in: Alexander Roßnagel (Hrsg.): Allgegenwärtige Identifizierung? Neue Identitätsinfrastrukturen und ihre rechtliche Gestaltung; Schriftenreihe des Instituts für Europäisches Medienrecht (EMR), Saarbrücken, Band 33; Dokumentation der Stiftungstagung der Alcatel SEL Stiftung für Kommunikationsforschung am 28. u. 29. April 2005; Nomos, Baden-Baden 2006, 83-91

Identitätsmanagement und informationelle Selbstbestimmung

Andreas Pfitzmann, Katrin Borcea-Pfitzmann

Fakultät Informatik
Technische Universität Dresden

01062 Dresden
pfitza@inf.tu-dresden.de
katrin.borcea@tu-dresden.de

Abstract: Informationelle Selbstbestimmung in der digitalen Welt erfordert selbstbestimmtes Identitätsmanagement in Nutzerhand: Statt durch Personenkennzeichen induzierte umfassende Persönlichkeitsprofile entstehen zu lassen, können so durch Pseudonyme benannte Teilidentitäten nachhaltig auseinander gehalten werden. Wir beschreiben die Grundzüge eines entsprechenden Identitätsmanagementsystems.

1 Einleitung

Ausgehend vom Ziel dieses Artikels – nämlich zu Identitätsmanagement und informationelle Selbstbestimmung zu informieren – werden einleitend zunächst die Begriffe etwas näher beleuchtet.

Wenn wir über *Management* von Prozessen und Objekten sprechen, dann muss festgehalten werden, dass JEDER allenfalls das managen kann, worauf ER Einfluss hat. *Selbstbestimmt managen* heißt dann, dass ICH allenfalls das managen kann, worauf ICH Einfluss habe. Management allgemein ist für MICH, als die durch den Managementprozess tangierte Person, desto *vertrauenswürdiger*, je vollständigere Information – und im Idealfall: je vollständigere Kontrolle – ICH über das Management (einschließlich seiner möglichen Auswirkungen) habe. Dabei wird Vertrauen „geschenkt“. Es muss wachsen können. Vertrauen kann, wie oft versucht (Wie oft werden wir aufgefordert: „Geben Sie uns mal Ihre Daten, wir passen schon auf sie auf!“), nicht eingefordert werden. Im Gegenteil – es würde sehr schnell in Misstrauen umschlagen.

Vor allem wenn es um *Informationen* geht, die spurenlos (oft nahezu kostenlos) kopiert und weitergegeben werden können, ist Vertrauenswürdigkeit außerordentlich wichtig. Man vergleiche dabei das physische Ausrauben (z.B. der eigenen Wohnung) mit dem informationellen „Ausrauben“ (z. B. Datenklau) hinsichtlich deren Wahrnehmbarkeit ...

Im Fall von *personenbezogener* Information, wird *selbstbestimmtes, vertrauenswürdiges Management* gar grundrechtsrelevant (vergleiche dazu Volkszählungsurteil [Vzu83], wo u.a. festgelegt ist: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“). Das Grundgesetz versteht also den deutschen Bürger als autonome Person, die ihre Interessen artikuliert und somit befähigt ist, einen eigenen Willen herauszubilden. Untersuchungen im Sozial- und Psychologiebereich haben ergeben, dass Menschen, die keine Kontrolle darüber besitzen, was mit ihren Daten geschieht, dazu neigen, sich an das anzupassen, was sie meinen, das die Mehrheit will. Wer selbstbestimmtes, vertrauenswürdiges Management personenbezogener Daten unterbindet, der untergräbt folglich den Mechanismus, wie Willensbildung und Kontrolle in einer pluralistischen Demokratie geschieht.

Wenn wir also über Identitätsmanagement sprechen, dann sehen wir den Benutzer als die zentrale Figur mit verbrieftem Recht auf Selbstbestimmung in der Informationsgesellschaft.

2 Wozu Identifizierung?

Wenn man sich im realen Leben umschaut oder auch bei der Benutzung von Anwendungen, dann ist es oftmals nicht die Identifizierung, die benötigt wird für ein problemloses Agieren, sondern das, was man braucht, ist in den meisten Fällen ein *Wiedererkennen*. Das heißt, ein *Feststellen der genauen zivilen Identität* ist meist unnötig. Im Prinzip müssen Informationen verfügbar sein, die es ermöglichen, auf frühere Prozesse zurückzugreifen und auf diese wieder aufzusetzen.

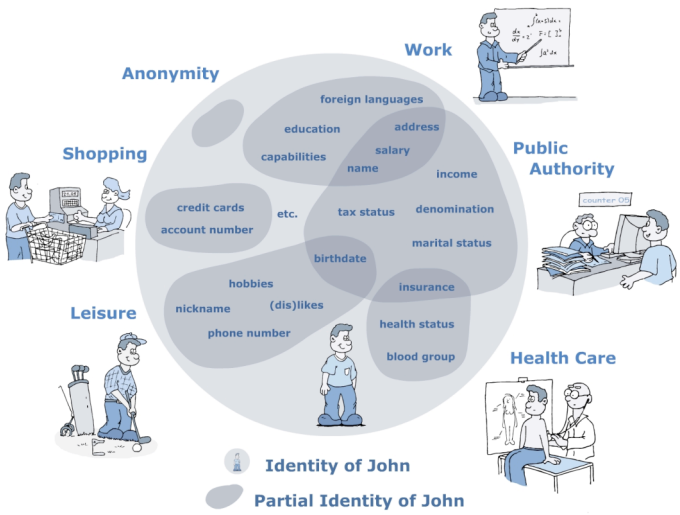

Abbildung 1: Teilidentitäten von John Primeur

Wird bspw. aus Denkfaulheit (was noch das positivste zu unterstellende Motiv ist) “Wiedererkennen“ grundsätzlich über „Feststellen der genauen zivilen Identität“ implementiert, so verbaut man sich Möglichkeiten für ein selbstbestimmtes informationelles Identitätsmanagement, mögliche Geschäftsfelder und, dies ist in diesem Zusammenhang wohl das Verhängnisvollste, man verhält sich demokratieunverträglich.

Ein Blick in das reale Leben verrät (vgl. Abbildung 1): Es gibt viele verschiedene sich überlappende Sektoren der Welt, in denen man sich je nach Lebensbereich unterschiedlich verhält. So trägt man bspw. im Arbeitsbereich eine etwas formellere Kleidung als im Bereich des Freizeitsports. Oft wird man in den unterschiedlichen Sektoren auch unterschiedlich, der Situation entsprechend genannt (z.B. „John“, „Mr. Primeur“, „Darling“ oder „Johnny-Boy“).

Folglich gehen wir davon aus, dass man in all den Bereichen nicht mit nur EINER Identität existiert und man sich nicht EINHEITLICH verhält. Jeder verfügt also über eine große Menge an Teilidentitäten, mit denen er in den entsprechenden Domänen agiert. Dieses *Partitionieren* der Identität in Teilidentitäten (bzw. partielle Identitäten) erleichtert auch das Kontrollieren von Informationen in der digitalen Welt, was dazu führt, dass John, um bei dem Beispiel der Abbildung zu bleiben, etwas benötigt, mit dem er seine Identität*en* – seine unterschiedlichen Teilidentitäten – managen kann.

Dabei sehen wir dieses Identitätsmanagementsystem allerdings als etwas, was nicht in der Kontrolle eines Dienstleistungsanbieters steht, sondern in der des Benutzers.

3 Identifikationsmöglichkeiten in der Praxis

Im Folgenden werden Identifikationsmöglichkeiten diskutiert, die bzgl. des bereits praktizierten und des geplanten Einsatzes gegenübergestellt werden.

Während das derzeitig gängige Vorgehen für die Identifikation die Vorlage des *Ausweises* (erforderlich bzw. angeraten und somit freiwillig) ist, ist für die nahe Zukunft bzw. in Reisepässen bereits teilweise eingeführt, die Ausstattung der Ausweise mit RFID-Chips vorgesehen. Dies erlaubt, dass jeder, der jemals Zugriff auf den Ausweis hatte, über ausreichend Informationen verfügt, um den RFID-Chip anzufunken. Das heißt, dass ein Vorzeigen des Ausweises nicht mehr nötig sein wird, sondern eine Identifizierung allein durch das Mitführen des Ausweises möglich sein wird.

Ein weiterer klassischer Bereich an Identifikationsmöglichkeiten umfasst die erkennungsdienstliche Behandlung, die klassische Forensik und die immer stärker in der Öffentlichkeit eingesetzte Videoüberwachung. Geplant und partiell auch bereits in der Praxis eingesetzt sind Biometrie und Genomdatenbanken. Ihre Befürworter wollen sie zur Massenanwendung bringen.

Jeder hat heutzutage mehrere Telefonnummern und Internetadressen, die ebenso wie eingeschaltete Mobiltelefone eine Identifizierung bzw. eine Ortung erlauben. In naher Zukunft werden Gerätekennzeichen sowie Kennzeichen der Software oder nicht explizit ausgeschaltete RFIDs (welche sich nicht von allein ausschalten wie bspw. ein durch einen leeren Akku abgeschaltetes Mobiltelefon) die Identifizierung erheblich erleichtern.

Diese Identifikationsmöglichkeiten sind grundsätzlich kombinierbar und können zusammen wie auch einzeln als *Personenkennzeichen* verwendet werden. Weiterführend können diese Personenkennzeichen zur Erstellung von Bewegungsprofilen dienen und somit den Traum der eingangs erwähnten, um die (angebliche) Sicherheit der Bürger bemühten Sicherheitsorgane, aber auch der organisierten Kriminalität erfüllen – die Schaffung des gläsernen Menschen.

Der Verlust der Kontrolle über personenbezogene Daten ist der Albtraum eines jeden Datenschützers und die Pflicht des (mündigen) Bürgers ist es, sich entsprechend zu positionieren. Dieses Positionieren ist allerdings wiederum situationsbezogen zu vollziehen. So gibt es Anwendungen, in denen man identifizierbar sein will (bspw. für ein Alibi) während man dies in anderen Situationen absolut nicht möchte, um sein Persönlichkeitsrecht zu schützen. Das heißt, es muss für den Bürger durchschaubar sein, was mit den Informationen über ihn geschieht und er muss Einfluss darauf haben können.

4 Identitätsmanagement

4.1 Ziele des Identitätsmanagement

Bezüglich des oben genannten Volkszählungsurteils und somit der Freiheit des Bürgers auf individuelle, selbstbestimmte Privatsphäre sind die derzeitigen Entwicklungen hinsichtlich der Archivierung sowie der Archivierungsverlängerung bspw. von Telekommunikationsdaten sehr kritisch zu betrachten. Sie bedeuten praktisch die Aufgabe des vom Bundesverfassungsgericht aus dem Grundgesetz hergeleiteten Rechts auf „Informationelle Selbstbestimmung“.

Um dieser Entwicklung grundsätzlich entgegenzuwirken, braucht es eine Lösung, die den Abbau der Demokratie – und somit implizierend des Gemeinwohls – durch den Staat bzw. die Gesellschaft als Ganzes unterbindet. Diese Lösung ist gegeben, wenn der Benutzer selbst als mündiger Akteur in den Telekommunikationsprozessen auftritt und somit auch das Management seiner Identitäten übernimmt. Nur *Identitätsmanagement in Nutzerhand* kann der Forderung nach datenschutzerhaltendem Identitätsmanagement gerecht werden.

Die mit dem datenschutzerhaltenden Identitätsmanagement verbundenen Ziele, die nicht nur einen rechtlichen Hintergrund haben, sondern auch einen sozialpsychologischen, stellen sich folgendermaßen dar:

- Die Benutzer sollen bzgl. der Preisgabe personenbezogener bzw. -beziehbarer Daten *so selbstbestimmt wie möglich* handeln können (Autonomie desjenigen, der managet).

- Um die Interessen der Kommunikationspartner zu berücksichtigen (und somit rückbezüglich auch desjenigen, der managet), soll die Korrektheit der Daten durch diesen ggf. geprüft werden können (*Fremdauthentikation*, vgl. [PWP90]).

- Vertrauen soll gefördert werden, u.a. durch *Datenvermeidung*, *Datensparsamkeit* sowie die Verwendung nutzergenerierter Pseudonyme und Credentials.

4.2 Implementierung von Identitätsmanagement

Nachdem die Ziele für die Implementierung diskutiert wurden, sollen nun die wesentlichen Implementierungsideen für Identitätsmanagement vorgestellt werden. Dabei erfordert die Implementierung, jeweils zu bedenken, wie viele Beteiligte kooperieren müssen, damit die jeweilige Maßnahme eingesetzt werden kann (eine entsprechende Diskussion zur Lateralität von Datenschutz- und Datensicherheits-mechanismen wurde in [Pfi01] geführt).

Eines der wesentlichen Implementierungskonzepte sind *Pseudonyme*. Das heißt, benötigt werden viele unverkettbare Pseudonyme statt wenige Personenkennzeichen. In manchen Zusammenhängen sind diese unilateral einsetzbar. Wird jedoch je nach Geschäftsfeld auch die Akzeptanz auf der Partnerseite benötigt, dann muss die Implementierung mindestens bilateral erfolgen.

Als zweites werden *digitale Pseudonyme* für die Selbstauthentikation [PWP90] benötigt. Vom Pseudonyminhaber kommen nur Nachrichten, die relativ zu diesem Pseudonym (selbstgenerierte Public Keys) digital signiert sind. Im einfachsten Fall sind digitale Pseudonyme also Signaturprüfschlüssel, beispielsweise von PGP. Auf diese Weise können unter dem Pseudonym bspw. auch Reputationen aufgebaut werden. (trilateral)

Für manche Anwendungen werden zusätzlich Fremdauthentikationen benötigt, z.B. ein Dritter sagt, dass jemand über gewisse Eigenschaften (z.B. Nachweis über den Besitz eines Führerscheins oder eines Abiturs) verfügt. Dieser Nachweis über Eigenschaften wird mittels *Credentials* (pseudonyme Fremdauthentikation) geführt und ist übertragbar zwischen allen Pseudonymen derselben Person (siehe auch [Cha85]). (multilateral)

4.3 Pseudonyme

Pseudonyme können einerseits nach ihrem initialen Personenbezug klassifiziert werden (Tabelle 1), andererseits nach ihrem Verwendungszusammenhang (Abbildung 2).

Pseudonymklasse	Beispiel
Öffentliches Pseudonym: Bezug zwischen Pseudonym und seinem Inhaber von Beginn an öffentlich bekannt.	Telefonnummer mit Inhaber, Wohnanschrift etc. im Telefon"buch" gelistet
Initial nicht-öffentliches Pseudonym: Bezug zwischen Pseudonym und seinem Inhaber ist zu Beginn zwar manchen (Identitätstreuhänder), aber nicht allen bekannt.	Kontonummer oder Kreditkartennummer mit Bank als Identitätstreuhänder
Initial unverkettbares Pseudonym: Bezug zwischen Pseudonym und seinem Inhaber ist zu Beginn nur dem Inhaber bekannt.	Biometrische Merkmale; DNA (solange keinerlei Register)

Tabelle 1: Pseudonyme, klassifiziert nach ihrem initialen Personenbezug

Während der Verwendung der Pseudonyme kann sich ihr Personenbezug ändern. Dies ist allerdings immer nur in einer Richtung – nämlich dem zunehmenden Personenbezug – möglich.

Die in Abschnitt 3 diskutierten Personenkennzeichen finden sich in Abbildung 2 als Personenpseudonyme wieder. Diese ermöglichen es Institutionen, unter Heranziehen von Informationen aus den unterschiedlichsten Bereichen detaillierte Dossiers zu erstellen, da alle unter dieser Pseudonymart durchgeführten Transaktionen miteinander verkettbar sind. Um dieses Problem zu umgehen, kann je nach Geschäftsbereich auf Rollen-, Beziehungs-, Rollenbeziehungs- oder Transaktionspseudonym ausgewichen werden, wobei ein Transaktionspseudonym maximale Unverkettbarkeit der Transaktionen und somit maximale Anonymität gewährleistet. Allerdings verhindert ein Transaktions-pseudonym ein Wiedererkennen (vgl. Abschnitt 2) in darauf folgenden Transaktionen und damit Reputationsaufbau, was nicht in jedem Fall erwünscht ist.

Selbstbestimmtes Identitätsmanagement ermöglicht eine transparente Gesellschaft mit autonomeren Bürgerinnen und Bürgern.

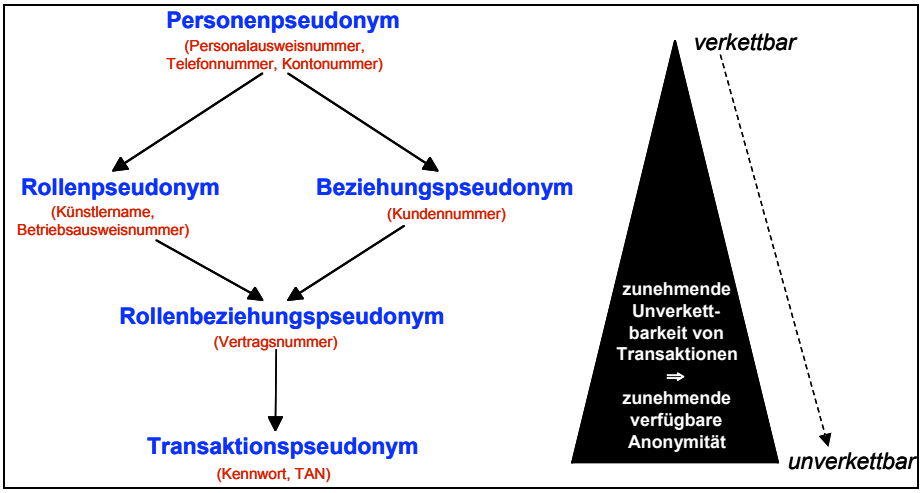

Abbildung 2: Pseudonymarten und ihr Verwendungszusammenhang (als Halbordnung)

Neben den genannten Arten an Pseudonymen existieren weitere, die hier nur kurz genannt sein sollen, da sie nichts Neues zur Anonymität beitragen: So wird von *Gruppenpseudonymen* gesprochen, wenn viele Benutzer ein Pseudonym gleichzeitig nutzen. Ein alltägliches Beispiel ist der Eintrag in einer Mailingliste, wobei der Bezeichner der Mailingliste das Gruppenpseudonym darstellt. Außerdem gibt es noch die *übertragbaren Pseudonyme.* Dabei wird ein Pseudonym von vielen Benutzern nacheinander verwendet. Man denke da bspw. an die Nummernautomaten in öffentlichen Einrichtungen (z.B. Meldestelle), wo die gezogenen Nummern an anderen Tagen wieder verwendet werden.

4.4 Credentials

Credentials werden, wie bereits in Abschnitt 4.2 beschrieben, als umrechenbare Autorisierungen eingesetzt. Allerdings ist dies nur durch eine entsprechende Gestaltung von Anwendungen realisierbar. Das heißt:

1. diese Anwendungen müssen Pseudonyme zunächst erst einmal zulassen und andererseits

2. muss die Wertemenge der Attribute klein gehalten werden.

Wenn der Attributraum sehr komplex und detailliert gestaltet wäre, könnten keine sinnvollen Anonymitätsmengen mehr erstellt werden. Das heißt, um eine Re-Identifizierung zu verhindern, muss die Anwendung so gestaltet sein, dass das, was an authentischer Information gefordert wird, nur soviel ist, wie die Anwendung wirklich braucht.

5 Projekte im Bereich Identitätsmanagement und das Projekt PRIME

Derzeit findet ein großer Rummel um die verschiedensten Identitätsmanagementsysteme statt. Verschiedene Projekte, die sich mit dem Thema Identitätsmanagement befassen, dabei jedoch sehr unterschiedlich den Bereich des Datenschutzes in ihre Konzepte integrieren, sollen hier beispielhaft genannt sein:

(.NET) Passport ist das völlige Gegenteil von dem, was wir in diesem Artikel beschrieben haben. Es zeichnet sich aus durch seine Eignung als zentrale Überwachungsinfrastruktur, charakterisiert durch genau eine entwerfende, implementierende und betreibende Instanz – durch Microsoft.

SUN ist der Initiator des Liberty Alliance Ansatzes, welcher zwar dezentral ist, jedoch bisher die Kontrolle nicht in Nutzerhand übergehen lässt.

Des Weiteren gibt es eine Reihe von Universitäts-Forschungsprojekten, wo Teilaspekte von Identitätsmanagement implementiert und erprobt wurden. Stellvertretend sollen der iManager (Universität Freiburg) und das DRIM (Dresden Identity Management, TU Dresden) genannt sein.

Ein großes EU-gefördertes Projekt, das sich ganz den Ansätzen dieses Artikels verschrieben hat, ist PRIME (PRivacy and Identity Management for Europe)[1]. Dies wurde im März 2004 mit rund 20 Partnern gestartet. Diese Partner kommen aus den verschiedensten Gebieten: z.B. Soziologen, Juristen, Ökonomen, Anwender, Gestaltungswissenschaftler und natürlich aus dem Technikbereich. Involviert sind sowohl große Firmen wie HP oder IBM als auch einige Universitäten und selbständige Forschungseinrichtungen wie bspw. das JRC in Italien oder Chaum LLC in den USA. Die Vision des PRIME-Projekts ist es, den Benutzern die Technik in die Hand zu geben, mit der sie sicher in der Informationsgesellschaft agieren und dabei die Souveränität über ihre Privatsphäre bewahren können.

PRIME hat es sich zur Aufgabe gemacht, auf der Basis verschiedener Forschungsansätze Lösungen zu entwickeln, die die Benutzer befähigen sollen, ihre Teilidentitäten in weitgehend natürlicher Weise zu verwalten und über ihren informationellen Privatbereich selbst bestimmen zu können.

Die Forschungsinhalte bewegen sich von der Entwicklung von Modellen über die Funktionalitätsimplementierung hin zum Einsatz in realen Anwendungsszenarien. Dafür arbeiten im Projekt Teams aus den Bereichen der Location Based Services, der Identifikation und Authentifikation bei der Reiseabwicklung sowie des kollaborativen eLearnings.

---

[1] http://www.prime-project.eu.org/

Zum Ende des Projektes im Februar 2008 werden sowohl ein Integrierter Prototyp für die PRIME-Plattform, der anhand von relevanten Szenarien zeigen soll, wie datenschutzförderndes Identitätsmanagement erreicht werden kann, als auch die entsprechenden Anwendungsprototypen aus den genannten Anwendungsbereichen zur Verfügung stehen. Außerdem werden im Rahmen des Projektes Tutorials entwickelt, die den Endnutzer für die Problematik sensibilisieren und mit den Mechanismen vertraut machen sollen.

6 Zusammenfassung und Ausblick

Mit dem Begriff Identitätsmanagement verbinden sich häufig Ansätze, wie sie z.B. von Microsoft mit dem Passport-System oder der Liberty Alliance verfolgt werden. Diese bieten Datensicherheitsdienstleistungen, welche keine oder kaum Datenschutzaspekte beinhalten. Jedoch sollte, wenn wir über Identitätsmanagement diskutieren, nicht vergessen werden, dass, auch wenn bestimmte Apparate (wie bspw. die Polizei, das Innenministerium oder Geheimdienste) intentional mehr Sicherheit für den Bürger wollen, sie doch ihr Eigenleben haben. Somit ist es mit oben genannten Plattformen, die die Verwaltung von persönlichen Informationen einem verteilten Netzwerk an Servern übertragen, nur eine Frage der Zeit, des Ziels und auch der entsprechenden rechtlichen Grundlagen, dass Daten auch in die Hände derjenigen fallen, in die sie nicht sollten. Nebenbei sollte dabei auch erwähnt werden, dass Abhör- und Überwachungs-schnittstellen, deren Einrichtung zugunsten der Sicherheit der Bürger erfolgt, auch für kriminelle Vereinigungen arbeiten.

Aus diesem Grund beschäftigt sich die Forschung im Bereich Datenschutz und Datensicherheit damit, den Einzelnen (Bürger) in eine Position zu bringen, die ihn befähigt, soviel wie möglich seiner Sicherheit und seines Datenschutzes selbst zu managen: *Datenschutzgerechtes Identitätsmanagement*.

Identitätsmanagement im Sinne des Datenschutzes ist nicht mit der Implementierung eines Systems getan. Viele Schritte sind notwendig, um ein umfassendes Identitätsmanagement zur Verfügung stellen zu können. Genannt sein sollen dabei verschiedene nutzerseitige Teilaspekte, wie ein Anonymitätsdienst, der eine anonyme Kommunikation zwischen dem Benutzer und dem Service-Betreiber ermöglicht, entsprechende Sicherheitsfunktionalität aufbauend auf Kryptografie, Regeln und Obligationen für datenschutzgerechte Datenhaltung, Möglichkeiten für die Pseudonymgenerierung und –verwaltung sowie ein „Data Tracking“ auf Nutzerseite, das die Historie von Transaktionen reflektiert. Des Weiteren gehören dazu Protokolle, auf deren Basis mit mehreren Parteien kommuniziert werden kann: für Credentials und andere Zertifikate, für die Interpretation von Kontextdaten inklusive Datenschutzinfoservice, für Datenschutzkontrollfunktionen, für Aushandlungen bei kontroversen Interessen und für den Werteaustausch.

Zusammenfassend kann gesagt werden, dass das Übertragen des natürlichen Identitätsmanagement in die digitale Welt nicht trivial ist und ein sehr komplexes Geflecht an interdisziplinären Anforderungen zu erfüllen hat. Ein Projekt, das sich der Erforschung hiervon verschrieben hat, ist das beschriebene PRIME-Projekt, dessen Ergebnis-Bausteine im Frühjahr 2008 verfügbar sein werden.

Literaturverzeichnis

[Chau85] D. Chaum: *Security without Identification: Transaction Systems to Make Big Brother Obsolete*. Communications of the ACM 28/10, S. 1030-1044, 1985.

[Pfi01] Andreas Pfitzmann: *Multilateral Security: Enabling Technologies and Their Evaluation*. In: R. Wilhelm (Ed.): Informatics - 10 Years Back, 10 Years Ahead, Schloss Dagstuhl, LNCS 2000, Springer-Verlag, Heidelberg 2001, S. 50-62, August 27-31, 2000.

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

[Vzu83] *Volkszählungsurteil: BVerfGE 65, 1 - Volkszählung*. BVerfGE.65. [1], 1983, http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm.