Digitale Identitäten – Überblick und aktuelle Trends

Identity-Lifecycle, Authentisierung und Identitätsmanagement

Marit Hansen, Martin Meints

In der Informationsgesellschaft ist das Thema Identität von wesentlicher Bedeutung: Dieser Artikel beschreibt relevante Trends im Lebenszyklus von digitalen Identitäten und greift exemplarisch die beiden Bereiche Authentisierung und Identitätsmanagement heraus, in denen aktuelle Entwicklungen zu berichten sind.

Marit Hansen

Leiterin des Referats „Privacy-Enhancing Technologies“ des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein; Arbeitsschwerpunkt: Identitätsmanagement.
E-Mail: LD10@datenschutzzentrum.de

Dr. Martin Meints

Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein im Projekt FIDIS.

E-Mail: LD102@datenschutzzentrum.de

1 Digitale Identität – das Spektrum

Digitale Identitäten sind Sammlungen von digitalen Informationen, die zu einem Individuum oder einer Organisation gehören. Hier beschränken wir unsere Sicht auf natürliche Personen, um deren Identitäten es geht. Grundsätzlich ist auch eine Erweiterung um die Organisationssicht denkbar.

Jede digitale Identität ist in der Regel charakterisiert durch eine Menge von Attributen (z.B. Eigenschaften einer Person) und weist häufig mindestens eine Kennung („Identifier“) auf. Digitale Identitäten sind digitale Repräsentierungen von Teilidentitäten, d.h. Teilen der gesamten Identität eines Person [HaKrRo+03, PfHa06]. Zwar bezieht sich jede digitale Identität gemäß ihrer Definition stets auf eine Person, jedoch ist dieser Personenbezug nicht unbedingt für einen Beobachter herstellbar, so dass es sich nicht zwangsläufig um personenbezogene Daten handelt. Wird als Kennung nicht der Echtname verwendet, kann man diese als *Pseudonym* auffassen.

Das Konzept der digitalen Identität umfasst ein breites Spektrum an möglichen Eigenschaften:

- *Größe/Datenmenge:* Es kann sich um eine einzelne, alphanumerische Kennung handeln, aber auch um ein riesiges Dossier zu einer Person.
- *Speicherort(e)/Kontrollbereich(e):* Nicht immer sind die Daten, die zu einer digitalen Identität gehören, beim Inhaber gespeichert, sondern sind möglicherweise verteilt auf verschiedene Organisationen, Örtlichkeiten und/oder Datenbanken. Ähnlich verhält es sich mit dem Ort der Verarbeitung, der stark variieren kann.
- *Integrität und Authentizität:* Bei der digitalen Identität kann es sich handeln um einerseits authentische, aktuelle, bewiesen korrekte Informationen oder andererseits unsichere Gerüchte (wie versehentliche *Missinformation* oder vorsätzliche *Desinformation*) oder Informationen mit lediglich einer gewissen Wahrscheinlichkeit an Korrektheit (wie Scoring-Daten [HiBa05, Hi06, We06] oder genetisch-basierte Prognosen);
- *Bewusstsein über die digitale Identität, die andere wahrnehmen:* Bei explizit kommunizierten Informationen ist sich der Betroffene grundsätzlich bewusst, welche Daten dabei dem Gegenüber offenbart werden. Anders verhält es sich mit impliziten Informationen, die (oft von Dritten) beobachtet oder geschlossen wurden (z.B. aus technisch bedingten Datenspuren oder aus dem Kommunikationsverhalten).
- *Verwendungszweck der digitalen Identität:* Identifier dienen der im Bezugsraum eindeutigen Adressierung der damit verbundenen digitalen Identität. Dabei kann es sich um eine Adressierung auf Datensatzebene handeln (z.B. als Indexwert in einer Datenbank zum schnelleren Zugriff auf die Daten) oder in Verbindung mit einem geeigneten technischen System um eine Funktion zur Erreichbarkeit einer Person (z.B. die Telefonnummer oder E-Mail-Adresse). Die darauf aufbauenden Applikationen, die dann über die Kennung hinaus Informationen verarbeiten, können dann diverse Zwecke haben.

Auch bei *objektbezogenen* Informationen kann es sich um personenbezogene Daten handeln, die dann ebenfalls zu Teilen von digitalen Identitäten der entsprechenden Person werden: z.B. die IP-Adresse des Nutzercomputers, SIM-Karten-Kennungen in der Mobiltelefonie, steganographisch eingebettete Seriennummern in Digital-

Rights-geschützten Daten oder RFID-Tags an gekauften Waren.

2 Lebenszyklus von digitalen Identitäten

Der Lebenszyklus („Lifecycle“) digitaler Identitäten umfasst die folgenden Phasen, die anschließend näher beschrieben werden:

- „Geburt“: Erschaffen einer digitalen Identität (bzw. Zuweisung an eine Person);
- „Leben“: Verwenden der digitalen Identität aus Sicht des Inhabers („Nutzersicht“) oder eines Dritten („Verarbeiter- bzw. Beobachtersicht“);
- „Tod“: Löschen oder Stilllegen einer digitalen Identität.

In einigen Fällen kann es möglich sein, Identitäten „wiederzubeleben“, also nach dem Stilllegen ein weiteres Mal in Verwendung zu bringen.

2.1 „Geburt“: Erschaffen von digitalen Identitäten

Je nach Anwendungskontext ist das Erschaffen von digitalen Identitäten auf verschiedene Weise möglich: Üblicherweise gibt die Anwendung vor, welche Freiheitsgrade für digitale Identitäten zur Verfügung stehen, z.B. Festlegung eines noch nicht vergebenen Login-Namens für einen eBay-Account oder Generierung eines Schlüsselpaares für asymmetrische Verschlüsselung wie z.B. bei PGP – Pretty Good Privacy.

Nicht immer ist der „Schöpfer“ der digitalen Identität auch ihr Inhaber selbst, z.B.:

- die Steuerverwaltung, die pro Person eine Steuernummer festlegt, die u.a. in einer internen Datenbank entsprechend gespeichert ist,
- der Access Provider, der dem Nutzer(rechner) eine IP-Adresse zuweist,
- der Hersteller von Netzwerkkarten, der pro Karte eine unterschiedliche MAC-Adresse im Chipsatz vorgibt, die wiederum Kennungen für einen Rechner im Netz und damit in der Regel auch einen (oder wenige) Nutzer darstellen,
- die Website, die einen Cookie mit einem entsprechenden Identifier setzt,
- der Software-Hersteller, der eindeutige Kennungen einbaut, z.B. bei Microsoft Windows sowohl im Betriebssystem als auch in Anwendungssoftware und ggf. sogar in damit erzeugten Dokumenten,
- die Signatur-Zertifizierungsstelle, die ein Zertifikat für ein generiertes Schlüsselpaar ausstellt, das einem Nutzer zugeordnet wird.

Übrigens verfügt der Schöpfer der digitalen Identität nicht immer über das Wissen, welche Person damit verbunden ist; in diesem Fällen kann er auch nicht als Identitätstreuhänder verwendete Kennungen in den Echtnamen auflösen.

Kennungen müssen eindeutig in ihrem Geltungsbereich sein; Globally Unique Identifiers (GUIDs) sind sogar weltweit eindeutig. Wie schon in der Beispielliste dargestellt, können solche Identifier auf Software-Ebene (wie in MS Office), Hardware-Ebene (Chipkennungen) oder Dienst-Ebene (Cookies) vergeben werden.

Es gibt Kennungen, die einen untrennbaren Bezug zu einer Person aufweisen, z.B. die DNA der Person, ihre Fingerabdrücke oder andere biometrische Eigenschaften. Deren digitale Repräsentationen gehören ebenfalls zu der Menge der digitalen Identitäten einer Person. Solche digitale Identitäten werden beispielsweise in Ausweisdokumenten, in Referenzsystemen für eine Einlasskontrolle oder in polizeilichen Datenbanken gespeichert.

Einige digitale Identitäten dienen primär der Authentisierung (siehe Abschnitt 3) oder enthalten Autorisierungen, z.B. digitale Credentials [CaLy01].

> Insgesamt ist eine Zunahme von digitalen Identitäten in allen Lebensbereichen der Informationsgesellschaft zu beobachten. Ebenso wird durch den wachsenden Einsatz von kontextübergreifenden Kennungen das Verketten von Daten aus völlig unterschiedlichen Zusammenhängen möglich, was zu aussagekräftigen Profilen führen kann. Allerdings fehlt den meisten Menschen das Bewusstsein darüber, wie ihre digitalen Identitäten aussehen und wie andere sie nutzen.

2.2 „Leben“: Verwenden von digitalen Identitäten

In Bezug auf existierende digitale Identitäten können verschiedene Subprozesse im Lebenszyklus identifiziert werden, die sich vor allem im Akteur der Verwendung unterscheiden:

- Verwendet der Inhaber seine digitale Identität *selbst* (siehe Abschnitt 2.2.1)?
- Oder sind es *andere* Parteien, die seine (oft unmittelbar personenbezogenen) Daten nutzen (siehe Abschnitt 2.2.2), z.B. indem sie Datensätze verarbeiten, die aus beobachteten oder beim Betroffenen oder Dritten erhobenen Informationen stammen, oder auch damit handeln oder indem sie die digitale Identität übernehmen und vorgeben, es handle sich um die eigene (Identitätsdiebstahl und ähnliche Effekte, siehe [KoLe06])?

2.2.1 Verwenden der eigenen digitalen Identität

Das Verwenden einer eigenen digitalen Identität kann sehr unterschiedlich aussehen und hängt ab von der Applikation und ihrem Zweck. Generell bedeutet jede Verwendung eine Weiterentwicklung der digitalen Identität, bei der sich Attribute und ihre Werte ändern können (z.B. bei der Bekanntgabe einer Adressänderung), welche hinzukommen, andere gelöscht werden oder auch Links zu weiteren digitalen Identitäten gesetzt werden. Allerdings muss man damit rechnen, dass frühere Versionen der digitalen Identität bei Kommunikationspartnern und Dritten weiterhin existieren, ggf. ergänzt um neue Versionen zum Update.

Dies müssen auch die nutzerkontrollierten Identitätsmanagementsysteme berücksichtigen (siehe Abschnitt 4), um den Nutzern einen Überblick zu liefern, wem diese welche Informationen gegeben haben.

Ein weiteres Beispiel für das Einbeziehen früheren Verhaltens sind Reputationssysteme, z.B. von eBay, wo Bewertungen von Transaktionspartnern gespeichert und numerisch ausgedrückt werden und damit einen Hinweis geben sollen, inwieweit sich ein eBay-Nutzer mutmaßlich gemäß den gegebenen Regeln verhalten wird.

2.2.2 Verwenden fremder digitaler Identitäten

Greifen Personen oder Organisationen auf digitale Identitäten zu, die nicht ihre eigenen sind, kann man zwischen dem passiven Beobachten und dem aktiven Nutzen unterscheiden.

Für einen Beobachter steht immer mehr Technik zur Verfügung, die die interessierenden Informationen zusammensammeln und aggregieren können, denn partielle Identitäten, die einzeln keine Bedrohung für den Datenschutz des Einzelnen darstellen, können verkettet und angereichert mit anderen Informationen eine erhebliche Aussagekraft haben:

- Sensortechnik kann verwendet werden, um biometrische Eigenschaften zu analysieren (z.B. für Verifikation in einem Authentisierungsprozess oder für Identifikation von Personen), oder RFID-Tags auszulesen (z.B. für Tracking-Zwecke).
- Profiling-Techniken [HiBa05, Hi06] ermöglichen die Sammlung und Analyse (z.B. durch Data Mining-Methoden oder durch Scoring) von Daten u.a. zum Zwecke der Personalisierung von Diensten, um die Kreditwürdigkeit von Personen einzuschätzen oder um illegale Aktionen zu verhindern (z.B. bei Intrusion Detection-Systemen). Verwandt sind die bereits genannten Reputationssysteme.
- Außerdem existieren automatisierte globale Überwachungssysteme zum Abhören von Kommunikationsdaten wie z.B. Echelon [Sc01]. Daneben sind kürzlich Pläne und Methoden der NSA bekannt geworden, soziale Netzwerke ausfindig zu machen und zu analysieren [AlNaRa+06].

Das Nutzen fremder digitaler Identitäten geschieht zu vielen verschiedenen Zwecken beispielsweise in Unternehmensdatenbanken wie beim Customer Relationship Management.

> Der Handel von Kundenadressen und darüber hinausgehenden Informationen (z.B. Kreditwürdigkeit) ist lukrativ: Nach [Ra06] werden jedes Jahr in Deutschland Milliarden Euro mit dem Handel privater und geschäftlicher Daten verdient. Die Daten stammen von Unternehmen und öffentlichen Stellen.

Der Adresshändler Schober[1] wirbt mit:

- „50 Mio. Privatadressen aus D und 10 Milliarden Zusatzinformationen – für jeden Anlass die richtige Zielgruppe“
- „5 Millionen Konsumenten mit konkreten Interessen und Kaufabsichten – attraktive Zielgruppen, wie z.B. Neuwagen-/Urlaubs-Interessierte, Hausbesitzer und viele mehr“
- „Alle 19 Millionen Gebäude Haus für Haus persönlich vor Ort bewertet. Kartografie, Regionaldaten, infas GEOdaten und vieles mehr“
- „Über 7 Millionen private E-Mail-Adressen mit Einwilligung für E-Mail-Werbung“

Tatsächlich gehören E-Mail-Adressen zu den Daten, bei denen der Missbrauch den Empfängern am deutlichsten präsent ist: durch unerwünschte Kommunikation (SPAM), bei der eben keine Einwilligung durch den Empfänger vorhanden ist. Aber auch unerwünschte Telefonanrufe oder SMS-Nachrichten machen sich die Erreichbarkeit über die Kennung Telefonnummer zu Nutze.

[1] Siehe http://www.schober.de/.

2.3 „Tod“: Stilllegen von digitalen Identitäten

Insbesondere wenn digitale Identitäten für Authentisierungszwecke in einer Organisation verwendet werden können, müssen die Accounts der Nutzer gelöscht (oder zumindest deaktiviert) werden, sobald sie nicht mehr der Organisation angehören [CaThCh+05]. Oft dürfen die digitalen Identitäten nicht vollständig gelöscht werden, weil es wichtig ist, Aktionen einzelnen Mitarbeitern auch nach ihrem Fortgang weiterhin zurechnen zu können, z.B. beim Führen eines Grundbuchs gilt dies für viele Jahre. Oder aber sie können nicht gelöscht werden, weil nicht klar ist, wo und bei wem Kopien von digitalen Identitäten oder Teilen davon gespeichert sind. In einigen Fällen ist zudem fraglich, ob die Besitzer der Daten diese wirklich umgehend rückstandsfrei löschen würden (z.B. beim Google-Cache oder bei Archiv-Diensten im Internet).

Da das Löschen so schwierig ist, kommt dem Datenminimierungsprinzip eine große Bedeutung zu, wonach die personenbezogenen Daten auf das minimal Erforderliche zu beschränken sind. Dies bedeutet vor allem, Verkettbarkeiten zu vermeiden, wo immer möglich:

- zur Person, um direkte Identifizierbarkeit zu verhindern, oder
- zu anderen Nutzungen derselben digitalen Identität, um das Erstellen von Profilen und aufgrund dessen wiederum eine Identifizierbarkeit zu unterbinden.

Zu diesem Zweck können Anonymisierungstools zu Einsatz kommen, die identifizierbare digitale Identitäten durch andere Kennungen ersetzen. So gibt es gibt Anonymisierungs-Tools, die auf IP-Ebene arbeiten (durch Proxies oder Mixe zusammen mit Dummy-Traffic), die bei Cookies ansetzen (Tools für Cookie-Management oder Cookie-Austausch), die für Formular greifen (Tools für das Ausfüllen von Formularen mit nicht-identifizierbaren Informationen) oder die durch das Anbieten von Einmal-E-Mail-Adressen das SPAM-Risiko minimieren.

> Zwar sind die Anonymisierungstools vielfältiger und bedienbarer geworden, doch ist ein Schutz gegen die Betreiber und Mitlauscher auf dem Weg durch das Internet die Ausnahme. Hinzu kommt, dass durch die Vorratsdaten-Gesetzgebung (Data Retention) die Betreiber zum Vorhalten von bestimmten Daten über einen längeren Zeitraum verpflichtet werden – was ein Missbrauchsrisiko nach sich zieht.

Für das Löschen von Accounts innerhalb von Organisationen sind dagegen einige Fortschritte erkennbar: Besonderes Augenmerk verdient die Entwicklung von Privacy Management Languages, die durch automatisiertes Datenschutzmanagement den Datenverarbeitungs-Workflow innerhalb von Organisationen unter Berücksichtigung der gesetzlichen Regelungen unterstützen können.

3 Authentisierung

Authentisierung ist ein wichtiger Bestandteil in vielen identitätsbezogenen Prozessen und wird daher gesondert betrachtet.

3.1 Einführung

Das Ziel der Authentisierung [KeMi03] ist unter anderem die Bindung eines digitalen Identifiers an eine physische Person oder ein physisches System (z.B. einen bestimmten Computer). Man unterscheidet die Authentisierung von der Autorisierung, die die Zuweisung der Rechte eines Benutzers in einem IT-System bezeichnet. Im Bereich der Authentisierung gibt es neben der Mensch-Maschine-Authentisierung noch die Maschine-Maschine-Authentisierung. Diese wird in diesem Artikel nicht weiter betrachtet.

In Abhängigkeit vom Umfang der Rechte eines Nutzers in einem IT-System kann die Authentisierung unterschiedlich stark, d.h. unterschiedlich zuverlässig, erfolgen. Unter anderem wird die Stärke der Authentisierung von den folgenden Aspekten beeinflusst:

- Art und Anzahl der Faktoren, die zur Authentisierung verwendet werden;
- Ein-/Mehrseitigkeit der Authentisierung;
- Art und Zahl der genutzten Kommunikationswege.

Als Faktoren bei der Authentisierung werden herangezogen [Pfi05, RoRa06]:

- Etwas, das man hat (Besitz), beispielsweise eine Chipkarte oder auch klassisch ein Türschlüssel;

- Etwas, das man weiß (Wissen), beispielsweise ein zuvor vereinbartes, vertrauliches Passwort oder eine PIN (üblicherweise vierstellige Persönliche Identifikations-Nummer);
- Etwas, das man ist (biometrische Merkmale), beispielsweise ein Fingerabdruck (physiologisches Merkmal) oder der Gang (verhaltensbezogenes Merkmal);
- Historisch, aber auch aktuell im Kontext von ortsgebundenen Diensten (z.B. Location Based Services): der Aufenthaltsort zu einer bestimmten Zeit.

Während sich ein Nutzer gegenüber einem IT-System in der Regel explizit und aktiv authentisieren muss, authentisiert sich ein System gegenüber dem Nutzer häufig nur durch seinen physischen (z.B. ein Geldautomat) oder virtuellen Ort (z.B. ein Internetserver über seine Internetadresse) und sein äußeres Erscheinungsbild. In diesem Falle spricht man von *einseitiger Authentisierung*. Von *beidseitiger Authentisierung* spricht man in dem Fall, in dem sich ein System auch aktiv gegenüber seinem Nutzer etwa durch Mitteilung eines zuvor vereinbarten, vertraulichen Kennwortes authentisiert.

Typischerweise tauschen Nutzer und System Authentisierungsinformationen über einen Kommunikationsweg, etwa ein lokales Netzwerk oder das Internet, aus. Ergänzend können aber auch weitere Kommunikationswege, etwa mobile Netze und dort registrierte und eingebuchte Geräte verwendet werde. Ein Beispiel hierfür ist der Einsatz mobiler Transaktionsnummern (mTAN) bei der Authentisierung von Geldtransaktionen. Der für die Authentisierung des berechtigten Kontonutzers benötigte TAN für die Online-Überweisung wird bei diesem Verfahren von der Bank dynamisch berechnet und an ein zuvor registriertes Mobiltelefon des Nutzers per SMS (2. Kommunikationsweg) gesendet.

Für die Stärke von Authentisierung gibt es bislang kein absolutes Maß. Neben den hier bereits genannten Aspekten spielt vor allem auch eine Rolle, wie robust die Authentisierung gegenüber automatisierten Angriffen von außen, z.B. die Erlangung unberechtigten Zugriffs auf ein IT-System unter Einsatz von Kennwortbibliotheken oder durch systematisches ausprobieren, ist. Eine wesentliche Rolle spielt in diesem Zusammenhang die Komplexität (auch Entropie genannt) der Informationen, die zur Authentisierung verwendet werden. So weist z.B. ein 8-stelliges, nichttriviales Kennwort eine deutlich höhere Komplexität auf, als etwa eine PIN.

Weitere Aspekte, die in diesem Umfeld betrachtet werden müssen, sind u.a. die Robustheit gegen den Einsatz von Kopien (z.B. geklonte Chipkarten, Spoofs für biometrische Sensoren), gegen Innentäter, gegenüber dem sog. Social Engineering, aber auch gegen technisches Versagen [Le06].

Typ	Visualisierung	Art des Identitäts-managements	Durch wen?	Welche Methoden?
Typ 1		**Account Management:** *zugewiesene Identität*	durch Organisation	Verzeichnisdienste
Typ 2		**Profiling:** *abgeleitete Identität*	durch Organisation	Data Mining-Tools
Typ 3		**Management eigener Identitäten:** *gewählte Identität*	durch den Nutzer selbst, unterstützt durch z.B. Serviceprovider	Zahlreiche, derzeit wenig integrierte Tools wie Anonymitätsdienste oder Passwort-Manager

Abb. 1: Übersicht über Typen von IMS

3.2 Trends

Bei der Authentisierung sind im Wesentlichen zwei Trends zu erkennen:

- Verwendung von bereits bestehenden Authentisierungen, die von der Stärke her in keinem ausgewogenen Verhältnis zu den daran gebundenen Rechten stehen. Ein Beispiel ist die Verwendung einer bereits bestehenden Authentisierung für immer mehr Rollen in verschiedenen IT-Systemen (Single Sign-On) ohne Anpassung der Stärke. Ein anderes Beispiel ist die Verwendung von Kreditkarteninformationen, um das Alter eines Besuchers einer Internetseite zu prüfen.
- Verstärkung der Authentisierung meist als unmittelbare Reaktion auf Identitätsdiebstahl; ein Beispiel hierfür ist die Einführung eines mTANs durch einige Kreditinstitute als Reaktion auf Phishing- und Pharming-Angriffe.

4 Identitätsmanagementsysteme (IMS)

Identitätsmanagementsysteme können den gesamten Lebenszyklus von digitalen Identitäten abdecken. In den letzten Jahren haben Forschung und Entwicklung in diesem Bereich den Nutzer verstärkt in den Mittelpunkt gerückt.

4.1 Einführung

Identitätsmanagementsysteme (IMS) lassen sich unter den Gesichtspunkten des Durchführenden des Managements, der Ziele des Managements und der hierfür eingesetzten Methoden in drei grundsätzliche Typen gliedern [BaMeHa05, Me06]. Abb. 1 fasst diese Typen zusammen.

Neben den hier vorgestellten Typen gibt es eine Reihe von Implementierungen, die Merkmale mehrerer dieser Grundtypen tragen (hybride Systeme), z.B.:

- Für die Typen 1 und 2: Identitätsmanagementsysteme mit integriertem Customer Relationship Management (CRM)
- Für die Typen 2 und 3: Management von Cookies durch den Nutzer
- Für die Typen 1 und 3: Credentialsysteme und elektronische Signaturen

Auf Typ 2-IMS wird in diesem Artikel nicht weiter eingegangen, da sie ausführlich im [Hi06] behandelt werden. Typ 1-IMS sind am Markt durchaus etabliert und weisen ein breites Spektrum an unterschiedlichen Produkten auf. Typ 3-IMS befinden sich noch in der Markteintrittsphase. Belege für diese Einstufung sind:

- Geringe Integration bislang existierender (Teil-)Lösungen; überwiegend finden sich am Markt spezialisierte Tools und Anwendungen, die nur wenige Funktionen und diese meist nur für bestimmte Dienste wahrnehmen;
- Hohes Engagement staatlich finanzierter Forschungseinrichtungen;

- Geringes Engagement kommerzieller Anbieter; viele Projekte sind Freeware und Open Source.

4.2 Trends

Bei Typ 1-IMS beobachten wir vor allem die folgenden Trends:

- Zunehmende Integration von Verzeichnisdiensten unter Einsatz von Meta-Directories oder Federation; dies korreliert auch mit Marktprognosen etwa der Gartner Group oder der Yankee Group[2], die bis 2008 noch ein erhebliches Wachstum des Marktes für Typ 1-IMS in den USA vorhersagen;
- Funktionale Erweiterung z.B. um Provisioning unter Anbindung von Human Resource Management Systemen oder Einbindung von CRM-Systemen;
- Differenzierung der Stärke der benötigten Authentisierung zur Berücksichtigung verschiedener Sicherheitsanforderungen angebundener IT-Systeme;
- Zunehmender Bedarf für standardisierte Schnittstellen für Typ 3-IMS (z.B. InfoCard von Microsoft) besonders dann, wenn partielle Identitäten von Klienten (Kunden, Bürgern) verwaltet werden.

Bezogen auf Typ 3-IMS sind noch grundlegende Aufgaben zu erfüllen, insbesondere:

- Technische Standardisierung;
- Integration bestehender Lösungen;
- Entwicklung geeigneter Benutzungsschnittstellen.

All diese Aspekten spielen eine Rolle in dem von der EU geförderte Projekt „PRIME – Privacy and Identity Management for Europe“[3], das die Entwicklung von IMS unter Nutzerkontrolle zum Ziel hat. Ein Kernbestandteil dieses Projekts sind private Credentials [CaLy01], mit deren Hilfe sich Autorisierungen an verschiedene Pseudonyme binden lassen. Damit ist eine autorisierte Nutzung möglich, ohne dass der Nutzer seine Identität aufdecken muss – sofern er sich regelkonform verhält.

Mittlerweile zeichnet sich ein Trend ab von zentralisierten IMS (die noch eine erhebliche Rolle spielen) hin zu verteilten, nutzerkontrollierten IMS mit datenschutzbezogenen Konfigurationsmöglichkeiten:

- Kim Cameron von Microsoft vertritt mit seinen „Laws of Identity“ [Ca05] Prinzipien für Transparenz und Datenschutz, was auch in die Gestaltung von InfoCard in der nächsten Microsoft Betriebssystemversion einfließen soll.
- Der Firmenzusammenschluss Liberty Alliance[4] verfolgt die verteilte Realisierung von IMS, wobei der Nutzer verschiedene Kontexte durch unterschiedliche „Circles of Trust“ trennen kann.
- Nach vereinzelten Entwicklungen im Open Source-Bereich[5] gibt es mittlerweile mit dem „Higgins Trust Framework“-Projekt[6] eine mächtige Initiative für nutzerkontrollierte IMS, der auch große Firmen beigetreten sind.

Damit wächst auch das Interesse von Standardisierungsinitiativen wie von ISO oder W3C, in denen sich gerade Arbeitsgruppen zum Thema „Privacy & IMS“ bilden.

Fazit

Unter Experten gibt es Fortschritte beim Verstehen digitaler Identitäten, nicht jedoch in der Gesellschaft. Angesichts immer komplexerer Systeme muss dem Risiko des „digital identity divide“ begegnet werden, z.B. durch geeignetes Design von nutzerkontrollierten IMS und durch Wissensvermittlung zu Identität und Datenschutz bereits in der Schule.

Literatur

AlNaRa+06 Aleman-Meza, B., Nagarajan, M., Ramakrishnan, C., Ding, L., Kolari, P., Sheth, A.P., Arpinar, I.B., Joshi, A., Finin, T., ‘Semantic Analytics on Social Networks: Experiences in Addressing the Problem of Conflict of Interest Detection’, *WWW 2006*, 15th International World Wide Web Conference, 2006.

BaMeHa05 Bauer, M., Meints, M., Hansen, M. (Hrsg.), *FIDIS Deliverable D3.1 – Structured Overview on Prototypes and Concepts of Identity Management Systems*, Frankfurt a.M. 2005. Download: http://www.fidis.net/486.0.html.

CaLy01 Camenisch, J., Lysyanskaya, A., ‘Efficient non-transferable anonymous multishow credential system with optional anonymity revocation’, *Advances in Cryptology – EUROCRYPT 2001*, LNCS Vol. 2045, 93-118. Springer Verlag, 2001.

Ca05 Cameron, K., The Laws of Identity, Mai 2005. Download: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

CaThCh+05 Casassa Mont, M., Thyne, R., Chan, K., Bramhall, P., *Extending HP Identity Management Solutions to Enforce Privacy Policies and Obligations for Regulatory Compliance by Enterprises*, HP Technical Report, HPL-2005-110, Juni 2005.

HaKrRo+03 Hansen, M., Krasemann, H., Rost, M., Genghini, R., *Identity Management Systems (IMS): Identification and Comparison*, Studie für das Institute for Prospective Technological Studies, Joint Research Centre Seville, Spanien, September 2003; http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMSStudy.pdf.

Hi06 Hildebrandt, M., ‘Profiling – From data to knowledge’, in diesem Heft.

KeMi03 Kent, S.T., Millett, L.I. (Hrsg.), *Who Goes There? Authentication Through the Lens of Privacy*, Washington, D.C. 2003. Download: http://www7.nationalacademies.org/cstb/pub_authentication.html.

KoLe06 Koops, B.-J., Leenes, R., ‘ID Theft, ID Fraud and/or ID-related Crime – Definitions matter’, in diesem Heft.

Le06 Leenes, R. (Hrsg.), *FIDIS Deliverable D5.2b – ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, Frankfurt a.M. 2006. Download: http://www.fidis.net/487.0.html.

Me06 Meints, M., ‘Protokollierung bei Identitätsmanagementsystemen’, *DuD* 5/2006, 304-307, Wiesbaden 2006.

Pfi05 Pfitzmann, A., *Security in IT Networks: Multilateral Security in Distributed and by Distributed Systems*, Script, Dresden 2005. Download: http://dud.inf.tu-dresden.de/~pfitza/SecCryptI_II.pdf

PfHa06 Pfitzmann, A., Hansen, M., *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, Working Paper v0.28, Mai 2006, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

Ra06 Rangol, N., ‘Datenhandel – „Guten Tag, welchen Score-Wert haben Sie?“’, *ARD-Ratgeber*, 13.06.2006. Download: http://www.ard.de/ratgeber/special/datenhandel/-/id=322978/nid=322978/did=320280/5frl6d/.

RoRa06 Royer, D., Rannenberg, K., *Mobilität, mobile Technologie und Identität*, in diesem Heft.

Sc01 Schmid, G., *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)* (2001/2098(INI)), Juli 2001.

We06 Weichert, T., Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, Februar 2006. Download: http://www.datenschutzzentrum.de/scoring/.

[2] Siehe http://www.informationweek.com/story/showArticle.jhtml?articleID=18312163.

[3] Siehe https://www.prime-project.eu/.

[4] Siehe http://www.projectliberty.org/.

[5] Z.B. das Transaktions-Log und P3P-Policy-Auswert-Tool iJournal für Mozilla: http://sourceforge.net/projects/mozpets/.

[6] Siehe http://www.eclipse.org/higgins/.