Wie viel Anonymität verträgt unsere Gesellschaft?

Stefan Köpsell, Andreas Pfitzmann

Fakultät Informatik
Institut für Systemarchitektur
TU Dresden
01062 Dresden
{sk13,pfitza}@inf.tu-dresden.de

Zusammenfassung: Ausgehend von einem Überblick über die Möglichkeiten anonymen Handelns in der Vergangenheit und in der heutigen Situation einer vernetzten Welt werden einige Verfahren vorgestellt, die Formen anonymen Handelns auch in diese neue Welt übertragen sollen. Anonymität wird dabei nicht als Selbstzweck, sondern als Mechanismus verstanden, um seine eigene Privatheit zu schützen. Es wird dargelegt, daß dies nicht nur verträglich, sondern notwendig für die Gesellschaft ist – wobei sich diese an die neue Situation anpassen muß.

1 Technik und Gesellschaft

Um eine kurze und einfache Antwort auf die Frage des Titels zu geben: viel, sehr viel! Die nachfolgenden Ausführungen sollen diese Behauptung durch einige Argumente belegen und gleichzeitig zum Nachdenken über den Nutzen von Anonymität für die Gesellschaft anregen.

Informatiker haben, wenn sie über Kommunikation nachdenken – und letztlich geht es bei Anonymität ja um das Verbergen von identifizierenden Merkmalen bei der Kommunikation mit anderen Entitäten – oftmals ein Schichtenmodell im Hinterkopf, sei es das ISO/OSI-Referenzmodell oder die einzelnen Kommunikationsschichten im Internet. Aus technischer Sicht ergeben sich im Zusammenhang mit Anonymität die Möglichkeiten, entweder auf ein Netz aufzubauen, das identifizierende Merkmale überträgt und diese in der „Anonymisierungsschicht“ zu entfernen, oder eine per se anonyme Kommunikationsinfrastruktur zu verwenden und bei Bedarf eine Selbstidentifikation durchzuführen. Interessanterweise kann man nun dieses „Schichtenmodell“ aus dem technischen Kontext herauslösen und auf unser tägliches Leben und somit in den Bereich „Gesellschaft“ übertragen. Noch interessanter (und aus unserer Sicht: bedenklicher) ist, daß in den letzten 15 Jahren im Vergleich zu „früher“ ein Wechsel zwischen diesen beiden Paradigmen der Schichtung vollzogen wurde.

Früher war Anonymität das Gegebene – sozusagen die untere Schicht. Bezahlt wurde mit (anonymem, weil nicht zuordenbarem) Bargeld. Informationen wurden über Broadcast-Medien wie Radio oder Fernsehen verteilt, die eine Zuordnung, wer welche Informationen empfangen hat, unmöglich machen (siehe Abbildung 1). Zeitungen wurden am Kiosk gekauft – wobei es völlig egal war, welches konkrete Exemplar einer Zeitung man kauft, da der Inhalt identisch ist. Briefe wurden noch in gelbe Kästen geworfen und waren trotz ihrer Individualität doch so gleich, daß sich kein Postbeamter gemerkt haben dürfte, wann

er welchen Brief von wem an wen zugestellt hat. Telefoniert wurde aus gelben Häuschen, die als Objekte des öffentlichen Raums durch eine große Gruppe von Menschen benutzt wurden. Generell gab es eine viel geringere Nutzung von elektronischen Datenverarbeitungsanlagen – statt dessen wurden papierene Akten, die von Menschen bearbeitet wurden, eingesetzt. Und damit war die den Menschen inne wohnende Vergeßlichkeit und die von großen Aktenbergen im Laufe der Zeit ausgehende Unauffindbarkeit verbunden.

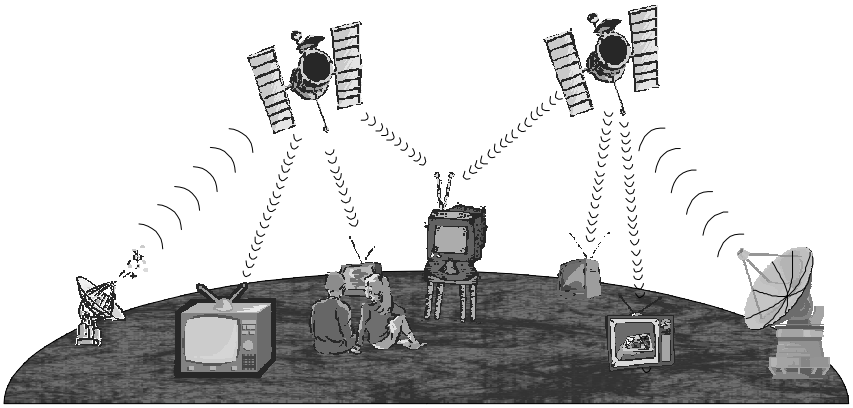


Abbildung 1: Broadcast bietet Empfängeranonymität

Um diese Grundform der Anonymität zu umgehen, waren aufwendige Maßnahmen notwendig. Die Selbstidentifikation, also die Bekanntgabe, wer man ist gegenüber Dritten, war ein bewußter Akt, in dem man typischerweise (s)einen (Personal)ausweis vorzeigte. Auch die Fremdidentifikation (also jemand identifiziert jemanden anderen) war ein Vorgang, der demjenigen, der identifiziert wurde, zumindest bekannt, wenn nicht in aller Regel bewußt gemacht wurde.

Die andauernde Veränderung und Erweiterung der technischen Möglichkeiten brachte (wie zu allen Zeiten in der Vergangenheit auch) entsprechende Veränderungen in der Gesellschaft und dem damit verbundenen „Schichtenmodell“. Die nahezu in allen Bereichen eingesetzte elektronische Datenverarbeitung verbunden mit den gigantischen Speichermöglichkeiten (zu sehr geringen Kosten), die effizienten Such-, Filter- sowie Auswertemöglichkeiten verhindern ein „Vergessen“ oder „Nichtmehrauffinden“ von Informationen. Die Grundannahme ist nicht mehr, daß Anonymität gegeben ist, die durch Identifikation aufgehoben werden muß. Vielmehr ist nahezu sämtliche Kommunikation mit identifizierenden Merkmalen verbunden, die die Anonymität erschweren, wenn nicht gar unmöglich machen und gleichzeitig Verkettungen von Kommunikationsvorgängen erlauben, die „früher“ nur mit sehr großem Aufwand herstellbar waren.

Bezahlt wird heute mit EC- oder Kreditkarten, deren eindeutige Nummern eine Zuordnung der Bezahlvorgänge zu einer Person und die Verkettung untereinander und somit Profilbildung ermöglichen. Es gibt selbst Überlegungen, in die bisher als „anonym“ geltenden

Euro-Banknoten RFID-Tags zu integrieren. Diese Tags enthalten eine eindeutige Nummer, die per Funk ausgelesen werden kann. Auch ein beschreibbarer Speicher ist vorstellbar, der dann einzelne Banknoten noch genauer kennzeichnet, um ihren Weg besser verfolgen zu können [Heise1].

Internet-Radio und *Video on Demand* oder das *Pay per View* Angebot von Premiere führen dazu, daß heute ganz genau analysiert werden kann, wer sich zu welcher Zeit für welche Informationen, Filme und Sendungen interessiert hat. Gleiches gilt für die digitalen Angebote vieler Zeitungen und Zeitschriften wie beispielsweise Spiegel-Online (www.spiegel.de/), Bild.de (www.bild.de/) etc. Erfolgt hier eine noch stärkere Verdrängung der „Papierausgabe“ – etwa mittels „elektronischem Papier“ und Online-Download der jeweils interessanten Artikel – so wird es nicht mehr möglich sein, anonym auf von der allgemeinen Meinung abweichende Informationen zuzugreifen. Gleichzeitig wird mit dem fortschreitenden Übergang zu elektronischen Medien die Personalisierung von Zeitungen und Ähnlichem zunehmen. Dies bedeutet, daß ich genau die Informationen vorfinde, dich mich interessieren – gleichzeitig weiß derjenige, der diese speziell auf mich zugeschnittenen Informationen bereitstellt, natürlich auch, wofür ich mich interessiere. Daß auch heute schon nicht alle Menschen bereit sind, auf Anonymität in diesem Bereich zu verzichten, sieht man an den „neutralen und diskreten braunen Umschlägen“, denen sich manche Versender von Printmedien bedienen.

Die gelbe Briefpost wird zunehmend von E-Mails abgelöst, deren Absender und Empfänger leicht zu identifizieren, deren Wege und Inhalte leicht zu speichern und deren Kommunikationsdaten noch in Jahren schnell abrufbar sind. Generell ist die Vorstellung vom anonymen Internet momentan eine Fiktion. Telefoniert wird heute mit Handys, die ihre eindeutige Kennung per Funk verbreiten, so daß es nicht nur sehr leicht möglich ist, ein Telefongespräch genau den an der Kommunikation Beteiligten zuzuordnen, sondern gleichzeitig auch noch exakt bestimmt werden kann, an welchen Orten sich die Kommunikationspartner befinden. Selbst wenn keine Kommunikation stattfindet, lassen sich Bewegungsprofile ohne großen Aufwand erstellen.

Die Fortschritte in der Speicher- und Verarbeitungstechnologie, der Erfaßbarkeit generell, führen dazu, daß die Anonymität aus vielen Bereichen des Lebens verdrängt wird, in denen sie noch vor nicht allzu langer Zeit als selbstverständlich und gegeben angenommen wurde. Mittels Mobilkommunikation, Videoüberwachung, Fingerabdrucks-, DNS- und anderer Biometrie-Datenbanken wird es möglich sein, immer genau zu wissen, welche Personen sich zu welcher Zeit an welchem Ort aufgehalten haben. Es wird möglich sein, weitgehend nachzuvollziehen, was sie dort getan haben.

Diese und andere Formen der Fremdidentifikation werden zudem so angewendet, daß demjenigen, der identifiziert wird, nicht bewußt gemacht wird, daß eine Identifizierung stattfand. Oftmals ist es noch nicht einmal durch den Betroffenen feststellbar. Zwar gibt es für manche Bereiche, in denen Eingriffe in die Privatsphäre vorgenommen werden (etwa bei der ständig steigenden Telefonüberwachung), gesetzliche Regelungen, die genau dieses „Wahrnehmen und Bekanntmachen“ zumindest im Nachhinein vorschreiben – jedoch findet dies in der Praxis oft schlicht nicht statt.

Durch die Einfachheit und gleichzeitige Präzision des Vergleichs digitaler Bitmuster ist heute jede „Unbestimmtheit“ beim Wiedererkennen bzw. Identifizieren von Personen und

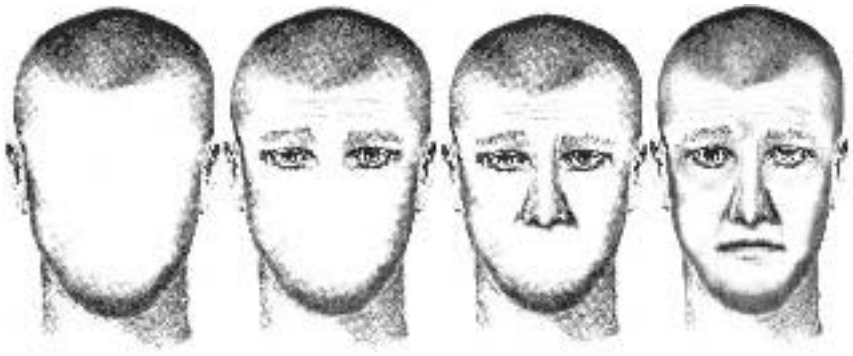


Abbildung 2: Beschreiben von fremden Personen ist schwierig und verhindert so das „Tratschen“ über andere [SZ]

der Verkettung ihrer Aktivitäten verlorengegangen. Die Maxime, daß man „mit Leuten reden sollte aber nicht über sie“ fand in der Vergangenheit sicher auch deshalb Beachtung, weil es extrem schwierig war, Leute, die man nicht persönlich kennt und die man (eventuell nur kurz) gesehen hat, präzise einem anderen zu beschreiben, so daß dieser sie ebenfalls erkennen würde. In einem Artikel der Sächsischen Zeitung ist dies sehr schön dargestellt – in einem Experiment versuchte die Reporterin, einen ihr unbekannten Mann, den sie in der Straßenbahn intensiv beobachtet hat, einem Polizeizeichner zu beschreiben und mit dessen Hilfe ein Phantombild zu erstellen [SZ]. Das Ergebnis war „eine gewisse Ähnlichkeit“ mit der beobachteten Person. Ganz anders sieht es aus, wenn man digitale Identifikatoren wie E-Mail- oder IP-Adressen benutzt. Hier ist ein „Reden über andere“ sehr leicht möglich.

Letztlich beschäftigt sich das Gebiet des technischen Datenschutzes damit, den Wandel, der sich in den letzten Jahren vollzogen hat (weg von der Gegebenheit Anonymität – hin zur permanenten Identifikation) ein Stück weit rückgängig zu machen oder wenigstens den heutigen Zustand in die Welt der zunehmenden Digitalisierung zu retten. Es kommt also darauf an, technische Verfahren zu entwickeln, die trotz einer Kommunikationsinfrastruktur mit identifizierenden Merkmalen eine anonyme Kommunikation ermöglichen.

Abschließend sei noch angemerkt, daß interessanterweise vor 15 Jahren Begriffe wie „anonym“ oder „Anonymität“ deutlich negativer belegt waren als heute, obwohl damals im Vergleich zu heute vielmehr „Grundanonymität“ gegeben war. Auch scheint die Gesellschaft gelernt zu haben, mit eingeschränkter Zurechenbarkeit zu leben, in Bereichen, in denen es „schon immer“ so war. Wie sonst ist zu erklären, daß noch niemand gefordert hat, daß auf allen Briefen ein Fingerabdruck des Absenders sein muß – wo doch spätestens nach dem 11. September klar geworden ist, welch tödliche Gefahr von einem Brief ausgehen kann?

2 Verfahren des technischen Datenschutzes

Dieser Abschnitt soll einige Verfahren des technischen Datenschutzes erläutern, die in Zusammenhang mit Anonymität stehen, deren Möglichkeiten und Grenzen aufzeigen, um

so schließlich analysieren zu können, ob diese Verfahren für die Gesellschaft „verträglich“ sind.

Generell beschränken sich die Darstellungen auf Kommunikation, die im Netz stattfindet, und die Anonymisierung der damit verbundenen Aktivitäten. Hierfür existieren Verfahren, die mit vernünftigem Aufwand zu realisieren sind. Maßnahmen zum Schutz gegen andere Beobachtungsformen, wie z.B. Videoüberwachung, werden nicht diskutiert – selbst wenn man natürlich Vorschläge machen könnte, die darauf hinaus laufen, nur noch maskiert auf die Straßen zu gehen.

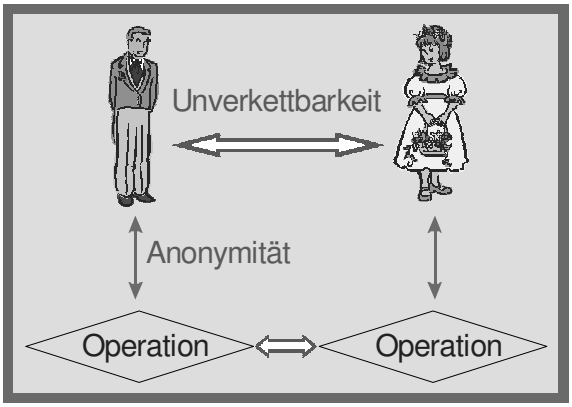


Abbildung 3: Anonymität fördert Unverkettbarkeit, Unverkettbarkeit fördert Unbeobachtbarkeit

Zunächst gilt es einige Begriffe zu klären [PfKö01]:

Anonymität bezeichnet dabei den Zustand, nicht unterscheidbar innerhalb einer Gruppe zu sein, die sich ähnlich (gleich) verhält. Einfach gesagt gilt, daß je mehr Mitglieder diese Gruppe hat und je ähnlicher das Verhalten der Mitglieder ist, desto größer ist die Anonymität. Man ist also, wenn man anonym sein will, auf die Mithilfe anderer angewiesen.

Verkettbarkeit bzw. ***Unverkettbarkeit*** beschreibt, in wieweit ein Angreifer durch seine Beobachtungen Rückschlüsse darüber ziehen kann, daß zwei Ereignisse bezüglich eines bestimmten Merkmals übereinstimmen. Dabei könnte den Angreifer z.B. interessieren, ob eine Nachricht von einem bestimmten Sender stammt oder ob zwei Nachrichten vom selben Sender stammen.

Unbeobachtbarkeit bezieht sich ebenfalls auf Ereignisse. Ein Ereignis ist dabei für einen Angreifer unbeobachtbar, wenn für alle für den Angreifer möglichen Beobachtungen unklar bleibt, ob das interessierende Ereignis nun aufgetreten ist oder nicht (beispielsweise ob eine bestimmte Person eine Nachricht empfangen hat).

- ***Pseudonymität*** beschreibt die Möglichkeiten der Verkettung, die sich durch bestimmte Merkmale oder Identifikatoren von Nachrichten und Personen ergeben. Dabei

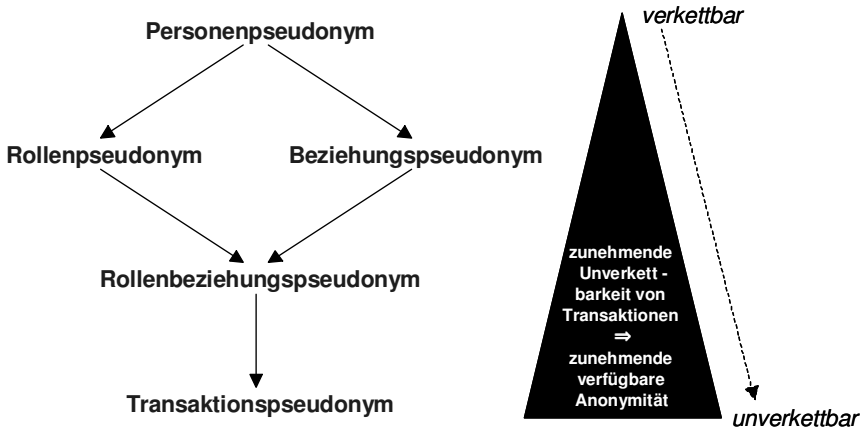


Abbildung 4: Verschiedene Arten von Pseudonymen

lassen sich unterschiedliche Klassen von Pseudonymen unterscheiden (siehe Abbildung 4):

- *Personenpseudonyme* bieten dabei die größte Verkettbarkeit von Aktionen in unterschiedlichen Kontexten, die der Pseudonyminhaber ausführt.
- Unter einem *Rollenpseudonym* versteht man einen durch den Inhaber gewählten Namen (Bezeichner), den er immer dann in der Kommunikation mit seiner Umwelt verwendet, wenn er sich in der zugehörigen Rolle befindet. So könnte ein Schriftsteller sich einen Künstlernamen zugelegt haben, den er als Autorenname für seine Bücher verwendet. Auf diese Weise muß nicht zwangsläufig bekannt werden, welche reale Person die Bücher geschrieben hat. Veröffentlicht der Autor unter seinem Pseudonym allerdings eine große Menge an Büchern, so kann man über die mögliche Verkettbarkeit – also das Wissen, daß alle Bücher vom selben Autor stammen – den Kreis der in Frage kommenden Personen eingrenzen und im Extremfall eben doch eine Identifikation durchführen.
- 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. Im technischen Sinne handelt es sich dabei einfach um Zufallszahlen, die mit der Transaktion verbunden sind.

Abbildung 5: Identitätsmanagement für nutzerbestimmte Preisgabe von Daten

Identitätsmanagement bzw. ***Identitätsmanagementsysteme*** ermöglichen nun die Anwendung der Mechanismen „Anonymität“ bzw. „Pseudonymität“ [HaRo03]. Dabei werden dem Nutzer Werkzeuge (Programme) zur Verfügung gestellt, die ihn dabei unterstützen, die für die jeweilige Kommunikation 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 (z.B. einen Server) herstellt und diesem ermöglicht, pseudonyme Transaktionen zu verarbeiten.

2.1 Anonymität im Internet

Es existieren einige Verfahren, die Anonymität im Internet garantieren. Dabei kann man diese Verfahren dahingehend unterscheiden, ob der Sender anonym bleibt, der Empfänger oder beide. Orthogonal dazu kann man eine Einteilung dahingehend vornehmen, gegen welche Angreifer Schutz besteht, d.h. welche Fähigkeiten und Verbreitung der Angreifer hat. Dabei wird gern ein Modell angenommen, das besagt, daß der Angreifer alle Leitungen des Netzes überwachen kann, daß er die auf diesen Leitungen übertragenen Daten beliebig manipulieren, löschen, hinzufügen etc. kann und daß er Teile des Anonymisierungssystems (Server, Nutzer etc.) selbst betreibt bzw. kontrollieren kann. Dieses Angreifermodell hat den Vorteil, daß nur wenig Einschränkungen bezüglich der Möglichkeiten des Angreifers gemacht werden (und man somit „auf der sicheren Seite“ ist) – wobei einige der Annahmen, die in der Vergangenheit noch illusorisch erschienen, dank ECHELON[1] und Telekommunikations-Abhörschnittstellen mittlerweile als in der Praxis zutreffend gelten können.

[1] Bei ECHELON handelt es sich um ein globales, von den USA betriebenes Überwachungssystem, das z.B. zum Abhören von Satelliten-Kommunikation genutzt wird.

Das erste Verfahren, das in diesem Kontext einen anonymen Austausch von Nachrichten ermöglicht, stammt aus dem Jahre 1981 [Chau81]. Dabei werden die Daten nicht direkt vom Sender zum Empfänger übertragen, sondern über mehrere Zwischenstationen, die sogenannten Mixe, 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. Letztlich verbirgt ein Mix die Zuordnung von eingehenden zu ausgehenden Nachrichten. Die Umkodierung (realisiert mittels kryptographischer Verfahren) sorgt dabei dafür, daß ein Beobachter, der vor und nach einem Mix lauscht, nicht einfach einen Bitmustervergleich der Nachrichten durchführen kann. Alle Nachrichten besitzen außerdem dieselbe Länge, so daß auch über dieses Merkmal keine Verkettung möglich ist. Umsortierung und Zwischenspeicherung verhindern Angriffe über zeitliche Verkettung. Um das gesamte Verfahren sicher zu gestalten, sind noch eine Reihe weiterer Details zu beachten, auf deren Darstellung hier verzichtet wird.

Das ursprüngliche Verfahren war für E-Mail Kommunikation gedacht. Mittlerweile existiert eine Reihe von weiterführenden Konzepten [PPW91] und Prototypen, die dieses Verfahren für andere Anwendungsgebiete adaptieren, z.B. Telefonie, Web-Surfen, Mobilkommunikation etc. Die wesentliche Aussage ist, daß anonyme Kommunikation im Internet möglich ist, bei der nur durch Zusammenarbeit mit allen Betreibern (aber z.B. nicht durch externe Überwachungsmaßnahmen) eine Deanonymisierung möglich ist. Dies bedeutet im Umkehrschluß natürlich auch, daß beim Vorliegen entsprechender Umstände, z.B. einer richterlichen Anordnung, ein Aufdecken sehr wohl möglich ist und es sich folglich nicht um absolute Anonymität handelt.

2.2 Werteaustausch

Neben dem reinen Informationsaustausch, also E-Mail Verkehr oder Web-Surfen ist auch ein anonymer (oder exakter: pseudonymer) Werteaustausch möglich [PWP90]. Dies soll im Folgenden an einem Beispiel vereinfacht dargestellt werden. Die an der Transaktion beteiligten Parteien wählen sich zunächst ein Transaktionspseudonym X bzw. Y und einigen sich auf einen (Werte-)Treuhänder T, über den sie das Geschäft abwickeln wollen. Generell sei angemerkt, daß die Idee, einen Treuhänder (eine vertrauenswürdige dritte Partei) in die Kommunikation einzubeziehen, ein häufig angewendetes Konzept ist, um im „Normalfall“ anonymes bzw. pseudonymes Handeln zu ermöglichen und gleichzeitig in Fällen, in denen es zu Unstimmigkeiten oder Rechtsverletzungen kommt, eine Schadensregulierung bzw. Deanonymisierung durchführen zu können (siehe Abbildung 6).

Im obigen Beispiel sendet nun der Nutzer X an den Treuhänder seine mit seinem Pseudonym signierte Bestellung und die für die Bezahlung notwendige Menge an anonymen, digitalen Münzen (Geld). Tleitet die Bestellung (zusammen mit der Information, daß das für die Bezahlung notwendige Geld hinterlegt ist) an den Diensteanbieter Y weiter. Dieser liefert die Ware an T und erhält dafür das deponierte Geld. In einem letzten Schritt sendet nun T die Ware an X (Abbildung 7).[2]

[2] Sollte Y nicht innerhalb einer gesetzten Frist liefern, so erhält X das Geld automatisch von T zurück.

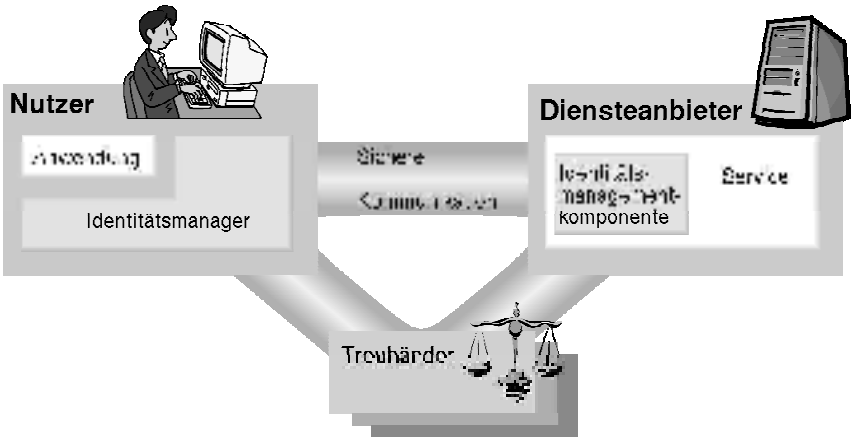
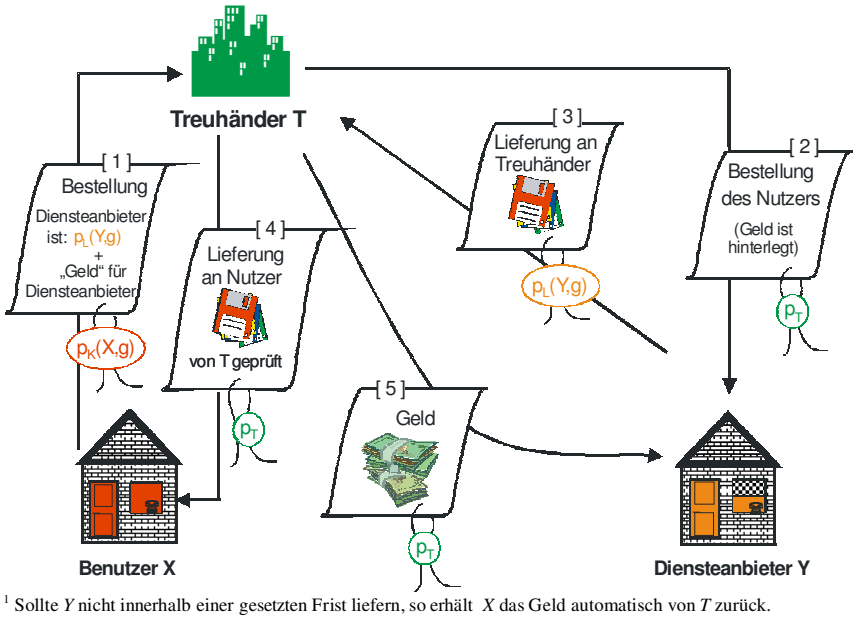


Abbildung 6: Treuhänder ermöglichen Schadensregulierung im Streitfall

Nutzer und Diensteanbieter erfahren nicht, welche reale Person sich jeweils dahinter verbirgt. Solange sich der Treuhänder an das Protokoll hält, kann kein Schaden entstehen. Versucht er zu betrügen, so besitzen die Parteien X und Y entsprechend digital durch T signierte Beweise, mit denen sie T zur Regulierung des Schadens zur Verantwortung ziehen können.

Dieses Beispiel soll zwei Dinge verdeutlichen. Zum einen, daß es sehr wohl möglich ist, auch Güter und Waren so auszutauschen, daß nicht notwendigerweise die Identitäten aller Beteiligten offengelegt werden. Das oft gehörte Argument: „Na ja, spätestens, wenn die Ware geliefert werden soll, muß ich ja doch sagen, wer ich bin...“ ist nicht zutreffend, da dieses Problem mit Hilfe von dritten Parteien bzw. im Fall von rein digitalen Gütern (Software, Musik, Filme etc.) durch die in Abschnitt 2.1 beschriebenen Anonymisierungstechniken gelöst werden kann. Zum anderen wurde dargelegt, daß es keinesfalls so ist, daß die Anonymität zu einem leichten und nicht regulierbaren Betrug führt. Es ist trotz Anonymität möglich, die Authentizität von Nachrichten zu gewährleisten. In vielen Fällen, in denen es zu strafrechtlich relevanten Tatbeständen kommen könnte, ist es möglich, die Protokolle so zu entwerfen, daß die Aktionen absolut anonym durchgeführt werden können – solange es sich bei der anzusetzenden Bestrafung um Geldstrafen handelt. Natürlich ist ein uneingeschränkt anonymes Handeln nicht mehr möglich, wenn Dienste genutzt werden, bei denen im Falle des Mißbrauchs Freiheitsstrafen vorgesehen sind. Aber auch in diesen Fällen ist es mit Hilfe von Treuhändern möglich, zunächst anonym zu agieren, und nur im Streitfall seine Identität preisgeben zu müssen. Dazu werden in das System sogenannte *Identitätstreuhänder* eingeführt.

Die beteiligten Kommunikationspartner (Nutzer, Diensteanbieter etc.) wählen sich je einen Identitätstreuhänder. Diesem gegenüber offenbaren sie ihre wahre Identität. Er stellt im Gegenzug (beliebig viele, unterschiedliche) Pseudonyme aus. Dabei bescheinigt der Identitätstreuhänder, daß er die wahre Identität der zu dem Pseudonym gehörenden Person kennt und bereit ist, diese Identität im Streitfall offenzulegen. Solange nur legale Aktio-



[1] Sollte *Y* nicht innerhalb einer gesetzten Frist liefern, so erhält *X* das Geld automatisch von *T* zurück.

Abbildung 7: Anonymer Werteaustausch

nen unter einem Pseudonym ausgeführt werden, bleibt die zugehörige Person geschützt. Gleichzeitig kann sich der Kommunikationspartner sicher sein, daß er andernfalls dem Täter habhaft wird.

Betrachtet man heutige E-Commerce-Lösungen im Internet, so wird schnell klar, daß diese datenschutzfreundliche Technologie zu einem Gewinn für beide Seiten führt. Der Nutzer, der wie viele Studien immer wieder zeigen, heute eine diffuse Angst vor dem Mißbrauch seiner Daten hat, wäre geschützt. Die Diensteanbieter, die immer wieder erleben, daß unter falschen Identitäten mit gestohlenen oder erfundenen Kreditkartendaten etc. Einkäufe getätigt werden, hätten die Gewißheit, zu ihrem Recht zu kommen.

Wer also mit dem neuen Medium Internet und den damit verbundenen neuen Technologien Geschäfte und gute Gewinne machen will, der muß auch bereit sein umzudenken und neue Sicherheitsverfahren einsetzen. Er kann nicht von der Allgemeinheit verlangen, daß sie ihr Recht auf informationelle Selbstbestimmung und Anonymität aufgibt, nur weil er nicht bereit ist, in die Absicherung seiner Geschäfte zu investieren.

2.3 Credentials

E-Government und E-Democracy sind zwei Schlagwörter, die den Trend hin zur digitalen, Internet-basierten Interaktion von Bürgern und Behörden beschreiben. Um auch auf diesem Gebiet datenschutzgerecht handeln zu können, wurde eine Reihe von kryptographischen Verfahren entwickelt. Eines mit sehr interessanten Möglichkeiten ist dabei das

Konzept der sogenannten Credentials [Chau85]. Dabei handelt es sich um digitale Beglaubigungen, mit denen derjenige, der sie besitzt, einem Dritten beweisen kann, daß er gewisse Rechte oder Eigenschaften besitzt. So könnte etwa die digitale Version eines Führerscheins ein solches Credential sein – wobei es für jede Fahrzeugklasse ein eigenes Credential geben könnte, mit dem man beweisen kann, daß man berechtigt ist, Fahrzeuge der entsprechenden Klasse zu führen. Ein Credential könnte aber auch eine digitale Bescheinigung des Geburtsjahres sein. Dieses könnte man dann im E-Commerce einsetzen, um zu beweisen, daß man über 18 Jahre alt und somit berechtigt ist, gewisse Medien (Filme, Computerspiele etc.) zu erwerben. Eine datenschutzfreundlichere Version dieses Credentials wäre übrigens eine Bescheinigung, die nicht das Geburtsjahr enthält, sondern nur aussagt, daß man über 18 Jahre alt ist.

Credentials können entweder unmittelbar einer Person zuordenbar oder aber auf ein Pseudonym ausgestellt sein. Vielfach ist es nämlich gar nicht notwendig zu wissen, welche konkrete Person sich hinter einer Aktivität verbirgt. Es ist einzig entscheidend, daß sie das (entsprechende) Recht dazu besitzt (z.B. weil sie über 18 Jahre alt ist).

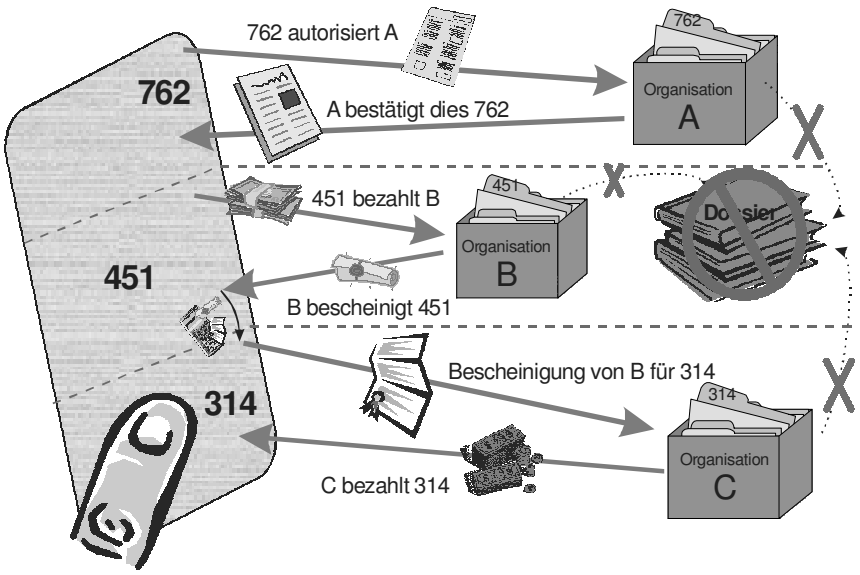


Abbildung 8: Bei einem Credentialsystem tritt eine Person mit verschiedenen Pseudonymen gegenüber unterschiedlichen Organisationen auf. Auf ein Pseudonym ausgestellte Credentials lassen sich auf ein anderes seiner Pseudonyme umrechnen – aber nur durch den Pseudonyminhaber.

Würde man jedoch bei jeder Transaktion immer exakt dasselbe Credential (Bitmuster) verwenden, so wären alle diese Transaktionen verkettbar. In Abschnitt 2 wurden ja bereits die unterschiedlichen Arten von Pseudonymen und die damit verbundenen Eigenschaften (Verkettbarkeit, Anonymität) erläutert. Es wurden daher kryptographische Verfahren

entwickelt, die es ermöglichen, Beglaubigungen von einem Pseudonym auf ein anderes Pseudonym zu übertragen – allerdings soll dies natürlich nur möglich sein, wenn beide Pseudonyme derselben Person gehören. Man kann also beispielsweise von der Führerscheinstelle seine (digitale) Fahrerlaubnis unter dem Pseudonym Micky Mouse erhalten und dann bei der Autovermietung diese unter dem Pseudonym Donald Duck vorlegen. Es wird verborgen, daß es sich dabei eigentlich um ein und dieselbe Person handelt.

Es bleibt das Problem, daß sich Credentials (wie alle digitalen Daten) beliebig oft und exakt kopieren lassen. Um zu verhindern, daß ein einmal auf eine bestimmte Person ausgestelltes Credential von einer Gruppe von Personen verwendet wird oder einfach an eine andere Person weitergegeben wird, bedient man sich des „Alles oder Nichts“ Prinzips. Dies bedeutet, daß eine Weitergabe von Credentials an andere Personen zwar prinzipiell möglich ist und nicht verhindert werden kann – allerdings erreicht man mit Hilfe kryptographischer Protokolle, daß man bei Weitergabe eines Credentials seine komplette Identität (also alle Credentials, die man besitzt) weitergibt. Dies schließt z.B. die digitale Signatur oder die Zugangsberechtigung zum Bankkonto mit ein. Der Empfänger kann also uneingeschränkt im Namen der anderen Person agieren. Die Annahme ist, daß niemand dazu bereit ist und somit keine Credentials weitergegeben werden.

Andere Lösungsmöglichkeiten für dieses Problem wären, daß man sichere Hardware (sogenannte „tamper resistant hardware“) verwendet. Darunter ist ein Gerät zu verstehen, das für seinen Besitzer die Credentials speichert. Der Besitzer erhält jedoch keinen unmittelbaren Zugriff auf diese. Er kann das Gerät nur veranlassen, bestimmte Aktionen mit den Credentials durchzuführen (beispielsweise sie verschlüsselt an das Gerät des Kommunikationspartners zu übertragen). Dadurch, daß zu keiner Zeit das Bitmuster der Beglaubigung außerhalb der sicheren Hardware verfügbar ist, kann es auch nicht kopiert werden. Allerdings besitzt diese Idee eine Reihe von Nachteilen. Es muß sichergestellt sein, daß die „sichere“ Hardware auch wirklich nicht ausgelesen oder manipuliert werden kann. Viele Versuche der Vergangenheit, solche Hardware zu bauen, sind immer wieder gescheitert. Jeder müßte solch ein Gerät besitzt. Und letztlich muß man sich darauf verlassen, daß das Gerät das und nur das tut, was man von ihm erwartet – man hat ja selbst keine Kontrolle mehr über die inneren Vorgänge im Gerät.

Eine andere Möglichkeit ist, Credentials mittels biometrischer Verfahren an eine Person zu binden. Allerdings zeigen auch die bisher verfügbaren biometrischen Verfahren noch erhebliche Schwächen, so daß eine sichere Zuordnung nicht möglich ist.

Die in diesem Abschnitt kurz vorgestellten Verfahren des technischen Datenschutzes belegen, daß ein anonymes bzw. pseudonymes Handel durchaus möglich ist und daß die Vorstellung, daß damit automatisch rechtsfreie Räume geschaffen oder Straftaten Tür und Tor geöffnet werden, falsch ist. Im Gegenteil: Werden die Technologien richtig angewendet, so ergibt sich sowohl ein Gewinn an Datenschutz als auch an Authentizität, Rechtsverbindlichkeit und Zurechenbarkeit.

3 Gesellschaftliche Änderungen

Es stellt sich oftmals gar nicht so sehr die Frage, wieviel Anonymität man braucht oder wieviel Anonymität gut ist. Vielmehr ist entscheidend (um es einfach zu sagen), wieviel

man über andere Leute „tratschen“ kann. Anonymität ist also kein primäres Ziel, sondern ein Mechanismus, um derartiges „Tratschen“ zu verhindern. Auch ist die absolute Anonymität vielfach nicht hilfreich. Es sei denn, man wollte einmal etwas sagen und dann nie wieder in Beziehung zu dieser Aussage gebracht werden und auch selbst diese Beziehung nicht mehr herstellen können. Das eigentliche Problem ist daher: **Wieviel Verkettbarkeit will man, und wer hat die Kontrolle über diese Verkettbarkeit?**

Natürlich ist es notwendig, daß sich in der Gesellschaft Veränderungen vollziehen, um die Verträglichkeit mit den neuen Möglichkeiten der Anonymität zu erhöhen. Beispielsweise beruht unser Rechtssystem bisher darauf, daß im Streitfall, also bei einem Prozeß, zunächst die Identitäten aller Beteiligten (Ankläger und Beklagter, Zeugen) festgestellt werden und erst danach die inhaltliche Untersuchung stattfindet.

Aber muß dies zwingend so sein? Sollte man nicht künftig zunächst eine inhaltliche Untersuchung durchführen, um dann zu entscheiden, ob die Offenlegung aller Identitäten wirklich notwendig ist? So könnte schrittweise entschieden und inhaltlich begründet werden, warum die Identifizierung beteiligter Personen wirklich notwendig ist. In Bagatellfällen, wie etwa Beleidigungen etc., könnte ohne Aufdeckung der kompletten Identität eine Schadensregulierung etwa über Geldstrafen erfolgen. Dieses Vorgehen würde zum einen unberechtigt Beschuldigte schützen. Wer heute der Kinderpornographie oder ähnlicher Straftaten angeklagt wird, muß oftmals unabhängig vom Ausgang des Verfahrens mit erheblichen Beeinträchtigungen seiner zivilen Existenz rechnen. Zum anderen würde eine anlaßunabhängige Deanonymisierung die gesamten Anonymisierungstechniken ad absurdum führen. Will man die Identität eines Pseudonyms feststellen, so reicht es, eine frei erfundene Anschuldigung vor Gericht vorzubringen. Damit ergibt sich die Gefahr, daß die Betreiber von Anonymisierungsdiensten als einzige Lösung die 100%ige, nicht aufdeckbare Anonymisierung sehen.

Ein erstes Umdenken hat bereits begonnen, indem z.B. verschiedene Datenschutzgesetze die Konzepte von Anonymität und Pseudonymität zur Realisierung von Datenvermeidung und Datensparsamkeit aufgreifen. Im deutschen Signaturgesetz ist das digitale Signieren unter einem Pseudonym ausdrücklich vorgesehen.

In einer europäischen Studie werden zur Zeit sehr umfangreiche Untersuchungen zum Thema Identitätsmanagement durchgeführt. Es werden Fallbeispiele untersucht, wie und in welchen Bereichen Anonymität bzw. Pseudonymität eingesetzt werden können, ohne daß damit die Rechtssicherheit verkleinert wird. Dies betrifft z.B. die elektronische Steuererklärung, Bankgeschäfte oder den gesamten Bereich des Gesundheitswesens. Außerdem wurde auf europäischer Ebene ein Projekt beantragt, daß es sich zum Ziel gesetzt hat, ein datenschutzförderliches Identitätsmanagementsystem zu implementieren und zu evaluieren. An diesem Projekt sind mehrere Universitäten und große IT-Unternehmen beteiligt.

Vielleicht ist es zukünftig viel interessanter, nicht die Frage zu stellen, wieviel Anonymität die Gesellschaft verträgt – sondern wieviel Überwachung und Überwachbarkeit einer Gesellschaft zuträglich ist. Wird nicht die demokratische Weiterentwicklung einer Gesellschaft behindert, wenn die Menschen nicht mehr ungehemmt ihre Meinung sagen, weil sie fürchten, daß alles über Jahre gespeichert wird und ihnen zugeordnet werden kann? Ist es förderlich für das Zutrauen in Recht und Gesetz, wenn z.B. Flugreisedaten und damit

verbundene persönliche Daten offen und uneingeschränkt für die USA zugänglich sind, obwohl es europäische Datenschutzregelungen gibt, die genau so etwas verhindern sollen? Was ist im Zuge des „ubiquitous computing“, der allgegenwärtigen Rechner und Sensoren zu erwarten? Eine erste Vorstellung, welche neuen Probleme dies mit sich bringt, liefert, daß man heute damit rechnen muß, in jeder Situation und bei jeder Gelegenheit von einem der zahlreichen Kamerahandys aufgenommen und sofort und für die Ewigkeit öffentlich zugänglich abgebildet zu sein.

Aber vielleicht führt das ja auch zu einem stärkeren Umdenken in der Bevölkerung, daß Datenschutz eben nicht Täter-, sondern Betroffenenschutz ist.

Literatur

[Chau81] David Chaum. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*. Communications of the ACM 24/2, 1981, S. 84-88

[Chau85] David Chaum. *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*. Communications of the ACM, Vol. 28, No. 10, Oktober 1985, S. 1030-1044

[HaRo03] Marit Hansen, Martin Rost. *Nutzerkontrollierte Verkettung. Pseudonyme, Credentials, Protokolle für Identitätsmanagement*. DuD - Datenschutz und Datensicherheit, 27. Jahrgang, Heft 5, 2003, Vieweg, S. 293-296

[Heise1] Heise News Ticker. *Euro-Banknoten mit Identifikationschips.* http://www.heise.de/newsticker/data/wst-23.05.03-001/

[PfKö01] Andreas Pfitzmann, Marit Köhntopp. *Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology*. v0.12, www.koehntopp.de/marit/pub/anon/, 2001

[PPW91] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner. *ISDN-MIXes – Untraceable Communication with very small Bandwidth Overhead*. Information Security, Proc. IFIP/Sec'91, Brighton, UK, 15-17 May 1991, D. T. Lindsay, W. L. Price (eds.), North-Holland, Amsterdam 1991, S. 245-258.

[PWP90] Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann. *Rechtssicherheit trotz Anonymität in offenen digitalen Systemen.* DuD - Datenschutz und Datensicherung 14. Jahrgang, Heft 5-6 (Mai-Juni), 1990, Vieweg, S. 243-253, 305-315.

[SZ] Katja Mielcarek. *Der Mann aus der Straßenbahn*. Sächsische Zeitung, Dresdner Druck- und Verlagshaus GmbH & Co. KG, Dresden, 10./11. Mai, 2003, S. M2