erschien in: Dieter Klumpp, Herbert Kubicek, Alexander Roßnagel (Hg.): next generation information society? Notwendigkeit einer Neuorientierung; Talheimer Verlag, Mössingen-Talheim 2003, Seite 290 – 299

Digitale Glaubwürdigkeit und Privatsphäre in einer vernetzten Gesellschaft

Andreas Pfitzmann, Sandra Steinbrecher

Heute bewegen viele Menschen sich im weltweiten Netz mit seinen Einkaufs- und Informationsmöglichkeiten genauso selbstverständlich wie in unseren Städten. Unterzugehen in der Masse ist dabei typisch für einen Stadtbummel, ebenso wie für die Fahrt mit der Straßenbahn dorthin.
Anonymität ist der Zustand nicht identifizierbar zu sein innerhalb der anderen Menschen, die gerade das Gleiche wie man selbst tun (der so genannten Anonymitätsmenge). Der Begriff der Anonymität ist demnach eng mit dem der Verkettbarkeit von Menschen und Handlungen verknüpft. Oft hat ein Mensch das Bedürfnis, dass bestimmten anderen Menschen unklar ist, ob, sowie wo, wann und unter welchen Umständen er eine bestimmte Handlung ausgeführt hat. Einfach gesagt gilt, dass je größer eine Gruppe ist und je ähnlicher sich die Mitglieder der Gruppe verhalten, desto größer ist die Anonymität jedes einzelnen Gruppenmitgliedes.
Im Zuge der Entwicklung der Informationsgesellschaft tritt dabei auch das berechtigte Bedürfnis auf, dass unklar ist,

- wer sich für welche Informationen interessiert:
  Klassische Medien wie Rundbriefe, Zeitung, Rundfunk und Fernsehen entsprechen dem Bedürfnis der Geheimhaltung des Interesses an Informationen, indem die Verteilung von Informationen an viele Menschen erfolgt, von denen jeder einzelne lokal in seinem Vertrauensbereich aus dem Informationsangebot das ihn Interessierende auswählen kann, ohne dass die Urheber der Informationen und Externe ihn beobachten können. Dabei wird durch die Menge der Leser und die Menge der Informationen in den klassischen Medien die Ungewissheit definiert, wer sich für was interessiert.
- wer mit wem Informationen austauscht:
  Die Geheimhaltung derjenigen, die Informationen austauschen, erfolgte schon immer klassischerweise über Boten, die typischerweise viele Informationen auf Papier von vielen Absendern an viele Empfänger transportieren. Dabei ist zwar in der Regel der Versand und Erhalt einer Botschaft beobachtbar, nicht jedoch welche erhaltene Botschaft zu welcher empfangenen gehört, d.h. durch die Mengen von Sendern und Empfängern wird die Ungewissheit definiert, wer wem eine Nachricht gesendet hat.

Eine Selbstidentifikation findet in der Regel nur auf Verlangen statt. Der Nutzer des ÖPNV zeigt dem Kontrolleur seine Jahreskarte, der Bibliotheksbesucher beim Ausleihen der Angestellten seinen Mitgliedsausweis, der Patient beim Arzt bei der Anmeldung seine Krankenkassen-Chipkarte. Alle diese Karten enthalten hoffentlich nur die persönlichen Informationen, die der Gegenüber zur Identifikation bzw. zum Berechtigungsnachweis benötigt.

Die Entwicklung der vernetzten Gesellschaft

Das Internet wurde jedoch mit dem ISO/OSI-Schichtenmodell genau umgekehrt konstruiert. Standardmäßig werden auf den unteren Kommunikationsebenen identifizierende Merkmale übertragen. Das Lesen einer Internetseite ist aus diesem Grund keinesfalls vergleichbar anonym

zum Lesen einer Zeitung. Wann immer sich ein Nutzer mit einem Rechner ohne Schutzmechanismen in die Weiten der vernetzten Welt begibt, d.h. zum Beispiel mit einem Browser im Internet surft, über einen Mailserver E-Mails versendet oder mit einem File-Sharing-Programm Dateien austauscht, kann sein Verhalten beobachtet werden. Der Grund dafür ist, dass jeder mit dem Internet verbundene Rechner in diesem über die so genannte IP-Adresse identifiziert wird, damit der Nutzer auch eine Antwort auf seine Internetanfrage erhalten kann (z.B. die angeforderte Webseite). Ein permanent an das Internet angebundener Rechner hat eine fest zugewiesene IP-Adresse, während Rechner, die sich durch Einwahl bei einem Internetserviceprovider (ISP) oder durch 'Einklinken' in ein mobiles Datennetz (W-LAN, Bluetooth) mit dem Internet verbinden, für diesen Zeitraum eine dynamisch zugewiesene IP-Adresse erhalten.
Fest zugewiesene IP-Adresse sind innerhalb eines Teilnetzes durch dessen Betreiber einem Nutzer zugeordnet. Auch jeder andere Beobachter, der die Zuordnung zwischen diesem und der IP-Adresse kennt, kann Internetanfragen diesem Nutzer zuordnen. Dazu reicht bereits der Empfang einer E-Mail vom beobachteten Nutzer, da diese die IP-Nummer seines Rechners enthält.
Von einem ISP dynamisch zugewiesene IP-Adressen sind hingegen nur für diesen mit dem Telefonanschluss (sei er stationär oder mobil), von dem er angewählt wurde, verknüpft. Selbiges gilt für Betreiber von mobilen Datennetzen, die 'sich einklinkende' Rechner über deren MAC-Adresse identifizieren, wenn der Nutzer keine Vorsichtsmaßnahmen trifft. ISPs bzw. Netzbetreiber wissen, wem sie wann welche IP-Adresse zugewiesen haben, und können Internetanfragen wiederum dieser IP-Adresse zuordnen. In der Regel werden sie auch eine mindestens für Abrechnungszwecke nötige Log-Datei darüber führen. Vielleicht haben die Nutzer gar persönliche Kennungen, zu denen sie zusätzlich zum Telefonanschluss bzw. zur MAC-Adresse zugeordnet werden können. Außenstehende Beobachter können hingegen ohne Kooperation mit dem ISP bzw. Netzbetreiber Internetanfragen nicht Nutzern zuordnen.
Bei Nutzung mobiler Telefonnetze können durch deren Betreiber gar Bewegungsprofile erstellt werden. Selbst wer gerade nicht telefoniert, SMS/MMS versendet oder in Zukunft immer mehr Dienste per UMTS nutzen wird, ist überwachbar durch sein Handy, das eine eindeutige Kennung per Funk verbreitet, so dass nicht nur der aktive Austausch von Informationen überwachbar ist, sondern eben auch Bewegungsprofile erstellt werden können.

Bewahrung der Privatsphäre in der vernetzten Gesellschaft
Ideal wäre, wenn die Vernetzung innerhalb der Gesellschaft von vorneherein so konstruiert worden wäre, dass Anonymität technisch grundsätzlich gewährleistet und nur im Bedarfsfall eine Selbstidentifikation durchgeführt wird. Da jedoch unrealistisch ist, dass ein entsprechendes Redesign erfolgt, bleibt Folgendes die Aufgabe des technischen Datenschutzes: Wenn anonymer Austausch von Informationen innerhalb der vernetzten Gesellschaft erfolgen soll, ergibt sich aufgrund der Konstruktion der Netze die Notwendigkeit, die eindeutig identifizierenden Merkmale, die das eigene Gerät im Netz überträgt, in einer „Anonymisierungsschicht“ zu entfernen. Theoretisch zufriedenstellende Möglichkeiten dazu wurden bereits in den 80er Jahren des letzten Jahrhunderts geschaffen.

Broadcast
Da Anonymität eines Nutzers davon abhängt, wie ähnlich sich seine Anonymitätsmenge verhält, ist die sicherste Lösung, die Interessen eines Nutzers geheim zu halten, die Verteilung jeder Information an alle Nutzer, das so genannte Broadcast, wie es bei der oben bereits genannten Verteilung über klassische Medien geschieht.
Die Verlagerung der klassischen Medien ins Internet, wo die Mehrzahl der Zeitungen, Zeitschriften,

Radio- und Fernsehsender bereits umfangreiche Angebote bereithält, und die Personalisierung der Angebote im Bereich des Fernsehens (z.B. Video on Demand, Pay per View) führt jedoch dazu, dass standardmäßig der Zugriff auf Informationen nicht mehr anonym erfolgt.
Dabei ist personalisierter Zugriff auf Informationen auch per Broadcast möglich. Will ein bestimmter Nutzer unbeobachtbar nur für ihn bestimmte Informationen empfangen, wird er mithilfe von impliziten Adressen adressiert, die nur ihm und dem Sender bekannt sind. Erst in seinem Vertrauensbereich werden die empfangenen Broadcast-Informationen nach den an ihn adressierten Informationen durchsucht. Falls der Empfänger auch gegenüber dem Sender anonym sein möchte, kann die Verteilung der impliziten Adressen anonym erfolgen. Falls verhindert werden soll, dass andere Teilnehmer die Nachricht lesen können, muss die Nachricht zusätzlich für den Empfänger verschlüsselt werden.
Praktische Umsetzung waren einige der Pagerdienste der Telekommunikationsunternehmen, die zu Beginn der 1990er Jahre in Mode waren. Jeder Funkruf wurde in dem Gebiet, in dem sich der gesuchte Empfänger befand, mit seiner Funkrufnummer ausgestrahlt. Der Pager durchsuchte diesen Datenstrom nach seiner eigenen Adresskennung und speicherte die zugehörigen Daten. Einige Geräte konnten auch ohne Angabe der eigenen Identität gekauft werden, was vor Außenstehenden anonymes Empfangen ermöglichte.
Wenn Adressen mehrfach verwendet werden (wie eben bei den Pager-Diensten), ist der Nachteil, dass alle Teilnehmer erkennen, welche Nachrichten an denselben Nutzer gesendet werden.

Kommunikation über Umwege

Effizienter ist es, Informationen, die nicht für viele potentiell Interessantes enthalten, nicht an alle zu verteilen, sondern sich Boten zu bedienen. In der vernetzten Gesellschaft werden dazu die Informationen über Umwege geleitet. Die dabei verwendete Methode des Umwegs beeinflusst die maximale "Stärke" der Beobachter, vor denen ein Nutzer gerade noch anonym ist, und die Menge der Nutzer, die den gleichen Umweg nutzen, die Anonymitätsmenge.
Gegenüber externen Beobachtern und Webservern genügt bereits die Einwahl über den ISP mit dynamisch vergebener IP-Nummer oder gemeinsame Benutzung eines Rechners, um die Anonymität eines einzelnen Nutzers innerhalb der betreffenden Gruppe von Nutzern zu gewährleisten. Ein Nutzer, der durch eine einzelne IP-Adresse identifizierbar ist oder der die Anonymität gegenüber seinem ISP oder Netzbetreiber wünscht, sollte zusätzlich Anonymisierungsdienste, die seinen Webzugriff über Umwege leiten, verwenden.
Die einfachste Lösung zum Web-Surfen ist die Verwendung von Anon-Proxies oder freien Proxies, die zwischen den Browser eines Internetnutzers und die von ihm angefragten Webserver geschaltet werden. Ein Proxy hat die Aufgabe, vom Nutzer angefragte Webseiten in seinem Namen abzurufen und für mögliche wiederholte Abrufe zwischenzuspeichern (Caching). Gegenüber einem Webserver tritt er als Client, gegenüber dem Browser jedoch als Webserver auf. Zu den Anon-Proxies zählen z.B. Anonymizer (www.anonymizer.com), Rewebber (www.rewebber.com) oder Freedom WebSecure (www.freedom.net). Offene Proxies werden unter Umständen unwissentlich/unbeabsichtigt durch ihren Betreiber als solche betrieben.
Proxies realisieren zwar Anonymität gegenüber dem eigenen ISP bzw. Netzbetreiber, nicht jedoch gegenüber dem Betreiber des Anon-Proxies, d.h. dieser kann die dem Nutzer zugeordnete IP-Adresse mit der angefragten Webseite verknüpfen. Damit wird das Vertrauen des Nutzers bzgl. Seiner Anonymität lediglich verlagert.
Gegen die Beobachtung durch einzelne Proxies hilft die Hintereinanderschaltung verschiedener Proxy-Server. Beim System Crowds[ReRu98] werden die Webzugriffe über zufällig ausgewählte

[ReRu98] M. K. Reiter and A. D. Rubin: Crowds: Anonymity for Web Transactions; ACM Transactions on Information

Teilnehmer des Systems geleitet, bevor sie den Webserver erreichen. Bei jedem Teilnehmer wird die Anfrage, gesteuert von einem Zufallsprozess, entweder direkt an den Server geschickt oder zu einem weiteren Teilnehmer. Die Kommunikationsinhalte werden bei Crowds im Gegensatz zu anonymen und freien Proxies zwischen den Nutzern verschlüsselt. Dies verbirgt den Inhalt der Anfragen vor fremden Blicken, nicht jedoch vor den Teilnehmern auf dem Weg einer Anfrage.
Leider realisieren weder Anon-Proxies, freie Proxies noch Crowds Unbeobachtbarkeit gegenüber externen Beobachtern, die große Teile des Netzes beobachten, also z.B. über Verkehrsanalysen Längen und Zeitpunkte von Nachrichten verketten könnten.
Der Schutz gegen Beobachter, die alle Bereiche überwachen können, ist unmöglich, da diese der Anfrage einfach auf ihrem gesamten Weg folgen könnten. Wohl ist es aber möglich und ratsam, den notwendigen "sicheren" Bereich immer kleiner zu machen oder diesen sogar so zu verteilen (räumlich und/oder organisatorisch), dass eine Anonymisierung noch sicher ist, wenn der Beobachter auch nur einen von vielen "sicheren" Bereichen nicht beobachtet.
Dies wird durch so genannte Mixe[Chau81] gewährleistet, die ursprünglich zum Versand von einzelnen Informationen über E-Mail entwickelt wurden. Dabei werden die Daten vom Sender mehrfach kodiert über mehrere Zwischenstationen, die so genannten Mixe, zum Empfänger geleitet. Jeder Mix empfängt dabei zunächst Nachrichten von mehreren Teilnehmern, bevor er sie umkodiert und umsortiert an den nächsten Mix bzw. an den Empfänger sendet. Eine Umkodierung besteht im wesentlichen aus einer Entschlüsselung. Umsortierung und Zwischenspeicherung verhindern Angriffe über zeitliche Verkettung, gleiche Nachrichtenlänge Angriffe über diese Eigenschaft. Mittlerweile existiert eine Reihe von weiterführenden Konzepten und Prototypen, die dieses Verfahren für viele Anwendungsgebiete adaptieren, z.B. für Echtzeit-Kommunikation per Telefon[PfPW91], Web-Surfen[BeFK01], Mobilkommunikation[FeJP96] etc.
Bei der Kommunikation über Mixe besteht prinzipiell die Wahl zwischen Mix-Netzen und Mix-Kaskaden. Bei ersteren wird für jeden Nutzer ein individueller Weg durch das Mix-Netz je nach Einschätzung der Vertrauenswürdigkeit und Zuverlässigkeit der Mixe gewählt; bei letzteren ist dieser Weg durch die Betreiber des Systems über feste Folgen von Mixen, die so genannten Kaskaden, vorgegeben. Da Anonymität eines einzelnen darauf beruht, dass sich möglichst viele andere ähnlich zu ihm verhalten, scheint die Verwendung von Mix-Kaskaden sinnvoller, da sie die Ähnlichkeit der Nutzer stärkt[BePS01]. Diesem Konzept folgt das Projekt AN.ON[BeFK01], während Onion-Routing[ReSG98] den ersten Weg wählte.
Auch für das immer populärer werdende File-Sharing gibt es inzwischen anonyme Realisierungen, von denen insbesondere Freenet[CSWH00] und GNUnet (www.gnu.org/software/GNUnet/) zu nennen sind. In diesen werden Informationen verteilt und verschlüsselt in einem Netz von Rechnern

---

and System Security 1(1), November 1998, pp. 66-92.

[Chau81] David Chaum: Untraceable electronic mail, return addresses and digital pseudonyms; Communications of the ACM, 24(2), 1981, pp. 84-88.

[PfPW91] A. Pfitzmann, B. Pfitzmann, and M. Waidner: ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead; Information Security, Proc. IFIP/Sec 91, pp. 245-258, Amsterdam, 1991.

[BeFK01] O. Berthold, H. Federrath, S. Köpsell: Web MIXes: A system for anonymous and unobservable Internet access; Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, Springer-Verlag, Heidelberg 2001, pp. 115-129.

[FeJP96] Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: MIXes in Mobile Communication Systems: Location Management with Privacy; Information Hiding, LNCS 1174, Springer-Verlag, Berlin 1996, pp. 121-135.

[BePS01] O. Berthold, A. Pfitzmann, R. Standtke: The Disadvantages of Free MIX Routes and How to Overcome Them; Designing Privacy Enhancing Technologies, LNCS 2009, Springer- Verlag, Berlin 2001.

[ReSG98] M.G. Reed, P.F. Syverson, D. Goldschlag: Anonymous Connections and Onion Routing; IEEE Journal on Selected Areas in Communication, Special Issue on Copyright and Privacy Protection, 1998.

[CSWH00] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong: Freenet: A Distributed Anonymous Information Storage and Retrieval System; Designing Privacy Enhancing Technologies, LNCS 2009, Springer-Verlag, Berlin 2001, pp. 46-66.

gespeichert, wobei jede Information über textuelle Schlüssel abrufbar ist. Richtet sich die Anfrage an einen Server, der die gewünschten Daten nicht lokal gespeichert hat, wird die Anfrage an benachbarte Rechner des Netzes weitergeleitet, bis die Daten auf einem Server gefunden werden. Auf dem Weg, den die Anfrage durch das Netz genommen hat, wird die Antwort dann zu dem entsprechenden Nutzer zurück übertragen. Unter der üblichen Annahme eines beschränkten Angreifers, der nicht alle Server kontrolliert und nicht alle Leitungen abhört, kann weder der Autor noch der Betreiber eines Servers noch sonst irgendein Nutzer wissen, in welchem Rechner welche Informationen gespeichert sind. Dies gewährleistet Zensurresistenz und Anonymität von Anfragern und Urhebern von Informationen. Im Zuge des neuen Urheberrechts versuchen aktuell auch klassische File-Sharing-Systeme durch Anonymitätskonzepte zu punkten, aber ihre Konzepte gehen kaum über die klassischen oben beschriebenen Proxy-Konzepte hinaus.
Neue Standards und die zunehmende Mobilität von Nutzern und Geräten stellen neue Aufgaben an den technischen Datenschutz. Das datenschutzgerechte IP-Routing bei Nutzung mobiler Geräte im Internet, der zusätzliche Schutz der Aufenthaltsorte von Teilnehmern und die Interaktion mit neuen Standards wie GPRS und UMTS erfordert ständige Anpassungen von Anonymitätsverfahren. Ein Wunsch für die Zukunft ist die Gewährleistung von Anonymität der Nutzer bereits beim Design neuer Standards.
Voraussetzung für alle Anonymitätskonzepte, insbesondere im Zuge der Mobilität, ist in jedem Fall ein Vertrauensbereich des Nutzers, der bloßes 'Über-die Schulter-Schauen' verhindert. In der Praxis wird der beste Schutz gegenüber externen Angreifern sinnlos, wenn die hochvertrauliche E-Mail in der Wartehalle des Flughafens gelesen wird. Vergleichbar dem, dass der Liebesbrief aus dem Briefkasten morgens in der Straßenbahn, statt abends im heimischen Schlafzimmer gelesen wird.
Ein wichtiges Ziel der Zukunft ist es, massentaugliche Anonymisierungsdienste zu schaffen, die eine gute Skalierbarkeit in der Hinsicht gewährleisten, dass der Nutzer eine Rückmeldung darüber erhält und in Grenzen mitbestimmen kann, wie groß seine eigene Anonymität zu einem bestimmten Zeitpunkt ist. Diese ist davon abhängig, wie ähnlich er sich zu den anderen Nutzern seiner Anonymitätsmenge gerade verhält. Bereits in der technischen Definition dieser Ähnlichkeit liegt eine große Herausforderung. Die obige Übersicht zeigt eine große Auswahl an verfügbaren Prototypen, wobei die Entwickler und Analysten der Systeme uns aber eine Messung und Skalierbarkeit der gewährten Anonymität, außer für kleine Beispiele, bisher schuldig geblieben sind.
Außerdem müssen die entwickelten Anonymisierungskonzepte im Interesse aller Mitglieder der Gesellschaft Strafverfolgung und Einzelüberwachung im berechtigten Einzelfall zulassen, ohne dass dabei die Anonymität der anderen Nutzer des entsprechenden Systems gefährdet wird. Auf allen höheren Anwendungsebenen sollte zudem eine Überprüfung der digitalen Glaubwürdigkeit einer Person erfolgen, sofern dies für die Nutzung eines elektronischen Angebotes vonnöten ist.

Glaubwürdigkeit in der vernetzten Gesellschaft

Das Vertrauen, das eine Person anderen Personen innerhalb einer Gesellschaft entgegenbringt, hängt in der Regel von Erfahrungen sowohl mit der betreffenden Person als auch mit anderen Personen in der Gesellschaft ab. Sozialwissenschaftler modellieren die Entscheidung, ob Personen einander vertrauen oder nicht, häufig als so genannte Trust Games[Dasg88]. Dabei haben sich im täglichen persönlichen Umgang gewisse Konventionen eingebürgert: Im Restaurant werden in der Regel auf mündliche Bestellung Essen und Getränke geliefert, wobei der Gast erst nach deren Verzehr ihren Gegenwert bezahlt. Dabei scheint es nur sehr selten zum Missbrauch zu kommen.

[Dasg88] P. Dasgupta: Trust as Commodity; in D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations, pp. 49-70, 1988.

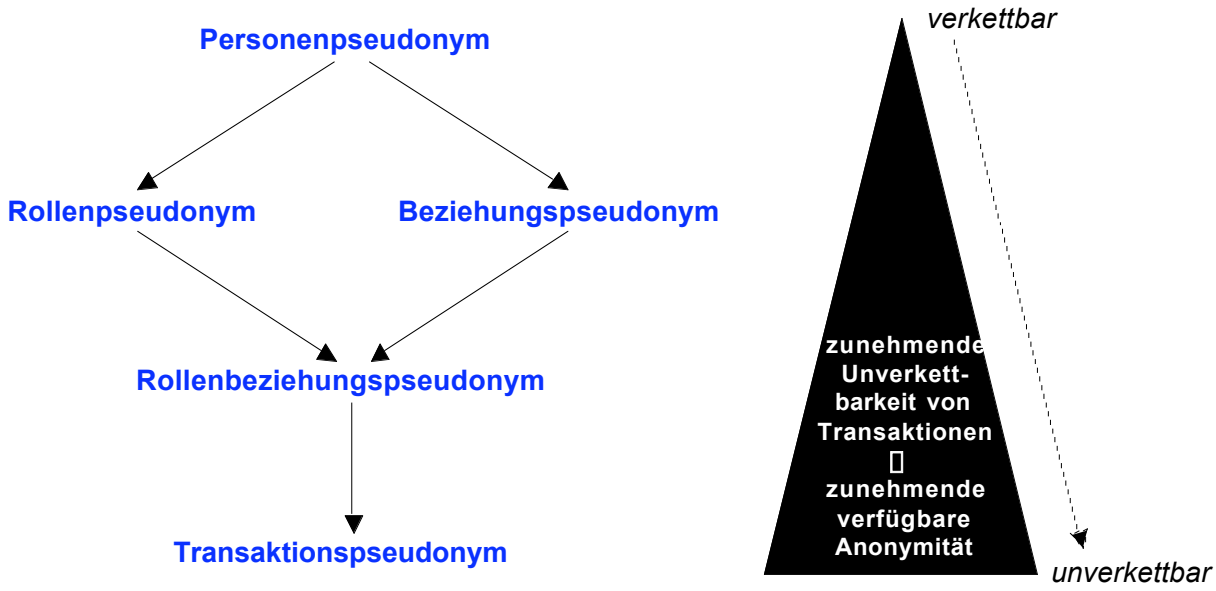
Sehr viel geringer scheint die Hemmschwelle von Konsumenten im Fernabsatzmarkt zu sein. Viele Anbieter lehnen aus diesem Grund insbesondere bei Erstbestellungen per Telefon oder Internet eine Lieferung auf Rechnung ab. Dabei würde die Kryptographie eine der handschriftlichen Unterschrift ähnlich sichere digitale Signatur bieten, die der Gesetzgeber dieser in Deutschland auch schon gleichgestellt hat. In Ermangelung massentauglicher Zertifizierungsstrukturen ist dies aber bisher praktisch keinesfalls umgesetzt. Damit muss die Erstbestellung nach wie vor oft zähneknirschend auf Papier oder durch Zahlung per Vorkasse oder Nachnahme erfolgen.
Während die technische Konstruktion des Internetzugangs und des Internets als solchem eine Massenüberwachung ermöglichen könnte, ist andererseits jedoch eine gezielte und direkte Überprüfung der Identität oder Qualifikation eines Nutzers durch den Diensteanbieter im Internet meist schwierig. Insbesondere der Nachweis spezifischer Eigenschaften eines Nutzers fehlt. Im Supermarkt um die Ecke kann der Verkäufer meist per 'Gesichtskontrolle' oder im Zweifelsfall durch Überprüfen des Personalausweises verifizieren, dass sein Gegenüber das erforderliche Alter für den Erwerb bestimmter Filme aufweist. Im Internet existiert diese Möglichkeit hingegen derzeit nicht.
Bei Realisierung einer entsprechenden Identitätskontrolle im Internet muss dabei berücksichtigt werden, dass die Kontrolle im Supermarkt nur kurz visuell erfolgt, während der entsprechende Internet-Shop übermittelte Daten dauerhaft maschinell speichern kann. Dies führt dazu, dass abgewogen werden muss zwischen dem Wunsch nach Privatsphäre des Einzelnen gegenüber der Glaubwürdigkeit, die andere, mit denen er agiert, von ihm erwarten können. Das Konzept des so genannten Identitätsmanagements gibt dem einzelnen die Möglichkeit, diese Abwägung praktisch vorzunehmen.

Identitätsmanagement

Bereits zahlreiche Dienstleister haben den Markt für Identitätsmanagement erkannt und bieten Identitätsmanagementsysteme an, die die Identität nebst verschiedener Eigenschaften eines Nutzers einmalig überprüfen. Auf Wunsch des Nutzers können diese Daten anderen Anbietern zur Verfügung gestellt werden, womit die Identifikation bei Nutzung eines neuen Dienstes im Internet einfacher für Nutzer und Anbieter und insbesondere auch zuverlässiger für letztere vonstatten geht.
Dabei muss zwischen client- und serverbasiertem Identitätsmanagement unterschieden werden. Clientbasiertes Identitätsmanagement belässt alle Daten unter Kontrolle des Nutzers und ermöglicht ihm situationsabhängig zu entscheiden, welche personenbezogenen Daten er welchem Kommunikationspartner zu welchem Zweck gibt, und eine Protokollierung, wann welche Herausgabe erfolgte. Diese Anwendung erfolgt natürlich bevorzugt in seinem persönlichen Endgerät. Beim serverbasierten Identitätsmanagement übergibt der Nutzer seine Daten an eine fremde Instanz, die für ihn den Überblick über diese und ihre Verwendung behält.
Zu den bekanntesten Vertretern des serverbasierten Identitätsmanagements gehören derzeit Microsoft .net Passport (www.passport.net) und das Liberty Alliance Project (www.projectliberty.org). Im ersteren Fall sind die personenbezogenen Daten auf einem zentralen Server, im zweiten Fall verteilt auf den Servern der an dem Projekt beteiligten Firmen gespeichert. Wichtigste Eigenschaft für den Nutzer dieser Systeme ist das Single-Sign-On (d.h. die Authentifikation bei einem Server wird auf alle anderen beteiligten übertragen), doch gerade in diesem Automatismus besteht die Gefahr für die Privatsphäre des betreffenden Nutzers.
Datenschutzkonforme Identitätsmanagementsysteme[CPHH02] ermöglichen dem Nutzer hingegen selbst, seine Anonymität bzw. Pseudonymität zu steuern, und sind natürlicherweise aus diesem

[CPHH02] Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, Els Van Herreweghen: Privacy-Enhancing Identity Management; in: IPTS-Report 67 (September 2002); JRC Seville, 2002; pp. 8-16.

Grund client-basiert. Pseudonymität beschreibt dabei die Möglichkeiten der Verkettung, die sich durch bestimmte Merkmale oder Identifikatoren von Nachrichten und Personen ergeben. Es lassen sich unterschiedliche Klassen von Pseudonymen unterscheiden (siehe Abbildung 1)[KöPf01]:



A B bedeutet „B ermöglicht stärkere Anonymität als A“

- Personenpseudonyme bieten die größte Verkettbarkeit von Aktionen in unterschiedlichen Kontexten, die der Pseudonyminhaber ausführt.
- Unter einem Rollenpseudonym versteht man einen durch den Inhaber gewählten Namen, den er immer dann in der Kommunikation mit seiner Umwelt verwendet, wenn er sich in der zugehörigen Rolle befindet. Auf diese Weise muss nicht zwangsläufig bekannt werden, wer sich dahinter verbirgt. Bei häufiger Verwendung des Rollenpseudonyms kann der Kreis der in Frage kommenden Personen meist jedoch eingegrenzt und im Extremfall eben doch eine Identifikation durchgeführt werden.
- Dasselbe Beziehungspseudonym wird verwendet, solange mit demselben Kommunikationspartner kommuniziert wird. Dies ist unabhängig von der Rolle, die man in der jeweiligen Situation innehat. Man verwendet also denselben Namen, egal ob man geschäftlich oder privat Kontakt zu einer bestimmten Person aufnimmt.
- Will man die Verkettbarkeit noch weiter reduzieren, so kommen Rollenbeziehungspseudonyme zum Einsatz. Dabei wird je nach Kommunikationspartner und Rolle ein anderes Pseudonym verwendet.
- Die stärkste Anonymität bieten Transaktionspseudonyme. Dabei wird für jede Transaktion ein anderes Pseudonym verwendet.

Beim datenschutzkonformen Identitätsmanagement wird der Nutzer unterstützt, die für die jeweilige Anwendung richtigen Pseudonyme zu wählen und so letztlich zu bestimmen, wer welche Informationen über ihn erhält und womit verketten kann. Gleichzeitig wird die notwendige Infrastruktur bereitgestellt, die insbesondere auch die Anbindung an den Kommunikationspartner

[KöPf01] M. Köhntopp, A. Pfitzmann: Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology, Draft v0.12, June 2001.

(z.B. einen Server) herstellt und diesem ermöglicht, pseudonyme Transaktionen zu verarbeiten. Dabei kann der Nutzer unter verschiedenen Pseudonymen im Netz agieren, wobei mit Hilfe von digitalen Zertifikaten (beglaubigte) personenbezogene Daten durch Treuhänder an Pseudonyme gebunden und übermittelt werden können. So kann ein Diensteanbieter für die Diensterbringung benötigte Daten authentisch erhalten, ohne dass der Nutzer notwendigerweise alle Bestandteile seiner realen Identität samt Interessen preisgibt bzw. ohne dass umfangreiche Profile über ihn erstellt werden können. Es ist darüber hinaus möglich, Treuhänderdienste in Anspruch zu nehmen, die in begründeten Fällen die Identität eines Nutzers aufdecken können. Ein datenschutzkonformes Identitätsmanagementsystem trägt dazu bei, dass die Interessen von Nutzern und Anbietern gleichermaßen gewahrt bleiben.

Auch im Bereich des Identitätsmanagements liegt in der Zukunft eine große Herausforderung darin, dem Nutzer wie bei den darunter liegenden Anonymisierungsdiensten eine Skalierbarkeit und Messung seiner Anonymität bzw. Pseudonymität zu bieten.

Datenschutzgerechte Identitätsmanagementsysteme zu schaffen, die sich auch am Markt bei vielen Anbietern durchsetzen, ist eine Herausforderung an die vernetzte Gesellschaft der Zukunft. Erst dadurch wird datenschutzgerechter und glaubwürdiger (und damit erfolgreicher) elektronischer Handel sowie ein Electronic Government möglich.