Datenschutzaspekte von Identitätsmanagementsystemen

Recht und Praxis in Europa

Marit Hansen, Henry Krasemann, Martin Rost, Riccardo Genghini

Wie sehen Recht und Praxis von Identity Management Systemen im europäischen Kontext aus?

Marit Hansen

Dipl.-Inform; Referatsleiterin „Privacy-Enhancing Technologies“ im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein

EMail: hansen@datenschutzzentrum.de

Henry Krasemann

Jurist beim ULD u.A. im Bereich Identitätsmanagement; Homepage: www.krasemann.info.

EMail: krasemann@datenschutzzentrum.de

Martin Rost

Sozialwissenschaftlicher Mitarbeiter im ULD; Homepage: www.netzservice.de/Home/maro/

EMail: martin.rost@datenschutzzentrum.de

Dr. Riccardo Genghini

Notary in Milan (Italy), Cen-ISSS E-Sign WS Chairperson, UNINFO-STT WS Chairperson, Member of ETSI and Liberty Alliance

E-Mail: riccardo.genghini@sng.it

Einleitung

Das Thema „technisch gestütztes Identitätsmanagement“ gewinnt weiter an Bedeutung. Inzwischen fördert die EU mehrere Projekte in diesem Bereich, die Zahl an Publikationen insbesondere in populären Zeitschriften nimmt zu. Die Spannweite der Definitionen von Identitätsmanagement oder Identitätsmanagementsystem (IMS) ist allerdings weit. Diese werden nachfolgend zunächst aufgegriffen, fokussiert und mit dem EU-rechtlichen und datenschutzrechtlichen Kontext abgeglichen. Es zeigt sich, dass sich die juristische Basis für Identitätsmanagement auf zwei Haupteigenschaften stützt: Zum einen ist für bestimmte rechtliche Kontexte eine zweifelsfreie Identifizierung einer Person notwendig; zum anderen ist die Gestaltbarkeit der Identität bereits in den Persönlichkeitsrechten verankert. Dem folgen einige kritische Anmerkungen zur bereits bestehenden Identitätsmanagement-Praxis sowie eine Vorstellung der aktuellen EU-Initiativen zum Thema „technisch gestütztes Identitätsmanagement“.

1 Begriffsklärung IMS

Es gibt vielfältige Definitionen von Identitätsmanagementsystemen. Nicht alle Systeme, die mit dem Verwalten von Identitäten in welch komplexer Form auch immer sind allein deshalb schon als Identitätsmanagementsystem zu bezeichnen.

Wir leiten die folgenden Kriterien für ein Identitätsmanagementsystem aus einem sozialpsychologisch abgesicherten Begriff ab:

- Bei der „Identität“, die im Fokus steht, geht es um die kommunikativ zugängliche Repräsentanz einer Person. In der Regel wird es sich dabei um eine natürliche Person und Informationen über sie handeln, doch trifft man auf die Bezeichnung IMS auch bei juristischen Personen. Auch die Identitäten von kommunikativ nicht trivial in Erscheinung tretenden Objekten werden künftig voraussichtlich eine größere Rolle spielen und haben womöglich Einfluss auf die Ausformung eines IMS.
- „Management“ bedeutet, dass Identitätsinformationen verwaltet und verarbeitet werden. Wir verstehen das „Managen“ als einen aktiven, gestalterischen Prozess desjenigen, um dessen Identitätsinformationen es geht. Außerdem gehört aus unserer Sicht zum Identitätsmanagement die Möglichkeit, über die Verwendung seiner Identität zu entscheiden bzw. verschiedene Identitäten[1] zu unterscheiden und zwischen diesen auszuwählen.
- Während Identitätsmanagement tagtäglich und von je her auch ohne Computerunterstützung im Sinne von Rollengestaltung einfach stattfindet, weist der Wortbestandteil „System“ auf die Unterstützung durch Informations- und Kommunikationstechnik hin, die wiederum in einen allgemeinen gesellschaftlichen Kontext eingebettet ist. Ein Identitätsmanagementsystem in einem allgemeinen Sinne umfasst dann sämtliche (Identitätsmanagement-)Applikationen, Infrastrukturen und spezielle Verfahren, die in Bezug auf die nutzerseitig kontrollierte Gestaltung von Identitäten in Kommunikationen eine Rolle spielen.

[1] Pseudonyme und die damit in Zusammenhang stehenden Informationen.

1.1 Anzahl möglicher Identitäten

Identitäten des Nutzers werden in IT-Systemen durch Datensätze repräsentiert. Unterstützt das System nur eine einzige Identität, sind die Freiheitsgrade für das „Managen“ von Identitäten eingeschränkt, denn es existiert keine Auswahl zwischen mehreren Identitäten. IMS-Funktionalität könnte hier darin bestehen, über die Herausgabe von Einzelinformationen eines Identitätsdatensatzes zu bestimmen.

Beispiele für die Zuordnung genau einer Identität sind Personalausweise, Pässe oder andere Formen von Autorisierungen, die auf Papier oder beispielsweise auf Chipkarte mit zugehörigem Hintergrund-IT-System gespeichert sind.

Am andere Ende des Spektrums befindet sich die Möglichkeit, genau keine Identität preiszugeben und anonym zu kommunizieren. Doch ohne Adressierbarkeit kommt auch diese Kommunikation nicht zustande. Bei der technischen Realisierung von Anonymität gibt es deshalb weiterhin Kennungen. Beispielsweise arbeiten Webanonymisierer so, dass für alle Nutzer dieselbe Absende-IP-Adresse sichtbar ist. Die Anonymität ist grundsätzlich um so stärker, je mehr Personen dasselbe Gruppenpseudonym als Kennung verwenden.

Diese beiden Extreme integrierend erlaubt Identitätsmanagement im Prinzip sämtliche Identitäten, unter denen Personen kommunizierend in Erscheinung treten, den jeweiligen Situationen angepasst explizit, und damit jederzeit rational zugänglich zu handhaben. Man handhabt kontextspezifisch zugeschnittene Autorisierungen, die einerseits den Datenaustausch effektivieren und die andererseits Verkettbarkeiten zwischen verschiedenen, unabhängig voneinander stattfindenden Kommunikationen verhindern [Hansen/Rost 2003].

Eine Voraussetzung für die Nutzung technisch gestützten Identitätsmanagement besteht in der Möglichkeit, auf einer anonyme Kommunikation gewährleistenden Infrastruktur aufsetzen zu können, so dass es zu keinen vom Nutzer unkontrollierbaren Verkettungen zwischen verschiedenen Kommunikationen kommen kann. Im herkömmlichen Leben ist diese Situation bei zufälligen Begegnungen der Standardfall. Auch wenn man keiner Person seine unverwechselbare Identität absprechen kann, bleibt diese doch im Normalfall, etwa bei Einwegbegegnungen an der Einkaufskasse, ohne Berücksichtigung.

Beim eigentlichen Identitätsmanagement geht es in der Regel somit um mehr als die Handhabung nur einer allgemeinen Identität. Anonymitätsdienste spielen insofern eine Rolle, als dass eine Basisanonymität im Kommunikationsnetz gewährleistet sein muss, damit nicht jede Aktion des Identitätsmanagers ohnehin verfolgbar ist. Reine Anonymisierer sehen allerdings keine Identitätsmanagementfunktionalität vor.

1.2 Wer soll managen?

In Bezug auf die Interpretation des Begriffs Identitätsmanagement(system) stellt sich die Kernfrage wie folgt: Wer soll oder darf die personenbezogenen Daten managen? Die Antwort wird durch die Unterscheidung „von der Personendatenverwaltung bloß Betroffener“ und „die Personendaten aktiv Gestaltender“ geformt.

- Die Datenschutzliteratur versteht unter Identitätsmanagement die grundsätzliche Kontrolle des Nutzers über seine eigenen Daten [vgl. Chaum 1985; Köhntopp 2000; Clauß et al. 2002]: Er soll Transparenz darüber haben und möglichst weitgehend bestimmen können, wem er welche Daten über sich offenbart. Dies schließt allerdings die Möglichkeit ein, dass Dritte, denen der Nutzer vertraut, das Identitätsmanagement im Auftrag abwickeln können.
- Staatlich kontrollierte Institutionen interagieren mit natürlichen Personen gemäß des komplizierten Konzepts „Bürger“. Dieser ist in Bezug auf das Management personenbezogener Daten sowohl als Betroffener staatlichen Handelns auch als Gestalter, wenn auch oft nur indirekt und vermittelt, aufzufassen. Im Normalfall wird einer betroffenen Person immerhin mitgeteilt, wenn sie staatlicherseits nur als Betroffener behandelt wird. Eine vergleichbare Konstellation besteht im betrieblichen Binnenverhältnis zwischen Management und Mitarbeiter. Hier wird zwar, weniger als im staatlichen Handeln, seitens des Managements die Autonomie der Person als prinzipiell unantastbar geachtet. Stattdessen geht es zumindest in anspruchsvolleren Positionen darum, die Souveränität der Selbstbestimmung des Mitarbeiters für die Zwecke der Organisation nutzbar zu machen. In beiden Konstellationen läuft Identitätsmanagement inhaltlich auf ein Aushandeln der angemessenen Verfügungsgewalt über Teile des auf die Person zugeschnittenen Datensatzes hinaus. Der Staat sieht sich aufgefordert, im Zweifel den mündigen Bürger zu unterstützen. Firmen haben im Zweifel weit weniger Skrupel, Identitätsmanagement vornehmlich im Sinne einer möglichst effektiven Verarbeitung von Personendaten auszulegen. Identitätsmanagement wird deshalb in diesem Kontext oftmals als ein Verwaltungsprozess ausgewiesen und beworben, der als Data Warehouse gestaltet die Authentifizierung, die Zugriffsrechte und die eingeräumten Vorrechte eines digitalen Arbeitnehmers umfasst.
- Unter Identitätsmanagementsystem verstehen professionelle Datensammler die Data-Warehouse-Software zur Verwaltung personenbezogener Daten, d.h. insbesondere Profilbildung und Übermittlung der Datensätze. Hier hat der Betroffene in der Regel weder Kontrolle noch ist für ihn die Verarbeitung seiner Daten transparent. In vielen Fällen ahnt er nicht einmal, dass seine Daten verarbeitet werden. Nach Art. 11 Abs. 1 EU-Datenschutzrichtlinie (1995/46/EG) muss der Betroffene allerdings spätestens bei der ersten Übermittlung seiner Daten informiert werden.

In diesem Beitrag betrachten wir IMS in der ersten Bedeutung. Für die datenschutzrechtlichen Aspekte von Data Warehouses sei auf das Schwerpunktheft DuD 10/1998 verwiesen.

1.3 Unterschiedliche Ausprägung und Funktionalität

Die Einsatzmöglichkeiten eines IMS sind weit gespannt. Dazu gehören u.a.:

- Komfortables Verwalten bereits vorhandener Identitäten/Accounts/Passwörter (Single Sign-On);
- Authentikation und Zugriffskontrolle;
- Rollenmanagement, insbesondere die Trennung von Berufs- und Privatleben und deren jeweils internen Differenzierungen;
- Erreichbarkeitsmanagement;
- Recht auf informationelle Selbstbestimmung: Balance von Anonymität und Authentizität/Zurechenbarkeit.

Je nach Einsatzbereich stehen unterschiedliche Funktionen im Vordergrund. Abgesehen

von der Präsentations- und Auswahlkomponente von kontextabhängig unterschiedlichen Pseudonymen ist eine History-Funktion typisch für alle Einsatzbereiche, in denen Datenweitergaben mitprotokolliert werden, damit der Nutzer sich ein Bild darüber machen kann, was der Kommunikationspartner über ihn weiß.

1.4 Ergebnis

Identitätsmanagementsysteme sind nach unserem Verständnis Werkzeuge für den Nutzer, um seine Rollen mit den zugehörigen Daten je nach Situation verwalten zu können.

Soweit im jeweiligen Kontext möglich, sollte ein Identitätsmanagementsystem dem Nutzer Folgendes bieten:

- *Steuerung*, wer in welchem Kontext welche seiner personenbezogenen Daten erhält und wie verwenden darf, und – da dies nicht immer möglich ist –
- *Darstellung*, wer welche seiner personenbezogenen Daten erhält und wie verwenden sollte bzw. welche Zusagen an die Verarbeitung bestehen.

2 Rechtliche Einordnung von IMS

Die Identität einer natürlichen Person ist rechtlich in zweierlei Hinsicht von Bedeutung:

- zur Identifizierung für rechtlich relevante Zwecke und
- um persönliche Freiheitsrechte (Name, Selbstbestimmung, Meinungsfreiheit usw.) in Zusammenhang mit einer natürlichen Person zu schützen.

Demnach besteht die Identität zum einen aus Elementen, die ihre Einzigartigkeit garantieren sollen, z.B. die in den meisten rechtlichen Systemen gängigen Attribute wie Name, das Geschlecht, Geburtstag, Geburtsort, Nummer der Geburtsurkunde, Identität der Eltern, Nationalität, Wohnort und Beruf; hinzu kommen biometrische Merkmale. Zum anderen umfasst die Identität Persönlichkeitsrechte, die in demokratischen Staaten in der Verfassung und weiteren Gesetzen niedergelegt sind und den Menschen die Möglichkeit geben, ihre Persönlichkeit zu entfalten und dadurch die Identität zu entwickeln.

Diese Persönlichkeitsrechte bilden gleichzeitig eine rechtliche Basis für das Identitätsmanagement, z.B. das Recht, unter bestimmten Bedingungen seinen Namen oder das Geschlecht zu ändern, über sein Aussehen zu entscheiden, seinen Wohnort festzulegen und zu wechseln und sogar auszuwandern. Außerdem haben die Menschen das Recht, in vielen Situation anonym oder unter (selbst gewähltem) Pseudonym aufzutreten.[2]

Es gibt im europäischen Rechtsrahmen keine generelle Verpflichtung, die eigene Identität zu offenbaren. Beispielsweise kennen einige demokratische Länder keinen Personalausweis oder erlegen dem Inhaber keine Verpflichtung auf, ihn bei sich zu führen.

> Übergreifend lässt sich festhalten, dass Identitätsmanagement an sich rechtskonform ist, solange es nicht in betrügerischer Absicht geschieht, in anderer Weise die Rechte von Dritten beeinträchtigt oder gegen die guten Sitten verstößt. Darüber hinaus sieht das Recht selbst Möglichkeiten für Identitätsmanagement vor.

So akzeptiert anerkanntermaßen das deutsche Recht Eigengeschäfte trotz Handelns unter fremden Namen. Sofern Name und Identität des Vertragspartners für den Abschluss eines Vertrages und dessen Durchführung keine Rolle spielen, kann unter einem beliebigen Pseudonym aufgetreten werden. Dies ist z.B. bei den täglichen Bargeschäften oder Übernachtung im Hotel meist der Fall.[3]

Auch das Signaturgesetz lässt für z.B. qualifizierte Zertifikate ausdrücklich Pseudonyme zu (Art. 8 Abs. 3 EU-Signaturrichtlinie 1999/93/EG bzw. im deutschen Recht § 5 Abs. 3 SigG).

3 Anforderungen des Datenschutzes an IMS

Zu den Persönlichkeitsrechten, die für Identitätsmanagement eine Rolle spielen, gehört in besonderem Maße das Recht auf informationelle Selbstbestimmung [vgl. Hansen 2003]. In diesem Abschnitt wird dargestellt, wie sich IMS-Funktionalität unmittelbar aus dem Volkszählungsurteil von 1983 (BVerfGE 65, 1) ableitet, wie der europäische Rechtsrahmen Kriterien für IMS beinhaltet und was sich an zusätzlichen Anforderungen für eine Realisierung im Sinne der Privacy-Enhancing Technologies ergibt.

3.1 Volkszählungsurteil: Nutzergesteuertes IMS

Das Volkszählungsurteil macht deutlich, dass das Recht auf informationelle Selbstbestimmung als Identitätsmanagement unter Nutzerkontrolle verstanden werden soll:

„Individuelle Selbstbestimmung setzt [...] – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“[4]

Nutzergesteuertes Identitätsmanagement zielt darauf ab, dass die Nutzer das Wissen ihrer Kommunikationspartner abschätzen und dies bei ihren Entscheidungen berücksichtigen können. Es geht dabei nicht nur um eine systemseitige Realisierung, sondern die Nutzer sollen befähigt werden, selbst verantwortungsvoll über die Herausgabe ihrer personenbezogenen Daten zu entscheiden.

3.2 EU-Datenschutzrichtlinie und IMS

Die Artikel 29-Gruppe, eingesetzt nach der EU-Datenschutzrichtlinie, hat sich bereits zu „Online-Authentifizierungssystemen“, die den Identitätsmanagementsystemen zuzurechnen sind, geäußert [Art. 29 2003]. Anhand der Fallstudie „Microsoft Passport“ wurden Kritikpunkte erarbeitet, die Microsoft zu bearbeiten zugesagt hat [Microsoft

[2] Vgl. z.B. Palandt, BGB, § 12 Rn. 8.
[3] Vgl. Palandt, BGB, § 164 Rn. 12.
[4] BVerfGE 65, 1 (Volkszählungsurteil) 1983.

2003]. U.a. wurden die folgenden datenschutzrelevanten Überlegungen angestellt:

- Wer Online-Authentifizierungssysteme konzipiert oder umsetzt, ist für die datenschutzrelevanten Aspekte verantwortlich. Die verschiedenen Akteure sollten ihre Pflichten in klaren Verträgen regeln.
- Online-Authentifizierungssysteme sollen anonym oder pseudonym genutzt werden können.[5] Sofern dies den vollen Funktionsumfang einschränken würde, sollte das System so aufgebaut sein, dass ein Minimum an Informationen für die Authentifizierung ausreicht und der Nutzer frei darüber entscheiden kann, zusätzliche Informationen (z.B. Profildaten) bereitzustellen.
- Die Benutzer müssen angemessen, d.h. auf leicht zugängliche und benutzerfreundliche Art und Weise, über die datenschutzrechtlichen Hintergründe des Systems informiert werden.
- Falls persönliche Daten in Drittländer übermittelt werden, sollten Authentifizierungsanbieter mit Dienstanbietern zusammen für den Schutz der Daten sorgen, sei es auf vertraglicher Basis oder durch verbindliche Unternehmensgrundsätze. Erfolgt die Übermittlung auf Grund einer Einwilligung, sollten dem Benutzer ausreichende Informationen und Auswahlmöglichkeiten angeboten werden, so dass er seine Zustimmung fallweise erteilen oder verweigern kann.
- Bei Verwendung von Kennungen sollten die Benutzer die Möglichkeit haben, diese zu aktualisieren.
- Die Verwendung einer Software-Architektur, die die Zentralisierung von personenbezogenen Daten der Internet-Nutzer auf ein Mindestmaß beschränkt, sollte gefördert werden, um die Fehlertoleranz zu erhöhen und die Entstehung von umfangreichen zentralisierten Datenbanken zu verhindern.
- Die Nutzer sollten die Möglichkeit haben, ihre Recht auf einfache Weise wahrzunehmen (z.B. Opt-Out) und auf Löschung ihrer Daten zu bestehen, wenn sie das System nicht mehr nutzen wollen. Sie sollten angemessen darüber informiert werden, wie sie bei Anfragen oder Beschwerden zu verfahren haben.
- Es sollten diejenigen technisch-organisatorischen Maßnahmen ergriffen werden, die dem jeweiligen Sicherheitsrisiko angemessen sind.

[5] Dies ergibt sich im Bundesrecht auch aus § 3a BDSG und § 4 Abs. 6 TDDSG.

4 IMS in der Praxis

Untersuchungen [Köhntopp 2001; Zehentner 2002; Art. 29 2003; Pfitzmann 2003] zeigen, dass alle bisher auf dem Markt vorhandenen Identitätsmanagement-Services und -Tools zumindest aus Datenschutzsicht Mängel aufweisen.

Zwar können alle Identitätsmanagement-Services und -Tools durch entsprechende Vertragsgestaltung und Einwilligungen der Nutzer datenschutzgerecht organisiert werden. Doch wird bei den gängigen Services und Tools das Vertrauen des Kunden in die Systeme und ihre Betreiber vorausgesetzt.

Eine wichtige Entscheidung des Kunden bei der Auswahl der Produkte dürfte daher die Frage sein, ob die Datenverwaltung und Datenhaltung bei einer Fremdfirma oder auf eigenen Systemen erfolgen soll. Produkte wie Microsoft Passport[6], Novell Digitalme[7] oder Yodlee[8] erfordern von dem User das Vertrauen in den IMS-Provider, dem die Daten anvertraut werden. Liberty Alliance[9] bietet diesbezüglich zwar die Möglichkeit, die Datenhaltung auf mehrere Anbieter zu verteilen und eine größere Kontrolle über deren Verwendung selbst in der Hand zu haben. Ohne Vertrauen in die angeschlossenen Unternehmen kommt aber auch diese Lösung nicht aus.

Aus Sicht des Datenschutzes wären daher diejenigen Identitätsmanagement-Applikationen zu bevorzugen, bei denen der Nutzer die Kontrolle über seine Daten behält. Einige Produkte verfolgen diesen Ansatz, indem sie die Daten direkt auf den Systemen des Nutzers verwalten, wie etwa Mozilla[10], Internet Explorer[11], CookieCooker[12] und Neuentwicklungen wie DRIM[13] oder ATUS[14]. Auch aus Datensicherheitsgründen ist eine zentrale Speicherung von Nutzerdaten bei einem externen Anbieter kritisch zu sehen, denn diese Datenbanken können begehrte Angriffsziele sein – sowohl für externe als auch für interne Angreifer. Die Nutzer müssen sich allerdings darüber im Klaren sein, dass sie im Falle der Datenverwaltung auf dem eigenen Computer auch selbst die Verantwortung für ein angemessenes Sicherheitsniveau übernehmen. Es bleibt eine offene Frage, wie dies mit den heute verbreiteten inhärent unsicheren Systemen vom Nutzer praktisch geleistet werden kann.

In allen Fällen muss den Herstellern der Produkte das Vertrauen entgegengebracht werden, dass sie keine Hintertüren in ihre Produkte eingebaut haben, die ein Ausspionieren erlauben. Open Source kann zur gesteigerten Vertrauenswürdigkeit der Produkte beitragen.

Beweisfestigkeit wird von praktisch keinem der bekannten Produkte aktiv unterstützt. Werden rechtlich bedeutsame Aktionen durchgeführt, ist es an dem Nutzer selber, sich um die Beweissicherung zu kümmern. Dies kann bei den E-Mail-Clients z.B. durch Einsatz von digitalen Signaturen geschehen, wobei die derart signierten Mails vom Nutzer selber verwaltet werden müssen. Auch Nachsignierungen im Falle z.B. einer Kompromittierung einer Signiertechnik muss der User selber durchführen oder auf Fremdprodukte ausweichen.

Die Usability lässt bei vielen Produkten zu wünschen übrig. Es wird eine der größten Herausforderungen für die Systemgestalter sein, die Funktionen eines datenschutzfördernden Identitätsmanagements dem Nutzer verständlich und leicht bedienbar zu machen.

5 EU-Projekte zu Identitätsmanagement

Privacy-Enhancing Technologies und speziell „Privacy and Identity Management“ sind mittlerweile in der EU zu einem wichtigen Thema geworden, das in verschiedenen Projekten bearbeitet wird.

5.1 RAPID

RAPID („Roadmap for Advanced Research in Privacy and Identity Management“)[15] war im Jahr 2002 das erste größer angelegte Projekt, das dazu dienen sollte, die noch junge Forschung und Entwicklung zu Identitätsmanagement zu fokussieren und eine Roadmap für kurzfristige (0-3 Jahre), mit-

[6] www.passport.com.
[7] www.digitalme.com.
[8] www.yodlee.com.
[9] www.projectliberty.org.
[10] www.mozilla.org.
[11] www.microsoft.com.
[12] cookie.inf.tu-dresden.de; Berthold/Federrath: CookieCooker: Cookies tauschen – Profile vermischen; in: DuD 27/5; 2003; 299.
[13] drim.inf.tu-dresden.de (Dresden Identity Management); Clauß/Kriegelstein: Datenschutzfreundliches Identitätsmanagement; in: DuD 27/5; 2003; 297.
[14] www.iig.uni-freiburg.de/telematik/atus/ (A Toolkit for Usable Security); Jendricke/Gerd tom Markotten: Benutzbare Sicherheit durch Identitätsmanagement; in: DuD 27/5; 2003; 298.
[15] www.ra-pid.org.

telfristige (3-5 Jahre) sowie längerfristige (5-10 Jahre) Forschungsfragen zu erstellen [Wilikens 2003].

5.2 IMS Study

Derzeit wird eine Studie („Identity Management Systems (IMS): Identification and Comparison Study") abgeschlossen, in der vornehmlich bereits existierende Identitätsmanagement-Lösungen auf Grundlage sozialpsychologischer, juristischer und technischer Grundlagen verglichen und bewertet werden. Die Kriterien für den Vergleich werden aus Szenarien für den Einsatz von Identitätsmanagement gewonnen. Darüber hinaus wurden weltweit rund 240 Experten über ihre Vorstellungen zu Identitätsmanagement befragt.

5.3 PRIME

Im Sechsten Europäischen Forschungsrahmenprogramm „Technologien für die Informationsgesellschaft" wird voraussichtlich ab 2004 das Projekt PRIME („PRivacy and Identity Management for Europe") gefördert. Das Konsortium besteht aus 22 Partnern aus Wirtschaft und Wissenschaft sowie dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. Ziel von PRIME ist die umfassende Erforschung und praktische Umsetzung von speziellen Mechanismen und Identitätsmanagement-Applikationen, die die Souveränität des Nutzers stärken sollen.

5.4 FIDIS

Ebenfalls erfolgreich bei der Ausschreibung zu diesem Förderprogramm war das Network of Excellence FIDIS („Future of IDentity in the Information Society"). Hier sind 24 europäische Institutionen am Diskurs zu einem verbesserten Verständnis von Identitäten und Identitätsmanagement auf dem Weg zu einer gerechteren Informationsgesellschaft beteiligt. U.a. kann FIDIS das Forum dafür sein, ein Regelwerk für Online-Identitäten im neuen technologischen Kontext zu entwickeln.

5.5 EASET

Das Projekt EASET („European Association for the Security of Electronic Transactions", siehe http://www.easet.net), das sich derzeit in der Start-Up-Phase befindet, wurde von Notaren aus neun EU-Mitgliedsstaaten mit dem Ziel gegründet, zugleich Zertifizierungen von Online-Transaktionen als auch weitergehende Identitätsmanagement-Dienstleistungen anbieten zu können.

Fazit

Man darf davon ausgehen, dass Identitätsmanagementsysteme in den nächsten Jahren weiterhin an Bedeutung gewinnen werden. Die Rechtsprechung im Bereich der EU unterstützt diese Entwicklung hin zu einem technisch gestützten Identitätsmanagement durch eine insgesamt vergleichsweise liberale Gesetzgebung.

Gerade für ein Rollenmanagement zwischen privatem und professionellem Leben, aber auch als komfortable Lösung für das Verwalten der zahlreichen eigenen Accounts ist von einer gesteigerten Nachfrage auszugehen. Allerdings hängt die Akzeptanz der Nutzer sowohl von der Usability als auch vom Vertrauensmodell ab: Kann der Nutzer wirklich die Kontrolle über die Daten behalten?

Für Anbieter empfiehlt es sich, zweigleisig zu fahren: Zum einen sollten sie Lösungen zur Verfügung stellen, die ein Identitätsmanagement auf Nutzerseite erlauben. Zum anderen können sie aber auch zentrale Lösungen anbieten für Nutzer, die damit einverstanden sind, dass die Anbieter beim Identitätsmanagement unterstützen. Rein anbieterseitiges „Identitätsmanagement im Auftrag des Nutzers" bedingt das absolute Vertrauen des Nutzers in den Anbieter.

Literatur

[Art. 29 2003] Artikel 29-Datenschutzgruppe: Arbeitspapier zu Online-Authentifizierungsdiensten; WP 68; 10054/03/DE; angenommen am 29. Januar 2003; europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_de.pdf.

[Chaum 1985] 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.

[Clauß et al. 2002] 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.

[Hansen/Rost 2003] Marit Hansen, Martin Rost: Nutzerkontrollierte Verkettung – Pseudonyme, Credentials, Protokolle für Identitätsmanagement; in: DuD 27/5; 2003; 293-296.

[Hansen 2003] Marit Hansen: Auf dem Weg zum Identitätsmanagement – von der rechtlichen Basis bis zur Realisierung; in: Bäumler/von Mutius (Hrsg.): Anonymität im Internet; Vieweg, Braunschweig 2003; 198-215.

[Köhntopp 2000] Marit Köhntopp: Identitätsmanagement; in: Bäumler/Breinlinger/Schrader (Hrsg.): Datenschutz von A-Z; Loseblattsammlung; Luchterhand, Neuwied 2000.

[Köhntopp 2001] Marit Köhntopp: „Wie war noch gleich Ihr Name?" – Schritte zu einem umfassenden Identitätsmanagement; in: Fox/Köhntopp/Pfitzmann (Hrsg.): Verlässliche IT-Systeme – Sicherheit in komplexen Infrastrukturen; Vieweg, Wiesbaden 2001; 55-75.

[Microsoft 2003] Microsoft: Building trust in Internet privacy: The New .NET Passport; 2003; www.microsoft.com/europe/whitepapers.mspx.

[Pfitzmann 2003] Birgit Pfitzmann: Privacy in enterprise identity federation -- policies for Liberty single signon; 3rd Workshop on Privacy Enhancing Technologies (PET 2003), Dresden, März 2003; erscheint im Tagungsband bei Springer.

[Wilikens 2003] Marc Wilikens: Challenges in privacy and identity management – Results from the RAPID project; in: DuD 27/5; 2003; 301-304.

[Zehentner 2002] Johann Zehentner: Privatheit bei Anwendungen für Identitätsmanagement im Internet; Diplomarbeit; Fakultät für Informatik der Technischen Universität München; Informatik XI: Angewandte Informatik / Kooperative Systeme; Dezember 2002; www11.in.tum.de/ publications/pdf/da-zehentne2002.pdf.