Informationelle Selbstbestimmung durch Identitätsmanagement

Informational Self-Determination by Identity Management

Marit Köhntopp, ULD SH, Kiel, und
Andreas Pfitzmann, TU Dresden

Schlagwörter: Identitätsmanagement, Datenschutz, Informationelle Selbstbestimmung, Pseudonym

Ein Identitätsmanagementsystem ermöglicht Nutzern, Art und Umfang der Herausgabe personenbezogener Daten zu kontrollieren. Damit ist es ein wichtiger Baustein für Datenschutz und mehrseitige Sicherheit. Wir beschreiben Anforderungen und Lösungen für ein umfassendes, datenschutzförderndes Identitätsmanagementsystem, das auf Pseudonymen beruht und eine mögliche Kooperation anderer Beteiligter einbezieht. Weiterhin diskutieren wir Grenzen und Risiken solcher Systeme.

An identity management system enables the user to control the nature and amount of personal information released. Thus, it is an important building block for implementing both privacy protection and multilateral security. We describe requirements and solutions for a comprehensive, privacy enhancing identity management system, which is based on pseudonyms and includes the possible co-operation of all parties involved. Finally, we discuss limitations and risks of such systems.

1 Einführung

Datenschutz ist zu einem zentralen Thema geworden, wie Umfragen zeigen.[1] Kein Mensch weiß heutzutage, wo überall er beim Nutzen globaler Netzdienste Spuren hinterlässt und wie diese ausgewertet werden. Diese Verunsicherung der Nutzer, wie es um ihren Datenschutz steht, gehört zu den größten

[1] S. Ergebnisse einer *Umfrage von Mummert & Partner* in Deutschland, vorgestellt im März 2001, http://www.mummert.de/deutsch/ press/a_press_info/01030b.html, der *US-Umfrage Pew Internet & American Life Project*: Trust and Privacy Online: Why Americans Want to Rewrite the Rules, Aug. 2000, http://pewinternet.org/ reports/toc.asp?Report=19, oder der *Harris-Umfrage von IBM* in USA, Großbritannien und Deutschland: IBM Multi-National Consumer Privacy Survey, New York, Okt. 1999, http://www.ibm.com/services/files/privacy_survey_oct991.pdf.

Hemmnissen des E-Commerce. Für ein Mehr an Datenschutz und Selbstbestimmung werden viele Konzepte diskutiert. Ein umfassender Ansatz für Datenschutz in Nutzerhand ist Identitätsmanagement.

1.1 Das Recht auf Datenschutz

Datenschutz ist ein Menschenrecht, das bspw. in der UN- sowie der Europäischen Menschenrechtskonvention festgeschrieben ist. Die Mitgliedstaaten der EU haben sich 1995 auf die EU-Datenschutzrichtlinie geeinigt. Grundlegende Rechtsnormen in Deutschland sind das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze. Hinzu kommen bereichsspezifische Bestimmungen.

Die Auffassung, was Datenschutz bzw. *Privacy* bedeutet, ist kulturell bedingt unterschiedlich. Während in den USA der Kern von Privacy als „the individual's right to be left alone" (Brandeis 1890) gesehen wird, steht im europäischen Kontext die demokratiebewahrende Informationsordnung im Vordergrund, wie sie im deutschen *Recht auf informationelle Selbstbestimmung* zum Ausdruck kommt: Jeder soll wissen und – soweit möglich – auch darüber entscheiden können, wer was wann über ihn weiß.[2]

1.2 Datenschutzgrundsätze

In den EU-Ländern dürfen personenbezogene Daten nur verarbeitet werden, soweit dies gesetzlich zugelassen oder von einer Einwilligung gedeckt ist. Der Umfang der verarbeiteten Daten muss sich auf das Erforderliche beschränken. Es gilt das Zweckbindungsprinzip, d.h. Daten dürfen grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden. Der Betroffene, um dessen Daten es geht, hat gegenüber der datenverarbeitenden Stelle das Recht auf Auskunft, was über ihn gespeichert ist, und Berichtigung und Löschung, wenn dort unrichtige oder unzulässige Informationen stehen. Beruht die Verarbeitung auf seiner Einwilligung, kann er diese auch später noch zurückziehen und Widerspruch einlegen: Seine personenbezogenen Daten sind dann in aller Regel zu löschen. Selbstverständlich sind die erforderlichen Sicherheitsmaßnahmen gegen einen Missbrauch der Daten zu treffen.

Hat der Nutzer seine Daten erst einmal herausgegeben, ist das Durchsetzen von Datenschutz schwierig: Es lässt sich kaum garantieren, dass die Daten nicht zu weiteren Zwecken verwendet werden, und gerade in der digitalen Welt können beliebig Kopien der Daten existieren.

Der heutige Datenschutz ist vor allem durch die fortschreitende IT-Entwicklung und die daraus resultierenden immer einfacheren Verarbeitungs- und vor allem Missbrauchsmöglichkeiten personenbezogener Daten motiviert. Es wird mittlerweile versucht, mit IT den Datenschutz zu unterstützen und in den Fällen der „Privacy Enhancing Technologies (PET)" sogar deutlich zu verbessern.

Die beste Datenschutztechnik ist die Gestaltung von Systemen und Verfahren nach dem Grundsatz der *Datensparsamkeit*, d.h. gemäß dem Erforderlichkeitsprinzip auch in IT-Systemen das Anfallen personenbezogener Daten zu minimieren, die Verwendungsmöglichkeiten einzuschränken und die Zweckbindung zu garantieren. *Transparenz* für den Nutzer, wo welche seiner Daten verarbeitet werden, ist für einen *vertrauenswürdigen* Datenschutz unabdingbar. Außerdem sollten sowohl die technischen Maßnahmen so weit wie möglich in die Systeme und Verfahren eingebaut werden (*Systemdatenschutz*) als auch die Nutzer selbst weitgehend die Kontrolle über ihren Datenschutz übernehmen können (*Selbstdatenschutz*).

1.3 Datenschutzrisiken

Täglich werden neu entdeckte Sicherheitslücken und Fälle von Datenmissbrauch gemeldet. Risiken für den Datenschutz ergeben sich schon aus der geringen Transparenz darüber, wo welche Daten über den Nutzer entstehen und was mit ihnen passiert. Dazu gehört der zunehmende Einsatz von meist ohne Wissen der Nutzer übertragenen Globally Unique IDentifiers (GUIDs), die einer eindeutigen Identifizierung dienen sollen. In globalen und multifunktional genutzten Netzen wie dem Internet können Daten aus verschiedenen Anwendungszusammenhängen oft mit wenig Aufwand recherchiert, verknüpft und zu Nutzerprofilen aggregiert werden, z.B. mit Data-Mining-Systemen.

Gleichzeitig fehlt im Internet eine Authentizität der Daten, so dass es einfach ist, unter dem Namen eines anderen zu agieren (*Identity Theft*). Dem soll zwar mit der Einführung der digitalen Signatur begegnet werden, doch könnte dies das Datenschutzproblem sogar noch verstärken: Nutzer könnten faktisch gezwungen werden, nunmehr auch dort authentische Datenspuren zu hinterlassen, wo diese im jeweiligen Anwendungskontext nicht erforderlich sind.

[2] Volkszählungsurteil, BVerfGE 65, S. 1 ff., 1983.

2 Ziele des Identitätsmanagements und seine Mechanismen

Identitätsmanagement bedeutet, dass eine Person grundsätzlich wählen kann, wie anonym bzw. mit welchen persönlichen Informationen und wie zurechenbar sie gegenüber ihren Kommunikationspartnern in Erscheinung tritt. Mit *Identitätsmanagementsystemen* lässt sich in der digitalen Welt das Recht auf informationelle Selbstbestimmung weitgehend technisch abbilden [12]. Im Folgenden werden die Ziele und Mechanismen skizziert.

2.1 Ziele von Identitätsmanagement

Die *Identität* einer Person umfasst alle Informationen, die mit ihr in Zusammenhang stehen. Untermengen der Identitätsinformation, sog. *Teilidentitäten*, repräsentieren die Person im jeweiligen Kontext. Sie können typisch sein für je eine Rolle, die die Person einnimmt, und mit bestimmten personenbezogenen Daten versehen sein.

Ein *Identitätsmanagementsystem* dient zur Verwaltung dieser Teilidentitäten: Sowohl die eigentlichen personenbezogenen Daten als auch Informationen über den Personenbezug an sich können damit gehandhabt werden [12]. Häufig ist es nicht notwendig, Informationen, die die Person identifizieren, herauszugeben. Vielmehr müssen lediglich für das Verfahren oder die Situation spezifische Eigenschaften nachgewiesen werden [8]. Hierzu kann z.B. der Nachweis der Volljährigkeit gehören, die Berechtigung zum Fahren eines Autos oder die Bestätigung einer vertraglichen Leistungserfüllung. Informationen, wie sie im Personalausweis stehen, sind bspw. zur fairen Abwicklung von Transaktionen in der Regel nicht erforderlich. Selbst für E-Government könnte vom Systemdesign her auf solche Informationen weitgehend verzichtet werden.

Die ersten Vorschläge zu einem technisch basierten, umfassenden Identitätsmanagement stammen aus den 1980er Jahren (insbesondere [7;8], darauf aufbauend z.B. [4;16]). Seitdem finden sich immer wieder Ansätze für generelle Modelle oder einzelne Teilkomponenten (z.B. das Konzept des Identity-Protectors [17], der Erreichbarkeitsmanager [18], die Identitätsmanagementkomponente im Projekt ATUS – A Toolkit for Usable Security [11;9] oder vielfältige Internet-Software und –Dienstleistungen [13]).

Ein *umfassendes Identitätsmanagementsystem* lässt den Nutzer steuern, wer wobei welche seiner personenbezogenen Daten erhält und wie verwenden darf. Dies bedeutet im Sinne *mehrseitiger Sicherheit* Formulieren, ggf. Aushandlung und soweit möglich Durchsetzen: Personenbezug, Umfang und Art der Daten sowie Bedingungen an die Verarbeitung der Daten wie Zweckbestimmung, Speicherdauer, Sicherheitsanforderungen oder etwaige Gegenleistung. Wo eine selbstbestimmte Steuerung nicht möglich ist, sollte das Identitätsmanagementsystem dem Nutzer darstellen, wer welche seiner personenbezogenen Daten erhält und wie verwenden darf (bzw. welche Zusagen an die Verarbeitung bestehen), z.B. durch Abwickeln von Auskunfts-, Berichtigungs- oder Löschungsbegehren sowie von Einwilligung und Widerspruch, Protokollieren der Herausgabe von Daten und Auswerten der Protokollierung danach, was Kommunikationspartner über den Nutzer in Erfahrung gebracht haben.

2.2 Mechanismen für Identitätsmanagement

Abgeleitet aus Datenschutzgrundsätzen wie Datensparsamkeit und Transparenz werden im Folgenden Mechanismen für Identitätsmanagement vorgestellt. Das Kernstück bilden Verfahren zur Gewährleistung von Anonymität und Pseudonymität. Dritte Parteien können spezielle Aufgaben wahrnehmen. Im Bereich des Nutzers ist darüber hinaus Funktionalität vorzusehen, die ihn unterstützt.

2.2.1 Anonymität

Anonymität lässt sich definieren als Zustand, innerhalb einer Menge von Subjekten, der *Anonymitätsmenge*, nicht identifizierbar zu sein [15]. Dem Identitätsmanagement sollte grundsätzlich Anonymität mit einer ausreichend großen Anonymitätsmenge zugrunde liegen, damit kein personenbezogener Datenfluss außerhalb des Identitätsmanagementsystems den Datenschutz gefährdet. Vorteilhaft ist, wenn diese Anonymität bereits vom allgemeinen Systemdatenschutz gewährleistet wird [1].

2.2.2 Pseudonyme und Credentials

Pseudonyme sind Bezeichner für Subjekte oder – im Fall der *Gruppenpseudonyme* – Mengen von Subjekten. *Pseudonymität* ist die Verwendung von Pseudonymen als Bezeichner [15]. Zurechenbarkeit lässt sich mit *digitalen Pseudonymen* realisieren, d.h. eindeutigen Bezeichnern, die geeignet sind, den

Pseudonyminhaber bzw. seine Daten zu authentisieren. Dies können öffentliche Schlüssel in einem digitalen Signatursystem sein.

Pseudonymität umfasst das Spektrum zwischen Anonymität und eindeutiger Identifizierbarkeit. Bzgl. Datenschutz ist die Verkettbarkeit von Pseudonymen bedeutsam. Hat jemand eine Reputation unter einem Pseudonym erlangt, kann er diese bei der wiederholten Verwendung desselben Pseudonyms ausbauen. Bestimmte Pseudonymarten ermöglichen es, gegen einen Missbrauch des Pseudonyminhabers im Schutze der Anonymität vorzugehen (s. 2.2.3).

Die Anonymität eines Pseudonyminhabers hängt davon ab, wieviel unmittelbar über die Zuordnung des Pseudonyms zur Person bekannt ist und inwieweit sich ein Personenbezug durch Beobachtung der Pseudonymverwendung, d.h. die Verkettung einzelner Aktionen, erschließen lässt. Generell bieten sowohl Rollen- als auch Beziehungspseudonyme stärkere Anonymität als Personenpseudonyme. Die Stärke der Anonymität steigt mit der Verwendung von Rollenbeziehungspseudonymen. Die stärkste Anonymität lässt sich mit Transaktionspseudonymen erreichen.

Weitere Möglichkeiten, um die Zuordnung zur Person nicht offenbar werden zu lassen und damit ihre Anonymität nicht zu schwächen, bestehen in der Verwendung kryptographischer Methoden wie *blinder digitaler Signaturen*, z.B. für übertragbare digitale Gutscheine, oder *Credentials*. Credentials sind 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 [7;16;3;5]. Mit Hilfe der gleichen Credentials unter verschiedenen Pseudonymen kann einer Verkettbarkeit entgegengewirkt werden.

Für Identitätsmanagement müssen die je nach Kontext geeigneten Pseudonyme verwendet werden.

2.2.3 Dritte Parteien

Dritte Parteien können Identitätsmanagement in vielerlei Hinsicht unterstützen, z.B. mit Treuhänderfunktionen für die Abwicklung von Geschäften im Internet [13].

Identitätstreuhänder verfügen über meist beweisgeeignete identifizierende Daten (z.B. Namen und Erreichbarkeit) eines bspw. am Werteaustausch Beteiligten und können diese offenlegen. Unter vorab definierten Umständen, z.B. Nichterfüllung einer Vertragsleistung, sollten sie dies tun. *Wertetreuhänder* nehmen alle auszutauschenden Werte der Beteiligten entgegen und stellen sie den Adressaten zu. Die Kenntnis der Identität der Beteiligten ist dazu nicht notwendig. Bei einer physischen Zustellung der Güter kann ein spezieller *Lieferdienst* beauftragt werden, der als einziger die Adressinformation besitzt, aber weder Absender noch Inhalt der Sendung kennen muss. Eine ähnliche Entkopplung ist mit einem *Bezahldienst* möglich. Ein *Haftungsservice* übernimmt, meist nachdem ein Beteiligter dort Geld für diesen Zweck hinterlegt hat, gegenüber anderen Beteiligten die Haftung in der vereinbarten Höhe des Betrags oder haftet bei anderen Vertragspflichten. Wiederum ist das Wissen über die Identität nicht erforderlich.

Hinzu kommen die Parteien für Public-Key-Infrastrukturen, die bspw. *Key-Server* oder *Zertifikats-Server* betreiben. Andere dritte Stellen, z.B. aus dem E-Government-Bereich, können das *Ausstellen von Credentials* übernehmen. Über einen *Datenschutz-Infoservice* lassen sich Informationen und Programme zu Identitätsmanagement verteilen. Dazu gehören Privacy-Tools, Konfigurationsempfehlungen oder Meldungen zu Sicherheitsrisiken. Wichtig sind Informationen über Verkettungsmöglichkeiten von personenbezogenen Daten in Zusammenhang mit öffentlichen Verzeichnissen, besonderen Geschäftsentwicklungen oder bestimmten Systemen.

2.2.4 Bausteine für Nutzerunterstützung

Identitätsmanagementsysteme unterstützen die Nutzer im Sinne der mehrseitigen Sicherheit in ihrem Selbstdatenschutz [8;12;11]. Zu den Methoden und Tools, die zu diesem Zweck eingesetzt werden können, gehören:

- Aushandlungskomponenten für Sicherheitsfunktionen eines Kommunikationsnetzes, das Sicherheitsfunktionen einschließlich Anonymität bereitstellt [6];
- explizite und regelbasierte Bestimmung über die Herausgabe von Personendaten und über Anforderungen an die Verwendung dieser Daten (z.B. auf der Grundlage von P3P – Platform for Privacy Preferences [2]) sowie Aushandlung darüber;
- Funktionen für Einwilligung, Widerspruch, Auskunft, Berichtigung oder Löschung der eigenen Daten beim Verarbeiter [10];
- nutzerseitige Unterstützung bei der Pseudonym- und Personendatenverwaltung durch Speichern und Darstellen von Kontext und Kontextwechseln, z.B. durch

Protokollieren der Daten und der Kontexte, in denen sie herausgegeben werden, z.B. Empfänger, Zeitpunkt, Aushandlungsergebnisse für Sicherheitsmechanismen und Zusagen für die Verwendung der Daten,

Führen eines um Kontextinformationen erweiterten Adressbuches der Kommunikationspartner,

Aggregieren von Kontextdaten, bspw. durch Einsatz von Data-Mining zur Darstellung des vermuteten Wissens der Kommunikationspartner über den Nutzer, ggf. unter Einbeziehung weiterer Daten, über die die Kommunikationspartner vermutlich verfügen und die vom Datenschutz-Infoservice bereitgestellt werden [12].

Als Warnfunktion können zusätzliche Filter vorgeschaltet werden, die den Datenstrom analysieren [11].

2.3 Beispiel: Datensparsamkeit im E-Commerce

Betrachtet man die aufeinander folgenden Phasen eines Online-Kaufs (siehe z.B. [9;6]), stellt sich die notwendige Verkettung der Informationen aus Kunden- und Anbietersicht unterschiedlich dar: Eine Produktrecherche kann bspw. anonym und unverbindlich ablaufen. Auch in der Aushandlungsphase müssen keine identifizierenden Informationen verlangt werden. Für den eigentlichen Werteaustausch müssen die Ergebnisse der Aushandlung verwendet werden, nicht aber Informationen über den Prozess der Aushandlung. Mit Quittungen über den erfolgreichen Werteaustausch, z.B. realisiert als Credentials, kann der Kunde Garantieleistungen wahrnehmen. Eine datensparsame Realisierung ermöglicht zwar dem Kunden selbst eine Verkettung seiner eigenen Aktionen, jedoch nicht dem Anbieter, weiteren Dienstleistern oder gar Beobachtern.

Im Internet werden heutzutage Cookies eingesetzt, um die Nutzeraktionen bei der Abwicklung verschiedener Phasen auch über die einzelnen Sitzungen hinaus zu verketten, wobei in vielen Fällen auch noch personenbezogene Daten an die Cookies gebunden werden. Diese Realisierung ist nicht datensparsam.[3] Besser wäre es, die Verkettung des Nutzerhandelns, die über verschiedene Phasen notwendig ist, durch *nutzerbestimmtes* (Wieder-)Verwenden seiner Pseudonyme, Binden von ausgestellten Credentials an verschiedene Pseudonyme oder durch vom Anbieter ausgegebene (anonyme) Zertifikate zu realisieren, und außerdem auf personenbezogene Daten, soweit möglich, zu verzichten. Insbesondere ist in vielen Fällen keine Verkettbarkeit durch den Anbieter nötig. Auch ohne sie kann noch eine Kundenbindung modelliert werden, bspw. wenn beim Einlösen eines anonymen Zertifikats dem Kunden ein weiteres anonymes Zertifikat gegeben wird, das dieser in der nächsten Transaktion benutzen kann [19].

Bisher fehlen verlässliche Mechanismen, um zu erkennen, welche Phasen in welchen Transaktionen die Wiederverwendung von Pseudonymen oder das Übertragen bestimmter Eigenschaften erfordern. Hinweise wie Wechsel von Uniform Resource Identifier (URI) oder z.B. das Etablieren einer verschlüsselten Verbindung für die Abfrage von Rechnungsdaten [11] reichen für ein umfassendes Identitätsmanagement nicht aus [13;9].

3 Gestaltung und Wechselwirkungen bei Identitätsmanagement

Generell spielen die beteiligten Parteien für das Realisieren von Schutzzielen und die Mechanismenwahl eine Rolle [14]. Im Folgenden werden unterschiedliche Gestaltungsarten in Abhängigkeit davon untersucht, welche Parteien an der Festlegung von Art, Umfang und Authentisierung der personenbezogenen Daten mitwirken.

3.1 Einbindung von Identitätsmanagement

Identitätsmanagementsysteme müssen ein Maximum an Kontrolle durch den Nutzer ermöglichen und sollten daher in seinem Bereich platziert werden [8;12]. Die Systeme enthalten in den Profilen, Regeln und gespeicherten Kontexten sensitive Daten, die den Nutzerbereich nicht oder zumindest nicht unkontrolliert verlassen sollten.

Das System muss vom Nutzer direkt bedienbar sein, aber auch Anwendungen im Nutzerbereich sollen die Funktionalität verwenden können, z.B. in Form eines Proxy [11]. Dem Identitätsmanagement muss eine

[3] Selbst die Verwendung temporärer Session-Cookies erstreckt sich in der Regel auf sämtliche Nutzerklicks bzgl. einer Domain in der jeweiligen Session, d.h. trennt nicht zwischen verschiedenen Phasen, in denen Verkettung (durch den Anbieter) nicht erforderlich ist.

konfigurierbare Sicherheits- und Datenschutzfunktionalität zugrunde liegen. Es soll Schnittstellen für eine Unterstützung des Identitätsmanagements außerhalb des Nutzerbereichs bieten.

3.1.1 Nutzerseitig

Auf Nutzerseite muss die Verwaltung der Teilidentitäten abgewickelt werden (s. Bild 1, ähnlich in [11]). Die dazu gehörenden Informationen wie z.B. Pseudonyme können in einer Profildatenbank gespeichert werden. Zur *Eigenauthentikation*, d.h. einer selbst vom Nutzer vorgenommenen Bestätigung, signiert der Nutzer die entsprechenden Daten digital [16]. Automatisch interpretierbare Regeldaten beschreiben, unter welchen Bedingungen Informationen herausgegeben werden. Die Kontextdatenbank dient zur Protokollierung, welche Daten der Nutzer für welchen Zweck wann an wen herausgegeben hat. Außerdem können ihre Informationen bei der Interpretation der Regeln einfließen, z.B. um über die Wiederverwendung eines Pseudonyms zu entscheiden. Die Kontextdatenbank enthält ebenfalls Informationen über Kommunikationspartner und kann bspw. mit einem Adressbuch verknüpft werden. Außerdem dient sie, ggf. erweitert um Zusatzinformationen, als Grundlage für das nutzerseitige Data-Mining.

Bei der Realisierung ist zu berücksichtigen, dass Aktualisierungen von Informationen bereits gespeicherte Daten nicht überschreiben, sondern dass neue Datensätze angelegt werden. An den Datensätzen sollten Zeitstempel für das Hinzufügen neuer Informationen sowie Gültigkeitsintervalle mitgeführt werden. So kann lückenlos ermittelt werden, wann welche Daten geändert wurden und gültig waren. Dies unterstützt eine strukturierte Kontextprotokollierung, die die Informationen über die Herausgabe von Daten unveränderlich archivieren kann, so dass sich daraus die Entwicklung möglichen Wissenszuwachses über die eigene Person bei anderen Parteien nachverfolgen lässt.

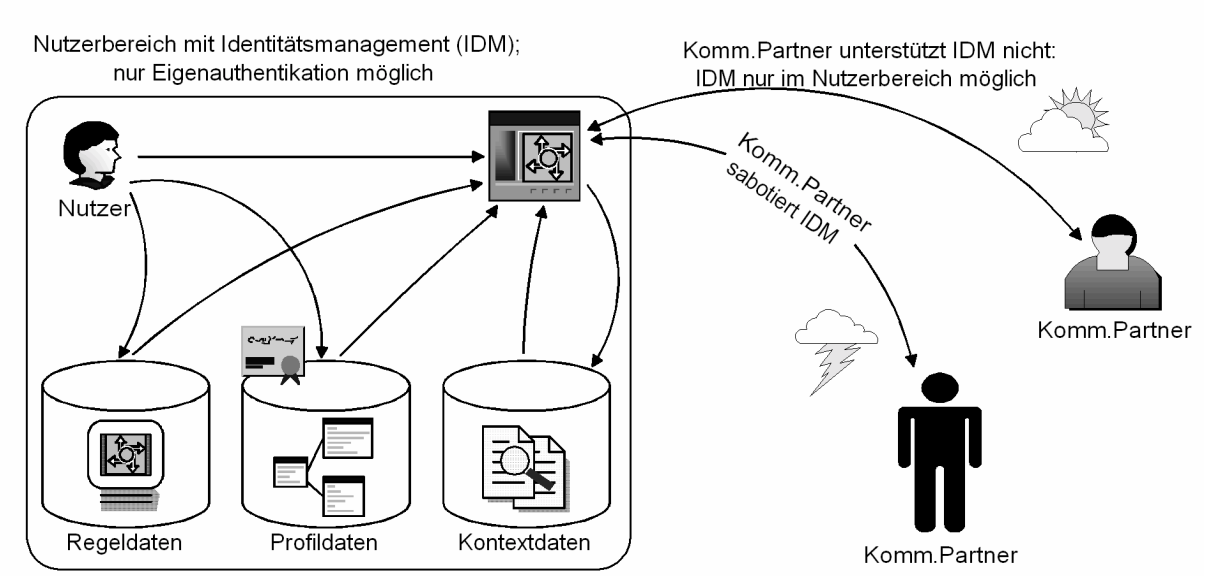

Bild 1: Nutzerseitiges Identitätsmanagement.

Wird das nutzerseitige Identitätsmanagement nicht durch die Kooperationspartner oder dritte Parteien unterstützt, fehlen wesentliche Funktionen. Insbesondere lässt sich mangels *Fremdauthentikation* (d.h. Bestätigungen durch andere Parteien) keine Verbindlichkeit[4] realisieren [16]. Weiterhin ist keine zuverlässige Interpretation der Kontextdaten für die Entscheidung der Pseudonymverwendung möglich. Bei Auswertung unsicherer Hinweise, z.B. URI oder Kontextinformationen wie dem Wechsel zu einer verschlüsselten Verbindung, können Kommunikationspartner das Identitätsmanagement insoweit sabotieren. Ein feingranulares und verlässliches Identitätsmanagement ist so nicht möglich. Schließlich fehlt bei einer rein nutzerseitigen Realisierung auch die Möglichkeit einer Aushandlung.

3.1.2 Kooperierende Kommunikationspartner

Fremdauthentikation für Nutzeraktionen ist durch kooperierende Kommunikationspartner möglich, z.B. mit digitalen Kundenkarten oder Gutscheinen des Anbieters. Weiterhin können sie strukturierte und verlässliche Informationen über die erforderlichen Pseudonyme und deren benötigte Eigenschaften sowie über

[4] Verbindlichkeit sichert, dass ein Nutzer belangt werden kann, um seine Zusagen innerhalb einer angemessenen Zeit zu erfüllen.

den Kontext geben (s. Bild 2). Zu diesen Informationen gehört insbesondere die Kennzeichnung von Anfang und Ende bei Transaktionen, in denen eine Verkettung nötig ist. Außerdem können Kommunikationspartner Aushandlungs- und Unterstützungsfunktionen für den Datenschutz der Nutzer bereitstellen.

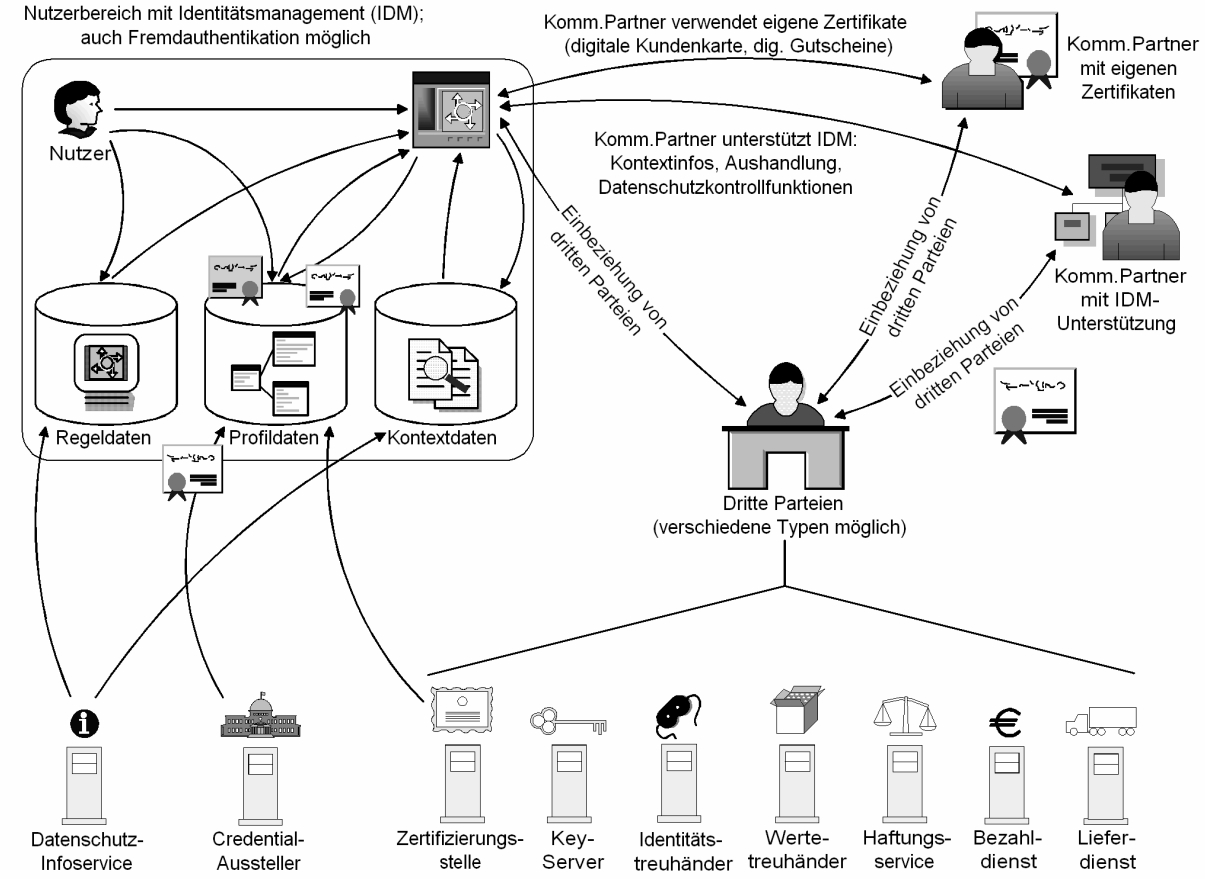

Bild 2: Identitätsmanagement mit kooperierenden Kommunikationspartnern und kooperierenden Dritten.

3.1.3 Kooperierende dritte Parteien

Dritte Parteien können zusätzliche Dienstleistungen erbringen (s. 2.2.3), z.B. für Verbindlichkeit sowie Garantie und Abwicklung von Lieferung oder Bezahlung. Durch Entkopplung verschiedener Datenflüsse können dritte Parteien zur Unverkettbarkeit beitragen (s. Bild 2). Von besonderer Bedeutung ist das Ausstellen von Credentials, die der Nutzer an unterschiedliche seiner Pseudonyme binden kann. Dadurch können Autorisierungen nachgewiesen werden, ohne dass jemand außer dem Nutzer selbst die verschiedenen Nachweise verketten kann. Mitglieder der Internet-Community können ebenfalls als Dritte agieren, z.B. um durch bereitgestellte Datenschutz-Tools oder –Informationen eine mangelnde Kooperation von Kommunikationspartnern auszugleichen.

3.1.4 Verteilte Realisierung

Ein Mehrwert einer verteilten Realisierung von Identitätsmanagement besteht darin, dass Wissen über Identitätsdaten oder Verkettung auf eine Vielzahl von Treuhändern aufgeteilt werden kann. Dadurch reduziert sich das Risiko eines Missbrauchs dieser Daten. Verteilte Kooperationsformen können auch die Verfügbarkeit unterstützen, um Wirkungen von Störungen zu kompensieren. Außerdem können Gruppenpseudonyme gemeinsam genutzt werden, um die Zugehörigkeit zu einer Gruppe zu kennzeichnen, dieselben Konfigurationen zu verwenden oder den Grad der Anonymität zu erhöhen.

3.2 Wechselwirkungen

Bei Identitätsmanagement steht der Selbstdatenschutz im Vordergrund. Er bleibt nicht auf Nutzerautonomie beschränkt, sondern muss ebenso wie die Online-Welt mehrseitig gedacht werden. Wie sich aus Abschnitt 3.1 ergibt, ist manche Funktionalität für Identitätsmanagement nur mit Unterstützung von

Kommunikationspartnern oder dritten Parteien möglich, die bestimmte Dienstleistungen erbringen. Eine solche Kooperation ist nicht unrealistisch, wenn man sich die Vorteile vor Augen hält, die ein sinnvoll gestaltetes Identitätsmanagement mit sich bringt: ein erhöhter Datenschutz der Kunden, bessere Datenqualität (wenn auch nicht personenbezogen) für Anbieter, neue Geschäftsmodelle für dritte Parteien. Für den Aufbau des gesamten Systems müssen die Anwendungen zu optimaler Datensparsamkeit umgestaltet werden, wie es Datenschutzgesetze bereits seit einigen Jahren fordern. Gerade in der Situation eines sich bisher nicht entfaltenden E-Commerce steckt hier für Firmen eine Chance, sich durch ein besonderes Datenschutzengagement zu profilieren.

Die PKI für digitale Signaturen, die gerade aufgebaut werden, lassen sich ebenfalls für Identitätsmanagement verwenden. *Ohne* Identitätsmanagementfunktionalität allerdings wäre die breite Einführung der digitalen Signatur mit einem hohen Risiko für den Datenschutz verbunden, da Nutzer dann zur Herausgabe ihrer authentischen Personendaten faktisch gezwungen werden könnten.

3.3 Schritte zu einer skalierbaren Entwicklung

Selbst wenn die Entwicklung umfassender Identitätsmanagementsysteme in Nutzerhand noch ein Jahrzehnt dauern dürfte, besteht bereits heute ein Bedarf. Die notwendigen Bausteine (s. Abschnitt 2) sind großenteils untersucht, die kryptographischen Mechanismen stehen zur Verfügung, Projekte zu datenschutzfördernden Techniken decken einzelne Komponenten ab. Um die Machbarkeit unter Beweis zu stellen, ist die Entwicklung von ausbaufähigen Prototypen wichtig. Zu diesem Zweck sind die Schnittstellen zwischen den einzelnen Komponenten zu spezifizieren. Mit Hinblick darauf, dass eine rein nutzerseitige Implementierung wenig Schutz und Effekt bringt, müssen von Anfang an mindestens beispielhaft die in wichtigen Anwendungen relevanten Parteien einbezogen werden.

Die Ausrichtung auf den Selbstdatenschutz und die Kooperation weiterer Parteien erlaubt die Verwendung der Systeme im internationalen Kontext. Allerdings fehlt in einigen Nationen die Möglichkeit, den Datenschutz praktikabel durch unabhängige Instanzen durchzusetzen. Identitätsmanagementfunktionalität sollte in die nationale und internationale Standardisierung eingebracht werden. Verwandte Standards, z.B. P3P für die Information über, Selektion von und künftig ggf. Aushandlung über Datenschutzfunktionen oder XML-Signature[5], sollten integriert und, wo sinnvoll, erweitert werden. Bei heutigen Konzepten sollte man bereits eine künftige Realisierung auch in mobilen Geräten wie PDAs und die damit verbundenen Standards einbeziehen. In jedem Fall ist sicherzustellen, dass weder technische Standards noch Rechtsnormen ein umfassendes, datenschutzförderndes Identitätsmanagement verhindern.

Die TU Dresden und das ULD SH arbeiten zusammen an einem umfassenden, datenschutzfördernden Identitätsmanagement. Dabei werden bisherige Komponenten zur mehrseitigen Sicherheit integriert [6;13]. Weiterer Projektpartner ist das IBM-Forschungslabor Zürich, das ein Credential-System [5] und Erfahrungen seines Pseudonym-Management-Projekts „idemix“[6] einbringt. Die Beteiligung des ULD SH garantiert einen unmittelbaren Austausch zwischen Juristen und Technikern, wie dies bei vielen Facetten zu Identitätsmanagement notwendig ist. Konzepte und das zu implementierende System sollen als Open-Source für eine Evaluation bereitgestellt werden, um den Grad der Vertrauenswürdigkeit zu erhöhen.

4 Grenzen und offene Fragen

Die Grenzen von Identitätsmanagementsystemen ähneln denjenigen von Firewalls, denn es geht um ein regelbasiertes Filtern der Kommunikation an einer zentralen Stelle in Abhängigkeit bestimmter Kontexte. Es kann nur die Kommunikation kontrolliert werden, die über diese zentrale Stelle abgewickelt wird. Werden erst nach Passieren des Identitätsmanagementsystems personenbezogene Daten in den Datenstrom gemengt, bleibt dies unentdeckt. In der Offline-Welt mit direkter Kommunikation, aber auch biometrischer Überwachungstechnik ist ein technikgestütztes Identitätsmanagement zurzeit nicht realistisch.

Für eine geeignete Interpretation ist Transparenz über die Datenflüsse und die Verarbeitung der eigenen personenbezogenen Daten bei den Kommunikationspartnern wichtig. Für herausgegebene Daten kann Zweckbindung mit einer feineren Granularität, als sie für eine Verkettung der Daten notwendig ist, rein technisch nicht garantiert werden. Daten, die ein Nutzer seinen Kommunikationspartnern offenbart hat und die dort gespeichert werden, sind seiner Kontrolle entzogen. Anonymitätssysteme können zwar für die Kommunikation sowohl Sender- als auch Empfängeranonymität garantieren, doch häufig möchte der

[5] http://www.w3.org/Signature/.

[6] http://www.zurich.ibm.com/csc/infosec/privacy/.

Nutzer persönliche Daten über sich mitteilen. Dies setzt der erreichbaren Datensparsamkeit jedes Identitätsmanagements Grenzen.

Ein universelles Identitätsmanagement lässt sich nicht in vollem Umfang realisieren. Strukturelle Grenzen liegen in der Unfähigkeit von Computern, dem Menschen vertraute Semantik vollständig korrekt zu interpretieren, aber auch darin, dass sich nicht alle Lebensbereiche über Technik erfassen und abwickeln lassen, sondern immer Lücken bleiben. Allerdings ist zu überlegen, wie ein Identitätsmanagement gestaltet sein muss, das sich in möglichst vielen Anwendungskontexten und darüber hinaus in verschiedenartigen Kulturen und Rechtsräumen einsetzen lässt.

Durch die Unvollkommenheit des Identitätsmanagements kann es dazu kommen, dass dem Nutzer eine Kontrollmöglichkeit über seine Daten lediglich vorgegaukelt wird. Beim Versuch zu bestimmen, was für Daten der Kommunikationspartner über einen gesammelt haben kann, besteht das Risiko des Über- oder Unterschätzens der Datenschutzrelevanz. Hier ist zu untersuchen, wie dem Nutzer dies zusammen mit dem Grad der Unsicherheit verdeutlicht werden kann. Außerdem ist abzuwägen, welche Anteile vom Identitätsmanagement implizit ablaufen können oder sollen und welche Funktionen dem Nutzer explizit und damit bewusst gemacht werden sollen bzw. müssen.

Leicht kann es zur Abhängigkeit vom Identitätsmanagementsystem kommen, das für einen die digitalen Identitäten verwaltet. Das System darf nicht manipulierbar sein, muss Vertraulichkeit und Integrität wahren und hat hohe Verfügbarkeitsanforderungen. Bislang ist unklar, ob solche vertrauenswürdigen Systeme gebaut werden können.

Doch selbst wenn durch Identitätsmanagement das Ziel der Datensparsamkeit erreicht wird und Daten für die Verarbeiter nicht personenbezogen vorliegen, können Probleme auftreten, die in den heutigen Datenschutzgesetzen nicht abgedeckt sind. Denn auch ohne eine Identifizierung können Menschen in ihren Persönlichkeitsrechten beeinträchtigt werden, z.B. durch Diskriminierung aufgrund bestimmter Eigenschaften oder durch Zustellen von auf die Person zugeschnittenen Nachrichten oder Werbung gemäß ihren erratenen Vorlieben oder psychologischen Profile.

5 Zusammenfassung und Ausblick

Mit Hilfe eines umfassenden Identitätsmanagementsystems kann Datenschutz in Nutzerhand weitgehend technisch realisiert werden. Es bezieht nicht nur die Nutzerseite, sondern auch kooperierende Kommunikationspartner und eine entsprechende Infrastruktur ein. Durch den hohen Aufwand und vielfältige Abhängigkeiten beim Einführen dieser Technik kann im ersten Anlauf kein perfektes System entstehen. Auf Erweiterbarkeit ausgerichtete Prototypen sollten einem Austausch zwischen Nutzern, Technikern, Juristen und Politikern dienen, um Erfahrungen für die Realisierung von Datenschutztechnik im gesellschaftlichen Kontext zu sammeln. Auch die Schwächen und Grenzen der jeweils verfügbaren Prototypen müssen offengelegt werden, damit Nutzer die Chance haben, den Grad an tatsächlich realisiertem Schutz abzuschätzen. Eine solche Offenheit ist zugleich Basis für ein berechtigtes Vertrauen in die Entwicklung der Systeme wie auch Grundlage für die Vermittlung der Kenntnisse, die dem Nutzer ein selbstbestimmtes Verwenden der Systeme ermöglichen.

Durch Wechselwirkungen mit anderen Techniken und Infrastrukturen kann und muss Identitätsmanagement im Zuge deren Entwicklung mitwachsen. Bei der Gestaltung sind auch diejenigen Datenschutzprobleme zu berücksichtigen, die erst durch seinen Einsatz hervorgerufen werden.

Literatur

[1] *Berthold, O.; Federrath, H.; Köpsell, S.:* Web MIXes: A System for Anonymous and Unobservable Internet Access. In: Federrath, H. (Hrsg.): Designing Privacy Enhancing Technologies. LNCS 2009. Berlin: Springer 2001, S. 115-129.

[2] *Berthold, O.; Köhntopp, M.:* Identity Management Based On P3P. In: Federrath, H. (Hrsg.): Designing Privacy Enhancing Technologies. LNCS 2009. Berlin: Springer 2001, S. 141-160.

[3] *Brands, S.:* Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy. Thesis, Brands Technologies, 1999.

[4] *Bürk, H.; Pfitzmann, A.:* Value transfer systems enabling security and unobservability. In: Security and Protection in Information Systems (IFIP/Sec. '86), North-Holland, 1989, S. 225-237.

[5] *Camenisch, J.; Lysyanskaya, A.:* Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation. Research Report RZ 3295 (#93341), IBM Research, November 2000.

[6] *Clauß, S.; Köhntopp, M.:* Identity Management and Its Support of Multilateral Security. Erscheint in: Computer Networks, North-Holland: Elsevier Herbst 2001.

[7] *Chaum, D.:* A New Paradigm for Individuals in the Information Age. In: Proc. of the 1984 Symposium on Security and Privacy, IEEE, Oakland 1984; S. 99-103.

[8] *Chaum, D.:* Security Without Identification: Transaction Systems to Make Big Brother Obsolete. In: CACM, Vol. 28 No. 10, Oktober 1985, S. 1030-1044.

[9] *Gerd tom Markotten, D; Jendricke, U.:* Identitätsmanagement im E-Commerce. In diesem Heft.

[10] *Grimm, R.; Löhndorf, N.; Roßnagel, A.:* E-Commerce meets E-Privacy. In: Bäumler, H. (Hrsg.): E-Privacy. Wiesbaden: Vieweg, 2000, S. 133-140.

[11] *Jendricke, U.; Gerd tom Markotten, D.:* Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet. In: Proceedings of the 16th Annual Computer Security Applications Conference; New Orleans, USA; Dezember 11-15, 2000.

[12] *Köhntopp, M.:* Identitätsmanagement – ein neues, altes Konzept. In: Datenschutz Nachrichten 3/2000; S. 7-12; s.a. http://www.koehntopp.de/marit/pub/idmanage/.

[13] *Köhntopp, M.:* „Wie war noch gleich Ihr Name?“ – Schritte zu einem umfassenden Identitätsmanagement. In: Fox, D.; Köhntopp, M.; Pfitzmann, A. (Hrsg.): Verlässliche IT-Systeme 2001 – Sicherheit in komplexen IT-Infrastrukturen. Wiesbaden: Vieweg, 2001, S. 55-75.

[14] *Pfitzmann, A.:* Multilateral Security: Enabling Technologies and Their Evaluation. In: Wilhelm, R. (Hrsg.): Informatics – 10 Years Back, 10 Years Ahead. LNCS 2000. Berlin: Springer, 2001, S. 50-62.

[15] *Pfitzmann, A.; Köhntopp, M.:* Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology. In: Federrath, H. (Hrsg.): Designing Privacy Enhancing Technologies. LNCS 2009. Berlin: Springer, 2001, S. 1-9; s.a. http://www.koehntopp.de/marit/pub/anon/.

[16] *Pfitzmann, B.; Waidner, M.; Pfitzmann, A.:* Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. In: DuD 14 (1990), H. 5-6, S. 243-253, 305-315.

[17] *van Rossum, H.; Gardeniers, H.; Borking, J.; u.a.:* Privacy-Enhancing Technologies: The Path to Anonymity. Achtergrondstudies en Verkenningen 5a/5b, Registratiekamer, Niederlande & Information and Privacy Commissioner/Ontario, Canada, Aug. 1995, http://www.ipc.on.ca/english/pubpres/sum_pap/papers/anon-e.htm.

[18] *Schneider, M.; Pordesch, U.:* Identitätsmanagement. In: DuD 22 (1998), H. 11, S. 645-649.

[19] *Syverson, P.F.; Stubblebine, S.G.; Goldschlag, D.M.:* Unlinkable Serial Transactions. In: Hirschfeld, R. (Hrsg.): Financial Cryptography 1997, Proceedings. LNCS 1318. Berlin: Springer, 1998, S. 39-55.

Dipl.-Inform. Marit Köhntopp studierte Informatik an der Universität Kiel. Seit 1995 arbeitet sie beim Landesbeauftragten für den Datenschutz Schleswig-Holstein im Bereich PET. Dort leitet sie verschiedene Projekte zu datenschutzgerechten und datenschutzfördernden IT-Systemen.

Adresse: Unabhängiges Landeszentrum für Datenschutz (ULD SH), Holstenstr. 98, D-24103 Kiel, Tel.: +49 431 988-1214, Fax: -1223, E-Mail: marit@koehntopp.de

Prof. Dr. Andreas Pfitzmann studierte Informatik und promovierte 1989 über „Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz“ an der Universität Karlsruhe. Seit 1993 ist er Professor an der Fakultät Informatik der TU Dresden. Er forscht über mehrseitige Sicherheit durch verteilte Systeme und lehrt über Sicherheit in verteilten Systemen.

Adresse: TU Dresden, Fakultät Informatik, D-01062 Dresden, Tel.: +49 351 463-8277, Fax: -8255, E-Mail: pfitza@inf.tu-dresden.de