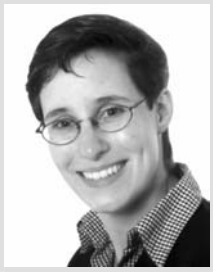
Nutzerkontrollierte Verkettung

Pseudonyme, Credentials, Protokolle für Identitätsmanagement

Marit Hansen, Martin Rost

Identitätsmanagement könnte das zentrale Datenschutzkonzept der Zukunft sein. Wichtige Bausteine wie Pseudonyme und Credentials sind mittlerweile entwickelt worden, anonyme Nutzung digitaler Dienste ist realisierbar. Ein Schwerpunkt der kommenden Forschung muss nun auf die Entwicklung von Methoden zur nutzerkontrollierten Verkettung sowie von Identitätsmanagement-Protokollen gelegt werden, denen eine Analyse der Kommunikationsstrukturen sozialer Systeme zugrunde gelegt werden sollte.



Marit Hansen

Dipl.-Inform; Referatsleiterin „PET – Privacy-Enhancing Technologies“ im ULD Schleswig-Holstein; Arbeitsschwerpunkt: Identitätsmanagement, PET
E-Mail:
marit.hansen@datenschutzzentrum.de

Martin Rost

Sozialwissenschaftlicher Mitarbeiter im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein

Homepage:
http://www.netzservice.de/Home/maro/
E-Mail:
martin.rost@datenschutzzentrum.de

Einleitung

Konzeptionelle Überlegungen zum Thema „Identitätsmanagement“ führen, wenn der Begriff „Identität“ traditionell bearbeitet wird, oftmals in eine Falle. Diese Falle besteht darin, dass die enge Bindung zwischen „Individuum“, „Identität“ und der traditionell dazugehörigen subjektphilosophischen Reflexionen zunächst einen theoriegeleitet-operationsfähigen Ansatz verhindern. Ein Jurist oder Informatiker sieht sich dann fast zwangsläufig vor das Problem gestellt, mit Begriffen arbeiten zu müssen, die aus der eigenen professionellen Perspektive schnell unkontrollierbar spekulativ und unangenehm ideologisch werden. Um einem operativ-pragmatischen Anspruch gerecht zu werden ist es aussichtsreicher, die Kommunikationssysteme, an denen Personen teilhaben, zu betrachten. Genauso geschieht es derzeit in der Praxis der ersten Prototyp-Entwicklungen zu rollengestützten Identitätsmanagementsystemen.[1]

1 Identitätsmanagement – die Idee

Als Ausgangspunkt für die nachfolgende Entwicklung eines Begriffs von einem technisch gestützten Identitätsmanagement dient die Idee, dass Nutzer Identitätsmanagement-Applikationen (IMA) verwenden, die ihnen helfen, computer-vernetzte Kommunikationen als soziale Situationen (genauer: als Systeme der Kommunikation) zu erkennen, in denen Rollen definiert, zugeschrieben, bewertet und gespielt werden.

Unter einem Identitätsmanagementsystem (IMS) ist dann eine Infrastruktur zu verstehen, zu der all die gesellschaftlichen (juristischen, ökonomischen, politischen, wissenschaftlichen, kulturellen) und technischen Komponenten zählen, die zu einem technisch gestützten Identitätsmanagement gehören und die verfahrensmäßig aufeinander abgestimmt sein müssen. Nachfolgend stehen ausschließlich Aspekte derart nutzerorientierter Identitätsmanagement-Applikationen im Vordergrund, nicht jedoch die Aspekte solcher serverseitig eingesetzter Applikationen, mit denen sich Nutzeridentitäten beobachten, auswerten oder verwalten lassen. Insofern interessieren wir uns hier ausschließlich für nutzerorientierte IMA.

[1] Vgl. die Beiträge von Clauß/Kriegelstein sowie Jendricke/Gerd tom Markotten in diesem Heft.

2 Identität in Sozialsystemem

Die Anzahl an Sozialsystemtypen, die den Rahmen möglicher personaler Identitätskonstruktionen aufspannen, ist überschaubar. Herauszuheben sind Interaktionssysteme sowie Organisationssysteme (vgl. auch [Rost03] zu Anonymität).

2.1 Interaktionssysteme

Ein bestimmter Typus an Identität und an Kommunikation ergibt sich in Situationen gemeinschaftlicher Verbundenheit, wie zum Beispiel in der Familie oder unter Freunden. Interaktionssysteme in Gemeinschaften wie auch der Umgang mit spontanen Begegnungen ist jedoch für ein Abwickeln mittels einer IMA weitgehend ungeeignet. Es könnte geradezu zu einem Indikator für eine freundschaftliche oder intime Beziehung werden, dass eine Kommunikation gemeinschaftlicher oder gar intimer Verbundenheit nicht mittels einer IMA verwaltet wird.

2.2 Organisationssysteme

Ein gänzlich anderer Typus an Identität stellt sich in Bezug auf Kommunikation ein, an der Personen und Organisationen (bzw. Organisationen untereinander) teilhaben.

Generell gilt, dass Organisationen die differenzierten gesellschaftlichen Funktionsprinzipien synthetisieren und unter einen bestimmten Primat stellen. Konkret heißt das: Firmen, die unter dem Primat der Kapitalverzinsung stehen, müssen ihre rechtliche, politische, wissenschaftliche, kulturelle (lokale oder auch religiöse Besonderheiten), psychische und natürliche Umwelt angemessen berücksichtigen. Behörden, die unter dem Primat der Rechtsverwirklichung stehen, müssen durchaus auch ökonomisch rational, politisch opportun, wissenschaftlich angemessen, kulturell neutral, kognitiv handhabbar und ökologisch orientiert agieren. Hier gilt nicht der Primat der Kapitalverzinsung – falls doch, wäre dies möglicherweise pathologisch und würde unter dem Titel „Korruption/ Bestechlichkeit" thematisiert werden –, sondern der des Vollzugs von Gesetzen. Man kann die Orientierungsprimate auch für andere Organisationen, etwa für wissenschaftliche Institute, Kirchen, Parteien usw. im gleichen Maße durchdeklinieren.

Eine solche Aufzählung der Orientierungen verweist bereits auf die endliche Anzahl an Kommunikationssystemen, die sich im sozialen Geschehen überhaupt nur ausbilden. Eine IMA muss hiernach die Rolle (respektive die Identität)

- eines Organisationsmitglieds (bspw. als Schüler, Mitarbeiter, Patient, Chefin),
- eines Kunden,
- eines Einwohners,
- eines Staatsbürgers,
- eines Klienten,
- eines an Informationen Interessierten,
- eines einzigartigen Individuums

formulierbar und handhabbar machen.

Diese Rollen bzw. Identitäten fungieren als grobschematisierte, generalisierte Kommunikations- und Erwartungsschemata moderner, funktional differenzierter Gesellschaften. Soziologisch gesehen bestimmt sich die Einzigartigkeit einer Person durch eine notwendig einzigartige Zusammenstellung dieser verschiedenen Rollen, die unausweichlich ins Leben treten und Behandlung erfordern. Quer zu diesen generalisierten Schemata liegen dann die je spezifisch-konkreten, sozusagen historischen Konditionierungen dieser Schemata. Schließlich ist man ein Mitarbeiter einer bestimmten Organisation (die Kunden hat, Einwohner verwaltet, Staatsbürger beteiligt, Patienten heilt, Petenten berät, Musik präsentiert), ist in einer bestimmten Funktion mit dem Fällen von Entscheidungen befasst und mit einer bestimmten Geschichte ausgestattet.

Mit dem erstmaligen Initiieren einer Beziehung hilft beiden Seiten der Rückgriff auf das abstrakte und doch zugleich identitätverleihende Grobschema („Kunde", „Bürger", „Klient", „Interessent" usw.), das ein bestimmtes Set an Kommunikationsmöglichkeiten und Kommunikationserwartungen festlegt. Mit der Fortsetzung der Interaktion wird das Grobschema zunehmend spezifischer, es stellen sich systemeigene, situationsangemessenere, lokale Feinregeln der Kommunikation ein; möglicherweise steht dabei ein mehrfacher Rollen- respektive Identitätswechsel an.

Die generelle Funktion dieser Schemata besteht aus soziologischer Sicht darin, unwahrscheinliche Kommunikationen anschlussfähig zu halten bzw. machen, also Kommunikationen spezifisch zu verketten, sprich: sie erwartungsstabil zu organisieren.

3 Verkettung

Abstrakt betrachtet finden Überlegungen zum technisch gestützten Identitätsmanagement Führung entlang der zentralen, strukturbildenden Kategorie der Handhabung der Differenz von Verkettbarkeit/ Nichtverkettbarkeit von Kommunikationen. Dabei lässt sich die beobachterorientierte Verkettbarkeit („linkability") bzw. die nutzerkontrollierte Verkettung („linkage") unter drei Aspekten thematisieren:

- Verkettung von Kommunikation und Person,
- Verkettung von Kommunikation in zeitlicher Hinsicht sowie
- Verkettung unabhängiger Rollen.

3.1 ... zur Person

Die Verkettbarkeit bzw, Verkettung von Kommunikationen und Handlungen, die einer bestimmten Person zugeordnet werden, behandelt die gegenwärtige Forschung unter dem Aspekt der Anonymität und Pseudonymität. Zur Abwicklung von Kommunikationen müssen Organisationen in nur seltenen Fällen einen Zugriff auch auf den Körper einer Person, zu der eine Beziehung steht, eingeräumt bekommen. Je nach Beziehungstyp kann aus einem differenzierten Set an unterschiedlichen Pseudonymtypen gewählt werden, die unterschiedliche Eigenschaften an Aufdeckwahrscheinlichkeit, an Möglichkeiten zur Ausbildung einer längerfristigen Systemgeschichte oder auch an Reputationsvererbung bieten.

3.2 ... zeitlich

Von Verkettbarkeit bzw. Verkettung spricht man ferner im Hinblick auf die Feingestaltung einer bislang nur grobschematisierten Rolle, bei der aktuelle kommunikative Ereignisse mit bereits vergangenen Ereignissen oder Entscheidungen in eine Beziehung zu setzen sind. Auf diese Weise wird eine Systemgeschichte aufgebaut. Die Mustererkennung im Hinblick auf die Bestimmung des Grob-Rollenschemas ist dabei strukturell „nur" auf eine Referenz angewiesen, nicht unbedingt auf das Mitführen eines systemeigenen Gedächtnisses. Dagegen ist die Fortsetzung einer bereits in der Vergangenheit bestimmten Beziehung auf ein systemeigenes Gedächtnis angewiesen. Insofern müssen IMA bzw. das IMS über eine History-Funktionalität verfügen.

3.3 ... unabhängiger Rollen

Verkettbarkeit bzw. Verkettung ist auch im Hinblick auf das Inbeziehungsetzen verschiedener Rollen von großer Bedeutung. Nutzer sind u.U. daran interessiert, Reputation, mit der eine bestimmte ihrer Rollen ausgestattet ist, auch in anderen Rollen nutzen zu können, wodurch sich die Effizienzvorteile von Vertrauenswürdigkeit einstreichen lassen.

Umgekehrt kann es aber auch von Interesse sein, dass diese Form der Verkettung, etwa mangels Reputation oder gar Negativreputation, unerwünscht ist. Besonders relevant sind die Fälle, in denen eine abstrakte, vertrauensfördernde Reputation transferiert werden soll, nicht aber die Quelle dieser Reputation.

In diesem Zusammenhang sind die *Convertible Credentials* zu nennen: Dabei handelt es sich um umrechenbare Beglaubigungen, durch die sich Autorisierungen, die ein Nutzer unter einem Pseudonym erworben hat, auf andere seiner Pseudonyme übertragen lassen, ohne dass sie auf die anderer Nutzer transferiert werden können. Mit Hilfe der gleichen Credentials unter verschiedenen Pseudonymen kann einer Verkettbarkeit durch einen Beobachter entgegengewirkt werden. Um dieses auf Kryptoalgorithmen basierende Konzept zu veranschaulichen, stelle man sich einen digitalen Führerschein vor, der die Berechtigung des Fahrers zum Führen eines Kraftfahrzeugs nachweist, doch bei jedem Vorzeigen anders aussieht, so dass sich nicht über eine Verkettung ein Bewegungsprofil erstellen lässt.

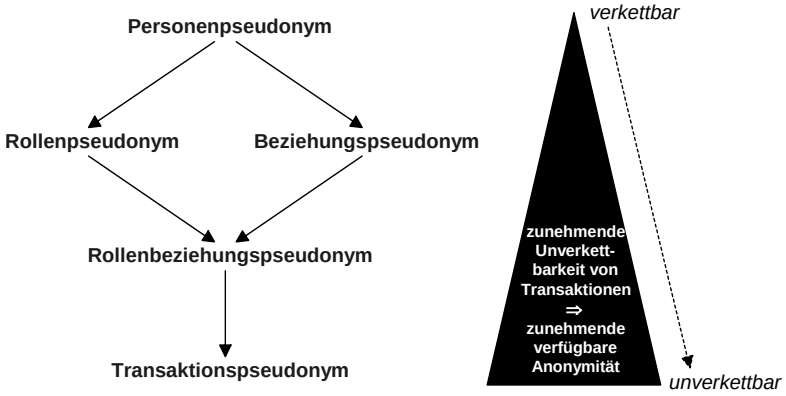


Abb. 1: Pseudonyme in Bezug auf Verkettbarkeit ihrer Verwendung

So könnte man auch digitale Personalausweise oder Kundenkarten realisieren.

3.4 Pseudonyme: anonym oder personenbezogen?

Während in den vorigen Abschnitten die Verkettbarkeit durch den Nutzer im Vordergrund stand, ist bei der Einstufung von Pseudonymen im Spannungsfeld zwischen Anonymität und eindeutigem Personenbezug der Blick von außen, d.h. die Sicht eines potenziellen Beobachters, relevant. Dabei wird Anonymität technisch gesehen als ein Nicht-Identifizieren-Können innerhalb einer Gruppe [PfKö01]. Je größer diese Anonymitätsgruppe ist, innerhalb der Einzelne nicht mehr ausgemacht werden kann, desto stärker ist der Anonymitätsgrad.

Für die Stärke von Anonymität sind bei Pseudonymen folgende Kriterien von Bedeutung:

- das Wissen über die Zuordnung zwischen einem Pseudonym und seinem Inhaber (vgl. Abschnitt 3.1) und
- die Verkettbarkeit bei Verwendung des Pseudonyms in verschiedenen Kontexten (vgl. Abschnitte 3.2 und 3.3).

Die meisten deutschen Rechtsnormen, die Pseudonyme oder Pseudonymisierung erwähnen, gehen von einer Zuordnungsfunktion zwischen dem Pseudonym und seinem Inhaber aus, die i.d.R. nicht nur dem Pseudonyminhaber bekannt ist.[2] Ob ein Pseudonym als personenbezogen oder als anonym einzustufen ist, hängt von der Kenntnis der Zuordnungsfunktion ab [vgl. RoSc00].

Für Identitätsmanagement spielen diese Pseudonyme, deren Zuordnung der Organisation als Kommunikationspartner oder einer dritten Partei („Identitätstreuhänder“) bekannt sind, eine wichtige Rolle, da unter bestimmten Bedingungen, z.B. im Missbrauchsfall, die „Identität“, d.h. der wirkliche Name, aufgedeckt werden kann. Doch die selbstgewählten Pseudonyme ohne bekannt gemachte Zuordnung sind ebenfalls von Bedeutung. Auch hier können dritte Parteien in einer fairen, missbrauchsfesten Geschäftsabwicklung unterstützen, indem sie bspw. als Werte- oder Haftungsservice ggf. für Schulden oder andere zugesagte Leistungen des Pseudonyminhabers einstehen.

Eine Verkettbarkeit bei Verwendung eines Pseudonyms in verschiedenen Kontexten, wie dies als zweites Kriterium für den Grad von Anonymität eingeführt wurde, bedeutet, dass ein Beobachter Profile anlegen und damit auf das Verhalten des Pseudonyminhabers und – wenn genügend aussagekräftige Informationen vorliegen – sogar auf die Person selbst schließen kann. Daher ist Anonymität i.A. um so stärker, je weniger Informationen mit dem Pseudonym zusammenhängen, d.h. insbesondere je seltener und je weniger kontextübergreifend ein- und dasselbe Pseudonym verwendet wird.

Nach [PfKö_01] werden *Transaktionspseudonyme* nur für je eine Transaktion verwendet, *Rollenpseudonyme* nur im Kontext je einer Rolle, *Beziehungspseudonyme* nur jeweils bei der Kommunikation mit einer bestimmten anderen Partei. Der Einsatz von *Rollenbeziehungspseudonymen* als Mischform beschränkt sich jeweils auf einen Kommunikationspartner und eine Rolle und ist damit in der Verwendung spezifischer als die genannten Rollen- oder Beziehungspseudonyme. Eine noch stärkere Anonymität können aber die Transaktionspseudonyme bieten (s. Abb. 1).

Auch eine Übertragbarkeit von Pseudonymen stärkt die Anonymität, denn dann ist keine eindeutige Zuordnung zu einer Person garantiert. Solche Pseudonyme, die von mehreren Personen gleichzeitig oder nacheinander genutzt werden können, bezeichnet man als *Gruppenpseudonyme*.

3.5 Zwischenergebnis

Zieht man ein erstes Fazit aus dieser hier notwendig knapp gehaltenen Diskussion der drei Verkettungstypen, so lässt sich die spezifische Funktionalität einer IMA bzw. eines IMS in der „Kontrolle von Verkettungen“ ausweisen. Eine IMA soll den Nutzer unterstützen, Typen der Kommunikationen zu erkennen bzw. zu gestalten und die dafür angemessenen Verkettungen zu kontrollieren. Als datensparsame Standardeinstellung sollten Transaktionspseudonyme genutzt werden; wenn über mehrere Kommunikationen hinweg an das Pseudonym angeknüpft werden soll, Rollenbeziehungspseudonyme. Credentials bieten die Möglichkeit, Autorisierungen nachzuweisen, ohne dass von außen diese verschiedenen Nachweise verkettbar wären.

4 Protokolle für Identitätsmanagement

Der Einsatz von IMAen macht insbesondere dann Sinn, wenn sie gesellschaftsweit im Sinne einer kommunikationstechnischen Grundversorgung eingesetzt werden. Dies wiederum setzt voraus, dass sie bezahlbar sind, dass sie sicher sind und dass ihre Nutzung einfach ist (vgl. [HaRo02]). Insofern sind besonders hohe Anforderungen an die Handhabbarkeit einer IMA zu stellen.

4.1 Hilfen im Handling

Selbstverständlich muss eine derartig tief in die Gesellschaftsstruktur eingreifende Technik wie das technisch gestützte Identitätsmanagement bereits in der Schule vermittelt werden. Trotzdem muss auch die Strategie gelten, dass bei der Usability-Gestaltung einer IMA entlang der Differenz explizit/implizit so viel wie möglich implizit, und das heißt: automatisiert, erfolgen kann. Eine solche Applikation muss nutzbar sein auch für solche Personen, die über eine

[2] Z.B. Signaturgesetz, Datenschutzgesetze; die Pseudonyme des Teledienstedatenschutzgesetzes könnten dagegen prinzipiell auch so gewählt sein, dass lediglich der Nutzer die Zuordnung kennt.

geringere als die gesellschaftlich durchschnittliche Intelligenz und technische Kompetenz verfügen. Neben datenschutzorientierten „Kommunikations-Stilvorlagen“, die den Nutzern anzuliefern etwa den Datenschutzbeauftragten auferlegt werden kann, könnte eine effiziente und beherrschbare Automatisierung dadurch gelingen, dass Identitätsmanagement-Applikationen auf spezielle Kommunikationsprotokolle zum Identitätsmanagement zugreifen können.

4.2 Identity Management Protocol Set

Unter einem „Identity Management Protocol Set (IMP)“ verstehen wir das Bündel der Protokolle, die IMS-relevante Funktionalität beschreiben und die Kommunikation koordinieren. Das IM-Protokoll-Set umfasst die Beschreibung von, Aushandlung über und Durchsetzung von:

- Voraussetzungen für Identitätsmanagement: „Basic IMS Protocol“;
- Grad und Art der Verkettbarkeit: „Linkability Protocol“;
- Rollenauswahl: „Role Trigger Protocol“;
- Integration von Datenschutzinformationen: „Privacy Information Protocol“.

4.3 Basic IMS Protocol

Eine zentrale Funktion eines Basic IMS Protocols, das für die infrastrukturellen Aufgaben zuständig wäre, bestünde darin, die Voraussetzungen für Identitätsmanagement zu behandeln. Konkret kann dies heißen, dass die Unbeobachtbarkeit der Kommunikationsverbindung gegenüber Dritten gesichert ist, dass Signaturverifikationen komfortabel durchgeführt werden, dass eine möglicherweise gewünschte Trusted Third Party direkt in die Kommunikationsverbindung eingebunden werden kann. Ggf. müssten die Kommunikationspartner aushandeln, was im jeweiligen Fall die Basisfunktionalität sein soll. Sofern sich die Aushandlungsergebnisse nicht durchsetzen ließen, wäre dies den Kommunikationspartnern über ihre IMA transparent zu machen.

4.4 Linkability Protocol

Die Verkettbarkeit sowohl zwischen Pseudonym und Pseudonyminhaber als auch zwischen verschiedenen Nutzungen oder Handlungen ist wesentlich für das Einschätzen des Wissens anderer über einen selbst, also für das Recht auf informationelle Selbstbestimmung. Ein Linkability Protocol würde dazu dienen, die Anforderungen der Kommunikationspartner an die Verkettung und ihre Ausgestaltung zu beschreiben, und hätte damit Auswirkung auf die Auswahl eines Pseudonyms und seinen Eigenschaften. Beispielsweise würde das Linkability Protocol Transaktionen kennzeichnen, in denen dasselbe Pseudonym zu verwenden wäre, z.B. beim Online-Einkauf oder bei personalisierten Diensten. Darüber hinaus könnte es ausdrücken, welcher Mehrwert mit einer Verkettung zu früheren Transaktionen verbunden wäre, z.B. bei personalisierten Diensten oder bei einer Belohnung von Stammkunden. Auch die Möglichkeiten des Zugriffs auf eigene Daten im Nachhinein, vielleicht sogar direkt in der IMA des Kommunikationspartners, könnten mit Hilfe dieses Protokolls beschrieben werden.

4.5 Role Trigger Protocol

Im Unterschied zu den vorher genannten Protokollen bestünde die Aufgabe des Role Trigger Protocols darin, Anforderungen speziell des Kommunikationstypus zu erfüllen. Es kann dafür sorgen, dass mit dem Kommunikationsinhalt für den Nutzer transparent auch der Typ des Sozialsystems mitgeliefert wird, dass durch die Nutzung bestimmter Adressierungsformen auch an eine möglicherweise bereits vorhandene Systemgeschichte angeknüpft werden kann, so dass bestimmte Einstellungen automatisch vorgenommen und bestimmte Ereignisse automatisch ausgelöst werden können. Der Nutzer soll in die Lage versetzt sein, bestimmten kommunikativen Offerten zuzustimmen oder sie abzulehnen. Typische Rollensets verlangen typische Formen von Adressierungen (Pseudonymen).

4.6 Privacy Info Protocol

Auch wenn ein Service keine Informationen per Basic IMS Protocol, Linkability Protocol oder Role Trigger Protocol gibt, wäre der Nutzer nicht zwangsläufig auf sich allein gestellt. Statt dessen könnte seine IMA über ein „Privacy Information Protocol“ Einschätzungen zum Datenschutzniveau dieses Services oder sogar detailliert zu möglichen Transaktionen von dritten Parteien (wie z.B. den Datenschutzbeauftragten) oder anderen Nutzern beziehen. Die IMA könnte dann diese Informationen bei der Auswahl der Pseudonyme oder der Interpretation der mitgeführten History berücksichtigen.

Fazit

Identitätsmanagement-Applikationen machen besonders im Umgang mit Organisationssystemen Sinn: In vielen Fällen des Alltags bedarf es für die Abwicklung zwischen Klientel und Organisation keines Zugriffs auf die eine, körperfixierte, alles synthetisierende Identität. Bislang fehlt es allerdings an einer Infrastruktur; mit deren Unterstützung die enorme Komplexität eines technisch gestützten Identitätsmanagements im Hinblick auf Verkettungen und Verkettbarkeiten bewältigbar wäre. Zentral dafür dürfte die Entwicklung eines speziellen Identitätsmanagement-Protokoll-Sets sein.

Literatur

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

[CPHV02] Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, Els Van Herreweghen: Privacy-Enhancing Identity Management; in: IPTS-Report 67; JRC Seville, 2002; 8-16; www.jrc.es/pages/iptsreport/vol67/english/IPT2E676.html.

[HaRo02] Marit Hansen, Martin Rost: Datenschutz durch computergestütztes Identitätsmanagement; in: Kubicek et al. (Hrsg.): Innovation@Infrastruktur (Jahrbuch Telekommunikation und Gesellschaft, Band 10); Hüthig, Heidelberg 2002; 255-268.

[PfKö01] Andreas Pfitzmann, Marit Köhntopp: Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology; v0.12, 2001-06-17, www.koehntopp.de/marit/pub/anon/; v0.8 in: Federrath (Hrsg.): Designing Privacy Enhancing Technologies; LNCS 2009; 2001; 1-9.

[RoSc00] Alexander Roßnagel, Philip Scholz: Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten; MMR 12 (2000); 721-732.

[Rost03] Martin Rost: Über die Funktionalität von Anonymität für die bürgerliche Gesellschaft, in: Bäumler/von Mutius (Hrsg.): Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Vieweg, Braunschweig 2003; 62-72.