgesehene Instanzen gibt, die im Streitfall auf Wunsch eines Geschäftspartners die Anonymität des anderen aufheben können. Wenn immer möglich, sollte letzteres vermieden werden, da, wenn bereits wenige Instanzen zusammen die Anonymität aufheben können, diese eine zu starke Machtposition haben, wogegen die Aufhebung zu unzuverlässig wird, wenn es sehr viele sein müssen (im Grenzfall die Gesamtheit aller Benutzer).

Zum zweiten kann man bezogen auf einen bestimmten Angreifer fragen, unter *wieviel möglicherweise Handelnden* sich der wirklich Handelnde verbirgt. Bei offenen Systemen sollten, wenn möglich, immer alle Benutzer bei allen Handlungen als Handelnde in Frage kommen. Praktische Grenzen kann es allerdings durch das Leistungsvermögen des Datenschutz garantierenden Kommunikationssystems geben [PfPW_88, Pfit_90], so daß etwa der eine Erklärung Abgebende bei Zusammenarbeit seines Geschäftspartners und des Netzbetreibers sich zwar unter vielen, nicht aber unter allen Benutzern verbergen kann. Dabei ist zu beachten, daß die Anzahl der möglichen Handelnden so groß sein muß, daß der Schaden, der nach einer Deanonymisierung einem einzelnen entstünde, nicht einfach allen möglichen Handelnden zugefügt werden kann, ohne daß der Schädiger dadurch einen größeren Nach- als Vorteil gewinnt [Mt 2,16]. Zum Beispiel könnte, wenn sich unter nur 10 Personen bekanntlich ein Kunde eines Verlages für verfassungsfeindliche Schriften befindet, die Verfassungstreue aller 10 in Frage gestellt und ihnen damit eine Anstellung in manchen Bereichen erschwert werden.

Drittens kann man die Anonymität nicht nur bzgl. isolierter Handlungen betrachten, sondern muß auch berücksichtigen, inwieweit der gerade betrachtete Angreifer mehrere Geschäfte oder Geschäftsteile miteinander in Beziehung setzen, sie *verketten* kann. Konkret besteht solch eine Verkettung meist darin, daß der Partner weiß, daß zwei Handlungen von derselben Person ausgeführt wurden. Die Verkettbarkeit muß aus Gründen des Datenschutzes möglichst gering gehalten werden, andererseits kann sie aus Gründen der Rechtssicherheit manchmal gewollt sein, insbesondere zwischen Teilen desselben Geschäfts oder etwa bei mehrfacher Kommunikation mit einer Bank zu Authentikationszwecken.

Die Stärke der Anonymität eines Benutzers wird dabei nicht nur durch die Kennzeichen bestimmt, die der Partner automatisch über den Benutzer erfährt, etwa Art und Uhrzeit des abgewickelten Geschäfts, sondern vor allem durch eigens gewählte Kennzeichen wie Kennummern oder digitale Signaturen (s. 3.1.2.1), sogenannte *Pseudonyme*.

Eine aus praktischer Sicht zweckmäßige grobe Einteilung von Pseudonymen nach der Stärke der durch sie realisierten Anonymität ist in Bild 5 dargestellt.

Ein Pseudonym wird als Personenpseudonym bezeichnet, wenn sein Besitzer es für viele verschiedene Geschäftsbeziehungen über lange Zeit hinweg verwendet, es somit einen Namensersatz darstellt. Hinsichtlich der Verkettungsmöglichkeiten mit der Person seines Besitzers können grob drei Arten von Personenpseudonymen unterschieden werden.

Betrachtet man den Zeitpunkt, zu dem ein Personenpseudonym erstmals verwendet wird, so ist bei öffentlichen Personenpseudonymen die Zuordnung zu einer Person zumindest im Prinzip allgemein bekannt (z.B. Telefonnummern), bei nichtöffentlichen Personenpseudonymen ist diese Zuordnung nur wenigen Stellen bekannt (z.B. Kontonummern ohne Nennung des Namens oder nicht im Teilnehmerver-

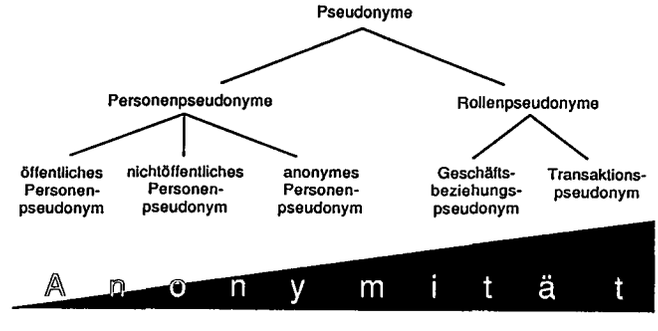

Bild 5 Einteilung der Pseudonyme nach ihrem Personenbezug

zeichnis aufgeführte Telefonnummern) und bei anonymen Personenpseudonymen ist diese Zuordnung nur dem Besitzer bekannt. Bei Verwendung von Personenpseudonymen sammelt sich bei einem Beobachter laufend personenbezogene Information an, so daß nach einer gewissen Zeit der Besitzer eines nichtöffentlichen oder anonymen Personenpseudonyms deanonymisiert werden kann. Jedes Personenpseudonym ist also ein potentielles Personenkennzeichen.

Diesen Nachteil vermeiden Rollenpseudonyme, die im Gegensatz zu Personenpseudonymen nicht der Person, sondern nur ihrer momentan ausgeübten Rolle zugeordnet sind. Geschäftsbeziehungspseudonyme sind solche Rollenpseudonyme, die für viele Transaktionen verwendet werden, z.B. eine Kontonummer bei den vielen Buchungen eines Kontos. Transaktionspseudonyme hingegen werden nur für eine Transaktion verwendet, z.B. Kennwörter bei anonym aufgegebenen Chiffreanzeigen. Bei Verwendung von Rollenpseudonymen können verschiedene Parteien über den Pseudonymträger gesammelte Information zumindest nicht einfach über die Gleichheit von Pseudonymen, sondern allenfalls über Korrelation von Zeiten, Geldbeträgen etc. verketten. Aber trotzdem besteht bei Geschäftsbeziehungspseudonymen die Gefahr, daß bei intensiv genutzten Beziehungen der Partner genügend pseudonymbezogene Information zur Deanonymisierung erhält. Aus der Sicht des Datenschutzes sollten daher, wenn immer möglich, Transaktionspseudonyme verwendet werden.

Wird im folgenden ein Pseudonym genauer angesprochen, etwa als das Pseudonym, das eine Person X bei einer Transaktion t, in der sie in der Rolle R (z.B. Kunde) auftritt, gegenüber einer anderen Person, die in einer Rolle S (z.B. als Dienstanbieter) auftritt, verwendet, so wird dies mit $p_R^S(X,t)$ bezeichnet. Im Einzelfall überflüssige Teile einer solchen Bezeichnung, z.B. die Transaktion bei Geschäftsbeziehungspseudonymen, werden weggelassen.

Kommunikation zwischen solchermaßen voreinander anonymen Partnern ist, wie in 2.2.1.2 bereits erwähnt, über ein Datenschutz garantierendes Kommunikationssystem ohne weiteres möglich, denn es gestattet, Nachrichten ohne Absenderangabe zu senden und unter beliebigen Pseudonymen zu empfangen, die nicht (wie sonst Adressen) den physikalischen Ort des Benutzers oder gar ihn selbst bezeichnen. Ebensowenig wird die Verwendung eines Kryptosystems erschwert, da die Schlüssel eines asymmetrischen Kryptosystems, das entweder selbst zum Verschlüsseln oder zum Schlüsselaustausch für ein symmetrisches System verwendet wird, statt identifizierbaren Benutzern auch Pseudonymen zugeordnet sein können.

Nachdem in diesem Kapitel gezeigt wurde, daß Anonymität für überprüfbaren Datenschutz in offenen digitalen Systemen notwendig und technisch realisierbar ist, soll in den folgenden Kapiteln behandelt werden, wie die gewünschte Rechtssicherheit erreicht werden kann, ohne die Anonymität etwa bei der Authentikation wieder aufzugeben.

3 Rechtssicherheit von Geschäftsabläufen unter Wahrung der Anonymität

In diesem Kapitel wird allgemein untersucht, was bei der Gestaltung von Geschäftsabläufen zu beachten ist, um Rechtssicherheit trotz Anonymität zu garantieren, ohne hierbei auf die derzeitige juristische Situation näher einzugehen (siehe hierzu [Rede_84, Clem_85, Köhl_86, Rede_86]).

Dazu werden wir in der Reihenfolge vorgehen, in der auch die Abwicklung des Rechtsgeschäfts mitsamt eventueller Schadensregulierung erfolgt. Vieles im folgenden Gesagte gilt auch für nicht anonyme Geschäftsabläufe in offenen digitalen Systemen, da auch dort davon auszugehen ist, daß sich Geschäftspartner am Anfang weder persönlich kennen noch in üblicher Weise voreinander ausweisen können, so daß anfänglich Anonymität (wenn auch nicht Unbeobachtbarkeit) herrscht.

3.1 Willenserklärungen

3.1.1 Anonymes Abgeben und Empfangen

Die Möglichkeit, Erklärungen anonym abzugeben und zu empfangen, ist bereits durch das Datenschutz garantierende Kommunikationssystem gegeben.

Wenn korrespondierende Erklärungen abgegeben werden sollen, bei denen man wünscht, daß entweder alle Beteiligten diese unterschreiben oder keiner (was bei den meisten für offene Systeme vorgesehenen Geschäften nicht der Fall ist), kann man dies wie einen kompletten Geschäftsablauf zum Austausch unterschriebener Erklärungen auffassen und etwa so abwickeln wie den nachher ausführlicher behandelten Austausch von Ware gegen Geld. Wo gewünscht, können spezielle Vertragsabschlußprotokolle [BGMR_85, EvGL_85] verwendet werden, die einen fast gleichzeitigen Austausch der Erklärungen erlauben, ohne dabei die Dienste eines Dritten in Anspruch nehmen zu müssen. Allerdings erhöhen solche Vertragsabschlußprotokolle den Kommunikationsaufwand stark.

3.1.2 Authentikation von Erklärungen

Häufig muß der eine Erklärung Abgebende eine Berechtigung zur Abgabe vorweisen. Ein wesentliches Hilfsmittel, um dies über ein Kommunikationssystem tun zu können, sind *digitale Signaturen* [Denn_82, Akl_83, GoMR_88, Bras_88].

3.1.2.1 Digitale Signaturen

Anstelle der eigenhändigen Unterschrift soll in Rechtsgeschäften über offene digitale Systeme eine sogenannte digitale Signatur dazu dienen, sicherzustellen, daß eine bestimmte Erklärung von einer bestimmten Person (oder auch Personengemeinschaft etc.), gekennzeichnet durch ein Pseudonym, abgegeben wurde.

Die Grundforderungen an eine digitale Signatur sind daher:

1. Niemand außer dem Besitzer eines Pseudonyms sollte fähig sein, ein Dokument mit der zu diesem Pseudonym gehörenden Signatur zu versehen.
2. Jeder kann nachprüfen, ob eine bestimmte Erklärung mit einer zu einem bestimmten Pseudonym gehörenden Signatur versehen ist.

Die erste Forderung bezieht sich dabei nur auf den Willen des Benutzers: Natürlich kann in einem rein digitalen System niemand einen Benutzer daran hindern, einem anderen Benutzer zu gestatten, unter einem von ihm verwendeten Pseudonym zu handeln. Dies entspricht der auch heute gegebenen Möglichkeit, einem anderen beliebig viele Blankounterschriften zur Verfügung zu stellen, und kann höchstens dem Benutzer selbst schaden, da man auch hier davon ausgehen muß, daß die so zustandegekommenen Erklärungen dem Besitzer des Pseudonyms als seine eigenen zugerechnet werden.

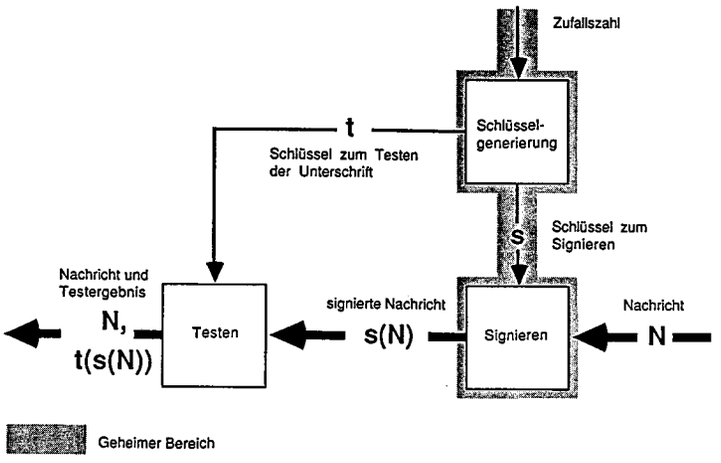

Bild 6 Signaturssystem

Der einfache Ansatz, auf die Einzigartigkeit der Pseudonyme zu vertrauen und diese wie herkömmliche Unterschriften der Erklärung beizufügen, genügt obigen Anforderungen leider nicht, denn jeder, der einmal eine unterschriebene Erklärung von einem Benutzer erhalten hätte, könnte das beigefügte digitale Pseudonym auf beliebig viele weitere Erklärungen kopieren. Insbesondere zählt zu diesem ungenügenden Ansatz die bisweilen diskutierte Möglichkeit, eine digitalisierte Kopie der handgeschriebenen Unterschrift zur Authentikation von Erklärungen zu verwenden, denn auch diese läßt sich, selbst wenn sie quer über eine Papierversion der Erklärung geschrieben war, in der digitalen Version mühelos von der Erklärung trennen und weiterkopieren. (Die Gedanken aus [Köhl_86] sind hier nicht anwendbar, da dort die Faksimileunterschriften wie bei Banknoten mit speziellen Papierformularen kombiniert werden, die nicht im digitalen System verschickt werden können. Außerdem ist schon beim heutigen Stand der Kopiertechnik der Aufdruck solcher Formulare nicht sicherer als die eigenhändige Unterschrift, höchstens noch die Papierstruktur o.ä.).

Deswegen benötigt man auch im nichtanonymen Fall ein vom Namen verschiedenes digitales Pseudonym (öffentliches Personenpseudonym), was einer der Gründe ist, ihn als Spezialfall des anonymen aufzufassen.

Abhilfe gegen obiges Problem schafft ein *digitales Signatursystem* (Bild 6). Ein solches ordnet jedem Pseudonym ein spezielles Funktionenpaar (s, t) zu; die Signierfunktion s dient zum Unterschreiben einer Nachricht und ist nur dem Besitzer des Pseudonyms bekannt, während das Testprädikat t dazu dient, zu testen, ob eine Nachricht mit s unterschrieben wurde. Das Testprädikat t kann jedem bekannt sein, insbesondere kann das Signatursystem stets so gewählt werden, daß der signierten Nachricht s(N) sowohl die Nachricht N selbst als auch das Testprädikat t entnommen werden kann.

Falls es die Realisierung des Signatursystems zuläßt, wird man das Testprädikat t (d.h. dessen Beschreibung) selbst als Pseudonym verwenden [Chau_81].

Bei praktischem Einsatz besteht diese Beschreibung des Testprädikats wie bei Kryptosystemen nur noch in einer Art Schlüssel, der in eine ansonsten allgemein bekannte Testfunktion eingesetzt wird, die standardisiert sein muß, so daß jeder jede Unterschrift ohne große Mühe testen kann.

Hier sei noch einmal (vgl. 2.2) erwähnt, daß ein Benutzer sich zum Testen, aber vor allem auch zum Unterschreiben von Nachrichten aus Aufwandsgründen eines Rechners bedienen muß. Da dieser die geheime Signierfunktion enthält, ist es hier fast noch wichtiger als bei der Anonymität, daß er sich völlig unter der Kontrolle seines Benutzers befindet. Dazu gehört, daß er seinen rechtmäßigen Benutzer erkennt und daß die Kommunikation zwischen Benutzer und Rechner ohne Zwischenschaltung anderer, nicht unter der Kontrolle des Benutzers stehender Geräte erfolgt.

Um einem Rechner das Erkennen eines rechtmäßigen Benutzers zu ermöglichen, werden zur Zeit Paßwort-Mechanismen verwendet (PIN, personal identification number); in Zukunft wäre aber auch die zusätzliche Verwendung biometrischer Daten, z.B. des Fingerabdrucks, zur Identifikation denkbar. Dieses würde das Erkennen zwar, außer bei Personen, die sich gar keine PIN merken können oder sie auf die Chipkarte schreiben, kaum zuverlässiger oder sicherer machen (auch Fingerabdrücke kann man nachahmen), könnte aber im normalen Betrieb verhindern, daß mehrere Personen (z.B. eine Familie) dieselbe Signatur verwenden und damit eine signierte Nachricht keiner einzelnen Person zugeschrieben werden kann.

Sofern der Zugang zum offenen System nicht nur von der Wohnung des Benutzers aus erfolgen soll, so daß der Rechner tragbar sein muß, muß dieser also dennoch über eine eigene Tastatur und eine eigene Anzeige verfügen, also äußerlich eher einem kleinen Taschenrechner als einer heutigen Chipkarte ähneln.

Ein einfaches und bekanntes Signatursystem erhält man bei Verwendung des asymmetrischen Kryptosystems RSA (vgl. 2.2.1.1):

Hier soll die Verschlüsselungsfunktion c eines Benutzers, die ja öffentlich bekannt sein darf, als Testprädikat verwendet werden. Das Anwenden der Entschlüsselungsfunktion d auf eine gegebene Nachricht gilt als Unterschreiben derselben. Dies kann tatsächlich niemand außer dem Besitzer des Pseudonyms, der ja als einziger d kennt, wenn er das Schlüsselpaar selbst erzeugt hat. Aufgrund der schönen Eigenschaft von RSA, daß sich, wenn man auf eine Nachricht erst die Ent- und dann die Verschlüsselungsfunktion anwendet (also andersherum als für die Geheimhaltung von Nachrichten notwendig), auch wieder die ursprüngliche Nachricht ergibt, kann jeder testen, ob eine Erklärung durch den Besitzer eines bestimmten Pseudonyms unterschrieben wurde, indem er die „entschlüsselte" Erklärung mit c verschlüsselt und prüft, ob sich wieder die richtige Erklärung ergibt. Da die Sicherheit von RSA nicht bewiesen ist, ist selbstverständlich auch die Sicherheit des auf RSA beruhenden Signatursystems unbewiesen.

Eine empfehlenswerte Alternative zu RSA stellt das GMR-Signatursystem dar [GoMR_88].

Dieses System ist ähnlich effizient wie RSA, bietet jedoch den Vorteil, daß es selbst gegen die denkbar stärksten (d.h. adaptiven aktiven) Angriffe als kryptographisch sicher bewiesen wurde: sein Brechen ist äquivalent zur Faktorisierung einer gegebenen Zahl bestehend aus zwei großen Primzahlen eines bestimmten Typs. Das GMR-System ist etwas komplexer als das RSA-System.

Wo möglich sollte das GMR- dem RSA-Signatursystem vorgezogen werden.

In Bild 7 (s. nächste Seite) ist die Übergabe einer signierten Nachricht vom Benutzer X an den Benutzer Y dargestellt, wobei X das Pseudonym p_A (für Abgebender) verwendet; links in einer funktionalen Schreibweise, rechts in der für den Rest des Papieres gewählten graphischen Notation, in der Nachrichten als Dokumente und Signaturen als Siegel dargestellt werden.

Für manche Anwendungen ist es sinnvoll, für digitale Signatursysteme zusätzliche Eigenschaften zu fordern:

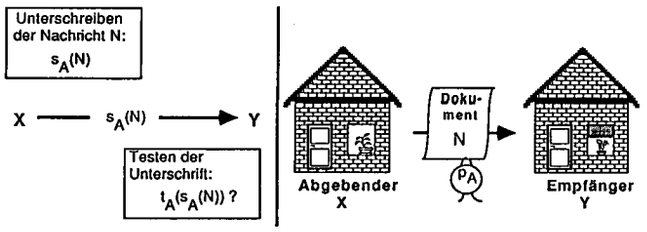

Bild 7 Übergabe einer signierten Nachricht von X an Y, in funktionaler Schreibweise links, in graphischer rechts

Der Empfänger z.B. einer mit GMR signierten Nachricht kann diese jedem anderen Teilnehmer zeigen und ihn damit von der Authentizität der Nachricht überzeugen. Der Unterzeichner hat über das Weitergeben seiner Signatur keine Kontrolle. Dieser Mangel wird durch *nicht herumzeigbare Signaturen* (undeniable signatures [ChAn_89]) behoben: Damit ein anderer Teilnehmer die Echtheit der Signatur glaubt, muß der angebliche Unterzeichner befragt werden; dieser kann von ihm tatsächlich geleistete Unterschriften nicht ableugnen.

Jedes Signatursystem (wie auch jedes asymmetrische Kryptosystem) kann mit hinreichend großem Aufwand gebrochen werden. In üblichen Signatursystemen trägt das Risiko hierfür der Unterzeichner. Durch ein *Knack-Schnapp-Signatursystem* [WaPf_89, WaPf1_89, Pfit_89, Bleu_90, BlPW_90] kann dieses Risiko auf den Empfänger verlagert werden: wird eine Unterschrift gefälscht, so kann der angebliche Unterzeichner diese Fälschung jedem Dritten nachweisen.

Eine weitere und im folgenden auch wirklich benötigte Variante, die *blind geleisteten Unterschriften*, werden in Abschnitt 3.1.2.2 beschrieben.

Nicht zu verwechseln mit digitalen Signatursystemen sind sogenannte *digitale Identifikationssysteme*. Während der Empfänger einer signierten Nachricht auch einem Dritten gegenüber die Signatur (und damit evtl. die Authentikation einer Erklärung) nachweisen kann, erlaubt ein Identifikationssystem dem Empfänger lediglich, den Abgebenden einer Erklärung zum Zeitpunkt der Abgabe als Besitzer eines bestimmten Pseudonyms zu identifizieren [WeCa_79, Bras_83, FiSh_87, Simm_88].

Der Einfachheit halber wird der Abgebende hierzu ein (möglicherweise speziell geformtes) Pseudonym der Erklärung beilegen oder die Erklärung mit einem nur ihm und dem ihn Identifizierenden bekannten Schlüssel eines symmetrischen Kryptosystems verschlüsseln. Nach Empfang der Erklärung kann ein Dritter die Authentikation der Erklärung jedoch nicht mehr überprüfen (wie schon oben erwähnt), so daß digitale Identifikationssysteme aus Gründen der Rechtssicherheit zur Authentikation einer Erklärung ungeeignet erscheinen.

3.1.2.2 Formen der Authentikation

Je nachdem, woher die Berechtigung zur Abgabe der Erklärung bezogen wird, kann man zwischen *Eigenauthentikation* und *Fremdauthentikation* unterscheiden.

Eigenauthentikation ist dann gegeben, wenn der Abgebende sich auf eine bereits früher von ihm selbst abgegebene Erklärung beruft, z.B. bei der endgültigen Bestellung einer Ware auf die Anfrage nach einem verbindlichen Angebot.

Hier will der Erklärende also zeigen, daß beide Erklärungen von derselben Person abgegeben wurden. Dies stellt eine gewollte Verkettung verschiedener Erklärungen dar und kann dadurch erreicht werden, daß der Abgebende in beiden Erklärungen dasselbe digitale Pseudonym verwendet und die Erklärungen mit der dazu gehörenden digitalen Signatur versieht. In klassischen Systemen hätte man sowieso bei allen Geschäften denselben Namen und dieselbe Unterschrift verwendet und eventuell, um die Verkettung verschiedener Erklärungen eines Geschäftsablaufs zu erleichtern, noch eine zusätzliche Kennummer.

Fremdauthentikation ist dann gegeben, wenn der die Erklärung Abgebende die Berechtigung zur Abgabe von anderen erhalten hat.

In diesem Fall benötigt er ein Dokument, etwa ein Zeugnis oder eine Kreditwürdigkeitsbescheinigung, das aussagt, daß der Träger eines gewissen Pseudonyms zu gewissen Erklärungen berechtigt ist, und das er der abzugebenden Erklärung beifügt. Zusätzlich muß er die eigene Erklärung wie oben mit der zu diesem Pseudonym gehörenden Signatur versehen.

Der Aussteller jenes Dokumentes kann dabei evtl. selbst wieder durch weitere Dokumente authentisiert werden.

Ohne weitere Maßnahmen gäbe die Fremdauthentikation den authentisierenden Dritten, z.B. Banken, falls sie für jeden Einkauf garantieren müßten, die Möglichkeit, in Zusammenarbeit mit den Empfängern der Erklärungen ungewollte Verkettungen abzuleiten.

Dies kann durch Verwendung *umrechenbarer Beglaubigungen* (credentials, [Chau_84]) verhindert werden, die gestatten, die für die Abgabe einer Erklärung notwendige Beglaubigung auf ein anderes Pseudonym ausstellen zu lassen als das, welches bei der Abgabe der Erklärung verwendet wird.

Hierzu muß ohne Mitwirkung des Ausstellers die erhaltene Beglaubigung in eine auf das aktuell verwendete Pseudonym lautende umgerechnet werden können. Einerseits darf niemand ohne den Willen des Erklärenden einen Zusammenhang zwischen den verwendeten Pseudonymen erkennen und andererseits der Erklärende eine erhaltene Beglaubigung nur auf seine eigenen Pseudonyme umrechnen können, nicht etwa auf die eines befreundeten Benutzers.

Ein erstes, auf RSA beruhendes Verfahren zur Umrechnung von Beglaubigungen wurde 1985 vorgeschlagen [Chau_85, ChEv_87]. Hierzu wird festgesetzt, daß allen möglichen Beglaubigungen (z.B. einer Bank) jeweils eine bestimmte RSA-Signierfunktion zugeordnet wird. Soll auf ein Pseudonym eine Beglaubigung ausgestellt werden, so heißt dies einfach, daß dieses Pseudonym mit der zu dieser Beglaubigung gehörenden Signierfunktion unterschrieben wird. Dies bedeutet natürlich, daß die möglichen Beglaubigungen stark pauschaliert sein müssen.

Genügt es, eine Beglaubigung genau einmal umrechnen zu können, so gestattet das Verfahren, das Pseudonym, auf das die Beglaubigung umgerechnet werden soll, so zu wählen, daß es für Unterschriften verwendet werden kann [Chau_89]. Möchte man eine Beglaubigung aber mehrfach verwenden und sie hierzu auch mehrfach umrechnen, so ist dies zwar möglich. Die Pseudonyme, auf die die umgerechneten Beglaubigungen lauten, sind dann aber zum Unterschreiben ungeeignet, die umgerechneten Beglaubigungen also nur in einem Identifikationssystem verwendbar.

Während die Anonymität des Verfahrens völlig sicher ist (im informationstheoretischen Sinne), ist die Sicherheit höchstens so groß wie die von RSA.

Ähnlich verwendet werden kann auch das spezielle, allerdings ebenfalls unbewiesene, Signatursystem aus [ChAn_89].

Ein auf einem beliebigen kryptographisch sicheren Signatursystem basierendes beweisbar kryptographisch sicheres Verfahren zur Umrechnung von Beglaubigungen wurde in

[Damg_88] vorgeschlagen. Aus Aufwandsgründen ist es allerdings praktisch nicht einsetzbar.

Sollte RSA gebrochen sein, aber andere sicherere asymmetrische Krypto- und Signatursysteme noch zur Verfügung stehen, so kann in Abwandlung einer in [Chau_81 Seite 86] vorgestellten Anwendung des dort behandelten Datenschutz garantierenden Netzes folgendes Schema verwendet werden: Finden sich n Benutzer, die auf Pseudonyme $p_1, \ldots, p_n$ jeweils eine gleichlautende Beglaubigung (also Signatur) erhalten wollen, so prüft die Organisation, die diese vergeben soll, ob alle n Benutzer berechtigt sind, die gewünschte Beglaubigung zu erhalten (d.h. ob sie sie schon auf ein der Organisation vorzulegendes anderes Pseudonym ausgestellt besitzen). Dann gestattet sie ihnen, in zufälliger Reihenfolge jeweils genau eine Nachricht, nämlich das jeweilige Pseudonym, auf einem Datenschutz garantierenden Kommunikationssystem, das ausschließlich für diesen Zweck (aufbauend auf einem bereits physikalisch vorhandenen) logisch realisiert werden muß, anonym zu veröffentlichen. Das Kommunikationssystem garantiert also, daß niemand feststellen kann, wer welches Pseudonym beigesteuert hat. Nun unterschreibt die Organisation alle veröffentlichten Pseudonyme.

Dazu kann jedes beliebige Signatursystem verwendet werden. Während aber das Verfahren der umrechenbaren Beglaubigungen informationstheoretisch sicher einen Benutzer X unter allen anderen Benutzern verbirgt, die bis zur Verwendung der von X erhaltenen Bestätigung diese ebenfalls erhalten haben, verbirgt das zuletzt beschriebene Verfahren ihn lediglich mit der Sicherheit des logisch realisierten Datenschutz garantierenden Kommunikationssystems unter den n Benutzern, die die Bestätigung gleichzeitig mit ihm erhalten haben.

Eine andere Idee, die ungewollte Verkettbarkeit durch Fremdauthentikation zu verhindern, basiert auf der Annahme der Existenz *sicherer, unausforschbarer Geräte*. In ein solches können, z.B. durch Kommunikation mit anderen sicheren Geräten, Berechtigungen eines Benutzers eingetragen und auch wieder gelöscht werden. Auf Wunsch kann das sichere Gerät eine eingetragene Berechtigung etwa mittels einer systemweit prüfbaren digitalen Signatur bestätigen.

Im Gegensatz zu den bisher behandelten Rechnern (vgl. 2.2, 3.1.2.1) muß für diese Anwendung das Gerät seine Funktion aufgrund geheimer Daten, z.B. Schlüssel eines Kryptosystems, erbringen, die vor dem Benutzer selbst verborgen bleiben müssen. Andernfalls könnte dieser die Berechtigungen im Gerät ändern oder ein Gerät nachbauen, das den anderen Benutzern und sicheren Geräten richtig erscheint, aber mehr oder andere Berechtigungen enthält.

Nach wie vor muß es aber in seiner Funktion auch durch den Benutzer, den es „bedient", kontrollierbar sein, so daß es sich, wie in 2.2 erklärt, physisch im Besitz dieses Benutzers befinden sollte. Hiervon wird auch in der Literatur zumeist ausgegangen [Riha_84, Chau1_85, Davi_85, Riha_85].

Die Existenz von Geräten, die diese beiden Forderungen zugleich erfüllen, ist höchst fraglich. Der Benutzer kann ja das Gerät, insbesondere auch während es gerade arbeitet, beliebig manipulieren und beobachten, wobei sich auch sehr aufwendige Maßnahmen lohnen können, da die Ausforschung eines einzigen Gerätes den Nachbau in sehr vielen Exemplaren erlaubt. Jede Verarbeitung von Information bewirkt aber zwangsläufig einen Energietransport innerhalb des Gerätes. Um ein Messen der Energietransporte (z.B. über elektromagnetische Abstrahlung) zu verhindern, muß das Gerät hinreichend gut abgeschirmt werden. Da ein Benutzer auch versuchen kann, sein Gerät durch zerstörendes Messen auszuforschen, muß ein sicheres Gerät zudem bemerken, wenn seine Schutzmechanismen von außen beeinträchtigt werden. In einem solchen Fall (und auch, wenn seine Funktion aufgrund eines internen Fehlers beeinträchtigt ist) muß das sichere Gerät sich selbst sofort unbrauchbar machen, d.h. seine geheimen Informationen löschen.

Damit ist ein Wettlauf zwischen Konstrukteuren sicherer Geräte und der Meßtechnik festgeschrieben, den vermutlich keiner von beiden auf Dauer gewinnt.

In der Praxis werden nichtsdestotrotz zur Zeit Chipkarten als sichere Geräte eingesetzt. Mögliche Anwendungen sind Berechtigungsausweise zur Benutzung z.B. von Datenbanken oder öffentlicher Fernsprecher (wobei die Berechtigung anfangs auf n-malige Benutzung lautet und bei jeder Benutzung verringert wird) oder auch der Einsatz in digitalen Zahlungssystemen (vgl. Abschnitt 5.5).

Geräte, die vor ihrem Besitzer sicher sein müssen, sollten unserer Meinung nach aber so wenig wie möglich verwendet werden.

3.2 Andere Handlungen

Damit es sich lohnt, die zu einem Rechtsgeschäft gehörenden Erklärungen anonym abzugeben und zu empfangen, müssen auch die übrigen, im Zusammenhang damit stehenden Handlungen die Anonymität wahren.

Wenn eine solche Handlung ebenfalls im Versenden von Information über das Kommunikationssystem besteht, z.B. dem Liefern einer Datenbankauskunft als Ware, so ist die Anonymität bereits durch das zugrundeliegende Datenschutz garantierende Kommunikationssystem gesichert.

Auch die Übergabe von Geld sollte bei einem offenen System in digitaler Form erfolgen können, evtl. in der Form mehrerer aufeinanderfolgender Erklärungen (vgl. Kap. 5).

Hiermit sind bereits die für diejenigen Rechtsgeschäfte, die über offene Systeme abgewickelt werden sollen, wichtigsten Handlungen erschöpft.

Wird ein Teil der Handlungen nicht über das Kommunikationssystem abgewickelt, so kann die Anonymität nicht vollständig erhalten werden; teilweise ist dies auch nicht wünschenswert. Im folgenden werden wir uns daher auf Erklärungen und Handlungen beschränken, die über das Kommunikationssystem ablaufen.

3.3 Sicherstellung von Beweismitteln

Aufbauend auf den in 3.1 erläuterten Möglichkeiten zur Authentikation muß nun untersucht werden, wie genügend Mittel zum Beweis der Abgabe und des Empfangs einer Willenserklärung sichergestellt werden können.

Wie in 3.1, so entstehen im Vergleich zum nicht anonymen Fall auch hier keine wesentlich neuen Probleme.

Man kann bei dieser Untersuchung nach zwei Kriterien gliedern:

Zum einen kann das Ziel der Beweisführung betrachtet werden. Dieses kann sein, die Abgabe oder den Erhalt einer Erklärung zu beweisen, es kann aber auch das Gegenteil der Fall sein, d.h. die Nichtabgabe oder der Nichterhalt sollen bewiesen werden.

Das zweite Ziel kann jedoch einfach dadurch erreicht werden, daß das erste vollständig erreicht wird. Eine nicht als abgesendet oder erhalten nachweisbare Erklärung kann dann als nicht abgegeben oder nicht erhalten betrachtet werden. Das zweite Ziel wird daher im folgenden nicht explizit verfolgt.

Zum anderen kann betrachtet werden, wer ein Interesse an der Beweisführung hat, der Abgebende oder der Empfänger.

Oft wird die Tatsache, daß die Erklärung abgegeben wurde, nur für eine der beiden Parteien vorteilhaft sein, so daß nur diese überhaupt ein Interesse am Nachweis hat und Beweismittel sammeln muß.

Für den Empfänger einer Erklärung ist dieser Nachweis einfach, wenn die Erklärung Dokumentencharakter hat, d.h. eine digitale Signatur trägt, da dann die Vorlage der Erklärung als Nachweis dafür genügt, daß der Besitzer des zur Signatur gehörenden digitalen Pseudonyms diese Erklärung abgegeben hat.

Darauf, daß der Abgebende einer Erklärung Beweismittel für diese Abgabe oder gar für ihren Eingang beim Empfänger sammeln muß, kann in vielen Fällen verzichtet werden, auch wenn die Tatsache, diese Erklärung abgegeben zu haben, für ihn günstig ist.

Kommt es auf den genauen Zeitpunkt der Abgabe nicht an, was gerade auf die Geschäfte des täglichen Lebens, die über offene Systeme abgewickelt werden sollen, zutrifft, so genügt es, wenn er diese Erklärung wiederholt, sobald ihre Abgabe bezweifelt wird, notfalls vor Gericht. Ebenso muß er keine Beweise dafür sammeln, daß er Information als Ware oder Nachrichten, die zur Übertragung digitalen Geldes gehören, geliefert hat. Im Gegensatz zum Abliefern von materiellen Waren oder Papierdokumenten kann der Abgebende die Information ja weiterhin speichern. Dem Empfänger erwachsen aus einer Doppellieferung ersichtlich keine Vorteile, denn die zweite Lieferung stellt lediglich eine Kopie der ersten dar, die er ebensogut hätte selbst erzeugen können.

Sollte der Eingang beim Empfänger doch bewiesen werden müssen, so hat man ähnliche Möglichkeiten wie bei nichtanonymen Erklärungen.

Eine Möglichkeit ist, eine unterschriebene Quittung zu verlangen, deren Erhalt leicht nachgewiesen werden kann (s.o.). Erhält der Abgebende nicht innerhalb eines definierten Zeitraumes die erhoffte Quittung, so muß diese im Notfall sofort gerichtlich erzwungen bzw. durch ein Gericht stellvertretend ausgestellt werden können. Dazu benötigt man für diese umstrittenen Erklärungen auch die folgende Alternative.

Diese zweite Möglichkeit ist, im offenen System sogenannte Schwarze Bretter einzurichten, an denen potentielle Empfänger eingangspflichtiger Erklärungen in gewissen Abständen nach solchen Erklärungen Ausschau halten müssen. Da dieses Ausschauhalten ihre Rechner übernehmen können, bedeutet dies vermutlich eine geringere Belastung als die Verpflichtung zum täglichen Leeren des Briefkastens.

Die Tatsache, daß sich eine Erklärung für einen Benutzer, der das Pseudonym p_E verwendet, an einem Schwarzen Brett befand, kann dann durch Zeugen bewiesen werden. Damit die Zeugen den Inhalt der Erklärung nicht erfahren, muß die Erklärung mit einem dem Empfänger der Erklärung bekannten Schlüssel verschlüsselt werden. Nimmt man hierzu an, daß dem Pseudonym p_E des Empfängers auf überprüfbare Art ein Schlüssel c_E eines asymmetrischen Kryptosystems zugeordnet ist (z.B. durch eine öffentliche Schlüsselbibliothek oder indem c_E selbst als Pseudonym verwendet wird), so kann der Abgebende durch Vorlage des Pseudonyms p_E und der unverschlüsselten Erklärung beweisen, daß demjenigen, der p_E als digitales Pseudonym verwendet, die Erklärung zugegangen ist. Am günstigsten ist es, eine öffentliche Stelle, z.B. die Post als Zeuge zu verwenden, die regelmäßig (z.B. täglich) ein Verzeichnis aller eingegangenen verschlüsselten Erklärungen veröffentlicht und unterschreibt, da in diesem Fall auch der Zeuge kontrollierbar ist und der Empfänger nichts an Anonymität einbüßt.

3.4 Erkenntnisverfahren

Tritt eine Situation ein, in der eine der beteiligten Parteien an der Rechtmäßigkeit des erreichten Zustands zweifelt, so muß wie in einem Erkenntnisverfahren die Substanz dieses Zweifels näher untersucht werden. Der Benutzer, der dies veranlaßt, muß dazu nicht seine Identität offenbaren, sondern es kann vorerst genügen, festzustellen, ob z.B. der Besitzer eines gewissen Pseudonyms wirklich betrogen wurde.

Da auf keinen Fall im voraus eine Deanonymisierung aller möglicherweise Beteiligten vorgenommen werden sollte (dies könnte Anlaß zu Mißbrauch geben), ist zu beachten, daß nicht jeder zu einer Beteiligung am Verfahren gezwungen werden kann. Daher müssen sich alle benötigten Beweismittel im Besitz solcher Benutzer befinden, deren Beteiligung gesichert ist. Dazu gehört die Partei, die das Verfahren veranlaßte und alle nicht anonymen Beteiligten, z.B. Notare, aber auch weitere anonyme, sofern ihnen Schaden entsteht, falls sie sich nicht beteiligen. So könnte z.B. eine anonyme Datenbank, die verklagt wird, Geld erhalten, aber keine befriedigende Auskunft geliefert zu haben, gezwungen sein, die gesendete Antwort offenzulegen, wenn andernfalls davon ausgegangen würde, daß sie gar nichts gesendet hat, so daß sie verurteilt werden würde. (Dazu, daß dies wirklich eine Drohung ist, vgl. 3.5. Außerdem ist zu beachten, daß es innerhalb des Datenschutz garantierenden Kommunikationssystems möglich ist, der Datenbank diese Vorladung unter ihrem Pseudonym sicher zuzustellen, vgl. 3.3.)

3.5 Schadensregulierung

Wurde festgestellt, daß ein unrechtmäßiger Zustand eingetreten ist, so muß gegebenenfalls analog zur heutigen Zwangsvollstreckung wieder ein rechtmäßiger Zustand hergestellt werden.

Im allgemeinen geschieht dies durch einen Eingriff in das Vermögen eines Benutzers. Dazu sollte er genügend Vermögen besitzen, der Zusammenhang zwischen den ermittelten Forderungen und diesem Vermögen klar sein und Zugriff auf das Vermögen oder den speziellen Teil, auf den sich die Forderungen beziehen, möglich sein.

Ob von vornherein gesichert werden kann, daß der Benutzer genügend Vermögen besitzt, ist nicht von der Anonymität, sondern von prinzipiellen Erwägungen bzgl. der jeweiligen Rechtsgeschäfte abhängig und auch derzeit nicht immer garantiert.

Die Erfüllung der restlichen Forderungen macht den Hauptunterschied zwischen anonymen und nicht anonymen Systemen aus:

Wird keine Anonymität gewünscht, so kann der Zusammenhang über den Namen (und weitere Angaben zur eindeutigen Identifizierung) hergestellt werden. Dies bedeutet, daß die Vermögensverwaltung und die Sicherstellung von Beweismitteln völlig unabhängig voneinander organisiert werden können, indem man einerseits alles Vermögen namentlich besitzt und sich andererseits alle Beweismittel auf namentlich bekannte Personen beziehen.

Soll die Anonymität gewahrt werden, so geht diese Unabhängigkeit verloren. Dies bedeutet nicht, daß es keine Möglichkeit zur Schadensregulierung mehr gibt, sondern nur, daß die Geschäftsabläufe komplizierter werden. Bereits bei der Sicherstellung von Beweismitteln muß immer auf einen Zusammenhang mit dem Vermögen, auf das evtl. zugegriffen werden soll, geachtet werden.

Aus diesem Grunde ergibt die in diesem Kapitel 3 durchgeführte Betrachtung der Bestandteile eines Geschäftsablaufs nicht automatisch fertige Protokolle für den ganzen Geschäftsablauf, sondern nur Hilfsmittel, die noch geschickt kombiniert werden müssen.

Die im einzelnen notwendigen Regelungen hängen vor allem davon ab, wer aufgrund des Rechtsgeschäfts für wie lange wozu verpflichtet wird.

Entsteht der Ruf nach Schadensregulierung etwa aufgrund eines großen Kredites, so ist die Voraussetzung für die Garantie, daß Vermögen zugreifbar sein wird, stets die vorherige Übergabe von Sicherheiten in Form materieller Güter, z.B. eines Grundstückes. Dies kann durch Anwenden des Beglaubigungsmechanismus (vgl. 3.1.2) ebenfalls anonym erfolgen, indem z.B. ein Grundbuchamt geeignete Bestätigungen über den Wert eines Grundstücks beglaubigt und das Grundstück sodann als belastet vermerkt, doch sind Geschäfte dieser Größenordnung eher untypisch für offene Systeme.

Weit typischer dürften Geschäfte sein, die im Kauf von Waren, insbesondere Informationen, geringen Wertes bestehen. Hier verpflichtet sich bei der derzeitigen Geschäftsabwicklung lediglich jemand, innerhalb einer kurzen Zeitspanne bei Lieferung der Ware eine gewisse kleine Menge Geldes zu bezahlen. Wegen seiner Wichtigkeit für offene digitale Systeme, und um beispielhaft komplette Geschäftsabläufe darzustellen, wird der Kauf einer Ware gegen geringes Entgelt in einem eigenen Kapitel (Kap. 4) dargestellt.

Mit zwei Ausnahmen kann das Erbringen einer Dienstleistung, z.B. die Verwaltung eines elektronischen Briefkastens (Mailbox), wie eine Folge vieler kleiner Kaufgeschäfte betrachtet werden. Die Verwaltung einer Mailbox könnte z.B. immer dann abgerechnet werden, wenn der Benutzer diese leeren möchte. Die Übergabe des Inhalts entspricht der Lieferung einer Ware.

Die beiden angesprochenen Ausnahmen hiervon sind die Dienstleistungen, die in Anspruch genommen werden müssen, um überhaupt ein Kaufgeschäft über das offene System abwickeln zu können: die Übermittlung von Nachrichten durch das Datenschutz garantierende Kommunikationssystem und die Bereitstellung und Verwaltung von Geld durch ein anonymes digitales Zahlungssystem.

Das Kommunikationssystem kann dabei z.B. pauschal bezahlt werden oder durch Hinzufügen von Geld (digitalen „Briefmarken") zu jeder Nachricht [Pfit_83]. Im ersten Fall können nicht zahlende Benutzer vom Kommunikationssystem ausgeschlossen werden, im zweiten Fall werden unbezahlte Nachrichten nicht weitertransportiert.

Die willkürliche Schädigung eines Benutzers durch das Kommunikationssystem müßte, da der Betreiber des Kommunikationssystems (i. allg. die Post) nicht anonym ist, wie heute üblich außerhalb des Systems evtl. gerichtlich verfolgt werden.

Die Dienste des anonymen digitalen Zahlungssystems können ebenso behandelt werden: die beteiligten Banken selbst können die geforderten Gebühren direkt einbehalten, die Kunden die Banken notfalls verklagen (letzteres kann unter Wahrung der Anonymität der Kunden über das Kommunikationssystem geschehen).

Stichwörter: Anonyme offene digitale Systeme, Anonyme digitale Zahlungssysteme, Anonyme Abwicklung von Rechtsgeschäften, Anonymität, Credentials, Datenschutz garantierende Kommunikationssysteme, Deanonymisierung, Digitale Pseudonyme, Digitale Signaturen, Eigenauthentikation, Fremdauthentikation, Identifikation, Informationelles Selbstbestimmungsrecht, Kryptographie, Massenüberwachung, Rechtssicherheit durch Technik, Schadensregulierung, Schwarzes Brett, Sicherstellung von Beweismitteln, Technischer Datenschutz, Treuhänder, Unbeobachtbarkeit, Unverkettbarkeit, Werteaustausch.

Rechtssicherheit trotz Anonymität in offenen digitalen Systemen*, *Teil 2*

Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann

Zusammenfassung: *Ausgehend von der zunehmenden Bedeutung der Abwicklung von Rechtsgeschäften über offene digitale Systeme wird die Forderung abgeleitet, diese Systeme so zu gestalten, daß ihre Benutzung unbeobachtbar durch Unbeteiligte und anonym vor Beteiligten stattfinden, aber dennoch die notwendige Rechtssicherheit garantiert werden kann. Es wird gezeigt, daß juristische Regelungen alleine nicht ausreichen, um dies überprüfbar garantieren zu können (Kap. 1).*

Als Ergänzung der juristischen Regelungen werden daher die bekannten technischen, d. h. informatischen Methoden und Vorschläge dargestellt, um einerseits die Unbeobachtbarkeit und Anonymität der Systembenutzung garantieren (Kap. 2) und andererseits unter Erhaltung der Anonymität über das offene System mit ausreichender Rechtssicherheit die typischerweise anfallenden Geschäfte abwickeln zu können (Kap. 3). Aufgrund der besonderen Wichtigkeit werden zwei Möglichkeiten zum betrugssicheren Werteaustausch (z.B. Informationsdienstleistung gegen Geld) zwischen anonymen Parteien (Kap. 4) und ein anonymes digitales Zahlungssystem und dessen Abwandlungen ausführlicher dargestellt (Kap. 5). Ein Ausblick auf offene Probleme und ein Fazit aus praktischer Sicht beschließen die Arbeit (Kap. 6).

Das Papier erscheint in zwei Teilen: der erste Teil enthält die Kapitel 1 bis 3, der zweite Teil die Kapitel 4 bis 6 sowie das Literaturverzeichnis für beide Teile.

4 Betrugssicherer Werteaustausch

Klassische Bareinkäufe in Läden könnten aus Sicht der Rechtssicherheit problemlos in völliger Anonymität durchgeführt werden, denn das räumliche Zusammensein der Geschäftspartner sichert, daß entweder Ware und Geld den Besitzer wechseln oder keines, so daß (wenn man z.B. von nachträglichen Reklamationen absieht) nie eine Schadensregulierung nötig wird.

Von solcher Gleichzeitigkeit kann man bei einem Austausch von Ware und Geld über ein Kommunikationssystem nicht ausgehen. Es werden zeitweise immer Geschäftspartner im Vorteil sein, so daß, wenn diese zu einem geeigneten Zeitpunkt die Kommunikation abbrechen, an sie Forderungen bestehen, die gegebenenfalls durchgesetzt werden müssen.

Die folgenden zwei Abschnitte beschreiben zwei Konzepte, wie die Durchsetzbarkeit von Forderungen gesichert werden kann. Wir bevorzugen das zweite.

4.1 Dritte garantieren die Deanonymisierbarkeit

Das erste Konzept garantiert die mögliche Deanonymisierung des Schuldners, falls dieser sich der Schadensregulierung widersetzen möchte, so daß dann wie im nichtanonymen Fall das gesamte Vermögen des Schuldners zur Verfügung steht.

Technisch wird diese Deanonymisierung ermöglicht, indem die am Geschäft Beteiligten sich durch eine besondere Form der Fremdauthentikation ausweisen: Sie identifizieren sich je gegenüber einem allen vertrauenswürdig erscheinenden und nicht anonymen Dritten, der ihnen oder dem Partner das Zeugnis ausstellt, notfalls den Besitzer eines bestimmten Pseudonyms identifizieren zu können (nichtöffentliches Personenpseudonym, vgl. 2.2.2).

Hierbei können zur Authentikation ein Dritter [Herd_85] oder eine Folge von Dritten [Chau_81] verwendet werden. Das Prinzip ist in Bild 8 nochmals für einen Dritten (eventuell aber verschiedene für verschiedene Benutzer) dargestellt. Seien hierzu X und Y die Benutzer und A und B die nicht

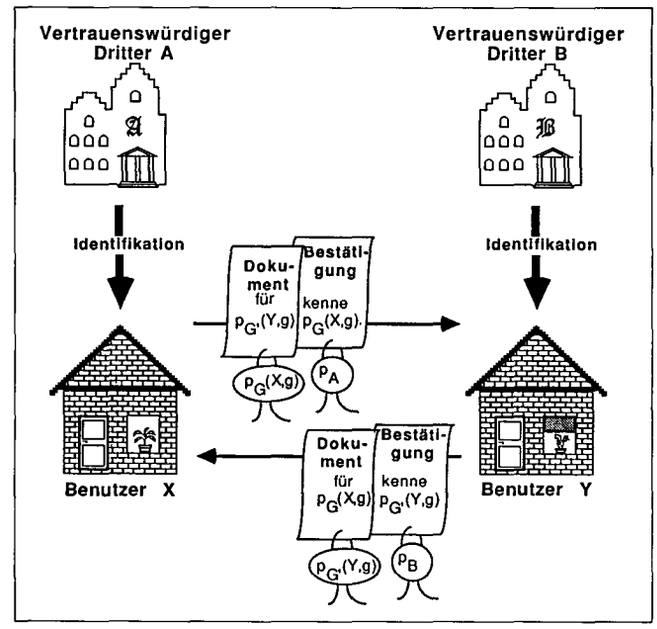

Bild 8

* Dies ist eine in den Abschnitten 2.2.1.1., 3.1.2.1., 3.1.2.2., 5.3 und 7 überarbeitete und um den Abschnitt 5.6 ergänzte Fassung eines in „Computer und Recht" (Dr. Otto Schmidt, Köln) 3/10–12 (1987) erschienenen Artikels.

anonymen Instanzen, die X bzw. Y identifizieren können, und seien

- p_G (X,g) das Pseudonym, das X im Geschäft g mit Y verwenden möchte,
- $p_{G'}$ (Y,g) das Pseudonym, das Y in diesem Geschäft (aber in einer anderen Rolle als X) verwenden möchte,
- p_A bzw. p_B die öffentlichen Personenpseudonyme von A bzw. B.

Die Identifizierbarkeit von X durch A wird gewährleistet, indem X sich sein Pseudonym p_G (X,g) von A unterschreiben lassen muß, bevor er es verwenden kann. Analog läßt sich Y sein Pseudonym $p_{G'}$ (Y,g) von B unterschreiben. Damit garantiert ist, daß A bei der Deanonymisierung stets die richtige Person identifiziert, muß X, bevor er von A sein Zeugnis erhält, z.B. mit seiner üblichen eigenhändigen Unterschrift oder, sicherer, mit einer zu einem öffentlichen Personenpseudonym gehörenden digitalen Signatur, die Erklärung „Das Pseudonym p_G (X,g) gehört X" unterschreiben und A aushändigen. Vertraut man dem vertrauenswürdigen Dritten nicht nur bezüglich der Anonymität, sondern auch bezüglich der Rechtssicherheit, so genügt hier auch die Verwendung eines Identifikationssystems (vgl. 3.1.2.1); z.B. könnte X sich durch seinen Fingerabdruck identifizieren. Analog wird bezüglich B verfahren.

Legen X und Y einander ihre unterschriebenen, also von A bzw. B bestätigten, Pseudonyme vor, bevor sie ein Rechtsgeschäft miteinander abwickeln, so wissen beide, daß bei Betrug X durch A und Y durch B identifiziert werden kann.

Im weiteren Verlauf des Geschäftes könnte es etwa geschehen, daß X sich an B wendet und beklagt, daß der Partner eine Kommunikationsbeziehung abgebrochen hat, obwohl er sie hätte fortführen müssen. X legt dazu Nachrichten von Y vor, die mit $p_{G'}$ (Y,g) unterschrieben sind und die B beweisen, daß eine Kommunikationsbeziehung bestand. B fordert daraufhin Y auf weiterzumachen, wobei von da an alle Nachrichten von Y an X über B laufen müssen. Weigert sich Y, wird er durch B deanonymisiert und die Untersuchung wird nach herkömmlichen Verfahren wie im nicht anonymen Fall fortgesetzt.

Beschuldigt X den anderen fälschlicherweise, indem in der Folge der Erklärungen der Rest unterschlagen wird, so ist das Schlimmste, was passieren kann, daß Y den Rest der Nachrichten nochmal senden muß. Da sie diesmal über B weitergeleitet werden, kann X nicht mehr behaupten, er hätte diese Nachrichten nicht erhalten.

Entsprechendes gilt, wenn Y sich an A wendet und beklagt.

Die Vor- (+) und Nachteile (–) dieses ersten Lösungskonzeptes sind:

– Wer sollte kontrollieren, daß A und B nicht die Identität von X oder Y preisgeben, obwohl sie dazu gar nicht berechtigt sind? A und B müssen also bzgl. des Datenschutzes absolut vertrauenswürdig sein, während dies bzgl. Betrugssicherheit nicht notwendig ist, da sie nicht die Zuordnung von Personen und Pseudonymen verfälschen können.
– Durch X oder Y können ungedeckte Schäden entstehen. Etwa könnte X bei Y eine Dienstleistung bestellen, die er auch erhält, aber zu deren Bezahlung er nicht das nötige Vermögen besitzt. Dann kann trotz Deanonymisierung von X der Y entstandene Schaden nicht behoben werden.
– Das Verfahren legt es aus Aufwandsgründen nahe, für p_G (X,g) bzw. $p_{G'}$ (Y,g) Personenpseudonyme zu verwenden, die, wie in 2.2.2 ausgeführt, zu einer allmählichen Deanonymisierung führen können.
+ Werden Personenpseudonyme verwendet, so ist kein Eingreifen von A und B in die einzelnen Geschäfte von X bzw. Y notwendig.

Wie die Fähigkeit zur Deanonymisierung auch auf mehrere Dritte verteilt werden kann, steht in [Chau_81 Seite 86]. Nach dem dort beschriebenen Verfahren kann der Träger des dem Partner übergebenen Pseudonyms nur durch Kooperation aller Dritter identifiziert werden. Erweiterungen dieses Schemas, um Ausfälle einiger Dritter zu tolerieren, sind in [Pfit_85] beschrieben.

Trotz der erhöhten Anonymität durch Verwendung mehrerer Dritter hat die Deanonymisierung immer noch den Nachteil, das Vorhandensein ausreichender Vermögenswerte nicht zu garantieren.

4.2 Treuhänder garantiert anonymen Partnern die Betrugssicherheit

Um zu sichern, daß keine ungedeckten Schäden entstehen können, bietet sich ein sehr einfaches Verfahren an, das zudem auch ohne Deanonymisierung auskommt: das Deponieren des Geldes bei einem nicht anonymen Treuhänder, so daß Forderungen nur noch an diesen entstehen können [Pfit_83 Seite 29 bis 33, Waid_85, WaPf_86]. Die eigentlichen Geschäftspartner können dann völlig anonym voreinander wie auch vor dem Treuhänder sein. Sollte der Treuhänder das in ihn gesetzte Vertrauen mißbrauchen, so kann er, da er nicht anonym ist, in üblicher Weise verklagt werden, ohne daß die eigentlichen Geschäftspartner ihre völlige Anonymität aufgeben müssen.

Statt also direkt Geld und Waren untereinander auszutauschen, übergeben alle Beteiligten dem Treuhänder Informationen darüber, wieviel Geld bzw. welche Ware (Information) sie genau erhalten wollen und sodann das Geld und die Ware selbst (wobei es genau in dieser Reihenfolge geschehen muß, denn erhält der Treuhänder zwar die Ware, nicht aber das Geld, so kann er dem Lieferanten den Schaden nicht ersetzen). Der Treuhänder prüft, ob das Erhaltene den Erwartungen der Beteiligten entspricht. Je nach dem Ergebnis der Prüfung gibt er das Erhaltene weiter oder bricht das Geschäft ab.

Um Geschäfte schnell abwickeln zu können, muß dieser Treuhänder innerhalb des offenen digitalen Systems sein. Es könnte z.B. die Deutsche Bundespost selbst sein, die ja auch zur Zeit ähnliche Aufgaben bei gewissen Geschäften über Bildschirmtext wahrnimmt.

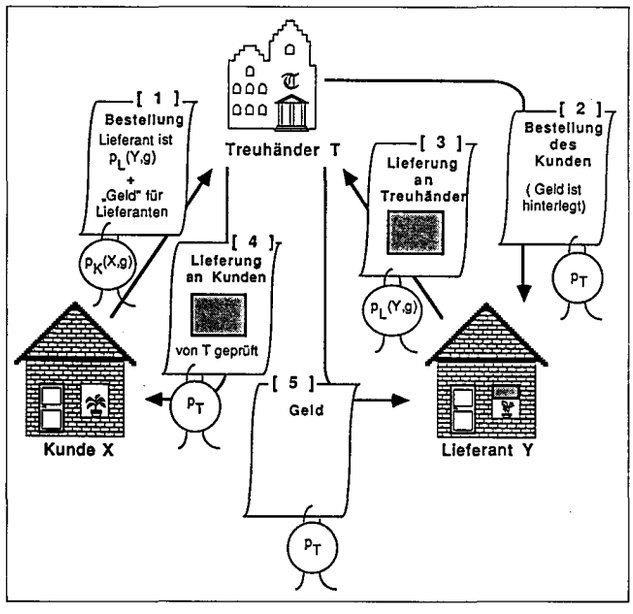

Bild 9

Betrachtet man wieder die Benutzer X und Y, wobei willkürlich X der Kunde und Y der Lieferant einer Ware (in der Form einer Information) sei, so kann diese Idee wie in Bild 9 angegeben konkretisiert werden, wobei die Nummern der Dokumente die Reihenfolge der entsprechenden Erklärungen angeben. Dabei bezeichne

- p_K (X,g) das Pseudonym von X als Kunde im Geschäft g,
- p_L (Y,g) das Pseudonym von Y als Lieferant im Geschäft g und
- p_T das öffentliche Personenpseudonym des nicht anonymen Treuhänders T.

Die bildliche Darstellung beim Versenden des Geldes ist stark vereinfacht, da Geld natürlich nicht einfach als eine einzelne Information oder Erklärung dargestellt werden kann – man könnte es sonst durch Kopieren vermehren (vgl. Kap. 5).

Wie in Abschnitt 3.3 erläutert, kann die Sicherstellung von Beweismitteln für sämtliche Handlungen durch den Handelnden, also für das Deponieren und Weiterleiten bzw. Rückerstatten des Geldes und das Liefern und Weiterleiten der Ware, entfallen und der Empfang der Bestellung (erst durch den Treuhänder, dann durch den Dienstanbieter) einfach durch Vorlage des Dokumentes bewiesen werden.

Dieses Konzept ist zwar aus Datenschutzgründen dem ersten vorzuziehen, hat aber einen Nachteil: es verlangt vom Treuhänder gewisse Prüfungen der Ware, die dieser nicht immer vornehmen kann bzw. aus Datenschutzgründen auch nicht immer vornehmen können soll.

Um diesen Nachteil zu lindern, können X und Y für die Ware eine Reklamationsfrist vereinbaren, während der der Treuhänder T zwar das erhaltene Geld einbehält, nicht aber die erhaltene Ware. Auf diese Weise muß der Treuhänder nur noch die „Echtheit" des erhaltenen Geldes sichern, nicht aber die Ware überprüfen, also insbesondere über sie auch keine Informationen erhalten.

Ist der Kunde X mit der Ware nicht zufrieden, weil etwa eine gestellte Anfrage falsch beantwortet wurde, so kann er innerhalb der Reklamationsfrist dem Treuhänder T untersagen, das Geld weiterzugeben, und muß nun nachweisen, daß die Ware in der Tat fehlerhaft war.

Kann man sicherstellen, daß ein evtl. zu Rate zu ziehendes Gericht schnell genug arbeitet, so kann X auch durch Reklamation Y keinen größeren Schaden, etwa durch Zinsverlust, zufügen.

Wollen X und Y ein Geschäft „Ware gegen Ware" abschließen, so müssen sie es in zwei Geschäfte „Ware gegen Geld" zerlegen, um bei jedem Austausch die Reihenfolge „Geld vor Ware" einhalten zu können.

Das so erweiterte Lösungskonzept des Treuhänders läßt sich wie folgt bewerten:

- – Der Treuhänder muß stets aktiv in das Geschäft einbezogen werden.
- \+ Es ist nicht nötig, daß einer der am Geschäft direkt Beteiligten dem Treuhänder vertraut, da beide am Geschäft direkt Beteiligten den Treuhänder kontrollieren und Fehler oder Betrugsversuche durch ihn gerichtlich verfolgen lassen können. Die Existenz ausreichender Beweismittel ist gesichert, die Vollstreckbarkeit eines Anspruchs gegen den Treuhänder wie im nicht anonymen Fall absicherbar.
- \+ Alle Forderungen von X an Y oder umgekehrt lassen sich durch Rückgriff auf die bei T hinterlegten Werte befriedigen.
- \+ Die am Geschäft direkt Beteiligten können ohne Mehraufwand Transaktionspseudonyme verwenden.
- \+ Die Anonymität der am Geschäft direkt Beteiligten ist völlig gesichert.

Falls der Dienstanbieter nicht anonym sein will, etwa ein Zeitungsverlag, kann man natürlich gleich diesen als Treuhänder wählen, wodurch diese Abwicklungsform mit derjenigen zusammenfällt, bei der der Kaufwillige gleich bei der Bestellung bezahlt und der Dienstanbieter, wenn er nicht liefern kann oder will, das Geld zurückerstatten muß.

Alle hier vorgestellten Konzepte haben allerdings ein gemeinsames Problem offengelassen, nämlich das, wie in einem digitalen System Geld dargestellt und anonym transferiert werden kann. Dies soll im folgenden Kapitel behandelt werden.

5 Anonyme digitale Zahlungssysteme

Ein Zahlungssystem soll seinen Benutzern dazu dienen, in sicherer Weise Geld zu transferieren.

Unabhängig vom jeweiligen Zahlungssystem ausgedrückt, ist Geld nichts anderes als eine rein quantitativ definierte Menge von Rechten. Um die Sicherheit und Anonymität von Zahlungssystemen betrachten zu können, muß man also nicht definieren, was bzw. wo genau in ihnen das Geld ist; im folgenden soll daher nur von Rechten gesprochen werden.

Insbesondere ist für die Sicherheit innerhalb eines Zahlungssystems ohne Belang, ob diese Rechte auf einem echten Guthaben oder (zum Teil) auf einem begrenzten Kredit beruhen, wobei natürlich ein Kredit außerhalb des Zahlungssystems hinreichend abgesichert sein muß.

Ein Zahlungssystem ist sicher, falls

- ein Benutzer erhaltene Rechte transferieren kann,
- er ein Recht nur dann verliert, wenn er hierzu den Willen hat,
- sofern ein zahlungswilliger Benutzer einen anderen Benutzer als Empfänger eindeutig bestimmt, auch nur dieser Empfänger das Recht erhält,
- er falls notwendig einen vollzogenen Transfer einem Dritten gegenüber nachweisen kann (Quittungsproblem) und
- die Benutzer auch bei Zusammenarbeit ihre Rechte an Geld nicht vermehren können.

Vertraut man nicht (nur) auf die Gutwilligkeit der Benutzer, so muß zumindest bei der Ausübung des Verfügungsrechtes in Form des Transfers das Recht nachgewiesen werden. Da hier nur Zahlungssysteme betrachtet werden, bei denen der ganze Transfer allein durch den Austausch digitaler Nachrichten abgewickelt wird (i. allg. über ein Kommunikationssystem) und da digitale Nachrichten beliebig kopiert werden können, die Rechte aber nach dem Transfer erlöschen müssen, genügt ein reiner Dokumentenbeweis nicht. Man benötigt daher zum Nachweis einen Zeugen, der die aktuelle Gültigkeit des Rechtes garantiert.

Um dem Zeugen seine Aufgabe zu ermöglichen, muß ihm jede Inanspruchnahme des Rechtes, das er bezeugen soll, bekannt sein, es darf also auch dann, wenn der Zahlungsempfänger dem Zahlenden vertraut, kein Übergang des Rechtes ohne Bestätigung durch den Zeugen stattfinden können.

In Abschnitt 5.1 bis 5.4 soll davon ausgegangen werden, daß die Benutzer in diesen Zeugen weder bezüglich Sicherheit noch bezüglich Datenschutz volles Vertrauen zu setzen wünschen.

Tut man dies doch, etwa weil der Zeuge ein sicheres Gerät in Form einer elektronischen Brieftasche ist, so vereinfacht sich das Problem erheblich. Hierauf wird in Abschnitt 5.5 näher eingegangen.

Ein Zahlungssystem, das zwar im obigen Sinne nicht sicher ist, aber ganz ohne aktiven Zeugen auskommt, wird in Abschnitt 5.6 beschrieben.

5.1 Grundschema eines sicheren und anonymen digitalen Zahlungssystems

Im folgenden soll diskutiert werden, wie ein sicheres und anonymes digitales Zahlungssystem mit Zeugen realisiert werden kann.

Hierzu wird angenommen, daß ein Benutzer X an einen anderen Benutzer Y des Zahlungssystems ein Recht transferieren möchte und ein Zeuge B (für Bank) diesen Transfer bestätigt. Der Einfachheit halber soll von nur einem Zeugen ausgegangen werden. Dieser eine Zeuge soll für Falschzeugnisse haftbar sein, d.h. entstehen aufgrund seines Falschzeugnisses neue Rechte an Geld, so muß er dieses Geld bereitstellen, und weigert er sich, vorhandene Rechte zu bezeugen, so kann der davon Betroffene dies einem objektiven Dritten (z.B. einem Gericht) beweisen. Dies wird erreicht, indem man diesen Zeugen finanziell hinreichend abgesichert und nicht anonym wählt. Er übernimmt damit in gewissem Sinne die Rolle einer Bank in herkömmlichen bargeldlosen Zahlungssystemen.

Man kann davon ausgehen, daß der Zahlende X und der Empfänger Y sich bereits unter gewissen Pseudonymen (vgl. 2.2.2) kennen. Diese Pseudonyme sind also von außerhalb des Zahlungssystems vorgegeben und werden als schützenswert betrachtet (i. allg. Rollenpseudonyme, z.B. Kundennummer und Bezeichnung eines Dienstanbieters). Ebenso vorgegeben ist das Pseudonym des Zeugen, der aber nicht anonym sein darf (öffentliches Personenpseudonym). Außerdem ist innerhalb des Zahlungssystems durch frühere Zahlungen bereits festgelegt, unter welchem Pseudonym X sich gegenüber dem Zeugen B als Besitzer des Rechtes, das er transferieren will, ausweisen kann. Seien also

- $p_Z(X,t)$ das Pseudonym des Zahlenden X im Transfer t gegenüber dem Empfänger,
- $p_E(Y,t)$ das Pseudonym des Empfängers Y im Transfer t gegenüber dem Zahlenden,
- p_B das für viele Zahlungen gleiche Pseudonym des Zeugen B und
- $p_Z^B(X,t)$ das Pseudonym des Zahlenden X im Transfer t gegenüber dem Zeugen B.

Unter diesen Voraussetzungen ergibt sich, analog zu heutigen Überweisungen, als Protokoll zum Transfer t des Rechtes von X an Y:

[1] **Pseudonymwahl.** Y wählt sich ein Pseudonym $p_E^B(Y,t)$, unter dem er dem Zeugen B als Empfänger des Rechtes im Transfer t bekannt sein möchte, und teilt X mit, daß er das Recht unter diesem Pseudonym $p_E^B(Y,t)$ erhalten möchte. Entsprechend teilt X das Pseudonym $p_Z^B(X,t)$, unter dem er das Recht transferieren will, Y mit. Die notwendigen Erklärungen sind mit $p_E(Y,t)$ bzw. $p_Z(X,t)$ authentisiert.

[2] **Transferauftrag des Zahlenden.** X erteilt dem Zeugen B den Auftrag, das Recht an $p_E^B(Y,t)$ zu übertragen. Dieser Auftrag ist mit $p_Z^B(X,t)$ signiert. Als Fremdauthentikation legt X diesem Auftrag eine Beglaubigung bei, die besagt, daß $p_Z^B(X,t)$ über das zu transferierende Recht verfügt und von B selbst mit p_B signiert ist. Da jeder Transfer von B beglaubigt sein muß, kann B nachprüfen, ob $p_Z^B(X,t)$ über das beglaubigte Recht tatsächlich noch verfügt oder es bereits transferiert wurde.

[3] **Bestätigung des Zeugen.** Der Zeuge B bestätigt X und Y den Transfer des Rechtes von $p_Z^B(X,t)$ auf $p_E^B(Y,t)$, wobei er sie unter diesen Pseudonymen adressiert.

[4] **Quittung für den Zahlenden.** Der Empfänger Y sendet an X eine Quittung, die nur $p_Z(X,t)$ und $p_E(Y,t)$ bezeichnet und mit $p_E(Y,t)$ authentisiert ist, und die den Erhalt des Rechtes bestätigt.

Verweigert Y die Quittung (was i. allg. nicht zu verhindern ist, da Y anonym ist), so kann X die Bestätigung des Transfers durch B (aus [3]) zusammen mit der Bestätigung von Y, das Recht unter diesem neuen Pseudonym $p_E^B(Y,t)$ empfangen zu wollen (aus [1]), als Ersatzquittung verwenden.

Genau diese Möglichkeit unterscheidet das Quittungsproblem vom allgemeinen Werteaustauschproblem, bei dem es nicht möglich ist, daß ein Dritter, etwa der Treuhänder, eines der beiden Tauschobjekte ersatzweise erzeugt.

[5] **Bestätigung für den Empfänger.** Der Zahlende X sendet an Y eine Bestätigung des Transfers, die nur $p_Z(X,t)$ und $p_E(Y,t)$ bezeichnet und mit $p_Z(X,t)$ authentisiert ist.

Auch Y kann notfalls die Bestätigung von B (aus [3]) zusammen mit der Bestätigung von X (aus [1]), das Recht an Y transferieren zu wollen, als Beweis dafür verwenden, das Recht von $p_Z(X,t)$ empfangen zu haben.

[6] **Umformen der Bestätigung.** Y wird die auf $p_E^B(Y,t)$ ausgestellte Bestätigung von B, das Recht erhalten zu haben, bei einem zukünftigen Transfer t' in Schritt [2] verwenden wollen. Um Verkettbarkeiten und damit mögliche Deanonymisierung zu vermeiden, sollte dort nicht $p_E^B(Y,t)$ als $p_Z^B(Y,t')$ verwendet werden.

Durch Verwendung der in 3.1.2.2 erwähnten umrechenbaren Beglaubigungen wird erreicht, daß Y die Bestätigung auf ein neues Pseudonym umrechnen kann. Dazu muß Y allerdings bereits in Schritt [1] des Transfers t zuerst das künftige Pseudonym $p_Z^B(Y,t')$ gewählt und daraus ein zur Umrechnung geeignetes $p_E^B(Y,t)$ gebildet haben.

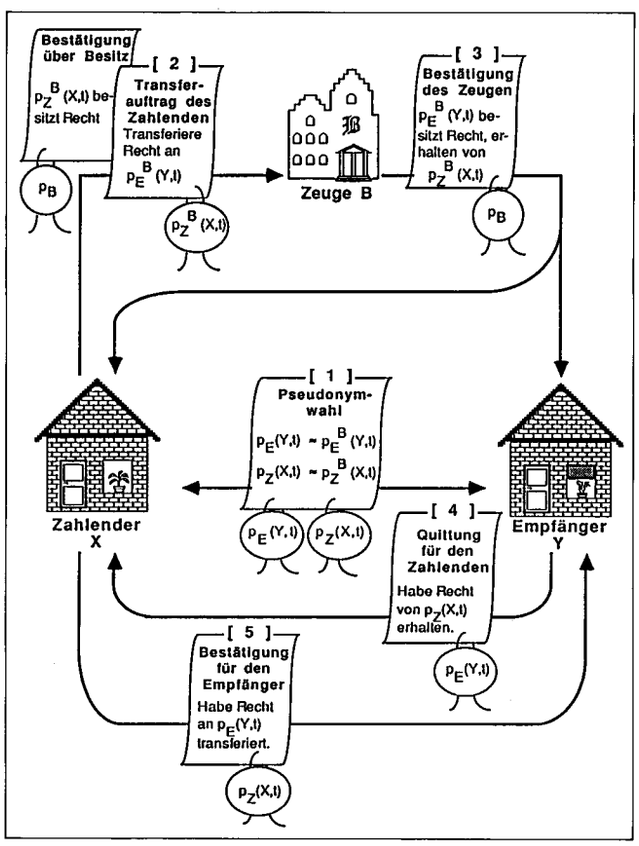

Bild 10

Das Protokoll ist in Bild 10 dargestellt, wobei die Authentikationen wieder als Siegel abgebildet sind.

Da man die in [6] erhaltene Bestätigung über den Empfang des Rechtes in einem zukünftigen Transfer verwendet, um dasselbe Recht, d.h. denselben Geldbetrag zu transferieren, ist es sinnvoll, in diesem Zahlungssystem wie bei Bargeld Rechte vorgegebener Nennwerte zu verwenden, aus denen man bei jeder Zahlung den gewünschten Betrag zusammensetzt. Natürlich muß man auch bei B Geld wechseln dürfen.

Damit man den umgeformten Bestätigungen bei ihrer Verwendung in [2] den Nennwert ansieht, verwendet B für jeden Nennwert N eine andere digitale Signatur, d.h. ein eigenes Pseudonym $p_{B,N}$.

Die Sicherheit des Protokolls ergibt sich daraus, daß am Ende eines Transfers jeder der drei Beteiligten genügend Dokumente über dessen Stattfinden hat (die er aufbewahren muß) und auch während des Transfers jeder einem objektiven Dritten stets entweder den aktuellen Zustand beweisen oder diesen überprüfbar herstellen kann, indem er die bisher von anderen erhaltenen Nachrichten vorlegt und seine eigenen, sofern deren Erhalt abgestritten wird, noch einmal sendet.

Außerdem können Forderungen innerhalb eines Transfers, die eingetrieben werden müssen, nur an den Zeugen entstehen, der nicht anonym ist.

Halten sich X und Y an das Protokoll, so ist die Anonymität des Protokolls maximal, da keiner durch den Transfer über einen anderen irgendwelche neue Information erhält: Der Zeuge erfährt bei einer Zahlung keines der Pseudonyme, die X und Y sonst verwenden, sondern nur zwei neue, die außer in dieser einen Zahlung nie mehr vorkommen. X und Y erfahren zwar voneinander auch die Pseudonyme, die sie bei dieser Zahlung gegenüber dem Zeugen verwenden, aber da diese mit nichts verkettbar sind und ohnehin klar war, daß irgendwelche Pseudonyme gegenüber dem Zeugen verwendet werden, stellt auch dies keine neue Information dar.

Daß die Anonymität des Protokolls maximal ist, heißt aber noch nicht, daß in jeder Situation starke Anonymität herrscht, denn es gibt andere Möglichkeiten zur Informationsgewinnung.

Zum einen gibt es außer den eigens gewählten Pseudonymen noch andere Kennzeichen für die Benutzer, die die Partner unabhängig vom gewählten Protokoll erfahren müssen. Hier sind das vor allem Betrag und Zeitpunkt der Zahlung. Insbesondere ist der Zahlende nur unter all denjenigen verborgen, die zu dieser Zeit ein Recht dieses Betrags besitzen können, was einen zusätzlichen Grund darstellt, nur wenige feste Nennwerte zuzulassen.

Zum anderen erzeugt das Zahlungssystem selbstverständlich keine zusätzliche Anonymität für Pseudonyme, die auch in anderen Situationen verwendet werden. Muß z.B. X den Transfer nachweisen, so werden dadurch die Pseudonyme $p_Z(X,t)$ und $p_E(Y,t)$ miteinander verkettet; dies ist gerade das Ziel des Nachweises.

Die Benutzer können also völlig selbst bestimmen, wieviel der ihnen ermöglichten Anonymität sie aufgeben wollen, indem sie manche Pseudonyme mehrfach verwenden oder durch Erklärungen verketten.

Hat Y in [4] die Quittung verweigert, so verwendet X als Ersatzquittung die Bestätigung des Zeugen aus [3] und die Bestätigung von Y aus [1]. Durch Verwendung der Ersatzquittung gegenüber einem Dritten (ungleich Y) erfährt der Zeuge also möglicherweise die Zuordnung von $p_Z^B(X,t)$ zu $p_Z(X,t)$ und von $p_E^B(Y,t)$ zu $p_E(Y,t)$, so daß im Verweigerungsfall die Anonymität leicht eingeschränkt wird.

Für den Fall, daß X und Y einander vertrauen und auf eine Quittung verzichten können, kann man die Bestätigung des Zeugen B an X über den Vollzug des Transfers einsparen. Die Bestätigung von Y in [1] ist aber weiterhin nötig, da X erst durch sie das Pseudonym $p_E^B(Y,t)$ von Y erfährt, und sie muß auch nach wie vor von Y mit $p_E(Y,t)$ authentisiert werden, damit X sicher ist, daß er sein Recht an den Richtigen transferiert. Außerdem muß in diesem Fall entweder X schon in [1] Y verbindlich mitteilen, was für eine Zahlung stattfinden wird, oder sie müssen sich am Ende noch einmal über deren Zustandekommen verständigen, da andernfalls nicht bemerkt würde, wenn beim Transfer, also entweder bei der Übertragung oder durch B, ein Fehler aufträte.

5.2 Einschränkung der Anonymität durch vorgegebene Konten

Es wäre denkbar, daß ein so vollständig anonymes Zahlungssystem wie das in 5.1 beschriebene nicht erwünscht ist, da dabei, zumindest ohne zusätzliche Vorkehrungen, niemand (insbesondere auch nicht das Finanzamt) Aussagen über den Besitz oder das Einkommen der Benutzer machen kann. Allerdings gilt das gleiche auch für gewöhnliches Bargeld, und selbst in bisherigen bargeldlosen Zahlungssystemen wird die im Prinzip vorhandene Information über Personen mit Konten bei mehreren Banken zumindest offiziell nur sehr selten zusammengeführt.

Aus diesen Gründen könnte jedem Benutzer nur der Besitz eines einzigen Kontos (oder einer bekannten Anzahl) gestattet sein, über das alle Zahlungen abgewickelt werden müssen. Dies kann durch Nichtanonymität der Konten oder mittels umrechenbarer Beglaubigungen für die Einrichtung anonymer Konten erzwungen werden. Auch für diese Situation kann man durch Abwandlung des Protokolls aus 5.1 ein sicheres Zahlungssystem konstruieren, das so anonym wie unter dieser Voraussetzung möglich ist.

Die Voraussetzung läßt sich dadurch ausdrücken, daß $p_Z^B(X,t)$ oder $p_E^B(Y,t)$ diesmal für alle Zahlungen eines Benutzers X bzw. Y gleich, d.h. von t unabhängig ist. Damit ist das Protokoll aus 5.1 nicht mehr völlig anonym, da X und Y einander in Schritt [1] unnötigerweise ihre sie eindeutig kennzeichnenden Kontonummern $p_Z^B(X,t)$ und $p_E^B(Y,t)$ mitteilen würden und B sähe, zwischen welchen zweien der festen Konten ein Transfer stattfindet.

Die Lösung ist, anonyme, bei jedem Transfer wechselnde Zwischenpseudonyme einzuführen, so daß zunächst X das Geld von seinem Konto abhebt und auf sein Zwischenpseudonym transferiert, dann unter diesem an Y unter dessen Zwischenpseudonym zahlt, und zuletzt Y das Geld wieder auf sein Konto einzahlt. Die einzelnen Transfers laufen dabei nach dem Protokoll aus 5.1 ab, insbesondere werden die Beglaubigungen, das Recht erhalten zu haben, zwischen den Teiltransfers auf andere Pseudonyme umgerechnet, so daß eigentlich Zahlender und Empfänger je zwei zusammengehörende Zwischenpseudonyme haben. Bezeichne

- $p_K(X)$ das vorgegebene, zum Konto gehörende Pseudonym einer Person X,
- $p_{ab}(X,t)$ das Pseudonym des Zahlenden X im Transfer t, unter dem er das Geld abhebt,
- $p_{ZwZ}(X,t)$ das Zwischenpseudonym des Zahlenden X im Transfer t, d.h. dasjenige, unter dem er an Y zahlt,
- $p_{ZwE}(Y,t)$ das Zwischenpseudonym des Empfängers Y im Transfer t, d.h. dasjenige, unter dem er das Recht von X empfängt, und
- $p_{ein}(Y,t)$ das Pseudonym des Empfängers Y im Transfer t, unter dem er das Geld einzahlt.

Davon wählt also X zuerst $p_{ZwZ}(X,t)$, berechnet ein passendes $p_{ab}(X,t)$, läßt als ersten Teiltransfer das Recht von $p_K(X)$

auf $p_{ab}(X,t)$ übertragen und rechnet die Bestätigung auf $p_{ZwZ}(X,t)$ um. Bei diesem Teiltransfer können die Schritte [1], [4] und [5] des Protokolls wegfallen, da X sich nicht seine eigenen Pseudonyme mitteilen muß und auch keine Quittung des Transfers benötigt. Auch das Beilegen der Beglaubigung in [2] kann unterbleiben, da B selbst den Kontostand weiß; nur im Streitfalle wird die Beglaubigung benötigt.

Nun muß Y $p_{ein}(Y,t)$ wählen und ein dazu passendes $p_{ZwE}(Y,t)$ berechnen. Daraufhin wird das Recht nach dem vollständigen Protokoll aus 5.1 von $p_{ZwZ}(X,t)$ auf $p_{ZwE}(Y,t)$ übertragen, wobei auch die Quittungen entstehen.

Nachdem Y die Bestätigung über den Erhalt des Rechtes auf $p_{ein}(Y,t)$ umgerechnet hat, transferiert er es auf $p_K(Y)$, wiederum unter Auslassung von [1], [4], [5] und diesmal auch des Schrittes [6].

Die Dokumente, die der Zeuge B im ersten bzw. zweiten Teiltransfer als Bestätigung über den Erhalt der Zahlung ausstellt, dürfen dabei nicht gleich aussehen, denn andernfalls könnte Y die Bestätigung aus dem zweiten Teiltransfer unter Umgehung des Kontos unmittelbar für eine neue Zahlung verwenden. Im Rahmen der umrechenbaren Beglaubigungen bedeutet dies, daß B für Abhebungen und Übertragungen zwei verschiedene digitale Signaturen, also zwei Pseudonyme, verwendet. Unterscheiden kann er die Fälle anhand dessen, ob das ihm mitgeteilte Pseudonym des Zahlenden zu einem Konto gehört oder nicht.

Damit Y innerhalb einer abschätzbaren Zeit sein Recht auf $p_K(Y)$ transferieren muß (was die Voraussetzung z.B. einer jährlichen Besteuerung wäre), darf eine Beglaubigung von B über eine Übertragung nicht beliebig lange zur Einzahlung berechtigen. B sollte nach Ablauf einer bestimmten Frist die zur Authentikation verwendeten Signaturschlüssel tauschen und nach einer weiteren Frist, die allen Zahlungsempfängern Zeit gibt, erhaltene Rechte auf Kontopseudonyme zu transferieren, Beglaubigungen, die mit dem alten Signaturschlüssel authentisiert sind, nicht mehr akzeptieren.

Die Sicherheit dieses Zahlungssystems folgt aus der Sicherheit des Zahlungssystems aus 5.1, da es sich nur um eine spezielle Verwendung desselben handelt.

Die Anonymität ist deswegen maximal unter der Voraussetzung, daß es feste Konten gibt, weil die schützenswerten Pseudonyme $p_K(X)$, $p_K(Y)$, $p_Z(X,t)$ und $p_E(Y,t)$ durch die Zwischenpseudonyme und das Umrechnen der Beglaubigungen völlig voneinander entkoppelt werden. Genauer heißt dies, daß weder Y $p_K(X)$ noch X $p_K(Y)$ noch B $p_Z(X,t)$ oder $p_E(Y,t)$ erfährt und daß jeder die Pseudonyme der anderen, die er schon kannte, aufgrund einer Zahlung zusätzlich nur mit neugewählten Pseudonymen verketten kann, die ansonsten nie mehr verwendet werden, also auch keine Information liefern.

Ansonsten gelten für Anonymität und Quittungen die gleichen Anmerkungen wie am Ende von Abschnitt 5.1. Dabei ist zu beachten, daß Betrag und Zeit einer Zahlung hier wesentlichere Verkettungen erlauben können als in 5.1, nämlich das Erkennen des Zusammenhangs zwischen den beiden an einer Zahlung beteiligten Konten. Um dies zu vermeiden, sollte zwischen den einzelnen Teiltransfers eine zufällig gewählte Zeitspanne verstreichen und der gesamte für eine Zahlung benötigte Betrag nicht auf einmal abgehoben bzw. eingezahlt werden.

5.3 Aus der Literatur bekannte Vorschläge

Die in 5.1 und 5.2 beschriebenen völlig anonymen und sicheren Zahlungssysteme sind durch Kombination von Elementen früher beschriebener anonymer digitaler Zahlungssysteme entstanden. Diese lassen sich aber am einfachsten und systematischsten als Abschwächungen obiger Systeme beschreiben, weshalb sie erst jetzt behandelt werden.

Von David Chaum, dem Erfinder des Mechanismus für das Umrechnen von Beglaubigungen, stammt auch die Idee, diese Umrechnung in Zahlungssystemen anzuwenden, wenngleich er sie in diesem Zusammenhang anders nennt, und eine Reihe darauf beruhender verwandter anonymer Zahlungssysteme [Chau_83, Chau_85, Chau_89].

Allen Vorschlägen von Chaum ist gemeinsam, daß sie von der Existenz fester, nicht anonymer Konten ausgehen. Auch enthalten sie alle keine Quittungen; statt dessen gibt es Varianten, die, ähnlich wie in 4.1, Deanonymisierung von Zahlendem oder Empfänger bei Zusammenarbeit des Partners und des Zeugen erlauben.

Der andere wesentliche Unterschied von Chaums Zahlungssystemen zu dem in 5.2 beschriebenen ist, daß sie, bis auf eine Variante [Chau_89 § 4.2.1], keinen Gebrauch davon machen, daß man die Zwischenpseudonyme so wählen kann, daß zu ihnen eine digitale Signatur existiert. Dies erschwert es, den Benutzern Sicherheit, insbesondere gegen den Zeugen B, zu garantieren, da der Besitzer eines Rechtes nun nicht mehr wie bei einer Überweisung eindeutig durch seine Unterschrift authentisiert erklären kann, wohin es transferiert werden soll. In den einfacheren Varianten wird diese Sicherheit gar nicht oder nur durch Einschränkung der Anonymität erreicht. In einer weiteren Variante [Chau_89 § 4.2.2] wird zumindest Sicherheit gegen den Zeugen B erzielt, indem B dem Zahlungsempfänger unterschreiben muß, daß er das Recht nur ihm gutschreiben wird, bevor ihm das Dokument über den Besitz des Rechtes vorgelegt wird. Hierzu händigt der Zahlende das Dokument dem Empfänger aus. Die Gültigkeit der Unterschrift von B muß natürlich begrenzt werden, da B sich sonst für immer weigern könnte, ein Recht zu transferieren mit der Begründung, er hätte schon jemand anderem bestätigt, es ihm gutzuschreiben, nur dieser hätte das Dokument über den Besitz noch nicht vorgelegt.

Der Verzicht auf namentliche Konten bei digitalen Zahlungssystemen kam erstmals im Zahlungssystem der anonymen Nummernkonten [Pfit_83, WaPf_86] vor, das ansonsten genau die üblichen Überweisungen mit digitalen Signaturen nachbildet. Die Anonymität der Konten ist dabei aber im Grunde keine Eigenschaft des Zahlungssystems, da sie nur etwas über Verkettungsmöglichkeiten der im Zahlungssystem verwendeten Pseudonyme nach außen aussagt und nichts mit der Sicherheit zu tun hat (sofern Kontoüberziehung verboten ist). Allgemein wäre jedes im strengen Sinne sichere digitale Zahlungssystem, das namentliche Konten verwendet, auch mit anonymen Nummernkonten sicher.

Die Verwendung von Transaktionspseudonymen gegenüber der Bank (also $p_Z^B(X,t)$ und $p_E^B(Y,t)$ in obigem Protokoll) wurde in [Bürk_86, BüPf_87, BüPf_89] vorgeschlagen. Das dortige Zahlungssystem entspricht dem aus 5.1, wenn man auf das Umrechnen der Beglaubigungen verzichtet. Die Sicherheit wird durch diesen Verzicht nicht eingeschränkt, jedoch die Anonymität, wenn auch nur in geringem Maße, da bei jedem Transfer t das Pseudonym $p_Z^B(X,t)$ gleich dem Pseudonym $p_E^B(X,t')$ aus einem früheren Transfer t' ist. Der Zeuge B kann also erkennen, daß es sich beide Male um dieselbe Person handelt, und falls der Zahlende W aus dem Transfer t' und der Empfänger Y aus dem Transfer t zusammenarbeiten (was besonders wahrscheinlich ist, wenn W und Y derselbe sind), können auch sie dies erkennen und dadurch die eigentlich schützenswerten Pseudonyme $p_Z(X,t)$ und $p_E(X,t')$ verketten.

Dieses System bliebe übrig, falls der Mechanismus der umrechenbaren Beglaubigungen aus 3.1.2.2, der zur Zeit nur mit

dem speziellen Krypto- bzw. Signatursystem RSA implementiert werden kann, gebrochen würde, andere Systeme für digitale Signaturen jedoch Bestand hätten. Da man von manchen anderen Systemen wenigstens beweisen kann, daß ihr Brechen ebenso schwierig ist wie das Lösen seit langem als schwierig bekannter mathematischer Probleme, ist dies nicht völlig unwahrscheinlich.

5.4 Einige Randbedingungen für ein anonymes Zahlungssystem

Die Verwendung eines anonymen Zahlungssystems sollte niemanden im Vergleich zu den heutigen Zahlungssystemen Nachteile bringen, insbesondere sollte ein Benutzer

- frei unter mehreren Banken als Zeugen seiner Zahlungen wählen können,
- Geld beliebig transferieren können, insbesondere auch in ein konventionelles Zahlungssystem außerhalb des offenen Systems und umgekehrt,
- Geld gegen Zinsen anonym anlegen können und
- entsprechend Geld gegen Zinsen anonym entleihen können.

Neben den Anforderungen der Benutzer an die bereitzustellenden Dienste sind aber auch die Forderungen der Banken und des Staates zu beachten, z.B. darf ein anonymes Zahlungssystem die vermögens- und einkommensabhängige Besteuerung nicht verhindern.

Hier sind insbesondere auch die Grenzen sinnvoller Anonymität zu bedenken, die in dieser Arbeit jedoch als außerhalb der Grenzen des offenen digitalen Systems angenommen und daher nicht näher betrachtet werden. Ohne ihre Betrachtung sind jedoch sinnvolle Aussagen über Sinn und Möglichkeit z.B. einer Besteuerung trotz und in Anonymität nicht möglich.

5.4.1 Transfer zwischen Zahlungssystemen

In den in 5.1 und 5.2 betrachteten Zahlungssystemen wurde stets von nur einem Zeugen, also einer Bank, ausgegangen. Sowohl aus wirtschaftspolitischen als auch aus Anonymitätsgründen sollte es ein anonymes Zahlungssystem aber erlauben, daß Zahlender und Empfänger verschiedene Banken verwenden, ja sogar, daß sie verschiedene Zahlungssysteme verwenden.

Verwenden Zahlender und Empfänger beide das anonyme Zahlungssystem, aber verschiedene Zeugen, so muß in Schritt [1] des Protokolls aus 5.1 der Empfänger Y neben dem Pseudonym $p_E^B(Y,t)$ noch einen Zeugen seines Vertrauens, B_E bestimmen. Im weiteren teilt der Zahlende in [2] seinem Zeugen B_Z den neuen Zeugen B_E mit. Da B_Z und B_E nicht anonym voreinander sind, können diese nun hinsichtlich der Zahlung beliebig kooperieren und als ein einziger Zeuge B betrachtet werden, wobei alle Kommunikation zwischen B und X von B_Z, alle zwischen B und Y von B_E übernommen wird.

Der Transfer zwischen einem nicht anonymen und dem anonymen Zahlungssystem kann sehr einfach realisiert werden: der Betreiber des nicht anonymen Zahlungssystems, also eine Bank, spielt die Rolle eines Mittlers, der in beiden Zahlungssystemen auftreten kann, der Transfer zwischen zwei Benutzern X und Y wird in zwei Transfers zwischen X und Bank bzw. Bank und Y aufgespalten. Auf dieselbe Weise kann ein Benutzer natürlich auch sich selbst Geld in ein anderes Zahlungssystem überweisen, ohne seine Anonymität im anonymen System zu beeinträchtigen.

5.4.2 Verzinsung von Guthaben, Vergabe von Krediten

In beiden in 5.1 und 5.2 betrachteten Zahlungssystemen können die Rechte, für die B als Zeuge dient, als bei der Bank B geführte Sichteinlagen betrachtet werden: der Besitzer des Rechtes kann jederzeit darauf zugreifen, aber B kann jeden Zugriff feststellen. Damit entsteht für eine Bank nur bedingt ein Anlaß zur Verzinsung, so daß man z.B. eine Aufrechnung mit den Bankgebühren erwägen, d.h. auf eine getrennte Verzinsung und Gebührenabrechnung verzichten könnte.

Beide Zahlungssysteme können aber leicht so erweitert werden, daß Guthaben für eine bestimmte Zeit fest angelegt werden können, also eine Verzinsung für die Bank sinnvoll wird: bei festen Konten ist dies trivial; ohne feste Konten könnte man durch Verwendung verschiedener Unterschriften p_B^{z1}, p_B^{z2}, ... des Zeugen unterschiedliche Fälligkeitszeitpunkte ausdrücken.

Möchte man Geldanlageformen erlauben, die von der Höhe des angelegten Guthabens abhängig sind, so muß man das anzulegende Guthaben für die Bank erkennbar zusammenfassen, was zweckmäßigerweise durch Verwendung des Zahlungssystems aus 5.2 mit festen Konten geschieht. Eine Verzinsung ist dann wie heute möglich.

Verzichtet man auf solche Anlageformen und verwendet das System aus 5.1, so muß man jedes einzelne Recht als eigenes Konto betrachten, wobei der Zeitpunkt der „Einrichtung" des Kontos anhand der Unterschrift des Zeugen festgestellt werden kann. Ein Recht kann dann verzinst werden, indem sein Wert allmählich steigt oder indem bei jedem Transfer Zinsen ausgezahlt werden [Chau_89].

Die Vergabe und Verzinsung eines Kredites gestaltet sich im Prinzip nicht schwieriger als heute. Bezüglich der Absicherung eines Kredites gilt das bereits in Kapitel 3 Gesagte: will der Kreditnehmer anonym bleiben, so muß er der Bank gewisse Sicherheiten übergeben; identifiziert er sich hingegen gegenüber der Bank, so muß er der Anonymität wegen lediglich den Kredit einmal sich selbst überweisen (z.B. auf ein zweites Konto) und kann hernach darüber wie über ein normales Guthaben verfügen.

Die Erhebung von Gebühren für die Kontoführung und für einzelne Dienstleistungen einer Bank gestaltet sich, wie in 3.5 schon angedeutet, im anonymen Fall kaum komplizierter als heute: Bei festen Konten kann die Bank ihre Forderungen direkt aus dem von ihr verwalteten Guthaben befriedigen. Geht man nicht von festen Konten aus, so müssen die Banken ihre Gebührenwünsche während des Transfers befriedigen, d.h. der Zahlende dem Transferauftrag einen „Gebührentransferauftrag" (eine digitale „Gebührenmarke") für die bezeugende Bank beilegen.

5.5 Sichere Geräte als Zeugen

Verzichtet man auf die Forderung der Anonymität vor dem Zeugen, so läßt sich ein anonymes Zahlungssystem sehr leicht realisieren: das Protokoll aus 5.1 kann so abgewandelt werden, daß ein Benutzer X in allen Zahlungen, in denen er als Zahlender oder Zahlungsempfänger auftritt, die Pseudonyme $p_Z^B(X,t)$ bzw. $p_E^B(X,t')$ gleich wählt (d.h. eine feste Kontonummer, als Geschäftsbeziehungspseudonym verwendet) und B die Pseudonyme $p_Z(X,t)$ und $p_E(Y,t)$ erfährt. Damit entfällt das Problem der Ersatzquittungen aus [4] und [5] sowie die Umformung der Bestätigung in Schritt [6].

Um die Annahme zu rechtfertigen, dem Zeugen hinsichtlich der Anonymität der Benutzer vertrauen zu dürfen, wird i. allg. der Zeuge als sicheres, unausforschbares Gerät gewählt (vgl. 3.1.2.2).

Als Einsatzmöglichkeiten bieten sich zwei Varianten an:

Die erste Variante verwendet ein einziges zentrales sicheres Gerät, das alle Transaktionen bezeugt.

Bereits aus den schon in 2.2 generell bemerkten Gründen ist diese Variante wenig wünschenswert. Hinzu kommt, daß gegenüber dem nicht vertrauenswürdigen Zeugen aus 5.1 und 5.2 kein entscheidender Gewinn erzielt wird. Das Protokoll wird zwar, wie oben erwähnt, stark vereinfacht, doch entlastet dies nur die Rechner, nicht die Benutzer des Zahlungssystems und eröffnet diesen auch keine neuen Möglichkeiten.

Als zweite Variante erhält jeder Benutzer ein eigenes sicheres Gerät als „elektronische Brieftasche", die seine Transaktionen (im Namen des Zahlungssystembetreibers) bezeugt.

Der Einsatz sicherer Geräte als elektronische Brieftaschen wurde in [EvGY_84, Even_89] vorgeschlagen, war aus Gründen der (scheinbar notwendigen) Protokollierung aber noch nicht anonym. Anonymisierte Versionen des Verfahrens finden sich in [BüPf_87, BüPf_89].

Der einzige echte Vorteil der (anonymen wie nichtanonymen) elektronischen Brieftaschen ist, daß sie als einziges Zahlungssystem off-line Transaktionen zulassen, also einem Benutzer erlauben, viele Zahlungen spontan zu leisten und zu empfangen, ohne in der Zwischenzeit mit einer zentralen Instanz kommunizieren zu müssen. Dieser Vorteil ist hier aber weniger schwerwiegend, da nur offene Systeme, denen ein Kommunikationsnetz zugrunde liegt, betrachtet werden.

Viel gravierender sind die Nachteile elektronischer Brieftaschen:

- Da Zahlungen nicht mehr über einen zentralen Zeugen abgewickelt werden, kann ein Verlust einer elektronischen Brieftasche zum Verlust bereits erhaltener Zahlungen führen. Um dies zu vermeiden, müssen relativ aufwendige Fehlertoleranzmaßnahmen ergriffen werden [WaPf_87, WaPf1_87, WaPf_90].
- Die Sicherheit eines Zahlungssystems mit elektronischen Brieftaschen als Zeugen basiert entscheidend auf der Ausforschungssicherheit der Geräte. Wie schon in 3.1.2.2 diskutiert, ist die Existenz dauerhaft sicherer Geräte stark zu bezweifeln, die Bewertung der Ausforschungssicherheit real vorhandener, vermeintlich sicherer Geräte kaum möglich.
- Der Einsatz sicherer Geräte macht den Einsatz kryptographischer Techniken, insbesondere zur gegenseitigen Authentikation elektronischer Brieftaschen, nicht überflüssig. Damit stellen die sicheren Geräte auch keine Notalternative für den Fall dar, daß alle Verschlüsselungs- und Signatursysteme gebrochen werden sollten. Sollten jedoch nur alle asymmetrischen Kryptosysteme und Signatursysteme gebrochen sein, so wäre in Verbindung mit einem symmetrischen Kryptosystem ein Einsatz noch sinnvoll, da die sicheren Geräte untereinander nur ein digitales Identifikationssystem (vgl. 3.1.2.1) benötigen.

Aufgrund der genannten Nachteile und des für offene digitale Systeme der betrachteten Art nur geringen Vorteiles elektronischer Brieftaschen erscheint uns ein Einsatz hier als nicht angebracht.

5.6 Zahlungssysteme mit Sicherheit durch Deanonymisierbarkeit

In [ChFN_88] wurde ein anonymes Zahlungssystem vorgestellt, das nur eine schwächere als die bisher verwendete Sicherheitsdefinition erfüllt:

- Ein Benutzer darf ein erhaltenes Recht nur einmal weitergeben. Gibt er es dennoch mehrfach weiter, so muß er dadurch deanonymisierbar werden.

Die Grundidee ist dieselbe wie die in Abschnitt 4.1: man hofft, daß das nach einer Deanonymisierung insgesamt zur Verfügung stehende Vermögen zur Schadensregulierung ausreicht.

Das System soll hier trotz seiner schwächeren Sicherheit kurz skizziert werden: Zum einen ist es auch nicht unsicherer als z.B. das heutige Kreditkartensystem, zum anderen stellt es für off-line Zahlungen die einzige Alternative zu den fragwürdigen elektronischen Brieftaschen aus Abschnitt 5.5 dar.

Hauptunterschied zu den obigen Zahlungssystemen ist, daß statt des Zeugen B der Zahlende X selbst dem Zahlungsempfänger Y den Transfer bestätigt. Verhält sich X korrekt, so bleibt seine Anonymität gewahrt. Verhält er sich inkorrekt und transferiert das Recht nochmals an einen anderen Empfänger Y*, so können dank eines kryptographischen Tricks mit hoher Wahrscheinlichkeit die beiden Transferbestätigungen von X so kombiniert werden, daß ihnen die Identität von X zu entnehmen ist. Wird das Recht bei B mehrfach geltend gemacht, so kann X durch B deanonymisiert werden.

Da im Transfer kein Zeuge benötigt wird, kann dieses Zahlungssystem unmittelbar für off-line Zahlungen eingesetzt werden; zu diesem Zweck wurde es in [ChFN_88] auch vorgeschlagen.

Zur Erhöhung der Sicherheit kann man es mit sicheren Geräten kombinieren: die Benutzer müssen statt beliebiger Rechner sichere Geräte verwenden, die die mehrfache Weitergabe eines Rechtes verhindern. Das kombinierte System erfüllt solange die stärkere Sicherheitsdefinition, wie die sicheren Geräte wirklich sicher sind; ansonsten ist es ebenso sicher wie das ursprüngliche System ohne sichere Geräte.

Das Zahlungssystem ist leider noch nicht vollständig veröffentlicht [ChAn1_89]. Zahlungssysteme, die die off-line Eigenschaft insofern einschränken, daß ein Zahlungsempfänger Y ein erhaltenes Recht nicht ohne vorherigen Kontakt mit der Bank weitergeben kann, sind in [ChFN_88, Chau1_89, CBHM_89] beschrieben. (Ein entsprechendes in [OkOh_89, OkOh1_89] vorgeschlagenes Zahlungssystem erwies sich laut David Chaum als fehlerhaft.)

6 Ausblick

6.1 Offene Probleme

Geht man davon aus, daß in Zukunft häufig Rechtsgeschäfte über offene digitale Systeme abgewickelt werden und für etliche Dienste (z.B. von digitalen Signatur-, Zahlungs- und Werteaustauschsystemen) sogar ein sozialer Benutzungszwang entstehen könnte, so kommt der Sicherheit dieser Systeme eine besondere Bedeutung zu.

Um zu vermeiden, daß unter großen Kosten Systeme eingeführt werden, die nicht die von den klassischen Systemen gewohnte Rechtssicherheit zulassen oder bei denen diese erst nachträglich und mühsam hergestellt werden muß (wie z.B. im Fall der Entwendung einer ec-Karte samt Geheimzahl für Bargeldautomaten), muß vorweg sichergestellt werden, daß die eingeführten Systeme von Anfang an Rechtssicherheit gewähren. Wie man bereits den vorangegangenen Kapiteln entnehmen kann, werden solche Systeme sehr komplex sein. Daher ist ein intuitives Bewerten nicht mehr zuverlässig

möglich, nicht nur für technische Laien, also z.B. Juristen, sondern auch für Informatiker. Die Sicherstellung der Rechtssicherheit muß also in Form eines Beweises erfolgen.

Ein Beweis der Rechtssicherheit würde zeigen, daß das Auftreten eines unrechtmäßigen Zustands ausgeschlossen ist oder andernfalls von der Entstehung genügender Beweismittel begleitet ist, die sich zudem in den richtigen Händen befinden, um die (ggf. zwangsweise) Wiederherstellung eines rechtmäßigen Zustands zu ermöglichen.

Geschieht dieser Beweis in konstruktiver Art, so gibt er zugleich den allgemeinen Ablauf eines Erkenntnisverfahrens an.

Um einen solchen Beweis der Korrektheit eines digitalen Signatur-, Zahlungs- oder Werteaustauschsystems führen zu können, fehlen jedoch nicht nur bewiesene Grundaussagen über die Sicherheit der verwendeten Hilfsmittel (wie Kryptosysteme, bei denen man solche Aussagen zumindest schon teilweise beweisen kann, oder „ausforschungssichere" Geräte), sondern auch eine präzise Formulierung der Behauptung, d.h. eine Charakterisierung dessen, was „Korrektheit" bzw. „Rechtssicherheit" bei dem betrachteten System überhaupt bedeuten soll.

Hierzu ist das derzeit geltende Recht nicht nur (selbstverständlich) nicht formal, sondern größtenteils auch noch nicht allgemein und abstrakt genug.

Hieraus leitet sich eine gemeinsame Aufgabe für Juristen und Informatiker her:

In solchen rechtlich geregelten Bereichen, wo auf informatischen Verfahren basierende Systeme eingeführt werden sollen, müssen ausgehend von den Gerechtigkeitsvorstellungen, die den derzeitigen rechtlichen Regelungen zugrundeliegen, geeignete allgemeine Forderungen an solche Systeme gefunden werden, sofern diese in der Rechtswissenschaft nicht ohnehin schon bekannt sind. Beispielsweise würde zu den Forderungen an ein Signatursystem sicher gehören, daß es Dokumenten Beweiswert verleiht, was etwa durch die (informellen) Grundforderungen an eine digitale Signatur in 3.1.2.1 ausgedrückt werden soll, aber auch, daß es vor unüberlegter Abgabe von Erklärungen schützt.

Sodann sind diese Forderungen in ein formales Modell zu übertragen.

Selbstverständlich müssen solch allgemeine Regelungen durch spezielle und allgemeinverständliche (also notwendigerweise informelle) Kommentare ergänzt werden, die beschreiben, welche konkreten Systeme für geeignet befunden wurden und wie sie zu benutzen sind, z.B. daß anstelle einer eigenhändigen Unterschrift stets auch eine digitale Signatur mit GMR gestattet ist. Das Risiko, daß die formalen und informellen Formulierungen nicht gleichbedeutend sind, dürfte für die Gesellschaft wesentlich leichter zu tragen sein als das, das die Einführung komplizierter Systeme ohne Beweis ihrer Rechtssicherheit darstellt.

6.2 Fazit aus praktischer Sicht

In den zurückliegenden Kapiteln wurden informell alle uns bekannten Vorschläge vorgestellt, die Rechtssicherheit und Anonymität bei Rechtsgeschäften, die ausschließlich über ein offenes digitales System abgewickelt werden, gleichermaßen berücksichtigen und fördern.

Aus praktischer Sicht kann man hieraus folgende Schlüsse ableiten.

1. Nur die Kombination aus juristischen und technischen Maßnahmen kann Datenschutz und Rechtssicherheit in offenen Systemen sicherstellen. Juristische Maßnahmen alleine reichen keinesfalls aus.
2. Es sind effiziente und kostengünstige technische Hilfsmittel bekannt, um die Anonymität der Benutzer in für den Benutzer kontrollierbarer Form sicherzustellen. Die hier vorgestellten Hilfsmittel schränken das Anwendungsspektrum offener digitaler Systeme in keiner Weise ein, und auch die Benutzung dieser Systeme wird nicht komplizierter.
3. Rechtssicherheit und Anonymität sind kein Gegensatz. Da die betrachteten Hilfsmittel in anonymen wie nicht anonymen Systemen dieselben sind, liegt der Schluß nahe, daß ein anonymes System genauso betrugssicher sein kann wie ein nicht anonymes. Beachtet man, daß die besonderen Probleme anonymer Schadensregulierung spezielle Vorkehrungen bei der Sicherstellung von Beweismitteln und zur Vermögensgarantie erfordern, die im nicht anonymen Fall z.T. als überflüssig betrachtet werden, so sind anonyme Systeme möglicherweise sogar sicherer als manche nicht anonymen (auch nicht digitale, wie beispielsweise Einkäufe in Läden).
4. Die Verwendung nicht Datenschutz garantierender Kommunikationssysteme und damit auch nicht anonymer offener Systeme allgemein gefährdet dauerhaft die Persönlichkeitsrechte aller Benutzer, denn eine nachträgliche Anonymisierung ist technisch schier unmöglich.
   Umgekehrt steht die Verwendung eines anonymen Systems einer freiwilligen oder vorgeschriebenen, willentlichen Selbstidentifikation eines Benutzers nicht entgegen, so daß nur dies alle Möglichkeiten für die Zukunft offenhält.

Da also Rechtssicherheit und Datenschutz einander harmonisch ergänzen können und beide zu den Grundprinzipien eines freiheitlichen demokratischen Rechtsstaates zu zählen sind, muß, wo immer möglich, die natürliche Anonymität des täglichen Lebens auch auf neue Systeme übertragen werden.

Für motivierende und fruchtbare Diskussionen und konstruktive Kritik danken wir Dr. Volker Anhäusser, Holger Bürk, Dr. Klaus Echtle, Dr. Jürgen W. Goebel, Prof. Dr. Winfried Görke, Dr. Helmut Redeker, Dr. Jochen Schneider sowie den Mitgliedern der Fachgruppe Informationsrecht im Fachbereich 6 der GI, die uns einst auf die juristischen Details des Themas aufmerksam machten. Der Deutschen Forschungsgemeinschaft (DFG) danken wir für ihre freundliche Unterstützung, die diese Arbeit erst möglich gemacht hat.

Literatur

Abbr_84 C. R. Abbruscato: Data Encryption Equipment; IEEE Communications Magazine 22/9 (1984) 15–21

Akl_83 S. G. Akl: Digital Signatures: A Tutorial Survey; Computer, IEEE 16/2 (1983) 15–24

Aßma_89 R. Aßmann: Effiziente Software-Implementierung von verallgemeinertem DES; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1989

AT&T_86 AT&T: Einchip-Prozessor zur Verschlüsselung digitaler Signale; Design&Elektronik, Markt&Technik 21 (1986) 8–11

BeMi_89 M. Bellare, S. Micali: Non-interactive Oblivious Transfer and Applications; Crypto '89, August 20–24 1989, Abstracts, 517–528

BGMR_85 M. Ben-Or, O. Goldreich, S. Micali, R. L. Rivest: A Fair Protocol for Signing Contracts; Proc. of 12th ICALP, LNCS 194, Springer-Verlag, Heidelberg 1985, 43–52

Bleu_90 G. Bleumer: Vertrauenswürdige Schlüssel für ein Signatursystem, dessen Brechen beweisbar ist; Studienarbeit

am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1990

BlFM_88 M. Blum, P. Feldman, S. Micali: Non-interactive zero-knowledge and its applications (extended abstract); 20th Symposium on Theory of Computing (STOC) 1988, ACM, New York 1988, 103–112

BlGo_85 M. Blum, S. Goldwasser: An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information; Proc. of Crypto 84, LNCS 196, Springer-Verlag, Heidelberg 1985, 289–299

BlPW_90 G. Bleumer, B. Pfitzmann, M. Waidner: A Remark on a Signature Scheme where Forgery can be Proved; Eurocrypt '90, Aarhus 1990

Bras_83 G. Brassard: On Computationally Secure Authentication Tags Requiring Short Secret Shared Keys; Crypto '82, Plenum Press, New York 1983, 79–86

Bras_88 Gilles Brassard: Modern Cryptology – A Tutorial; LNCS 325, Springer-Verlag, Berlin 1988

BüPf_87 H. Bürk, A. Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, Proc. of the 4th International Conference on Computer Security, Monte Carlo 1986; erscheint bei: A. Grissonnanche (ed.), North-Holland, Amsterdam; Überarbeitung: Interner Bericht 2/87, Fakultät für Informatik, Universität Karlsruhe 1987

BüPf_89 H. Bürk, A. Pfitzmann: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399–416

Bürk_86 H. Bürk: Digitale Zahlungssysteme und betrugssicherer, anonymer Wertetransfer; Studienarbeit am Institut für Informatik IV, Universität Karlsruhe 1986

Bund_83 Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 – 1 BvR 209/83 u.a.; Datenschutz und Datensicherung DuD 4 (1984) 258–281

CBHM_89 D. Chaum, B. den Boer, E. van Heyst, S. Mjølsnes, A. Steenbeek: Efficient Electronic Checks; Eurocrypt '89; Houthalen 1989, Abstracts, 171–174

ChAn_89 D. Chaum, H. van Antwerpen: Undeniable Signatures; Crypto '89, August 20–24 1989, Abstracts, 205–212

ChAn1_89 D. Chaum, H. van Antwerpen: Private Kommunikation, 1989

Chau_81 D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of ACM 24/2 (1981) 84–88

Chau_83 D. Chaum: Blind Signatures for untraceable payments; Proc. of Crypto 82, Plenum Press, New York 1983, 199–203

Chau_84 D. Chaum: A New Paradigm for Individuals in the Information Age; Proc. of the 1984 Symposium on Security and Privacy, IEEE, Oakland 1984, 99–103

Chau_85 D. Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of ACM 28/10 (1985) 1030–1044; Übersetzung: Sicherheit ohne Identifizierung. Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen; Informatik-Spektrum 10/5 (1987) 262–277; Datenschutz und Datensicherung DuD 1 (1988) 26–41

Chau1_85 D. Chaum: Cryptographic Identification, Financial Transaction, and Credential Device; United States Patent, Patent Number 4,529,870; Date of Patent: Jul. 16, 1985, Filed Jun. 25, 1982

Chau_89 D. Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; Amsterdam 1986; Überarbeitung: SMART CARD 2000: The Future of IC Cards, North-Holland, Amsterdam 1989, 69–93

Chau1_89 D. Chaum: Online Cash Checks; Eurocrypt '89; Houthalen 1989, Abstracts, 167–170

ChEv_87 D. Chaum, J.-H. Evertse: A secure and privacy-protecting protocol for transmitting personal information between organizations; Crypto '86, LNCS 263, Springer-Verlag, Berlin 1987, 118–167

ChFN_88 D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash; Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 319–327

Clem_85 R. Clemens: Die elektronische Willenserklärung – Chancen und Gefahren; Neue Juristische Wochenschrift NJW 34 (1985) 1998–2005

Damg_88 I. Damgård: Payment systems and credential mechanisms with provable security against abuse by individuals; Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 328–335

DaPr_89 D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer (2nd ed.); John Wiley, Chichester 1989

Davi_82 G. Davida: Chosen Signature Cryptanalysis of the RSA (MIT) Public Key Cryptosystem; TR-CS-82-2, University of Wisconsin, Milwaukee (October 1982)

Davi_85 D. W. Davies: Apparatus and methods for granting access to computers; UK Patent Application, Application No. 8503481, Date of filing 11 Feb. 1985, Application published 4 Sept. 1985

Denn_82 D. E. Denning: Cryptography and Data Security; Addison-Wesley, Reading 1982 (reprinted with corrections 1983)

DES_77 Federal Information Processing Standards Publication 46 (FIPS PUB 46): Specification for the Data Encryption Standard; January 15, 1977

DiHe_76 W. Diffie, M. E. Hellman: New Directions in Cryptography; IEEE Trans. on Information Theory IT-22/6 (1976) 644–654

Even_89 S. Even: Secure Off-Line Electronic Fund Transfer Between Nontrusting Parties; SMART CARD 2000: The Future of IC Cards, North-Holland, Amsterdam 1989, 57–66

EvGL_85 S. Even, O. Goldreich, A. Lempel: A Randomized Protocol for Signing Contracts; Communications of ACM 28/6 (1985) 637–647

EvGY_84 S. Even, O. Goldreich, Y. Yacobi: Electronic Wallet; Crypto '83, Plenum Press, New York 1984, 383–386; Intern. Zurich Seminar on Digital Communications, Zürich, IEEE 1984, 199–201

FiSh_87 A. Fiat, A. Shamir: How to Prove Yourself: Practical Solutions to Identification and Signature Problems; Crypto '86, LNCS 263, Springer-Verlag, Berlin 1987, 186–194

GGSS_78 H.-U. Gallwas, H. Geiger, J. Schneider, J. Schwappach, J. Schweinoch: Datenschutzrecht – Kommentar und Vorschriftensammlung; Kohlhammer, Stuttgart 1978

GoMi_84 Shafi Goldwasser, Silvio Micali: Probabilistic Encryption; 14th Symposium on Theory of Computing (STOC) 1982, ACM, New York 1982, 365–377; Überarbeitung: Journal of Computer and System Sciences 28 (1984) 270–299

GoMR_88 S. Goldwasser, S. Micali, R. L. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; 25th Symposium on Foundations of Computer Science (FOCS) 1984, IEEE Computer Society, 1984, 441–448; Überarbeitung: SIAM J. Comput. 17/2 (1988) 281–308

Herd_85 S. Herda: Authenticity, Anonymity and Security in OSIS. An Open System for Information Services; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer-Verlag, Heidelberg 1985, 35–50

Hors_85 P. Horster: Kryptologie; Reihe Informatik/47, Bibliographisches Institut, Mannheim 1985

Inge_84 I. Ingemarsson: Critique of the Security of Public-key Systems; Intern. Zurich Seminar on Digital Communications, Zürich, IEEE 1984, 171–173

Köhl_86 H. Köhler: Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen; Datenschutz und Datensicherung, Teil I: DuD 6 (1986)

337–344, Teil II: DuD 1 (1987) 7–12, Teil III: DuD 2 (1987) 61–67

LeMa_89 A. K. Lenstra, M. S. Manasse: Factoring – where are we now?; IACR Newsletter 6/2 (1989) 4–5

LuRa_88 M. Luby, C. Rackoff: How to construct permutations from pseudorandom functions; 18th Symposium on Theory of Computing (STOC) 1986, ACM, New York 1986, 356–363; Überarbeitung: SIAM J. Comput. 17/2 (1988) 373–386

Mt 2, 16 Matthäus: 2,16; in Die Bibel

OkOh_89 T. Okamoto, K. Ohta: Divertible Zero Knowledge Interactive Proofs and Commutative Random Self-Reducibility; Eurocrypt '89; Houthalen 1989, Abstracts, 95–108

OkOh1_89 T. Okamoto, K. Ohta: Disposable Zero-knowledge Authentications and Their Applications to Untraceable Electronic Cash; Crypto '89, 1989, Abstracts, 443–458

PfAß_90 A. Pfitzmann, R. Aßmann: Efficient Software Implementations of (Generalized) DES; Proc. SECURICOM 90, 8th Worldwide Congress on Computer and Communications Security and Protection, March 13–16, 1990, Paris, 139–158

Pfit_83 A. Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes; Interner Bericht 18/83 der Fakultät für Informatik, Universität Karlsruhe 1983

Pfit_85 A. Pfitzmann: How to implement ISDNs without user observability – Some remarks; Interner Bericht 14/85 der Fakultät für Informatik, Universität Karlsruhe 1985

Pfit_89 B. Pfitzmann: Für den Unterzeichner sichere digitale Signaturen und ihre Anwendung; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1989

Pfit_90 A. Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Dissertation, Universität Karlsruhe 1989; IFB 234, Springer-Verlag, Heidelberg 1990

PfPf_89 B. Pfitzmann, A. Pfitzmann: How to Break the Direct RSA-Implementation of MIXes; Eurocrypt '89; Houthalen 1989, Abstracts, 228–235

PfPW_88 A. Pfitzmann, B. Pfitzmann, M. Waidner: Datenschutz garantierende offene Kommunikationsnetze; Datenschutz und Datensicherung DuD 3 (1986), 178–191; Überarbeitung: Informatik-Spektrum 11/3 (1988) 118–142

PoKl_78 G. J. Popek, C. S. Kline: Issues in Kernel Design; Operating Systems, An Advanced Course; LNCS 60, Springer-Verlag, Heidelberg 1978; Nachgedruckt in: Springer Study Edition; Springer-Verlag, Heidelberg 1979, 209–227

Rede_84 H. Redeker: Geschäftsabwicklung mit externen Rechnern im Bildschirmtextdienst; Neue Juristische Wochenschrift NJW 42 (1984) 2390–2394

Rede_86 H. Redeker: Die Benutzung von technischen Medien zur Einlegung von Rechtsmitteln; Computer und Recht CR 2/8 (1986) 489–491

Riha_84 K. Rihaczek: Fälschungssichere elektronische Orderpapiere; Datenschutz und Datensicherung DuD 3 (1984) 197–204

Riha_85 K. Rihaczek: Der Stand von OSIS; Datenschutz und Datensicherung DuD 4 (1985) 213–217

RiSh_84 R. L. Rivest, A. Shamir: How to Expose an Eavesdropper; Communications of ACM 27/4 (1984) 393–395

RSA_78 R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of ACM 21/2 (1978) 120–126 und 26/1 (1983) 96–99

ScSc_84 C. Schwarz-Schilling (ed.): Konzept der Deutschen Bundespost zur Weiterentwicklung der Fernmeldeinfrastruktur; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn 1984

ScSc1_84 C. Schwarz-Schilling (ed.): ISDN – die Antwort der Deutschen Bundespost auf die Anforderungen der Telekommunikation von morgen; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn 1984

ScSc_86 C. Schwarz-Schilling (ed.): Mittelfristiges Programm für den Ausbau der technischen Kommunikationssysteme; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn 1986

Sedl_88 H. Sedlak: The RSA cryptography processor; Eurocrypt '87, LNCS 304, Springer-Verlag, Heidelberg 1988, 95–105

Shan_49 C. E. Shannon: Communication Theory of Secrecy Systems; The Bell System Technical Journal 28/4 (1949) 656–715

Simm_88 G. Simmons: A Survey of Information Authentication; Proceedings of the IEEE 76/5 (1988) 603–620

Thom_84 K. Thompson: Reflections on Trusting Trust; Communications of ACM 27/8 (1984) 761–763

TuCh_85 M. Turoff, S. Chinai: An Electronic Information Marketplace; Computer Networks and ISDN Systems 9/2 (1985) 79–90

VaVa_85 U. Vazirani, V. Vazirani: Efficient and Secure Pseudo-Random Number Generation; Crypto '84, LNCS 196, Springer-Verlag, Berlin 1985, 193–202

VHVD_88 I. Verbauwhede, F. Hoornaert, J. Vandewalle, H. De Man: Security considerations in the design and implementation of a new DES chip; Eurocrypt '87, LNCS 304, Springer-Verlag, Berlin 1988, 287–300

Waid_85 M. Waidner: Datenschutz und Betrugssicherheit garantierende Kommunikationsnetze. Systematisierung der Datenschutzmaßnahmen und Ansätze zur Verifikation der Betrugssicherheit; Diplomarbeit, Interner Bericht 19/85 der Fakultät für Informatik, Universität Karlsruhe 1985

WaPf_86 M. Waidner, A. Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer-Verlag, Heidelberg 1985, 128–141; Überarbeitung erschien in: Datenschutz und Datensicherung DuD 1 (1986) 16–22

WaPf_87 M. Waidner, B. Pfitzmann: Verlusttolerante elektronische Brieftaschen; 3. Fachtagung Fehlertolerierende Rechensysteme, IFB 147, Springer-Verlag, Heidelberg 1987, 36–50; Überarbeitung: Datenschutz und Datensicherung DuD 10 (1987) 487–497

WaPf1_87 M. Waidner, B. Pfitzmann: Anonyme und verlusttolerante elektronische Brieftaschen; Interner Bericht 1/87 der Fakultät für Informatik, Universität Karlsruhe 1987

WaPf_89 M. Waidner, B. Pfitzmann: Unconditional Sender and Recipient Untraceability in spite of Active Attacks – Some Remarks; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 5/89, März 1989

WaPf1_89 M. Waidner, B. Pfitzmann: The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability; Universität Karlsruhe 1989; Eurocrypt '89 voraussichtlich: LNCS, Springer-Verlag, Berlin 1990

WaPf_90 M. Waidner, B. Pfitzmann: Loss-tolerant Electronic Wallet; Proc. Smart Card 2000, Amsterdam 1989; gekürzte Version: 20th International Symposium on Fault-Tolerant Computing (FTCS-20); IEEE Computer Society, 1990

WaPP_87 M. Waidner, B. Pfitzmann, A. Pfitzmann: Über die Notwendigkeit genormter kryptographischer Verfahren; Datenschutz und Datensicherung DuD 6 (1987) 293–299

WeCa_79 M. N. Wegman, J. L. Carter: New Classes and Applications of Hash Functions; 20th Symposium on Foundations of Computer Science (FOCS) 1979, IEEE Computer Society, 1979, 175–182