T U M

I N S T I T U T F Ü R I N F O R M A T I K

Privatheit und Zugriffskontrolle bei Agenten-basierter Verwaltung von Benutzerprofilen

Wolfgang Woerndl

TUM-I0106
November 01

T E C H N I S C H E U N I V E R S I T Ä T M Ü N C H E N

TUM-INFO-11-I0106-100/1.-FI

Druck: Institut für Informatik der
Technischen Universität München

Privatheit und Zugriffskontrolle bei Agenten-basierter Verwaltung von Benutzerprofilen

Wolfgang Wörndl
Technische Universität München
woerndl@in.tum.de

Inhaltsverzeichnis

1 Einleitung

Der Verlust der Privatheit ist die größte Bedrohung des 21.Jahrhunderts.
Wall Street Journal (16.09.1999)

Die weltweite Vernetzung von Informations-Quellen führt u.a. dazu, dass Benutzer[1] Probleme haben, in der Fülle von Information, die für sie wichtige und relevante herauszufinden. Ein erfolgversprechendes Konzept ist die *Personalisierung* von Information, wozu (möglichst gute) *Benutzerprofile* nötig sind. Ein Benutzerprofil enthält dabei neben allgemeinen und demographischen Angaben über den Benutzer z.B. auch Interessensgebiete, Qualifikationen oder getätigte Transaktionen.

Es gibt mittlerweile im Internet auch viele Systeme, die Profile von Benutzern anlegen und versuchen, daraus persönliche Web-Seiten oder Empfehlungen abzuleiten. Das Problem dabei ist, dass die Benutzerprofile an unterschiedlichen Stellen erfasst und verwaltet werden, und Benutzer somit wenig Kontrolle und Übersicht haben, welche Daten wo, wie und von wem verwaltet werden. Eine mögliche Lösung ist, die Benutzerprofile in *dezentralen Benutzerprofilagenten* unter der Kontrolle des Benutzers zu speichern, so dass die gleiche Benutzerinformation für verschiedene Dienste verwendet werden kann. Dienste können dabei z.B. eine personalisierende Web-Site, Community Unterstützungssysteme oder auch E-Commerce Systeme oder Agenten sein.

Manche Dienste sind jedoch vertrauenswürdiger als andere für einen Benutzer und Benutzer wollen nicht alle Informationen im Profil für jeden Dienst zur Verfügung stellen. Die *Privatheit* (engl. privacy) der Benutzer bzw. Benutzerprofile muss also gewährleistet werden können. Man braucht daher einen Mechanismus zur Zugriffskontrolle auf die Benutzerprofilinformationen, sowie Möglichkeiten, weitere Aspekte von Privatheit, wie *Anonymität* und *Pseudonymität*, abbilden zu können. Das Ziel dieses Artikels ist es, diese Lösungsmöglichkeiten für Zugriffskontrolle und Privatheit aufzuzeigen und die Eignung für eine dezentrale Verwaltung von Benutzerprofilen zu bewerten.

Zunächst werden in diesem Artikel die Grundlagen von Benutzerprofilen, deren Modellierung, Verwendung und Speicherung dargelegt. Dann werden in Kapitel 3 Sicherheitseigenschaften, Privatheit und Datenschutz in diesem Szenario erläutert. In Abschnitt 4 werden bestehende Verfahren für Zugriffskontrolle in Hinblick auf eine Eignung im betrachteten Umfeld diskutiert. Anschließend werden Möglichkeiten sogenannter *Privacy Enhancing Technologies (PET)* dargestellt und bewertet. Der Beitrag endet schließlich mit einem Ausblick.

---

[1] Es werden der Einfachheit halber in diesem Text nur die männlichen Bezeichnungen verwendet

2 Benutzerprofile und deren Verwendung und Verwaltung

2.1 Benutzerprofile

Nachdem in diesem Artikel Zugriffskontrolle und Privatheit bei Verwaltung von Benutzerprofilen betrachtet werden, soll in diesem Abschnitt erläutert werden, was Benutzerprofile sind und wie sie verwendet werden können. Auch werden Möglichkeiten zur Speicherung und Verwaltung von Profilen insbesondere auch unter dem Gesichtspunkt der Privatheit diskutiert. Zunächst werden einige grundlegende Begriffe geklärt.

2.1.1 Identität und Benutzerprofile

Eine *Identität* ist aus soziologischer Sicht das „dauernde innere Sich-Selbst-Gleichsein, die Kontinuität des Selbsterlebens eines Individuums, die im wesentlichen durch die dauerhafte Übernahme bestimmter sozialer Rollen und Gruppenmitgliedschaften sowie durch die gesellschaftliche Anerkennung als jemand, der die betreffenden Rollen innehat bzw. zu der betreffenden Gruppe gehört, hergestellt wurde“ [Köh00].

Eine Identität beinhaltet zunächst mal die „Identifizierung“ einer Person, z.B. durch den Namen, die Nummer des Personalausweises und/oder der Wohnanschrift eines Individuums [GGPS97]. Darüberhinaus enthält eine Identität auch weitere zum Teil mehr oder weniger dynamische Eigenschaften einer Person, wie z.B. politische Anschauungen, Interessen oder Funktionen. Diese einen Benutzer charakterisierenden Eigenschaften nennt man – insbesondere im Umfeld einer elektronischen Speicherung und Verarbeitung – *Benutzerprofil*. Welche Eigenschaften oder *Attribute* ein Benutzerprofil enthalten kann, wird im folgenden Abschnitt 2.1.3 erläutert. Eine Identität in diesem Sinne wird in der Literatur z.T. auch als *Persona* bezeichnet [SoCr98, DGLP97, P3P00].

Eine Person kann unterschiedliche Rollen übernehmen (z.B. beruflich und privat) und somit mehrere Identitäten annehmen. Bei einer eher temporären oder willkürlich wählbaren Identität spricht man auch von einer *Pseudoidentität* oder einer *virtuellen Identität*. *Identitätsmanagement* impliziert die Möglichkeit einer Person, seine Identität oder Rolle, in der man gegenüber einem Kommunikationspartner auftritt, zu wählen [FeBe00]. Dazu gehört auch die Entscheidung, welche Teile des Benutzerprofils dem Partner offenbart werden. Der (oft unbewusste) Wechsel der Identität lässt sich auch in der realen Welt beobachten: Beispielsweise kann eine Person tagsüber eine Rolle als Angestellter einer Firma ausüben, danach anonym einige Einkäufe tätigen und schliesslich am Abend die private Identität in der Familie einnehmen.

Verschiedene Identitäten können dadurch modelliert werden, indem das Profil eines Benutzers in einzelne Profile für jede Identität aufgeteilt wird, oder indem man die Attribute des Profils folgendermaßen gruppiert. Attribute eines Profils gelten dann entweder

- für alle Identitäten eines Benutzers (z.B. Größe und Gewicht einer Person)
- nur für eine oder mehrere Identitäten (z.B. Nummer des Firmenausweises)
- oder haben bei verschiedenen Identitäten unterschiedliche Ausprägungen (z.B. berufliche und private Interessen)

2.1.2 Pseudonymität

Ein *Pseudonym* ist ein Bezeichner für eine (virtuelle) Identität. Es soll die Zuordnung und Verkettung bestimmter Handlungen zu einer Person ermöglichen, ohne den bürgerlichen Namen des Benutzers aufzudecken, oder eine Zuordnung zu einem anderen Pseudonym der gleichen Person erlauben zu müssen. Ein Pseudonym ist also ein „Spitzname" eines Benutzers in einem bestimmten Kontext und wird z.B. oft in Internet-Chats oder Diskussionsforen verwendet. Bei der Betrachtung von Pseudonymen sind insbesondere folgende drei Eigenschaften interessant (nach [Köh99]):

- Zuordnung: Wie wird ein Pseudonym einer Person zugeordnet? Kann das Pseudonym frei gewählt werden? Ist es auf eine andere Person übertragbar?
- Verkettbarkeit: Wie können Pseudonyme verkettet werden? Das bedeutet, wie ist es ersichtlicht, dass mehrere Transaktion von dem gleichen Benutzer getätigt wurden. Wenn gar keine Verkettung möglich ist, spricht man von *Anonymität*.
- Aufdeckbarkeit: Wer kann wie die Zuordnung eines Pseudonyms zu einer Person aufdecken?

Diese Eigenschaften spielen eine Rolle, wenn man verschiedene Ausprägungen von Pseudonymität betrachtet. Man kann sich dabei eine Reihe von *Pseudonymitätsstufen*, einer Einteilung nach dem Grad der Anonymität, vorstellen [FiHü01, FeBe00, PfKö01]:

- Preisgabe der/einer Identität
- Persönliches Pseudonym, z.B. ein Spitzname
- Rollen-Pseudonym, z.B. anhand einer Rolle oder Aufgabe in einer Firma
- Ein Pseudonym pro Kommunikationspartner
- Völlige Anonymität, d.h. ein neues Pseudonym pro Transaktion

2.1.3 Modellierung von Benutzerprofilen

Es gibt verschiedene Ansätze, Benutzerprofile zu modellieren. Typischerweise werden die Attribute in einem Profil inhaltlich in einzelne Abschnitte gegliedert und hierarchisch aufgebaut. Ein Profil kann u.a. folgende Informationen enthalten:

- Identifikator(en) (z.B. ein X.500 Verzeichnisname)
- (Verweis auf) digitale Signatur bzw. Zertifikat des Benutzers
- demographische Informationen (z.B. Email-Adresse oder Postanschrift)
- Zahlungsinformation (z.B. Daten einer Kreditkarte)
- Beziehungen (mit anderen Benutzern)
- Bewertungen, Interessen, Qualifikationen, persönliche Präferenzen
- Transaktions-Historie (z.B. gekaufte Produkte oder besuchte Web Seiten)

Es gibt verschiedene Ansätze zur Modellierung von Benutzerprofilen. vCARD [HSD98] ist ein Standard, der eine elektronische Visitenkarte abbilden soll und enthält

daher Informationen wie z.B. die private und berufliche Postanschrift. Das in Abschnitt 5.3.6 noch näher behandelte Platform for Privacy Preferences (P3P) Project [P3P00] enthält auch ein Datenformat für Benutzerinformationen. Modelle für E-Commerce sind z.B. ECML (www.ecml.org) und CPExchange (www.cpexchange.org).

Der genaue Aufbau eines Benutzerprofils soll in dieser Arbeit nicht diskutiert werden. Für die Repräsentation eines Profils bietet sich eine Darstellung in der *Extensible Markup Language (XML)* [XML00] an, da damit insbesondere auch eine einfache und übersichtliche Strukturierung von Daten erreicht werden kann. Abb. 1 zeigt ein Beispiel für ein Benutzerprofil in XML.

```
<PROFILE>
  <IDENTIFICATION>
    <IDENTIFICATOR TYPE="X.500">
       @c=DE@o=TU-MUENCHEN@cn=WOERNDL</IDENTIFICATOR>
  </IDENTIFICATION>
  <DEMOGRAPHIC>
     <EMAIL>woerndl@in.tum.de</EMAIL>
     <POSTAL> ... </POSTAL>
  </DEMOGRAPHIC>
  <INTERESTS>
    <INTEREST>web applications</INTEREST>
    <INTEREST>travelling</INTEREST>
    <INTEREST>baseball</INTEREST>
  </INTERESTS>
  <RATINGS>
    <MOVIE>
      <NAME>Dances With Wolves</NAME>
      <RATING TYPE="percentage">95</RATING>
    </MOVIE>
    <BOOK>
      <NAME>Lonely Planet Australia Guide</NAME>
      <ISBN>123456789</ISBN>
      <RATING TYPE="textual">Very Good</TEXT>
    </BOOK>
  </RATINGS>
  <MISC>
    <BOOKMARK>http://www.traveller-world.com</BOOKMARK>
    <BOOKMARK>http://www.rosenheim89ers.de</BOOKMARK>
    <CONFIGURATION APP="http://drehscheibe.in.tum.de">
      <BACKGROUNDCOLOR>grey</BACKGROUNDCOLOR>
      <STARTPAGE>courses</STARTPAGE>
    </CONFIGURATION>
  </MISC>
  <TRANSACTIONS>
     <LOG AREA="web">
        <SITE>http://www11.in.tum.de</SITE>
        <DATE>04-07-2001 10:43</DATE>
     </LOG>
  </TRANSACTIONS>
</PROFILE>
```

Abb. 1: Beispiel Benutzerprofil

Ein Identifikator ist ein (in der Regel eindeutiger) Bezeichner für eine Identität, z.B. ein X.500 Verzeichnisname. Das hier gezeigte Profil ist inhaltlich in einzelne Kategorien gegliedert. In den XML-Auszeichnungselementen stehen die Bezeichnungen der

Attribute bzw. der Kategorien von Profil-Attributen. Als Elemente sind die Ausprägungen der Attribute vorhanden. Die Attribute können z.B. auch Konfigurationseinstellungen einzelner Anwendungen sein.

Bestehende Ansätze, auch mit unterschiedlicher Ausrichtung oder Anwendungs-Domäne, lassen sich in ein entsprechendes XML-Dokument, wie im obigen Beispiel gezeigt, überführen [Ian01].

Die XML-Form ist nicht unbedingt geeignet für eine effiziente Speicherung des Profils[2], insbesondere bei sehr umfangreichen und/oder dynamischen Daten wie z.B. Web Zugriffslogs. Sie kann aber sehr gut zur Veranschaulichung des Konzepts eines Benutzerprofils dienen.

2.1.4 Abbildung mehrerer Identitäten

Wie in Abschnitt 2.1.1 erläutert wurde, kann ein Benutzer mehrere Identitäten annehmen, dies muss auch im Benutzerprofil abgebildet werden können. Dazu können in dem hier verwendeten XML-Format im <IDENTIFIKATION> Abschnitt mehrere Identifikatoren angegeben werden (Abb. 2). Auch ist es möglich, für Identitäten Pseudonyme zu definieren.

```
<PROFILE>
  <IDENTIFICATION>
    <IDENTIFICATOR TYPE="X.500" ID="work">
       @c=DE@o=TU-MUENCHEN@cn=WOERNDL</IDENTIFICATOR>
    <IDENTIFICATOR TYPE="PassportNumber" ID="private">
       123456789</IDENTIFICATOR>
    <PSEUDONYM ID="private">
       nickname</PSEUDONYM>
  </IDENTIFICATION>
  <DEMOGRAPHIC>
     <EMAIL ID="work">woerndl@in.tum.de</EMAIL>
     <EMAIL ID="private">mail@wolfgang-woerndl.de</EMAIL>
     <HEIGHT ID="work,private" UNIT="cm">180</HEIGHT>
  </DEMOGRAPHIC>
  <INTERESTS ID="private">
    <INTEREST ID="work">web applications</INTEREST>
    <INTEREST>travelling</INTEREST>
    <INTEREST>baseball</INTEREST>
  </INTERESTS>
</PROFILE>
```

Abb. 2: Benutzerprofil mit verschiedenen Identitäten

Eine Zuordnung von Identitäten zu Profil-Attributen geschieht über ein XML-Attribut „ID“ (z.B. „work“) im Tag der Elemente. Dadurch werden alle Teile des Profils, die mit dem gleichen „ID“ Attribut gekennzeichnet sind, der gleichen Identität des Benutzers zugeordnet. Bei verschiedenen Identitäten in einem Element und einer übergeordneten Kategorie, gilt die speziellere Ausprägung. Es ist auch möglich ein Element mehreren Identitäten zuzuordnen. Wenn kein „ID“ vorhanden ist, gilt der Profileintrag für alle Identitäten.

---

[2] Für eine effizientere Verarbeitung kann das Profil z.B. in einer relationalen Datenbank abgelegt werden.

2.2 Verwaltung von Benutzerprofilen

Es gibt verschiedene prinzipielle Möglichkeiten, Benutzerprofile zu verwalten, die im folgenden insbesondere auch hinsichtlich Privatheit diskutiert werden.

2.2.1 Erfassung und Speicherung der Profile bei den nutzenden Diensten

Im World Wide Web (WWW) werden heutzutage auf vielfache Weise Profile von (Web-)Benutzern erstellt und verwaltet. Zum Beispiel werten Internet-Shops wie amazon.com Aktionen von Benutzern aus, um auf dieser Grundlage Empfehlungen zu generieren. Aktionen können dabei z.B. die Web-Zugriffe eines Benutzers, der Kauf von Artikeln oder die explizite Bewertung von Produkten sein. Auch versuchen viele Web-Sites ihre Seiten oder die Bannerwerbung auf den Seiten gemäß den Präferenzen der Benutzer zu personalisieren, zum Teil geschieht dies bei Bannerwerbung auch übergreifend über mehrere Sites. Einzelne Web-Zugriffe können dabei u.a. mit Hilfe von *Cookies*[3] einem Benutzer – genauer ausgedrückt, einem Benutzer eines bestimmten Web-Browsers auf einem bestimmten Rechner – zugeordnet werden.

Benutzer werden auch aufgefordert, persönliche Daten explizit in Web-Formulare einzugeben, um z.B. Personalisierungs-Funktionen zu nutzen oder an Gewinnspielen teilzunehmen. Damit kann dann auch eine Zuordnung von beobachteten Daten anonymer Benutzer, wie z.B. Eingaben in Suchmaschinen im WWW, zu personenbezogenen Daten hergestellt werden. Es ist daher anzunehmen, dass für die meisten WWW-Benutzer ein mehr oder weniger detailliertes Profil bei verschiedenen Institutionen oder Firmen mit oder ohne Wissen bzw. Einverständnis des Benutzers vorhanden ist. Zum Teil sind diese Profile anonymisiert, zum Teil enthalten sie aber sicherlich auch den bürgerlichen Namen und andere personenbezogene Daten eines Benutzers [Les01].

Allerdings hat diese Server-seitige Speicherung bei den Diensten, die sie nutzen, inhärente Probleme:

- Profilinformationen können nur für denjenigen Dienst verwendet werden, der diese Daten gesammelt hat. Die Information über bei Barnes&Noble gekaufte Bücher kann nicht für Empfehlungen auch bei Amazon genutzt werden. Auch müssen Benutzer immer wieder neu die gleichen Informationen wie eine Email-Adresse eingeben und wenn sich diese ändert, kann sie nicht in einem Schritt allen betreffenden Diensten bekannt gemacht werden.
- Eine Server-seitige Speicherung von personenbezogenen Daten verursacht Probleme in bezug auf Privatheit. Benutzer haben keine Kontrolle darüber, welche Informationen über sie von wem und warum gespeichert werden

2.2.2 Server-seitige Profilverwaltung

Es gibt einige Ansätze, Benutzerprofile Server-seitig zu speichern und für mehrere Dienste wiederzuverwenden, z.B. Passport (www.passport.com) von Microsoft oder

---

[3] Ein Cookie ist ein kurzer Text, der vom Browser gespeichert und bei einem Besuch an den Server, der das Cookie gesetzt hat, zurückgeschickt wird. Damit kann ein Web-Server einen Benutzer wiedererkennen.

Novell's digitalme (www.digitalme.com). Dabei werden Dienste wie Verwaltung von Benutzername/Passwort für verschiedene Web-Server oder Übermittlung von Adress-, Zahlungs- und anderen Informationen an E-Commerce Systeme angeboten.

Der Schwerpunkt liegt dabei auf Abwicklung von Zahlungen („consumer wallet" bei Passport) oder der Verwaltung von elektronischen Visitenkarten („meCards" bei digitalme). Es wird kein komplettes Benutzerprofil modelliert und auch eine Erweiterung oder Anpassung von Profilfeldern ist nicht vorgesehen. Eine wichtige Funktion ist bei diesen Anwendungen das „single sign on". Benutzer müssen sich nur einmal authentifizieren, z.B. bei einem Passport-Server und können dann verschiedene Passport-fähige Dienste nutzen, ohne sich jedesmal neu anzumelden.

Allerdings gibt es gerade bei Passport einige Unzulänglichkeiten aus Sicht von Sicherheit und Privatheit, auf die genauer in [KoRu00] eingegangen wird. Unter anderem werden persistente Cookies benutzt, um die Anmelde-Informationen auf dem Browser zu speichern. Auch könnten böswillige Sites relativ einfach eine Zugehörigkeit zu Passport vortäuschen und dabei an Benutzername/Passwort unaufmerksamer Benutzer herankommen. Des weiteren ist die Kommunikation eines Passport-fähigen Dienstes mit dem Passport-Server nicht verschlüsselt.

Das Problem bei allen vorhanden, kommerziellen Systemen ist es auch, dass sie zu sehr auf die Vermarktung der Benutzerdaten und nicht auf den Schutz der Privatheit ausgerichtet sind. Ferner könnten Daten aus unterschiedlichen Quellen ohne Einverständnis des Benutzers zusammengeführt werden. Außerdem wird dem Benutzer die Möglichkeit genommen, Informationen nur teilweise herauszugeben, wenn er glaubt, ein Dienst ist nicht vertrauenswürdig. Selbst bei Zusicherung einer Speicherung nur zu einem vereinbarten Zweck kann es Probleme geben, wenn z.B. die Firma, die Profile verwaltet, Konkurs anmelden muss und vorher noch seine Kundendatei verkauft.

Ein Vorteil einer zentralisierten Speicherung auf einem Server wäre, dass ein Zugriffskontrollsystem und andere Sicherheitsmechanismen eventuell leichter zu realisieren wären. Allerdings stellt dies auf der anderen Seite auch einen „single point of attack" dar und ist dadurch z.B. durch „denial of service" Angriffe leichter lahmzulegen als ein stärker verteiltes System.

2.2.3 Client-seitige Speicherung

Eine Möglichkeit, Benutzerprofile für verschiedene Dienste wiederzuverwenden, besteht darin, diese Client-seitig, also auf dem Rechner des Benutzers, abzulegen. Dazu gibt es Werkzeuge wie z.B. Jotter (ww.jotter.com). Es bietet eine personalisierbare Symbolleiste (vgl. Abb. 3) mit Hilfe dessen ein Benutzer sein Profil pflegen kann und Funktionalitäten wie automatisches Ausfüllen von Web-Formularen oder Initiierung von personalisierten Suchvorgängen nutzen kann.

Abb. 3: Jotter

Diese Client-seitige Speicherung kann das Vertrauen des Benutzers in die Verwaltung seines Profils verbessern, da die Information auf seinem eigenen Rechner gespeichert sind, es gibt dabei aber auch einige Probleme. Die Profile sind nicht (auf einfache Weise) portabel: Informationen, die auf einem Rechner abgelegt sind, können nicht (ohne weiteres) auf einem anderen Rechner verwendet werden [MuSc00]. Auch ist trotz der Client-seitigen Speicherung nicht unbedingt absolute Kontrolle für den Benutzer gegeben, weil die Weitergabe und Verbreitung seiner Profilinformationen durch das Werkzeug im einzelnen kaum überwacht werden kann.

2.2.4 Infomediaries

Eine Verwaltung von Benutzerprofilen durch eine dritte Partei im Auftrag des Benutzers wird durch Anwendungen realisiert, die man als *Infomediary* [HaSi99, Cra99] bezeichnet. Der Begriff stammt von Hagel/Singer:

> "In order for customers to strike the best bargain with vendors, they'll need a trusted third party – a kind of personal agent, information intermediary, or infomediary – to aggregate their information with that of other consumers and to use the combined market power to negotiate with vendors on their behalf." ([HaSi99], S.19)

Ein Infomediary kann sowohl Server- als auch Client-seitig realisiert werden. Weniger entscheidend aus Sicht der Privatheit ist dabei der physikalische Ort der Speicherung, sondern die Frage, wer die Kontrolle über die Benutzerprofile ausübt. Also z.B. die Festlegung, welche Daten überhaupt gesammelt werden, wer die Zugriffsrechte vergibt und die Pflege und Löschung von Daten vornimmt. Dies sollte von Benutzer selber oder einer vertrauenswürdigen dritten Partei erfolgen. In [KoWö01] wird dazu der Ansatz von „ID-Repositories" vorgestellt. Dabei werden die Benutzerprofile in verteilten, von den nutzenden Diensten unabhängigen, ID-Repositories verwaltet, was auch eine gute Skalierbarkeit und Ausfallsicherheit der Architektur ermöglicht.

Eine dezentrale Speicherung von Benutzerprofilen bietet aber noch keine Verbesserung der Privatheit der Benutzerinformationen per se, ist aber die Grundlage und Voraussetzung für ein leistungsfähiges Zugriffsschutzsystem unter der Kontrolle des Benutzers. Unabhängig von einer Server- oder Client-seitigen Speicherung braucht man ein Zugriffsschutzsystem, dessen Realisierungsmöglichkeiten in diesem Beitrag diskutiert werden.

2.3 Szenario: Agenten-basierter E-Commerce und Community Unterstützung

Nachdem jetzt erläutert wurde, was Benutzerprofile sind, und wie man sie speichern kann, soll jetzt die Verwendung der Profile diskutiert werden.

2.3.1 *Personalisierung von Informationen*

Ein typisches Anwendungsgebiet für Personalisierung von Informationen ist eine adaptive Web-Site. Adaptive Web-Sites versuchen ihre Seiten anhand von Präferenzen des Benutzers zu personalisieren. Dies kann entweder durch Beobachtung der Aktionen eines Benutzers oder durch explizite Angabe von Präferenzen geschehen. In beiden Fällen wird ein Benutzerprofil aufgebaut, das dann ausgewertet werden kann.

Bei einer Personalisierung werden oftmals Empfehlungssysteme (engl. recommender systems) verwendet, die meist auf einer der folgenden Techniken basieren:

- Inhaltsbasiertes Filtern: Inhalte, wie z.B. Dokumente, werden mit Schlüsselwörtern versehen, die mit – explizit gemachten oder implizit abgeleiteten – Interessen eines Benutzers verglichen werden
- Kollaboratives Filtern [Koch01a]: Es wird versucht, Benutzer mit ähnlichen Interessen zu finden und abzugleichen. Dies wird z.B. bei Online-Buchhändlern wie amazon.com verwendet
- Regelbasiertes Filtern: Die Generierung von Empfehlungen geschieht auf Basis von Benutzer-spezifischen Regeln

In allen Fällen werden verschiedene Informationen über den Benutzer aus dessen Profil benötigt.

2.3.2 *Benutzerprofile und Software-Agenten*

Wie in Abschnitt 2.2 erläutert, ist es vorteilhaft, Benutzerprofile dezentral und unabhängig von den Diensten, die sie verwenden, zu verwalten. Zur Realisierung möglichst unabhängiger Komponenten bietet sich die Verwendung von *Software-Agenten* an, da diese (mehr oder weniger) autonom – also unabhängig von anderen Komponenten oder Interaktion mit dem Benutzer – agieren. (Software-)Agenten sind weiterhin durch folgende Eigenschaften charakterisiert, die sie von anderen, konventionellen Programmen unterscheiden:

- Proaktivität: Agenten können von sich aus Aktionen initiieren
- Kooperation: Agenten kooperieren oft mit anderen Agenten um ein (gemeinsames oder komplementäres) Ziel zu erreichen
- Adaption: Agenten können sich an veränderte Situation anpassen oder aus Erfahrungen lernen
- Kommunikation durch Austausch von Nachrichten

Diese Eigenschaften bedingen auch Anforderungen hinsichtlich Sicherheit und Privatheit. Das Agentenparadigma ermöglicht außerdem eine Modularisierung von Diensten in einer offenen Architektur und die lose Kopplung unabhängiger Komponenten [BBB+97, KLW01]. Für die Kommunikation zwischen den Agenten wird eine Agent Communication Language (ACL) verwendet. Eine ACL wie FIPA ACL [FIPA99] oder KQML [FLM97] definiert ein Schema zum Austausch von Nachrichten zwischen Agenten hinsichtlich Syntax, Semantik und Pragmatik und basiert auf der Sprechakt-Theorie. Dies erlaubt die Verwendung einer Sprache zur Kommunikation zwischen unabhängig voneinander entwickelten Software-Agenten [KLW01].

Es ist hier im Kontext dieses Artikels nicht entscheidend, dass die Speicherung und Verarbeitung von Benutzerprofilen durch Software-Agenten erfolgt, sondern nur durch autonome, dezentrale Komponenten, um eine Unabhängigkeit der Systemkomponenten zu garantieren. Eine zentralisierte Verwaltung sensibler Daten hat eventuell ganz andere Anforderungen, auf die hier nicht näher eingegangen wird.

Im Zusammenhang der Verwaltung von Benutzerprofilen sind insbesondere zwei Gruppen von Agenten-basierten Systemen interessant, die daher im folgenden etwas genauer betrachtet werden sollen:

- Agenten-basierter E-Commerce und
- Agenten-basierte Community-Unterstützungssysteme

2.3.3 Software-Agenten und Electronic Commerce

Software-Agenten können das Kaufen und Verkaufen von Produkten und Dienstleistungen im Internet unterstützen, wobei die Agenten in der Regel als Vermittler zwischen einem Käufer und Verkäufer auftreten, daher spricht man dann auch von *Agent-Mediated E-Commerce* [MGM99].

Agenten können verschiedene Phasen des elektronischen Handels unterstützen, z.B. Produktauswahl, Preisbestimmung oder auch die Festlegung von Liefermodalitäten. Ein wichtiger Aspekt ist dabei die *Verhandlung*. Agenten agieren autonom, verfolgen verschiedene Ziele und versuchen unabhängig voneinander ein möglichst günstiges Ergebnis zu erreichen. Durch eine Automatisierung von Verhandlung durch Agenten ist neben einer Optimierung von Marktabläufen auch Kostenreduzierung im E-Business möglich.

Ein Beispielsystem unter vielen Projekten ist MIT's *Kasbah* [CDGM97, ChMa96]. Dabei erzeugt ein Benutzer, der ein Gut kaufen oder verkaufen will, einen Agenten und versieht diesen mit strategischen Informationen, wie z.B. erwarteter oder maximaler Preis. Der Agent versucht dann proaktiv in einem elektronischen Marktplatz ein möglichst gutes Ergebnis zu erzielen. Am Ende einer Transaktion gibt es dabei auch die Möglichkeit, den Partner zu bewerten, was dazu dienen kann, Reputation und Vertrauen zwischen Benutzern aufzubauen. Dies kann von den Agenten verwenden werden, um z.B. Agenten (bzw. deren Benutzer) auszuschließen, die nicht ein Mindestmass an Reputation vorweisen können.

Bei einem sinnvollen Einsatz von Agenten für E-Commerce sind oftmals Information über den Benutzer nötig, in dessen Auftrag er handelt, z.B. Präferenzen und Zahlungsinformationen, oder auch dessen Reputation. Dabei stellt sich insbesondere auch das Problem, die Privatheit der Profilinformationen sicherzustellen, da der Benutzer einen Teil der Kontrolle über sein Profil einem autonom agierenden Agenten anvertraut.

2.3.4 Community-Unterstützungssysteme

(Virtuelle) Communities bezeichnen Gruppen von Personen, die eine Gemeinsamkeit, z.B. ähnliche Interessen, haben. Eine genauere Definition findet sich bei Mynatt et.al.:

„[A community] is a social grouping which exhibit in varying degrees: shared spatial relations, social conventions, a sense of membership and boundaries, and an ongoing rhythm of social interaction." ([MAIO97], S. 211)

Im Gegensatz zu einer „Gruppe" oder einem „Team" ist eine Community nur eine lose gekoppelte Menge von Menschen. In der Regel fehlt bei Communities ein gemeinsames Ziel und ein Gruppenbewustsein. Communities können aber eine gute Quelle zur Beschaffung von Informationen sein, weil Wissen oft nur schwer externalisierbar ist und daher die direkte Interaktion mit Experten eine wichtige Rolle im Wissensmanagement spielen kann [KLW01]. Dies soll durch *Community-Unterstützungssysteme* [Koch01b] realisiert werden, welche meist einen Teil der folgenden Funktionalitäten anbieten:

- Bereitstellung eines Mediums für direkte Interaktion zwischen Benutzern, z.B. durch ein Chat-System
- Verwaltung von Community-Informationen, z.B. Anmerkungen zu Publikationen in einer Forschergruppe
- Aufdecken und Visualisieren von Beziehungen zwischen Community-Mitgliedern, z.B. Finden eines Benutzers mit den gleichen Interessen
- Filterung und Personalisierung von Informationen, z.B. Generierung einer Liste von Produkten, die Benutzer mit ähnlichen Interessen für gut befunden haben

Im Projekt IMC/Cobricks (Information Management for Communities / Bricks for supporting communities[4]) [BKL+01, Koch00] werden Agenten-basierte Systeme zur Unterstützung von Communities untersucht. Dabei werden die in dezentralen Benutzerprofilagenten gespeicherten Informationen über Benutzer von *Community Agenten* verwendet. Ein Community Agent verwaltet dabei die Informationen einer Community, z.B. Beiträge von Mitgliedern, und stellt Dienste wie Empfehlungsgenerierung oder den Abgleich von Benutzern, die an einer vergleichbaren Aufgabe arbeiten, bereit.

Ein Beispiel einer Anwendung in dieser Architektur ist das *CommunityItemsTool* [KLW01]. Es ermöglicht einen Austausch von Community-Informationen wie z.B. Bookmarks oder bibliographische Referenzen in einer Forscher-Community. Benutzer können u.a. die Referenzen in einer persönlichen Ordnerstruktur ablegen oder Bewertungen abgegeben, wobei diese Benutzerinformation in einem Benutzerprofilagenten gespeichert werden.

2.3.5 Anwendungsszenario

Die erläuterten Anwendungen für Agenten-basierte Verwaltung von Benutzerprofilen lassen sich zu folgendem Szenario (Abb. 4) zusammenfassen.

---

[4] Siehe auch http://www11.in.tum.de/proj/imc/

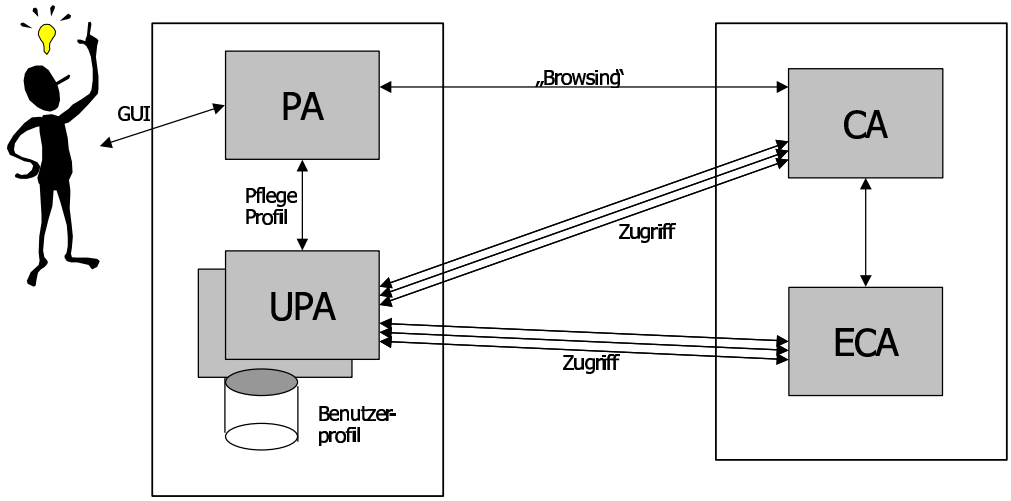

Abb. 4: Anwendungsszenario

Der Benutzer greift über ein „Personal Assistant" Werkzeug (PA) auf die Komponenten zu. Der PA kann ein erweiterter Web-Browser oder auch ein Client-seitiges Infomediary (vgl. Abschnitt 2.2.4) sein. Ein Community Agent (CA) oder E-Commerce Agent (ECA) stellt Personalisierungs- und andere Dienste für den Benutzer bereit. Dazu benötigen sie Informationen aus dem Profil des Benutzers, wozu sie mit dem Benutzerprofilagenten (user profile agent, UPA) kommunizieren. Die Dienst-Agenten (CA, ECA) können gegebenenfalls auch untereinander Informationen austauschen. Der UPA verwaltet das Profil des Benutzers, welcher seine Daten über eine Schnittstelle pflegt, die z.B. der PA zur Verfügung stellt. Für eine Kommunikation zwischen den Agenten ist nicht unbedingt eine Initiierung durch den Benutzer erforderlich, sondern es ist auch möglich, dass ein Dienst-Agent von sich aus personenbezogene Informationen anfordert, da es sich um autonome Komponenten handelt. Auch kann es sein, dass der UPA (vom Benutzer oder anderen, dazu autorisierten, Komponenten oder Agenten) geänderte Profilinformationen an die betreffenden Dienst-Agenten ohne Abfrage derer weitergibt. Wichtig bei dem Szenario ist, wie schon erwähnt, eine Trennung der Benutzerprofilverwaltung von den Diensten, die sie nutzen.

Das Szenario deckt die oben beschriebenen Anwendungen in den Bereichen Community Support und E-Commerce ab. Der Fokus dieses Beitrags ist es, dabei die Privatheit zu untersuchen. Dies ist hier besonders wichtig, da durch den Einsatz von – zumindest konzeptionell – autonomen Agenten zur Verwaltung von personenbezogenen Informationen auch ein Teil der Kontrolle über sein Profil für den Benutzer zunächst mal verloren geht. Bevor mögliche Lösungen dafür betrachtet werden, soll im nächsten Abschnitt zunächst geklärt werden, was „Privatheit" eigentlich ist und welche Anforderungen sich daraus ergeben.

3 Privatheit, Sicherheit und Datenschutz

There was of course no way of knowing whether you were being watched at any giving moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to.

George Orwell, "1984"

Ausgehend von dem recht allgemeinen Konzept der „Privatheit" werden im Folgenden auch rechtliche Rahmenbedingungen und Charakteristika von Schutzzielen für mehrseitige Sicherheit in Hinblick auf Privatheit untersucht. Das Ziel dieses Kapitels ist es, Anforderungen an ein technisches System für Privatheit und Zugriffskontrolle in dem erläuterten Umfeld zu erarbeiten.

3.1 Privatheit

Überlegungen zu *Privatheit* (engl. privacy) reichen schon sehr lange zurück. Bereits 1890 schrieben Samuel D. Warren und Louis D. Brandeis:

„... The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world ... so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasion upon his privacy, subjected him to mental pain and distress far greater than could be inflicted by mere bodily injury." (aus: [WaBr1890])

Weiterhin definieren sie Privatheit als Recht, alleine gelassen zu werden („to be let alone"). Der Grund der Publikation bestand darin, dass durch technologische Fortschritte die Privatheit bedroht schien, z.B. auf dem Gebiet der Fotografie und der zunehmenden Veröffentlichung von Fotos in Boulevard-Zeitungen [FiHü01]. Obwohl obiger Text schon mehr als 110 Jahre zurückliegt, ist die prinzipielle Aussage, dass Privatheit immer wichtiger für ein Individuum wird, noch gültig und wieder sehr aktuell.

Die wohl am häufigsten verwendete Definition von Privatheit ist von Alan Westin:

"Privacy is the claim of individuals, groups or institutions to determine for themselves, when, how and to what extent information about them is communicated to others." (aus: [Wes67])

Essentiell ist dabei der Aspekt der *Kontrolle*. Benutzerinformation sollen schon verwaltet werden können, schließlich kann der Benutzer dadurch personalisierte Dienste nutzen. Wichtig ist aber, dass der Benutzer jederzeit überwachen und bestimmen kann, welche persönlichen Daten wie verwendet werden, und keine Informationen ohne sein Einverständnis weitergegeben werden.

Es gibt verschiedene Aspekte oder Dimensionen von Privatheit [FiHü01, Lau00], u.a. die Privatheit der Person, die z.B. einen Schutz vor physischer Annäherung impliziert. Mit der Verbreitung des Internets und einer stark zunehmenden Speicherung personenbezogener Daten wird die Dimension der Privatheit in Bezug auf persönliche

Daten immer wichtiger und ist hier in dem Umfeld einer Verwaltung von Benutzerprofilen besonders interessant. Dies wird auch als *„Information Privacy“* bezeichnet:

> “Information Privacy refers to the claims of individuals that information about themselves should generally not be available to other individuals or organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.” (aus: [Cla99])

Der Anspruch auf Privatheit ist dabei kein absolutes oder unabdingbares Recht, ergibt sich aber auch aus entsprechenden gesetzlichen Vorgaben, die in Abschnitt 3.2 besprochen werden.

Westin teilt die Menschen in drei Kategorien ein [Les01]: Menschen, die sehr beunruhigt sind bezüglich ihrer Privatheit (25% laut [Les01]) und starke Einschränkungen in Kauf nehmen, um ihre Privatheit zu schützen. 12% der Personen sind überhaupt nicht besorgt und geben persönliche Daten in beliebiger Weise heraus. Die Mehrzahl der Menschen (63%) fällt in eine dazwischenliegende Kategorie: Bedenken bezüglich der Gefahren, aber auch Interesse an möglichen Vorteilen einer Teilaufgabe von Privatheit und z.B. der Verwaltung von Benutzerprofilen zur Personalisierung von Diensten. Benutzer haben dabei insbesondere folgende Bedenken in Bezug auf die Privatheit ihrer persönlichen Daten [Cra99, MaLa01]:

- Gewährleistung einer sicheren Speicherung und Übertragung sensibler Daten
- Unwissenheit darüber, welche Benutzerinformationen überhaupt von wem gespeichert sind
- Befürchtung einer unbefugten Preisgabe oder Verwendung personenbezogener Daten
- Uneinheitliche oder unklare gesetzliche Situation (siehe dazu auch die Ausführungen über rechtliche Rahmenbedingungen im Kapitel 3.2)
- Verbesserte technologische Möglichkeiten, große Mengen an personenbezogenen Daten mit relativ geringen Aufwand zu sammeln und auszuwerten (z.B. mit Methoden des *data minings*[5])
- Unsicherheit über Möglichkeiten einer nachträglichen Korrektur oder Löschung von Daten

Daher ist es wichtig, Mechanismen zur Verfügung zu stellen, die es erlauben, die Privatheit personenbezogener Daten sicherzustellen. Benutzer müssen über die Speicherung und Verwendung personenbezogener Daten informiert und in die Lage versetzt werden, Entscheidungen bezüglich der Verwaltung ihrer Daten zu treffen. Dies wird in der Literatur auch als „informed consent“ [LiLo98], oder „notice & choice“ [Cra99] bezeichnet.

Man kann nicht davon ausgehen, dass die geforderte Kontrolle, Informiertheit und Entscheidungsmöglichkeit für Internet-Benutzer gegeben ist:

---

[5] Beim data mining wird versucht, mit Hilfe statistischer Methoden komplexe Zusammenhänge und Trends in Massendaten herauszufinden

"People are not in control of the technology that surrounds them. We have important data and personal information scattered in hundreds of places across the technology landscape, locked away in applications, product registration databases, cookies, and Web site user tracking databases." (aus [Mic01])

Ein weiterer wichtiger Punkt ist in diesem Zusammenhang auch das *Vertrauen* der Interaktionspartner, was im Internet oftmals nicht gegeben ist. Vertrauen kann ich diesem Zusammenhang definiert werden als „Gewissheit (d.h. die innere Repräsentanz des Eintretens) einer erwünschten Zukunft. Es beruht

- auf der Kontinuität des regelhaften und erwünschten Verhaltens der Umgebung
- oder auf der Hilfe vertrauter Menschen (auch in unwägbarer Lage)
- oder auf der eigenen Kenntnis und Beherrschung der Lage (einschließlich ihrer Unwägbarkeiten)" ([Gri01], S.69)

Ein Fehlen dieser Gewissheit in dem betrachteten Szenario erfordert Mechanismen, um Vertrauen zwischen den Akteuren aufzubauen, z.B. durch eine Verbesserung der „eigenen Kenntnis und Beherrschung der Lage".

Privatheit ist eine deutsche Bezeichnung für „privacy". Manchmal wird synonym dafür auch der Begriff „Datenschutz" verwendet, obwohl mit Datenschutz hauptsächlich die rechtlichen Rahmenbedingungen gemeint sind, was nur einen Teil von „Privatheit" ausmacht.

3.2 Gesetzliche Rahmenbedingungen für Datenschutz

In diesem Beitrag sollen Möglichkeiten der Informatik zur Verbesserung der Privatheit bei der Verwaltung personenbezogener Daten diskutiert werden. Eine technische Lösung hat jedoch zum einen relativ wenig Sinn, wenn keine gesetzlichen Mittel vorhanden sind, um dies gegebenenfalls auch rechtlich durchzusetzen[6]. Zum anderen ergeben sich aus den gesetzlichen Rahmenbedingungen Grundsätze und Anforderungen auch für das Zugriffskontrollsystem auf technischer Ebene (vgl. dazu Abschnitt 3.5). Daher soll hier ein kurzer Überblick über relevante juristische Aspekte von Datenschutz und Privatheit gegeben werden. Es werden die Richtlinien der OECD, das deutsche Bundesdatenschutzgesetz (BDSG) und Teledienstedatenschutzgesetz (TDDSG), sowie die Situation in den USA betrachtet.

3.2.1 OECD Richtlinien

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat 1980 in einer „Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten" sieben Grundsätze zum Schutz personenbezogener Daten aufgestellt [OECD80, Cla99].

---

6 Allerdings gibt es z.Zt. kaum weltweit gültige Rechtsvorschriften und ist die Anwendung nationaler Gesetze im grenzüberschreitenden Internet sehr problematisch [Bäu00]

Es sollte eine Beschränkung der Beschaffung personenbezogener Daten geben ("collection limitation"). Daten sollen im Hinblick auf ihren Verwendungszweck erheblich und, soweit es der Verwendungszweck erfordert, sachlich richtig, vollständig und auf den neuesten Stand gebracht sein ("data quality"). Die Zwecke, für die personenbezogene Daten beschafft werden, sollen im einzelnen angegeben werden ("purpose specification"). Die Verwendung der Daten soll beschränkt sein ("use limitation"). Personenbezogene Daten sollen durch angemessene Sicherungsmaßnahmen gegen Gefahren wie Verlust, unbefugten Zugang sowie unbefugte Zerstörung, Verwendung, Änderung oder Preisgabe geschützt werden ("security safeguards"). Es soll allgemein gewährleistet werden, dass Entwicklung, Praxis und Politik hinsichtlich personenbezogener Daten durchschaubar sind (Transparenz, "openness"). Der Betroffenen soll ein Recht auf Auskunft über die Datenerfassung und Korrektur, Löschung, Vervollständigung und Änderung haben ("individual participation"). Ein Verantwortlicher für eine Datensammlung soll für die Beachtung der Maßnahmen verantwortlich sein, welche die oben genannten Grundsätze verwirklichen ("accountability").

Diese Richtlinien sind zwar rechtlich nicht verbindlich, sind aber in viele nationale Gesetze eingegangen.

3.2.2 Bundesdatenschutzgesetz und Teledienstedatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) enthält einige allgemeine Grundsätze über den Umgang mit personenbezogenen Daten. Ein Datum gilt nach dem BDSG als *personenbezogen*, wenn es Angaben über persönliche oder sachliche Verhältnisse einer bestimmbaren natürlichen Person enthält. Entscheidend ist also die Verknüpfung von Daten mit der Identität einer Person. Das BDSG legt fest, dass Betroffene ein Recht auf Auskunft haben, welche Daten warum gespeichert werden, sowie die Möglichkeit, eine Korrektur, Löschung und Sperrung seiner Daten zu verlangen.

Spezieller auf die Anforderungen des Datenschutzes in der Informationsverarbeitung geht das Teledienstedatenschutzgesetz (TDDSG) ein, das ein Teil des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) ist. Das TDDSG legt fest, welche personenbezogenen Daten ein Anbieter speichern darf, wie er damit umgehen muss und wie der Benutzer Kontrollmöglichkeiten ausüben kann. Zwei Prinzipien lassen sich insbesondere daraus ableiten: Datensparsamkeit und Zweckbindung [ScEn00, FHO98].

Ein Grundsatz ist die *Datensparsamkeit* bzw. *Datenvermeidung*, dies wird auch als *Erforderlichkeit* der Datenerfassung bezeichnet. Dabei muss ein Diensteanbieter sicherstellen, nur die für die Erbringung des vom Benutzer erwünschten Dienstes notwendigen (personenbezogenen) Daten zu erheben und zu verarbeiten. Darunter fällt auch die Möglichkeit, einen Dienst anonym oder unter einem Pseudonym anzubieten, soweit dies technisch machbar ist. Verweigert der Benutzer eine Herausgabe personenbezogener Daten, darf er nicht vom Dienst ausgeschlossen werden.

Das zweite wichtige Prinzip ist die *Zweckbindung* bei der Speicherung personenbezogener Daten. Der Zweck einer Datenerfassung muss sich entweder aus den

gesetzlichen Regelungen ergeben oder der Benutzer hat für die Erhebung und Nutzung zu einem spezifizierten Zweck seine ausdrückliche Einwilligung erteilt. Daten dürfen dann nur für diesen Zweck verwendet werden.

3.2.3 Situation in den USA

Die Situation in den USA bezüglich rechtlicher Rahmenbedingungen ist auch im Hinblick auf Privatheit von einem etwas anderes Rechtsverständnis als in Europa geprägt. Es gibt weniger gesetzliche Regelungen, sondern man geht von einer Selbstregulierung des Marktes aus. Verstöße gegen Privatheitsansprüche werden daher eher als Bruch einer Vereinbarung zwischen einem Unternehmen und einem Kunden bzw. als Betrug gewertet, und nicht der Missachtung eines Gesetzes.

Um die aus EU-Sicht nicht ausreichenden gesetzlichen Vorschriften auszugleichen und für EU-Bürger ein „angemessenes Schutzniveau" [Tät00] gegenüber Drittstaaten wie den USA zu gewährleisten, wurde die sogenannte „safe harbour" Vereinbarung getroffen. Sie sieht im Grundsatz vor, dass US-amerikanische Firmenzusammenschlüsse sich gemeinschaftlich verpflichten, für die von Europa zu ihnen exportierten Daten ein Datenschutzniveau einzuhalten, das europäischen Maßstäben entspricht. Dabei sollen die folgenden Prinzipien gelten [Tät00]:

- „notice": Informationspflichten über die Art der Datenerhebung und -verarbeitung sowie über ihren Zweck, die Empfänger und die Wahlmöglichkeiten hinsichtlich der Begrenzung und der Nutzung und Übermittlung
- „choice": Wahlrecht hinsichtlich der Nutzung der Daten
- „onward transfer": bei der Weitergabe der Daten an Dritte wird sichergestellt, dass dort das Datenschutzniveau nicht abfällt
- „security": technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung
- „data integrity": Sicherstellung der Integrität der Daten, also von Richtigkeit, Vollständigkeit, Aktualität und Erforderlichkeit im Einzelfall
- „access": das Recht der Betroffenen auf Auskunft über die zu ihrer Person gespeicherten Daten
- „enforcement": eine effektive Durchsetzung der Prinzipien

Es fehlen dabei zwar einige Punkte aus den deutschen Datenschutzgesetzen wie Datensparsamkeit oder das Verbot des Ausschlusses von Benutzern bei Verweigerung der Zustimmung einer Speicherung personenbezogener Daten. Die „safe harbour" Grundsätze können aber, zusammen mit den anderen, oben erläuterten Prinzipien gesetzlicher Regelungen, als Grundlage für die Speicherung und Nutzung personenbezogener Daten aus rechtlicher Sicht mit angesehen werden (vgl. Anforderungen in Abschnitt 3.5).

3.3 Privatheit and E-Commerce

Privatheit hat einem hohen Stellenwert bei Electronic Commerce, was auch eine Betrachtung von Privatheit wichtig macht. Umfragen unter Internet Benutzern zeigen, dass diese Bedenken in bezug auf ihre Privatheit haben. Zum Beispiel äußerten 87% der Befragten in einer Studie von Ackermann et.al. Besorgnis bezüglich ihrer Privatheit im Internet [ACR99]. Benutzer sind außerdem weniger gewillt, Informationen herauszugeben, wenn es sich um personenbezogene Daten handelt:

> "In a scenario involving a banking Web site, 58% of respondents said that they would provide information about their income, investments, and investment goals in order to receive customized investment advice. However only 35% said they would also supply their name and address so that they could receive an investment guide booklet be mail." ([ACR99], S. 5)

Die Bereitschaft, Daten bereitzustellen, sinkt also deutlich, wenn dies nicht mehr anonym erfolgt. Diensteanbieter können somit auch von einer Verbesserung der Mechanismen zum Schutz der Privatheit profitieren, da Benutzer dann eher bereit sind, mehr und bessere persönliche Informationen herauszugeben, wenn sie sicher sein können, dass diese Daten nicht in unbeabsichtigter Weise verwendet werden [BeKö00].

Forrester Research argumentiert in einer Studie „Surviving The Privacy Revolution" vom Februar 2001 [For01], dass Privatheit einer der wichtigsten Gesichtspunkte beim Erfolg von E-Commerce ist, und dass Unternehmen, die keine Maßnahmen zum Schutz der Privatheit ihrer Kunden treffen, Nachteile erleiden könnten. Insbesondere gilt dies auch für Aspekte mobiler Kommunikation („M-Commerce"), wobei z.B. Dienste, die den aktuellen Standort des Benutzers auswerten, eine wichtige Rolle spielt. Die Privatheit in mobilen Diensten und Interaktion hat noch andere Anforderungen, als das hier betrachtete Szenario, wobei darauf in diesem Beitrag nicht näher eingegangen wird.

Bei E-Commerce ist insbesondere im Privatkundengeschäft Vertrauen sehr wichtig, was im Internet u.a. durch den Verlust eines persönlichen Kontaktes beim Abschluss eines Geschäftes oftmals nicht gegeben ist. Die Befürchtung vor einem „gläsernen Internet-Kunden" hält außerdem viele Menschen davon ab, im Internet aufzutreten [Gri01]. Dies könnte durch verbesserte technologische Unterstützung ausgeglichen werden.

3.4 Schutzziele mehrseitiger Sicherheit und Privatheit

Um konkrete Anforderungen für Privatheit in diesem Szenario zu entwickeln, können auch die folgenden Schutzziele mehrseitiger Sicherheit dienen.

3.4.1 Mehrseitige Sicherheit

In dem hier betrachteten Szenario interagieren verschiedene, über ein offenes Netzwerk verbundene Teilnehmer miteinander, die z.T. einander nicht kennen oder vertrauen. Jeder Kommunikationspartner verfolgt verschiedene Interessen und hat unterschiedliche Anforderungen in bezug auf Privatheit und Sicherheit. Es muss deshalb ein Abgleich

konkurrierender Interessen erfolgen. Zum Beispiel könnte bei einer E-Commerce Transaktion ein Händler möglichst viel über seinen Kunden wissen wollen, während ein Benutzer möglichst wenig von sich Preis geben will oder anonym auftreten will, z.B. um unerwünschte Werbung zu verhindern. Auch ist es möglich, dass unbefugte Dritte durch Abhören von Kommunikationsbeziehung an sensible Daten herankommen. *Mehrseitige Sicherheit* ([PSWW00], [WoPf00]) bedeutet die Berücksichtigung der Sicherheitsanforderungen aller beteiligten Parteien.

Sowohl a priori fehlendes Vertrauen der Kommunikationspartner, als auch potentielle Angriffe von Dritten sollen dabei durch Schutzmechanismen wie z.B. Verschlüsselung oder Anonymität bei der Kommunikation ausgeglichen werden. Dies ist insbesondere wichtig bei der Verwaltung von sensiblen Daten, wie z.B. Benutzerprofilinformationen.

In der Begriffswelt der mehrseitigen Sicherheit wurden Schutzziele entwickelt, die für Verwaltung von Benutzerprofilen sehr relevant sind und die daher im folgenden näher untersucht werden.

3.4.2 Schutzziele mehrseitiger Sicherheit

Tabelle 1 zeigt die Schutzziele mehrseitiger Sicherheit und deren (beispielhafte) Bedeutung bei der Verwaltung von Benutzerprofilen ([PSWW00], [WoPf00], [CC98]).

Schutzziel	**Bedeutung bei Benutzerprofilverwaltung**
Vertraulichkeit: Sichert die Geheimhaltung von Daten während der Übertragung, kein unbefugter Dritter kann den Inhalt der Nachricht erkennen	Unbefugte (d.h. vom Benutzer nicht autorisierte) dürfen keinen Zugriff auf persönliche Daten erhalten. Dies betrifft sowohl die Speicherung und Übertragung der Daten, als auch die Verwendung der Benutzerprofile, also insbesondere auch die Weitergabe von Daten
Verdecktheit: Versteckt die Übertragung einer Nachricht, kein Dritter soll die Existenz einer Nachricht erkennen können	Die Übertragung (von Teilen) eines Benutzerprofils von Profilagenten zu einem Dienst soll verdeckt stattfinden
Unbeobachtbarkeit: Sichert, dass ein Benutzer Dienste oder Ressourcen nutzen kann, ohne dass andere beobachten können, dass der Dienst oder die Ressource genutzt wird	Die Kommunikation mit einem Dienst darf nicht ersichtlicht sein, da ein unbefugter Dritter z.B. aus der Nutzung einer Informationsquelle zu gesundheitlichen Fragen auf eine Krankheit einer Person schließen könnte
Anonymität: Kommunikationspartner und Dritte erfahren nicht die Identität eines Benutzers	Benutzer sollen anonymisiert mit einem Dienst kommunizieren können

Pseudonymität: Nutzung einer Ressource ist einem Benutzer zurechenbar, ohne dass dieser seine Identität offenbaren muss	Um personalisierte Dienstleistungen geben zu können, ist eine vollständige Anonymität nicht immer wünschenswert, sondern eine Interaktion mit einem Pseudonym nötig
Zurechenbarkeit: Sichert, dass das Senden (bzw. Empfangen) von Information gegenüber Dritten bewiesen werden kann	Z.B. ist bei einer Bestellung von Produkten durch einen E-Commerce Agenten im Auftrag eines Benutzers für den Händler ein Nachweis der Bestellung nötig
Integrität: Sichert, dass (ungefugte) Modifikationen einer Nachricht durch den Empfänger erkannt werden können	Benutzerprofilinhalte sollen bei der Kommunikation von Benutzerprofilagenten zum Community Agenten nicht verändert werden können, bzw. eine Manipulation muss erkannt werden können
Verbindlichkeit: Sichert, dass ein Nutzer belangt werden kann, um seine Zusagen innerhalb einer angemessenen Zeit zu erfüllen	Betrifft auch die Einhaltung von Zusagen der Verwendung von Attributen aus dem Benutzerprofil, z.B. keine Weitergabe an Dritte
Verfügbarkeit: Sichert die Nutzbarkeit von Diensten und Ressourcen für einen Benutzer	Keine besondere Relevanz in bezug auf Privatheit beim Zugriff auf Benutzerprofile
Erreichbarkeit: Sichert, dass mit einer Ressource (z.B. hier auch ein anderer Nutzer) Kontakt aufgenommen werden kann, wenn gewünscht	Keine besondere Relevanz in bezug auf Benutzerprofilverwaltung, schlechte Erreichbarkeit (oder Verfügbarkeit) kann tendenziell die Privatheit von Benutzern verbessern

Tabelle 1 Schutzziele und deren Relevanz bei Benutzerprofilverwaltung

Diese Ziele müssen sowohl gegenüber dem Kommunikationspartner, als auch gegenüber potentiellen Dritten, betrachtet werden. Die Schutzziele sind nicht unabhängig voneinander, sondern haben Wechselwirkungen. Zum Beispiel wird Vertraulichkeit durch Unbeobachtbarkeit impliziert, Verdecktheit verstärkt Anonymität, wobei Anonymität komplementär zu Zurechenbarkeit ist.

3.4.3 Aspekte einer E-Privacy

Wie schon angeführt, haben verschiedene Schutzziele unterschiedliche Bedeutung in dem hier betrachteten Szenario des Zugriffs auf dezentrale Benutzerprofile. Die Schutzziele lassen sich in Kategorien einordnen, die die Hauptaspekte einer *„E-Privacy“* [Bäu00] ausmachen. Anonymität und Pseudonymität sind verwandt und lassen sich daher eine Kategorie „Identitätsziele“ einordnen. Weiterhin haben Vertraulichkeit, Verdecktheit und Unbeobachtbarkeit miteinander zu tun und können zu „Vertraulichkeitszielen“

zusammengefasst werden. Schließlich kann man Integrität, Verbindlichkeit und Zurechenbarkeit als eine Menge von „Absicherungszielen“ auffassen.

Noch nicht berücksichtigt ist dabei folgender, bei einer Verwaltung von personenbezogenen Daten wichtige Aspekt: Wie kann sich der Benutzer im klaren sein, welcher Aspekt seiner Person zu irgendeinem Zeitpunkt überwacht wird, und unter welchen Umständen dies geschieht [MaLa01]? Dies kann man als „Transparenzziel“ bezeichnen und es ergibt sich auch aus den rechtlichen Rahmenbedingungen für Datenschutz.

Als Kategorien einer E-Privacy lassen sich also zusammenfassend festhalten[7]:

- Identitätsziele: Anonymität, Pseudonymität
- Vertraulichkeitsziele: Vertraulichkeit, Verdecktheit, Unbeobachtbarkeit
- Absicherungsziele: Integrität, Verbindlichkeit, Zurechenbarkeit
- Transparenzziele: Überwachungs- und Kontrollfunktionen für Benutzer

3.5 Anforderungen

Die erläuterten Vertraulichkeitsziele beziehen sich hier auf die Vertraulichkeit bei der Datenübertragung – in unserem Szenario – vom Benutzerprofilagent zu einem Diensteanbieter. Es muss zunächst auch festgelegt werden können, ob dieser Dienst überhaupt eine Zugriffserlaubnis auf die betreffenden Profilattribute haben soll. Ein wichtiger Punkt bei den Vertraulichkeitszielen ist daher auch die Möglichkeit, Zugriffsrechte für einzelne Attribute des Benutzerprofils festlegen zu können.

Die Anforderungen an ein technisches System zur Gewährleitung von Privatheit lassen sich daher aus drei Ausgangspunkten ableiten:

- Gesetzliche Rahmenbedingungen
- Schutzziele mehrseitiger Sicherheit
- Notwendigkeit eines Zugriffskontrollsystems

Dem Benutzer müssen also Mechanismen zur Verfügung gestellt werden, um zu bestimmen, welcher Dienst-Agent welche Zugriffsrechte auf das dezentral verwaltete Benutzerprofil ausüben darf. Dies ist eine Hauptfunktion des in Kapitel 2.1.1 erläuterten Identitätsmanagements. Dabei kann man insbesondere folgende konkrete Anforderungen an die Zugriffskontrolle feststellen:

- Flexibilität bei der Zugriffskontrolle, z.B. durch Aushandlung
- Wählbare Granularität (Rechte für einzelne Profilattribute, sowie auch für Kategorien möglich)
- Kontrolle der Weitergabe von Daten
- Geeignete Benutzerschnittstellen zur Administration von Rechten
- Möglichkeit, Optionen wie „Zugriff nur bei gesicherter Übertragung“ zu realisieren
- Integration von „Zweckbindung“

---

[7] Die Einordnung der Schutzziele in Kategorien dient hier hauptsächlich dazu, die Anforderungen in Kapitel 3.5 zu strukturieren, manche Ziele spielen in mehreren Kategorien eine Rolle

- Möglichkeiten zur zeitlichen Begrenzung und Zurückziehbarkeit von Rechten

Die Gesichtspunkte lassen sich in die vier erläuterten Kategorien einer E-Privacy einordnen, so dass man zusammenfassend folgende Anforderungen an ein System zur Sicherstellung von Privatheit bei Agenten-basierter Verwaltung von Benutzerprofilen formulieren kann:

- Identitätsziele:
    - Mechanismen für Identitätsmanagement
    - Zweifelsfreie Überprüfung der Identität der Kommunikationspartner
    - Möglichkeit für Benutzer, anonym zu kommunizieren
    - Möglichkeit der Verwendung eines Pseudonyms
    - Unverkettbarkeit von Pseudonymen (bzw. Verkettbarkeit nur unter der Kontrolle des Benutzers)
    - Möglichkeiten, verschiedene Stufen von Pseudonymität zu wählen (vgl. Abschnitt 2.1.2)
- Vertraulichkeitsziele:
    - Möglichkeit zur Festlegung von Zugriffsrechten für Benutzerprofil-Attribute (Zugriffskontrollsystem)
    - Flexibilität bei der Zugriffskontrolle, z.B. durch Regeln und Verhandlung, sowie bei der Granularität der Rechtevergabe
    - Realisierung von Unbeobachtbarkeit und Verdecktheit in den Kommunikationsbeziehungen
    - Möglichkeit, Daten über eine gesicherte Verbindung zu übertragen
    - Datensparsamkeit, Datenvermeidung bzw. Erforderlichkeit eines Zugriffs
    - Einhaltung von (technischen und organisatorischen) Richtlinien zur Sicherheit bei der Datenspeicherung und -verarbeitung
- Absicherungsziele:
    - Speicherung des Profils unter der Kontrolle des Benutzers
    - Zweckbindung von Profilzugriffen
    - Regelung der „Weitergabe von Daten“
    - Möglichkeit, Zugriffsrechte zeitlich zu beschränken und ggf. auch wieder zurückziehen zu können
    - Entscheidungsmöglichkeit beim Benutzer bezüglich der Herausgabe von Daten
    - Möglichkeit der Unterstützung von vertrauenswürdigen Organisationen (z.B. für die Prüfung der zugesagten Verwendung der Daten)
    - Möglichkeiten der Zurechenbarkeit und Unabstreitbarkeit (z.B. Nachweis einer Bestellung)
    - Einhaltung gesetzlicher Rahmenbedingungen
    - Verantwortlichkeit derjenigen Unternehmung oder Organisation, die personenbezogene Daten speichert

    - Möglichkeit der Durchsetzung der erläuterten Prinzipien gegenüber Unternehmungen, die personenbezogene Daten verarbeiten
    - Integritätsanforderung: Daten können gegen Verfälschung insbesondere während einer Übertragung in offenen Netzen geschützt werden
    - Möglichkeit der Signierung eines Zugriffsrechts (vgl. Abschnitt 5.2.2: „Authentifizierung, Zertifikate und digitale Signaturen“)
- Transparenzziele:
    - Möglichkeit, vergebene Zugriffsrechte jederzeit überprüfen zu können, auch durch vertrauenswürdige Institutionen
    - Möglichkeit für Benutzer, Zugriffe überwachen zu können, Protokollierung aller Zugriffe
    - Sinnvolle Benutzerschnittstellen zur Festlegung von Rechten
    - Vertrauenswürdiger Benutzeragent

Um diese Anforderungen umsetzen zu können, müssen verschiedene Mechanismen angewandt werden. Zunächst ist ein Zugriffskontrollsystem erforderlich, um dem Benutzer eine Festlegung zu erlauben, wer wie auf sein Benutzerprofil zugreifen darf. Dies alleine reicht aber nicht aus, da damit Gesichtspunkte wie zum Beispiel Identitätsmanagement oder Anonymisierung nicht abgedeckt werden können. Dafür gibt es sogenannte „Privacy Enhancing Technologies“, die diese Aspekte behandeln. Daher sollen in den folgenden beiden Kapiteln dieses Beitrages untersucht werden, ob und welche Teile der Anforderungen mit den bestehenden Mechanismen und Verfahren erfüllt werden können.

4 Zugriffskontrolle

Wie erläutert sind die beiden wichtigsten bestehenden Ansatzpunkte, die zur Verbesserung der Privatheit bei Zugriff auf dezentrale Benutzerprofile verwendet werden könnten, Modelle und Verfahren zur *Zugriffskontrolle*, sowie Mechanismen, die versuchen die Privatheit im Internet zu verbessern (*Privacy Enhancing Technologies*). In diesem Abschnitt soll zunächst untersucht werden, inwieweit bestehende Modelle und Systeme zur Zugriffskontrolle geeignet sind, zur Lösung der Aufgabenstellung beizutragen.

Die einzelnen Mechanismen und Verfahren werden hier nur sehr kurz und im Überblick behandelt. Auch werden einzelne Aspekte, die für Benutzerprofilverwaltung interessant erscheinen, herausgestellt, auch wenn diese nicht unbedingt die Kernpunkte eines vorgestellten Ansatzes sind.

In diesem Abschnitt werden Grundlagen von Zugriffskontrolle und Modelle zur Realisierung behandelt, sowie Administration von Zugriffkontrolle. Des weiteren werden

XML-basierte Verfahren diskutiert und schließlich das Kapitel in einer Bewertung zusammengefasst.

4.1 Grundlagen, Zugriffsrechte und Zugriffskontrollmatrix

Zugriffskontrolle ist der Teil eines Sicherheitsmodells, der die Autorisierung von Zugriffsanforderungen an Ressourcen von (bereits authentifizierten) Benutzern oder Systemkomponenten behandelt. Auch ist die Administration von Zugriffsrechten wichtig, also die Entscheidung, wer auf welche Weise Rechte oder auch Zugriffsregeln o.ä. festlegt (siehe Abschnitt 4.4).

Benutzerprofile enthalten Daten, die vor unerlaubten oder unerwünschten Zugriff geschützt werden sollen, dies fällt also genau in die Domäne der Zugriffskontrolle. Daher sollen nach einem Überblick über die Grundlagen der Zugriffskontrolle verschiedene Modelle und Systeme betrachtet werden und auch deren Eignung in Hinblick auf dezentrale Benutzerprofilverwaltung untersucht werden.

Es werden bei der Zugriffskontrolle folgende Entitäten unterschieden:

- Objekte: (passive) Komponenten, die geschützt werden sollen (z.B. Dateien oder Attribute in einem Benutzerprofil)
- Subjekte: Systemkomponenten, die auf Objekte zugreifen (z.B. Benutzer, Programme oder Software-Agenten)
- Zugriffsrechte: Mögliche Zugriffsaktionen (z.B. Lesen, Schreiben, Löschen, Ausführen, ...)

Die Beziehung zwischen diesen Entitäten ist der Kernpunkt der Zugriffskontrolle. Der Zugriff der Subjekte auf die Objekte muss eingeschränkt und festgelegt werden können. Ein Zugriffskontrollsystem hat außerdem zu gewährleisten, dass alle Subjekte und Objekte eindeutig identifiziert werden und jedes Objekt von der Rechteverwaltung erfasst wird [Eck01].

Der Ausgangspunkt für die Realisierung einer Zugriffskontrolle ist die *Zugriffskontrollmatrix* (engl. access control matrix, ACM). Dabei stellen die Subjekte (in unserem Szenario die E-Commerce und Community Agenten) die Zeilen einer zweidimensionalen Matrix dar, die Objekte (hier die Attribute des Benutzerprofils) die Spalten der Matrix. In den Schnittpunkten der Matrix stehen die Rechte für den Zugriff des Subjekts auf das betreffende Objekt (vgl. Beispiel in Tabelle 2).

	Email-Adresse	**Kreditkartennummer**	**private Interessen**
E-Commerce Agent A		Lesen	
Community Agent B	Lesen		
Community Agent C			Lesen, Schreiben

Tabelle 2 Zugriffskontrollmatrix

Es können auch mehrere Attribute zusammengefasst werden und z.B. Rechte sowohl für alle „privaten Interessen“ als auch einzelne Interessen verwaltet werden, die Granularität der betrachteten Objekte ist also auch wichtig.

Die Implementierung erfolgt mit Hilfe der in den folgenden Abschnitten erläuterten Konzepte und Modelle. Eine direkte Implementierung der ACM ist in der Regel nicht sehr effizient, weil die Matrix oft nicht sehr dicht besetzt ist, also nur für relativ wenige Objekt/Subjekt Paare explizite Rechte festgelegt sind.

4.2 Konzepte zur Implementierung

Es gibt im Prinzip drei Alternativen, die Zugriffskontrollmatrix zu implementieren, nämlich eine spalten- oder zeilenweise Realisierung, sowie eine kombinierte Vorgehensweise.

4.2.1 Zugriffskontrollliste

Eine spaltenweise Implementierung der ACM ist die *Zugriffskontrollliste* (engl. access control list, ACL). Dies ist eine Liste pro schützendem Objekt, die die Zugriffsrechte von Subjekten definiert. Die Zugriffskontrollliste realisiert somit eine Objekt-bezogene Sichtweise. Der Vorteil dabei ist, dass es leicht ist, festzustellen, welche Subjekte auf ein Objekt Zugriff hat, also z.B. eine Frage der Art „wer hat Zugriff auf meine Kreditkartennummer?“ zu beantworten. Auch ist eine Rechterücknahme relativ einfach zu realisieren. Ein Nachteil einer ACL ist es, dass sie nicht (oder nur mit großem Aufwand) transparent ist in bezug auf eine mögliche Fragestellung des Benutzers „welche Rechte hat Community Agent X beim Zugriff auf mein Profil?“.

Die Zugriffskontrollliste ist effizient bei vielen Objekten, bietet aber keine gute Skalierbarkeit bei sehr vielen Subjekten, was eventuell bei Benutzerprofilverwaltung der Fall sein könnte. Daher wurde eine Erweiterung des ACL-Konzeptes vorgeschlagen, bei dem nicht mehr die Rechte einzelner Subjekte festgelegt werden, sondern den Subjekten Rollen zugeordnet werden oder sie in Gruppen eingeteilt werden und die Zugriffsrechte nur noch für diese Rollen in der ACL festgelegt werden (siehe Rollen-basierte Zugriffskontrolle, Abschnitt 4.3.3).

4.2.2 Zugriffsausweise

Ein *Zugriffsausweis* (engl. capability) ist ein unverfälschbares Ticket, das den Inhaber zum Zugriff auf die im Ticket genannten Objekte berechtigt. Dies entspricht einer zeilenweisen bzw. Subjekt-bezogenen Implementierung der ACM.

Die Zugriffskontrolle kann dadurch im Vergleich zur ACL vereinfacht werden, da nur noch der Zugriffsausweis überprüft werden muss und nicht mehr möglicherweise sehr lange Listen durchsucht werden müssen. Auch ist ein Vorteil, dass man bei einer Benutzerprofilverwaltung in übersichtlicher Weise die Zugriffsrechte einer einzelnen Community ausdrücken kann. Durch eine fälschungssichere Realisierung lässt sich zudem ein dezentrales Sicherheitsmanagement durchführen, da die Komponenten, die die Capabilities ausstellen von den Komponenten, welche die Zulässigkeit von Zugriffen prüfen, getrennt werden können.

Ein Zugriffsausweis ist üblicherweise unabhängig von Inhaber des Ausweises. Somit kann auch eine Delegation von Rechten erfolgen (Ausweisweitergabe), was allerdings nicht immer wünschenswert beim Zugriff auf Benutzerprofile erscheint. Bei Verwaltung von personenbezogenen Daten muss die Weitergabe von Zugriffsrechten beschränkt werden können. Ein weiteres Problem bei Capabilities ist es, dass eine Rechterücknahme problematisch ist, da sich die Frage stellt, wie ein Widerruf eines Ausweises bekannt gegeben und in einem verteilten System durchgesetzt werden kann. Mögliche Lösungen sind eine Rückforderung ausgegebener Zugriffsausweise, was nicht immer praktikabel ist [Eck01], oder das ungültig machen von Capabilities.

4.2.3 Kombinierter Ansatz

Um die Nachteile – insbesondere das Rechterücknahmeproblem – von Zugriffsausweisen zu umgehen, können die beiden vorgestellten Konzepte zur Realisierung der Zugriffskontrollmatrix kombiniert werden. Eine Lösung dieser Art wird als Schlüssel/Schlossverfahren bezeichnet [Eck01].

In der Grundform des Schlüssel/Schlossverfahrens wird jedem Subjekt s eine Capability-Liste zugeordnet, die Paare der Form (o,K) enthält. Dabei bezeichnet o ein Objekt, auf das s unter Anwendung des Schlüssels K zugreifen darf. Jedes Objekt o besitzt seinerseits eine Zugriffskontrollliste, die Einträge der Form (L,α) enthält, wobei L ein Schloss ist und α diejenigen Zugriffsrechte sind, die den Benutzer des zum Schloss L passenden Schlüssels K eingeräumt werden.

Möchte nun ein Subjekt s auf das Objekt o zugreifen, so legt es der Zugriffskontrolle von o seine Capability (o,K) vor. Ein Zugriff ist dann zulässig, wenn der Schlüssel K in ein Schloss L der Zugriffsliste von o passt, d.h. wenn es einen Eintrag (L,α) gibt, mit K=L. Dieser Test muss unter Berücksichtigung der angeforderten Zugriffsrechte erfolgen.

Das Problem der Rechterücknahme kann dann einfach und effizient dadurch realisiert werden, indem das Schloss L eines Objektes verändert wird, so dass in dem Zugriffsausweis enthaltene Schlüssel K nicht mehr passt.

Diese beschriebene Form ist jedoch für einen praktischen Einsatz zu aufwändig, daher wird die Kombination von ACL und Zugriffsausweisen meist in einer stark vereinfachten Form eingesetzt, Windows NT verwendet z.B. ein „access token“ für jeden authentifizierten Benutzer [Eck01].

4.3 Strategien und Modelle

Die Konzepte zur Implementierung behandeln noch keine Modelle, wie man gewünschte Strategien umsetzen kann. Dies wird in diesem Abschnitt besprochen.

4.3.1 Diskrete Zugriffskontrolle

Die bisher vorgestellten Möglichkeiten einer Realisierung der Zugriffskontrollmatrix fallen in den Bereich der *diskreten Zugriffskontrolle* (engl. discretionary access control,

DAC; auch als „benutzerbestimmbare“ Zugriffskontrolle bezeichnet). DAC basiert auf dem Eigentümer-Prinzip auf Basis von authentifizierten Benutzern oder Gruppen von Benutzern. Das bedeutet, dass der Eigentümer (engl. owner) eines Objektes – oftmals ist dies der Erzeuger – entscheiden kann, inwieweit er Zugriffsrechte an andere Benutzer weitergibt. Die Rechtevergabe in einem UNIX-Dateisystem ist ein typisches Beispiel für diskrete Zugriffskontrolle.

Ein Benutzer mit Leserecht kann dabei auch durch Kopieren einer Information und Zuweisung entsprechender Zugriffsrechte an die Kopie, die Information auch anderen Benutzern zugänglich machen, obwohl dies vielleicht nicht vom ursprünglichen Erzeuger der Ressource so vorgesehen war (vgl. Abb. 5). Aus diesem Grunde lassen sich unautorisierte Informationsflüsse in diesem Modell kaum vermeiden.

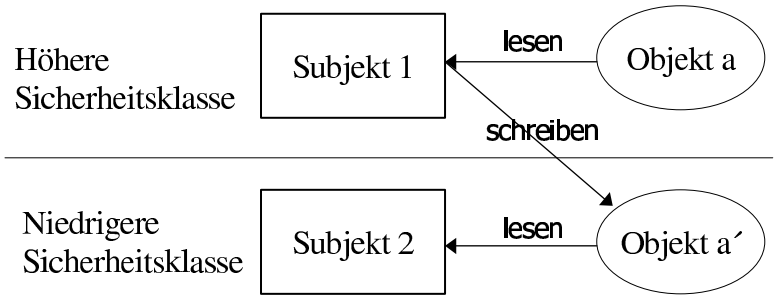

Abb. 5: Unerlaubter Informationsfluss bei DAC

Das Problem bei DAC ist somit, dass die Umsetzung einer Sicherheitspolitik von der Diskretion der Subjekte abhängt, was besonders auch bei Verwaltung von Benutzerprofilen nicht erwünscht oder zweckmäßig ist. Auch ist z.B. keine Zuordnung von Aufgaben und einem Zweck zu einem Zugriff möglich. Daher ist diskrete Zugriffskontrolle in der Grundform ohne zusätzliche Mechanismen nicht geeignet, Zugriffskontrolle für Benutzerprofile zu verwirklichen.

4.3.2 Mandatorische Zugriffskontrolle

Mandatorische Zugriffskontrolle (engl. mandatory access control, MAC; auch als „systembestimmte“ oder „regelbasierte“ Zugriffskontrolle bezeichnet) versucht den Mangel einer systemglobalen Zugriffsstrategie bei diskreter Zugriffskontrolle zu vermeiden, indem der Zugriff verweigert wird, wenn es eine systembestimmte Festlegung gibt, die den Zugriff verbietet, obwohl die benutzerbestimmbaren Rechte vorhanden wären. Somit kann das Szenario in Abb. 5 vermieden werden. MAC setzt nicht bei der Kontrolle des Datenzugriffs an, sondern bei der Kontrolle der Informationsflüsse [Opp97].

Der bekannteste Vertreter von MAC ist das Modell von Bell-LaPadula [BeLa73]. Die Zugriffsrechte sind dabei beschränkt auf die Menge {execute, read, append, write}. Die Objekte und Subjekte werden dabei von vertrauenswürdigen Systemkomponenten in

Sicherheitsklassen SC eingeteilt, die nicht überschritten werden dürfen. Die Sicherheitsklassen stellen eine Hierarchie dar, z.B. „Streng Geheim“ >= „Geheim“ >= „Vertraulich“ >= „Unklassifiziert“. Eine Dominanz-Relation „>=“ definiert einen Verband über den Systemklassen. Der Zugriff auf ein Objekt ist nur dann gestattet, wenn eine bestimmte Relation (abhängig vom geforderten Zugriffsrecht) zwischen den Sicherheitsklassen des Objekts und Subjekts erfüllt ist. Insbesondere sollen die beiden folgenden Regeln gelten:

- “no-read-up” (auch „simple security property“ genannt): Lesen oder Ausführen eines Objektes o durch Subjekt s ist nur dann gestattet, wenn die betreffenden Zugriffsrechte vorhanden sind und gilt: SC(s) >= SC(o). Dieser Grundsatz verhindert das Lesen von vertraulichen Daten von Subjekten niedrigerer Systemklassen
- “no-write-down” (oder „*-Eigenschaft“): Ein Zugriff „append”, also das Anfügen an eine Information, ist nur dann erlaubt, wenn ein entsprechendes Zugriffsrecht existiert und gilt: SC(s) <= SC(o). Für einen schreibenden Zugriff muss gelten: SC(s) = SC(o). Damit soll ein zufälliges oder absichtliches Hinunterschreiben von sensiblen Daten auf Stufen niedrigerer Systemklassen vermieden werden

Bell-LaPadula ist ein recht restriktives, formalisiertes Modell mit beschränkter Ausdrucksfähigkeit, eine konkrete Anwendung für ein System zur Benutzerverwaltung erscheint nicht möglich. Ein Problem ist auch das „blinde Schreiben“, wobei Objekte, also Benutzerprofilinhalte in unserem Kontext, von Subjekten niedrigerer Systemklassen überschrieben werden können, auch wenn kein lesender Zugriff darauf erlaubt ist. MAC wurde für den militärischen Bereich entwickelt und wird hauptsächlich auch dort angewendet.

Ein weiterer Nachteil bei einem Einsatz von MAC in dem betrachteten Szenario ist, dass eine Einteilung von Objekten in Sicherheitsklassen nicht so ohne weiteres möglich ist. Auch soll der Zugriff auf personenbezogenen Daten nicht abhängig von einer globalen Einteilung in Sicherheitsklassen sein, sondern von den persönlichen Präferenzen des Benutzers unter Berücksichtigung des Kontextes des Zugriffs, insbesondere des Zwecks.

Allerdings braucht man in unserem Szenario systembestimmte Festlegungen zumindest zusätzlich zu diskreten Zugriffsrechten, sonst wäre z.B. die Verhindung der Weitergabe von Informationen oder Rechten nicht möglich.

4.3.3 Rollen-basierte Zugriffskontrolle

In der Praxis wird oft *Rollen-basierte Zugriffskontrolle* (engl. role based access control, RBAC) [FeKu92] verwendet. Dabei werden die Zugriffsrechte nicht an Subjekte vergeben, sondern Zugriffsrechte an zu definierende Rollen erteilt und den Subjekten (möglicherweise mehrere) Rollen zugewiesen. Die Rollen entsprechen an Subjekten zugeteilten Aufgaben. Oftmals werden die Rollen hierarchisch organisiert, wodurch es ermöglicht wird, Rechte zu vererben.

Der Unterschied von RBAC zu DAC ist, dass es Benutzern nicht erlaubt ist, die Zugriffsrechte im eigenen Ermessen an andere Benutzer weiterzugeben [FeKu92]. RBAC ist also eine Form mandatorischer Zugriffskontrolle, wobei es für praktische Anwendungen leichter zu realisieren ist und daher eine größere Bedeutung besitzt, als die erläuterte Grundform von MAC, da es nicht auf starren Sicherheitsklassen beruht.

Ein Vorteil von RBAC in Hinblick auf die Verwaltung von Benutzerprofilen besteht in der Möglichkeit, Zugriffsrechte mit Aufgaben zu verbinden. Man könnte z.B. eine Rolle „Lieferant" definieren, lesenden Zugriff auf Profildaten wie Postanschrift oder Zahlungsinformationen für diese Rolle gestatten und E-Commerce Agenten zur Abwicklung einer Bestellung im Auftrag des Benutzers diese Rolle zuweisen. Allerdings erscheint es nicht praktikabel, eine sinnvolle Zuordnung von Subjekten zu Rollen und Zugriffsrechten zu Rollen explizit vom Benutzer für alle Profilattribute durchführen zu lassen. Auch ist die Rollenzuweisung keine vollständige Realisierung einer Zweckbindung des Zugriffs, wie es in den Anforderungen verlangt wurde. Des weiteren lässt sich die Verwendung von Daten nicht vernünftig modellieren. Benutzer sollen z.B. den Zugriff auf Daten in Abhängigkeit davon, ob die Information weitergegeben wird, erlauben oder verbieten können.

Ein weiterer Vorteil eines Rollen-basierten Ansatzes ist es eventuell, dass anonymisierte Zugriffe leichter realisiert werden könnten, nachdem die Rechte nicht mehr an Subjekte, sondern nur noch an Rollen gebunden sind. Ferner kann RBAC die Skalierungsprobleme einer ACL-basierten Implementierung verbessern, weil nicht mehr einzelne Rechte für alle Subjekte vergeben werden müssen.

Nachdem in den bisher betrachteten Modellen keine (explizite) Modellierung der Erforderlichkeit und Zweckbindung gemacht wurde, soll im folgenden Abschnitt ein Modell betrachtet werden, dessen Ziel eine Formalisierung von Zugriffskontrolle hinsichtlich Aspekten der Privatheit und des Datenschutzes ist.

4.3.4 Ein Modell für Privatheit in Zugriffskontrolle

Simone Fischer-Hübner hat ein formales[8] Modell ausgearbeitet, das u.a. die Modellierung des Zwecks eines Zugriffs beinhaltet und damit eine Datenschutz-konforme Zugriffskontrolle sicherstellen soll [FiHü01, FHO98]. Es werden dabei neben Subjekten, Objekten und Zugriffsrechten u.a. modelliert:

- Rollen („user role"): Den Subjekten werden wie bei RBAC Rollen zugewiesen, wobei die Rollen hier die Verantwortlichkeiten bezüglich der Administration regeln
- Objektklassen („object-classes"): Jedes Objekt ist genau einer Objektklasse zugeordnet
- Aufgaben („tasks"): Jedes Subjekt hat genau eine (aktuelle) Aufgabe aus einer Menge von Aufgaben

[8] Der Ansatz wird im folgenden aber nur informell und zusammenfassend beschrieben

- Zwecke („purposes“): Jede Aufgabe hat (genau) einen Zweck, jeder Objektklasse ist mindestens ein Zweck zugeordnet
- Einwilligung („consent“): Der Betroffene eines Zugriffs auf ein Objekt kann in die Verarbeitung für bestimmte Zwecke einwilligen

Mit Hilfe dieser Konzeptualisierung können nun in Form von Invarianten Anforderungen an ein Zugriffsschutzsystem formuliert werden. Um einen Datenschutz-orientierten Zustand zu erreichen, muss (etwas vereinfacht) erfüllt sein: „ein Subjekt hat nur dann Zugriff, wenn es für seine aktuelle Aufgabe erforderlich ist“ (Erforderlichkeit), sowie: „ein Subjekt hat nur dann Zugriff, wenn der Zweck seiner aktuellen Aufgabe in den Zwecken der Objektklasse des Objektes enthalten ist oder eine Einwilligung des Betroffenen für den Zweck der Aufgabe und das Objekt vorliegt“ (Zweckbindung).

Weitere Eigenschaften können in Form von Einschränkungen („constraints“) z.B. bezüglich der Erfassung bzw. Erzeugung von Daten festgelegt werden. Die Formalisierung ist ein „task-based privacy model“, wobei alle Aktionen durch Zustandsübergangsfunktionen beschrieben werden und wodurch eine Einhaltung der Datenschutz-Invarianten bewiesen werden können soll.

Das Modell bietet eine Integration von Datenschutz-relevanten Aspekten in die Zugriffkontrolle, insbesondere erscheint eine Formalisierung des Zwecks und der Erforderlichkeit eines Datenzugriffs sinnvoll und notwendig. Allerdings stellt sich in diesem sehr komplexen Schema die Frage, wie der Benutzer damit umgehen soll und wie z.B. die Menge der Aufgaben und Zweck in einem konkreten Szenario gewählt werden können. Auch ist eine Implementierung bisher nur im Betriebssystemumfeld verwirklicht[9], die Realisierung bei einer Agenten-basierten Verwaltung von Benutzerprofilen erscheint unklar.

4.4 Administration von Zugriffsrechten

In Hinblick auf Administration bei der Zugriffskontrolle muss festgelegt werden können, wer autorisiert ist, Zugriffsrechte für Objekte zu vergeben und in welcher Art und Weise dies geschehen soll. Diese Aufgabe stellt sich bei allen vorgestellten Verfahren.

Bei mandatorischer Zugriffskontrolle ist eine Festlegung von Sicherheitsklassen und Einordnung von Subjekten und Objekten in diese Klassen erforderlich. Dies wird von einem Sicherheits-Administrator systemweit festgelegt. Bei einer Verwaltung von Benutzerprofilen ist eine systemweite Definition jedoch nicht unbedingt sinnvoll, da jedem Benutzer die Möglichkeit gegeben werden sollte, selbst die Zugriffsrechte auf sein Benutzerprofil geeignet festlegen zu können.

Bei diskreter Zugriffskontrolle gibt es verschiedene Möglichkeiten [SaSa94]: zentralisierte (von einem Administrator festgelegt), hierarchische (anhand einer Organisationsstruktur), kooperative (Kooperation mehrerer Administratoren nötig), dezentrale (erlaubt Delegation von Rechten) oder Eigentümer-bestimmte (Besitzer eines Objekts bestimmt Rechte) Administration. RBAC bietet ein ähnliches Spektrum von

[9] Vgl. dazu www.rsbac.org

Möglichkeiten, dabei können Rollen definiert werden, denen entsprechende Rechte zur Manipulation von Zugriffsrechten zugewiesen werden können.

Bei Verwaltung von Benutzerprofilen ist der Benutzer Eigentümer seines Profils und sollte die volle Kontrolle darüber haben, also insbesondere auch die Zugriffsrechte von Diensten auf seine Profil-Attribute bestimmen können. Daher erscheint eine Eigentümer-bestimmte Administration am zweckmäßigsten. Dabei stellen sich allerdings in der Praxis die folgenden Probleme:

- Benutzer brauchen detailliertes Wissen über das Zugriffsschutzsystem: wie werden Rechte festgelegt, was hat das für Auswirkungen etc. Die Rechte-Administration muss leicht zu erlernen und zu benutzen sein
- Eine Kenntnis über die Subjekte ist erforderlich, Benutzer müssen die Dienste, die auf die Profilinformationen zugreifen wollen, in Hinblick auf die Vertrauenswürdigkeit einschätzen können
- Rechte müssen nicht nur für einzelne Profil-Attribute, sondern auch für Kategorien oder Gruppen von Attributen definierbar sein; die gewünschte Granularität ist nicht immer vorgesehen
- Eine einfache Zurückziehbarkeit vergebener Rechte ist oft nicht möglich
- Die Festlegung von Rechten ist mit einem gewissen Aufwand, es ist wohl nicht realistisch dies von jedem Benutzer zu erwarten

Daher ist bei der Administration von Zugriffsrechten ein flexiblerer Ansatz notwendig, z.B. in Form einer Aushandlung von Rechten des Benutzerprofilagenten mit dem Dienst-Agenten, der einen Zugriff anfordert. Dies muss unter Berücksichtigung der Verwendung der Daten (Zweckbindung), unter dem Grundsatz der Datensparsamkeit und transparent für den Benutzer erfolgen. Mit den bestehenden Verfahren ohne zusätzliche Unterstützung ist dies nicht in sinnvoller Weise realisierbar.

4.5 XML-basierte Verfahren

Seit der Entwicklung von XML [XML00] zu einem wichtigen Standard zum Datenaustausch in heterogenen Umgebungen sind einige XML-basierte Ansätze zu Zugriffskontrolle entstanden, die in diesem Abschnitt diskutiert werden. Es geht dabei darum, Zugriffsrechte in einem XML-Schema auszudrücken. Dies bietet sich insbesondere auch für die Verwaltung von Benutzerprofilen an, da XML-Dokumente sowohl Rechner-verarbeitbar als auch für menschliche Benutzer verständlich sind, und dies daher die Transparenz für Benutzer bei der Administration von Zugriffskontrolle verbessern kann.

4.5.1 Zugriffskontrolle für XML Dokumente

Das Ziel von XACL (XML Access Control Language, [KuHa00a, KuHa00b]) ist es, XML-Dokumente mit einem Zugriffsschutzmechanismus zu versehen, insbesondere auch um einen sicheres Aktualisieren von XML-Datenbeständen zu realisieren. Jedem XML-Dokument wird eine sogenannte „policy“ zugeordnet, die die Zugriffsrechte auf das

Dokument in XACL in Form einzelner Regeln spezifiziert. Abb. 6 (nach [KuHa00a, KuHa00b]) zeigt ein Beispiel für eine solche Zugriffsregel.

```
<policy>
  <xacl>
    <object href="/profile/demographic/email"/>
    <rule>
      <acl>
        <subject>
          <uid>Amazon Agent</uid>
        </subject>
        <action name="read" permission="grant">
          <provisional_action name="log"/>
        </action>
        <action name="write" permission="deny"/>
      </acl>
    </rule>
  </xacl>
</policy>
```

Abb. 6: XACL Beispiel

Es gibt folgende Menge von Zugriffsrechten, hier „Aktionen“ genannt: {read, write, create, delete}. Es ist sowohl explizites Erlauben als auch Verbieten von Zugriffen für Teile von XML-Dokumenten vorgesehen. Die Zugriffe können mit einem Parameter versehen werden, der angibt, ob die Rechte nach oben bzw. unten im XML-Baum propagiert werden sollen. Es ist auch die Angabe einer Rolle als Subjekt möglich, damit können Zugriffsrechte vergleichbar zu RBAC spezifiziert werden.

XACL enthält als Erweiterung traditioneller Zugriffskontrolle sogenannte „Provisional Actions“ [KuHa00b]. Zugriffe können dabei abhängig von einer „Provision“ gemacht werden, d.h. Zugriffsanfragen können mit einer zusätzlichen Bedingung verknüpft werden, die erfüllt sein muss, um den Zugriff zu erlauben. Bisher ist folgende Menge von Provisions vorgesehen: {write, create, delete, transform, log, verify, encrypt}, wobei die drei letzteren folgende Semantik haben:

- “log”: Protokollierung der Authorisierungsentscheidung und/oder Zugriffen
- “verify”: Überprüfung des Zugreifers mittels einer digitalen Signatur
- “encrypt”: Aktion ist nur erlaubt, wenn das zu lesende Objekt verschlüsselt wird

Die Menge der Provisions kann erweitert werden. Damit könnten sich z.B. Bedingungen wie „Leseoperation wird nur gestattet, wenn der Zugreifer einer Nutzungsbedingung zustimmt“ oder „Zugriff auf Kreditkartendaten werden nur erlaubt, wenn die Daten verschlüsselt übertragen werden“ realisieren lassen.

Zu XACL vergleichbare Systeme sind der Ansatz von Damiani et.al. [DVPS00], sowie *Author-X* [BCF01], wobei bei letzterem der Schwerpunkt mehr auf einer Integration von Benutzer-Authentifikation, Verschlüsselungsverfahren und dem Ablauf liegt, als der Spezifikation von Zugriffsrechten. XACL oder eines der anderen Verfahren könnte in unserem Szenario interessant sein, da die Benutzerprofile in Abschnitt 2.1.3 als XML-Dokument modelliert wurden. Aus der Sicht der Zugriffskontrolle bieten sie aber

im wesentlichen nur ein anderes Realisierungsschema bekannter Verfahren, mit der Ausnahme der Provisions bei XACL.

Alle angesprochenen Projekte benutzen zur Adressierung von Teilen von XML-Dokumenten den W3C Standard XPath [XPa99]. Dabei wird die hierarchische Struktur von XML abgebildet, indem einzelne Ebenen im XML-Baum durch ein „/"-Symbol getrennt werden. Ein Beispiel: Um die Email-Adresse im Profil in Abb. 1 anzusprechen, müsste das Objekt „/profile/demographic/email" (vgl. Beispiel in Abb. 6) adressiert werden. Damit können beliebige Teile eines XML-Dokumentes adressiert werden und somit eine flexible Granularität von Objekten, die auch bei der Verwaltung von XML-Benutzerprofilen notwendig ist, erreicht werden.

4.5.2 Digital Rights Management

Vergleichbar mit den soeben angesprochenen Ansätzen zur Zugriffskontrolle auf XML-Dokumente sind Verfahren des „Digital Rights Managements". *Digital Rights Management (DRM)* behandelt dabei die Spezifikation von Rechten, Bedingungen und Konditionen für den Gebrauch digitaler Inhalte [Xrml00]. Das Ziel dabei ist es, den Handel von digitalen Medien zu fördern und dabei die Urheber-Rechte der Rechteinhaber zu schützen. Es gibt mehrere (konkurrierende) Ansätze, darunter *Open Digital Rights Language (ODRL)* (www.odrl.net) und *eXtensible rights Markup Language (XrML)* (www.xrml.org, [Xrml00]).

Die Projekte behandeln dabei insbesondere auch die Prozesse und erforderlichen Software-Komponenten für eine sichere – und unabstreitbare – Durchführung eines Kaufes und der Auslieferung von multimedialen Inhalten, was in dem hier betrachteten Szenario eher nicht so interessant ist. Es ist aber auch eine Methodik enthalten, um Zugriffsrechte in einer XML-Sprache ausdrücken zu können. Die Zugriffsrechte beinhalten bei DRM u.a. „play", „display" oder „print", sind aber erweiterbar. Ein wichtiger und interessanter Punkt dabei ist, dass Zugriffsrechte mit Einschränkungen („constraints") versehen werden können. Damit lassen sich u.a. folgenden Arten von Restriktionen formulieren:

- nach Benutzern oder Benutzergruppen
- nach zeitlichen Einschränkungen (z.B. nur über einen gewissen Zeitraum)
- nach räumlichen Gesichtspunkten (z.B. nach Länder) oder auch nach IP-Adressen etc.

Dies ist auch bei Benutzerprofilverwaltung interessant. Damit lassen sich eventuell Einschränkungen wie „Lesen ist erlaubt, die Information darf aber nicht weitergegeben werden" formulieren. Enthalten sind auch Modelle zur Abbildung von Rechteinhabern sowie der Administration von Rechten.

Die Ansätze für DRM sind zwar sehr auf multimediale Inhalte ausgerichtet, z.B. durch Integration von „Watermarking"-Mechanismen zur unsichtbaren Kennzeichnung von digitalen Medien, Ideen wie die Formulierung von Nutzungs-Restriktionen lassen sich aber auch für die Verwaltung von Rechten in bezug auf Benutzerprofile einsetzen.

4.5.3 XML Tickets

Fujimura et.al. beschreiben in [FNS99, FuNa98] ein XML-Schema, mit dessen Hilfe man „elektronische Tickets“ modellieren kann (vgl. Beispiel in Abb. 7, aus [FNS99]). Ein *XML Ticket* ist dabei ein digitales Medium, das ein bestimmtes Recht des Inhabers des Tickets garantiert. Als Anwendungsgebiete werden u.a. Software Lizenzen, Zugriffsrechte für Ressourcen oder Eintrittskarten genannt.

```
<SignedDescription>
  <Ticket typeID="eventTicket" ticketID="001234">
    <IssuerID fingerprint="..."/>
    <OwnerID fingerprint="..."/>
    <Validity>
      <NumberOfTimes>ONCE</NumberOfTimes>
      <ValidPeriod>2001-10-03</ValidPeriod>
    </Validity>
    <View resource="http://ticket.ntt.co.jp/ticket1.gif"/>
    <Promise>
      <Place>Boston Symphony Hall</Place>
      <Seat>H24</Seat>
    </Promise>
  </Ticket>
  <Signature>...</Signature>
</SignedDescription>
```

Abb. 7: Beispiel XML Ticket

Ein XML Ticket definiert eine Zusicherung des Ausstellers des Tickets, dass der Ticket-Inhaber ein spezifiziertes Versprechen oder Recht besitzt. Der Ansatz schlägt ein „general-purpose digital ticket framework“ vor, bei dem verschiedene Charakteristikas von Tickets wie Anonymität, Übertragbarkeit, Verfahren bei der Einlösung des Tickets und einmalige oder mehrfache Gültigkeit abgebildet werden können. Das Ticket wird vom Aussteller digital signiert (vgl. dazu auch die Ausführungen zu XML Signature in Abschnitt 5.2.2). Insbesondere diese Signierung der XML Tickets ist für eine Benutzerprofilverwaltung interessant, da damit fälschungssichere Rechte, z.B. zum Zugriff auf bestimmte Profilattribute, ausgegeben werden könnten.

4.5.4 FIRM

Einen Ansatz, der zwar nicht XML verwendet, aber von der Zielsetzung und Ausrichtung her vergleichbar zu den XML-basierten Verfahren zu DRM ist, bietet das Projekt *FIRM (Framework for Interoperable Rights Management)* [RW97a, RW97a, Rös97]. Dabei wurde ein Modell für Sicherheit und Zugriffskontrolle in offenen Umgebungen mit Hilfe von elektronischen Verträgen zwischen Kommunikationspartnern entwickelt. FIRM geht nicht von einem Informationszugriffs-Paradigma aus, sondern von einer Verwaltung von Beziehungen („relationsship management“) und der Anwendung eines Modells für (elektronische) Verträge darauf. Die zu schützenden Objekte werden von den Zugriffsrechten darauf getrennt, wobei letztere in Form von Beziehungsobjekten

(„relationsships objects“, auch „commpacts“ in dem Modell genannt) verwaltet werden, die Verweise auf „echte“ Verträge darstellen.

Das Framework besteht aus zwei Teilen:

- Domänen-unabhängige Sprache bzw. Objektmodell zur Repräsentation von generischen Prinzipien von Verträgen
- Format zur Spezifikation von (Domänen-abhängigen) Zugriffsrechten

FIRM ist damit selbst keine Sprache, um Zugriffsrechte auszudrücken, sondern stellt den Rahmen dafür bereit.

Die Möglichkeit einer konkreten Anwendbarkeit von FIRM in dem betrachteten Szenario ist nicht so einfach zu beurteilen, da das Modell sehr abstrakt gehalten ist, aber eine Idee, weniger von Zugriffen und Zugriffsrechten, sondern mehr von der Konzeptualisierung der Beziehungen zwischen den Interaktions-Partnern auszugehen, ist sicherlich auch im Bereich Benutzerprofilverwaltung sinnvoll.

4.6 Bewertung

Wie bei der Herleitung der Anforderungen in Kapitel begründet, braucht man in dem betreffenden Szenario ein Zugriffskontrollsystem, um grundsätzlich die Fragestellung zu entscheiden, welcher Dienst auf welche Teile des Benutzerprofils wie zugreifen darf. Die verschiedenen Modelle und Strategien der Zugriffskontrolle haben dabei unterschiedliche Eigenschaften, auf die jeweils in den einzelnen Teilabschnitten hingewiesen wurden.

Ein Hauptproblem beim Einsatz der bestehenden Verfahren zur Zugriffskontrolle für dezentrale Benutzerprofile ist, dass voraus gesetzt wird, dass der Eigentümer der Daten – also der Benutzer – Zugriffsrechte für einzelne Subjekte, hier den Dienst-Agenten, vergibt. Alternativ werden wie bei RBAC Subjekte in Rollen oder Gruppen eingeteilt. Es stellt sich dabei jedoch die Frage, wie der Benutzer damit umgehen soll, da es nicht praktikabel erscheint, für alle Attribute und zugreifende Subjekte einzelne Zugriffsrechte oder Rollenzuordnungen festzulegen. Auch sind dem Administrator nicht unbedingt die Dienste bzw. deren Vorgehensweise bei der Verarbeitung persönlicher Daten, bekannt, so dass eine Zugriffskontrolle z.B. in Abhängigkeit der Verwendung der Daten mit den bestehenden Systemen nicht zu realisieren ist. In Abschnitt 5.4 wird das „Platform for Privacy Preferences Project“ vorgestellt, dass versucht, Datenschutzpraktiken von Firmen und Institutionen zu formalisieren.

Fehlende Aspekte im Detail bei den meisten Systemen sind insbesondere:

- Bei einem Zugriff auf personenbezogenen Daten ist der Zweck des Zugriffs sehr wichtig und muss abgebildet werden können
- Keine Modellierung des Rechts „Weitergabe von Daten“
- Keine Aushandlung oder Verhandlung von Rechten
- Keine Möglichkeiten, Zugriffe als „verpflichtend“ oder „optional“ zu kennzeichnen, wie dies z.B. bei Web-Formularen üblich ist
- Optionen bei den Zugriffsrechten wie „wenn notwendig“ oder „wenn möglich“

- Alternativen oder Abhängigkeiten in Zugriffsanfragen sind nicht vorgesehen, z.B. für Zahlungsinformationen: „Zugriff auf Daten Bankverbindung zwecks Lastschrift oder Kreditkarte“
- Keine (einfach zu realisierende) inhaltliche Gruppierung von Attributen (z.B. Strasse und Hausnummer)
- Keine Möglichkeiten, eine notwendige Übertragung über eine gesicherte Verbindung abzubilden
- Keine Berücksichtigung von Aspekten des Identitätsmanagements, wie z.B. Anonymisierung oder Verwendung von Pseudonymen

Die betrachteten Zugriffsverfahren auf Basis von XML erscheinen prinzipiell gut geeignet, Zugriffsrechte für Benutzerprofile abzubilden, da Benutzerprofile in XML modelliert werden können und damit eine Zugriffskontrolle für XML-Dokumente anwendbar ist. Allerdings stellen sich dabei genauso wie bei den andere Verfahren die angesprochenen Probleme. Eine Modellierung in einer XML-Sprache kann zu Absicherungs- und Transparenzzielen beitragen, z.B. durch eine digitale Signierung von in Form von XML Tickets ausgegeben Zugriffsrechten.

Eine Umsetzung von gesetzlichen Rahmenbedingungen ist zum Teil durch Zugriffskontrolle gegeben. Datensparsamkeit kann z.B. bei den meisten Verfahren durch eine Grundeinstellung „kein Zugriff“ und Gewährung expliziter Zugriffsrechte für vertrauenswürdige Subjekte realisiert werden. Allerdings ist eine Modellierung von Zweckbindung nur ansatzweise bei einigen Verfahren vorhanden.

Es fehlt auch an einer Integration in eine Umgebung mit autonom intergierenden Agenten. Dabei spielen auch die Prozesse und Abläufe beim Datenzugriff eine stärkere Rolle als bei statisch festzulegenden Zugriffsrechten vorgesehen. Bei einer Aushandlung zwischen Agenten kann sich der Kontext eines Zugriffs ändern, was von einem Administrator von Zugriffsrechten kaum vollständig berücksichtigt werden kann. Gerade im Agenten-Bereich wurden Fragen von Zugriffskontrolle und Privatheit bisher wenig untersucht.

Interessante Aspekte bei den vorgestellten Verfahren hinsichtlich einer dezentralen Verwaltung von Benutzerprofilen unter Beachtung von Privatheit sind insbesondere:

- Integration eines formalen Modells für Zweckbindung und andere bei Betrachtung von Privatheit relevanter Aspekte in dem Ansatz von S. Fischer-Hübner (Abschnitt 4.3.4)
- Zugriffkontrolle in Abhängigkeit von Bedingungen, wie z.B. der Protokollierung von Zugriffen in Form von „Provisional Actions“ bei XACL (Kapitel 4.5.1)

Ein Zugriffskontrollsystem kann nur wenig zu Identitätsmanagement oder Anonymisierung beitragen. Dazu wurden Anwendungen entwickelt, die im folgenden Kapitel behandelt werden.

5 Privacy Enhancing Technologies (PET)

You have zero privacy anyway, get over it!

Scott McNealy, CEO Sun Microsystems (25.01.1999)

Dieses pessimistische Zitat drückt eine vorhandene allgemeine Unsicherheit bezüglich der Privatheit im Internet aus, es gibt aber durchaus Systeme und Anwendungen, die eine Verbesserung erreichen. Im diesem Kapitel sollen diese Anwendungen untersucht werden, insbesondere dahingehend, ob sie für eine Agenten-basierte Verwaltung von Benutzerprofilen geeignet sind.

5.1 Kategorisierung

Privacy Enhancing Technologies (PET) sind Anwendungen, die die Privatheit von Benutzern und deren Daten im Internet verbessern sollen. Üblicherweise werden diese Systeme in folgende Gruppen aufgeteilt [Cra00a]:

- Verschlüsselungs- und Filtersysteme
- Verfahren zur Anonymisierung und Pseudonymisierung
- „Policy Tools“: Anwendungen, die es Diensteanbeitern und Benutzern erlauben, Praktiken im Bezug auf Privatheit von Diensten offenzulegen und auszuwerten

Diese Anwendungen erscheinen geeignet, zumindest einen Teil der Anforderungen aus Kap. 3.5 zu erfüllen. Anonymisierung, Pseudonymisierung und Verschlüsselung sind wichtig für Vertraulichkeit und die Erfüllung der Identitätsziele. Policy Tools können zu allen Anforderungen, insbesondere auch zu Absicherung- und Transparenzzielen beitragen.

Im folgenden soll daher genauer untersucht werden, inwieweit diese Anwendungen geeignet sind, die Problemstellung der Gewährleistung der Privatheit bei Agenten-basierter Verwaltung von Benutzerprofilen zu lösen.

5.2 Verschlüsselungs- und Filtersoftware

5.2.1 Verschlüsselung

Mit Hilfe von *Kryptographie* (Verschlüsselungsverfahren) ist man in der Lage, Daten in eine Form zu transformieren, die ein Abhören durch Angreifer bei der Kommunikation über offene Netzwerke unmöglich, oder zumindest unpraktikabel aufwändig macht [Kyus98]. Kryptographie soll also eine gesicherte Übertragung über unsichere Netze ermöglichen. In unserem Szenario betrifft dies z.B. die Kommunikation der Benutzerprofil- und Community-Agenten oder auch den Datentransfer vom Browser des Benutzers zu einem (Server-seitigen) Dienst zur Profilverwaltung. Eine Verschlüsselung

bei der Kommunikation macht die anderen besprochenen Mechanismen, z.B. zur Zugriffskontrolle, nicht überflüssig, sondern wäre ergänzend dazu.

In der Kryptographie gibt es zwei verschiedene Methoden zur Verschlüsselung:

- *asymmetrische* Verschlüsselung (*Public-Key-Verfahren*): eine Nachricht wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und somit ist (nur) der intendierte Empfänger in der Lage ist, die Nachricht zu dekodieren (mit seinem privaten Schlüssel)
- *symmetrische* Verschlüsselung (*Private-Key-Verfahren*): es wird nur ein einziger Schlüssel für Ver- und Entschlüsselung verwendet wird

Symmetrische Verfahren haben das Problem des Schlüsselaustausches: Wie kommen alle Kommunikationspartner in den Besitz des notwendigen Schlüssels? Für eine Anwendung im Internet werden daher oft asymmetrische Verfahren verwendet, dessen Nachteil ein größerer Aufwand bei der Kodierung bzw. Dekodieren im Vergleich zu symmetrischen Verfahren ist.

Bekannte und recht verbreitete Anwendungen von Verschlüsselung sind *Pretty Good Privacy (PGP)* [Gar94] für die Verschlüsselung von Emails, sowie „Secure Socket Layer". *Secure Socket Layer (SSL)* [FKK96] ist ein von Netscape entwickeltes Verfahren zur gesicherten Übertragung zwischen Web-Browser und -Server, das asymmetrische und symmetrische Kryptographie kombiniert. Mit Hilfe eines Public-Key-Verfahrens wird dabei ein Sitzungsschlüssel generiert, der dann für die (symmetrische) Verschlüsselung der eigentlichen Datenübertragung verwendet wird. Insbesondere Kreditkartendaten werden im WWW oft über SSL übertragen. Benutzer haben (zu Recht) mehr Vertrauen in SSL im Vergleich zu ungesicherten Verbindungen.

Eine Verschlüsselung durch SSL (bzw. das etwas allgemeinere Transport Layer Security (TLS) oder vergleichbarer Verfahren) kann eine vertrauliche Übertragung gegenüber unbefugten Dritten von Daten, z.B. vom Speicherort der Benutzerprofile zum Dienst, der die Daten nutzt, sicherstellen. Dies löst somit einen Aspekt der Vertraulichkeitsanforderungen. Allerdings muss auf der anderen Seite durch die benötigten Zertifikate und digitale Signaturen die Identität des Benutzers aufgedeckt werden, so dass die Privatheit in Hinblick einer anonymen Kommunikation abnimmt.

5.2.2 Authentifizierung, Zertifikate und digitale Signaturen

Bei allen Public-Key-Verfahren stellt sich folgendes, fundamentale Problem: Woher weiss man, dass der öffentliche Schlüssel wirklich demjenigen gehört, der behauptet dessen Eigentümer zu sein? Eine Lösung dafür ist die *Zertifizierung* von Schlüsseln. Ein *digitales Zertifikat* ist dabei eine Bescheinung einer unabhängigen und vertrauenswürdigen dritten Partei, der *Zertifizierungsstelle* (certification authority, CA), die die Korrektheit der im Zertifikat enthaltenen Daten, also insbesondere der Name und andere Daten des Inhabers des Zertifikats und die Zuordnung des öffentlichen Schlüssels zu diesem Zertifikat, korrekt sind. Diese Bescheinigung erfolgt mit Hilfe einer *digitalen Signatur*.

Dazu wird eine Nachricht vom Absender mit seinem privaten Schlüssel verschlüsselt, so dass der Empfänger durch Anwendung des dazugehörigen öffentlichen Schlüssels prüfen kann, ob die Nachricht wirklich von dem Inhaber des privaten Schlüssels – bzw. der betreffenden digitalen Signatur – stammt. Es gibt auch im XML-Umfeld dazu einen entsprechend Standard, *XML Signature* [XSig01], um XML Dokumenten mit einer digitalen Signatur zu versehen. Dies könnte in unserem Szenario verwendet werden, um das (mit XML modellierte) Benutzerprofil bzw. oder Teile davon zu signieren.

Die digitale Signatur ist seit 2001 in Deutschland rechtsgültig, d.h. rechtlich ist eine digitale Signatur unter bestimmten Voraussetzungen einer eigenhändigen Unterschrift gleichgestellt. Die Anforderungen, die dabei gestellt werden, sind im Signaturgesetz, sowie der Signaturverordnung geregelt. In welchen Fällen die Gleichstellung zutreffen soll, ist im Rahmen des „Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäfteverkehrs“ vom 1.8.2001 festgelegt worden. Es ist daher zu erwarten, dass die digitale Signatur an Bedeutung und Verbreitung gewinnt, was auch die Voraussetzung wäre, dass digitale Signaturen für eine Authentifizierung der (End-)Benutzer in unserem Szenario eingesetzt werden können.

Dazu ist der Aufbau einer *Public Key Infrastructure (PKI)* nötig, was ein allgemeiner Begriff für eine technische (und organisatorische) Infrastruktur für das Ausstellen, Verteilen und Verwalten von (öffentlichen und privaten) Schlüsseln für asymmetrische Kryptographie und den dazugehörigen Zertifikaten ist.

Mit Hilfe einer digitalen Signatur kann auch die Zurechenbarkeit gewährleistet werden, was zu den Absicherungszielen gehört. Z.B. könnte so ein E-Commerce Agent die Bestellung eines Benutzers durch den Nachweis einer entsprechend digital signierten Nachricht belegen. Darüber hinaus bieten digitale Signaturen auch eine Möglichkeit, die Integrität von Nachrichten zu gewährleisten.

Als weiteres, konkretes Beispiel für ein Authentifikations-System sei das auf symmetrischer Verschlüsselung basierende *Kerberos* [SNS98] erwähnt. Es dient der Authentifikation von Subjekten für den Zugriff auf verschiedene Netzwerkdiensten, sowie der Generierung von (zeitlich beschränkten) Sitzungsschlüsseln. Ein Benutzer oder eine System-Komponente – bei Kerberos „Principal“ genannt – authentifiziert sich dazu bei einem zentralen Kerberos-Server und erhält dabei ein „Ticket“, das nur für einen Dienst (z.B. Datei-Server) gültig ist. Der Kerberos-Server muss dazu entsprechend abgeschirmt und geschützt werden. Im Gegensatz zu einem Zugriffsausweis der Zugriffskontrolle dient ein Kerberos-Ticket nur authentifizierten Nutzung eines Dienstes [Eck01]. Nachteilig bei dem Versuch der Anwendung von Kerberos auf das betrachtete Szenario ist die Abhängigkeit von einem zentralen Server.

Es gibt auch einen Ansatz, Authentifizierungs-Dienste mit Hilfe von XML zu beschreiben, nämlich die *Security Assertion Markup Language (SAML)* (www.oasis-open.org/committees/security/). Das Ziel dabei ist es, die Interoperabilität von E-Commerce Anwendungen durch Bereitstellung eines XML-Schemas zum Austausch von Authentifizierungs- und Authorisierungsinformationen zu verbessern. Insbesondere geht

es dabei auch um die Spezifikation der Delegation von Rechten, um Benutzer zu authentifizieren [Wag01].

Neben der Unterstützung der oben erläuterten Methoden zur Verschlüsselung durch digitale Zertifikate, braucht man unabhängig davon Verfahren zur Authentifizierung von Benutzern und Agenten in unserem Szenario. Eine E-Commerce Anwendung muss z.B. zweifelsfrei überprüfen können, welche Person eine Bestellung abgegeben hat. Auf der anderen Seite braucht der Benutzerprofilagent eine Möglichkeit zur Kontrolle, dass Profildaten wirklich an denjenigen Dienst übermittelt werden, für den sie bestimmt sind.

5.2.3 Filtersoftware

Eine weitere Anwendungsklasse von Privacy Enhancing Technologies ist *Filtersoftware*, die versucht, die technischen Möglichkeiten zur Verfolgung von Benutzeraktionen z.B. über Cookies oder „Web Bugs“[10] zu verhindern. Sogenannte „Cookie Cutters“ erlauben es, die Verwendung von Cookies zu verhindern bzw. zu kontrollieren und können damit die Privatheit von Benutzern etwas verbessern. Allerdings gibt es auch andere Möglichkeiten als Hilfe von Cookies, das Benutzerverhalten nachzuverfolgen und aufzuzeichnen, so dass diese Werkzeuge nur bedingt geeignet sind und keinesfalls vollständig für den Schutz der Privatheit dienen können.

In diesen Bereich von Werkzeugen fallen auch Anwendungen zum Filtern von Internet-Inhalten, in erster Linie zum Jugendschutz (Child Protection Software), was aber in dem hier betrachteten Szenario nicht relevant ist.

5.3 Anwendungen zur Anonymisierung

Als nächstens sollen in diesem Abschnitt Möglichkeiten zur Anonymisierung untersucht werden, die Aspekte der Identitäts- und Vertraulichkeitsanforderungen betreffen.

5.3.1 Anonymisierungs-Proxies

Eine relativ einfache Möglichkeit, anonym auf Web-Seiten zuzugreifen, wird durch *Anonymisierungs-Proxies* wie z.B. www.anonymizer.com realisiert. Der Benutzer kann dabei über ein Web-Formular eine Web-Adresse eingeben, die dann vom Proxy abgerufen wird. Damit greift der Benutzer (nur) auf den Proxy, statt direkt auf den Dienst zu und kann somit „Datenspuren“ (z.B. seine IP-Adresse in den Log-Dateien des Web-Servers) vermeiden. Zusätzlich entfernt der Proxy weitere potentiell personenbezogenen Daten (wie z.B. Cookies) in den Headern der Web-Anfrage. Der Anonymisierungs-Proxy muss dabei vertrauenswürdig sein.

Mit Hilfe von Anonymisierungs-Proxies kann das Identitätsziel einer anonymen Kommunikation und eine Verbesserung der Vertraulichkeit erreicht werden. Dies könnte für eine anonymisierte Übermittlung von Profildaten genutzt werden, so dass z.B. Interessen ausgewertet werden können, ohne dass eine Zuordnung zu Web-Zugriffen

---

[10] Web Bugs sind kleine, für den Benutzer nicht sichtbare, Bilder auf Web-Seiten, dessen Zweck es ist, den Zugriff auf Web-Seiten von Benutzern verfolgen zu können

oder anderen Aktionen eines Benutzers gemacht werden kann. Allerdings bieten Anonymisierungs-Proxies gegenüber Angreifern, die die Kommunikation in einem offenen Netz abhören, wenig Schutz, weil durch Beobachtung des Nachrichtenverkehrs eine Zuordnung von eingehenden zu ausgehenden Nachrichten am Proxy erfolgen kann.

5.3.2 Crowds

Ein etwas anderer Ansatz zur Anonymisierung ist *Crowds* [ReRu97]. Dabei werden die Web-Anfragen einzelner Benutzer in einer Menge von Crowds-Benutzern „versteckt". Eine Web-Anfrage wird nicht an den betreffenden Web-Server direkt, sondern an einen zufällig ausgewählten, anderen Crowds-Benutzer – bzw. dessen Crowds-Client, „Jondo" genannt – geschickt. Die Anfrage durchläuft damit zunächst mehrere Jondos anderer Teilnehmer und ein Diensteanbieter kann Anfragen nicht mehr einem bestimmten Benutzer zuordnen.

Ein Vorteil von Crowds ist es, dass keine zentrale Komponente wie etwa ein Anonymisierungs-Proxy erforderlich ist. Auch könnten in unserem Szenario die Benutzerprofilagenten die Rollen der Jondos einnehmen. Im Vergleich zu den anschließend auf dem Mix-Konzept basierenden Verfahren bietet Crowds eine bessere Performance. Allerdings kann ein Angreifer, der den Kommunikationsverkehr abhört, durch eine zeitliche Verkettung von Nachrichten eine Verfolgung von Nachrichten erreichen. Crowds bietet also aus kryptographischer Sicht keine perfekte Anonymisierung. Auch erzielt Crowds nur eine Sender- und keine Empfängeranonymität. Ein Nachteil ist auch, dass eine genügend große Menge von (aktiven) Benutzern vorhanden sein, um eine Anonymität zu gewährleisten.

5.3.3 Mix-Konzept

Viele Systeme in der Literatur basieren auf dem *Mix-Konzept* [PPW88, Pfi90], das auf David Chaum zurückgeht [Cha81]. Dabei wird die Kommunikationsbeziehung zwischen Sender und Empfänger einer Nachricht durch Knoten im Netzwerk, sogenannte *Mixe* verborgen, die eine Verkettung von Nachrichten verhindern. Ein Mix speichert dabei genügend viele Nachrichten von verschiedenen Absendern, kodiert diese um, so dass keine direkte Zuordnung mehr zu den ursprünglichen Nachrichten mehr möglich ist, und verändert die Reihenfolge der ausgehenden Nachrichten. Dabei entstehen Verzögerungszeiten in den Mixen, was auch notwendig ist, um zu verhindern, dass Angreifer, die die Kommunikationsbeziehungen abhören, aus der zeitlichen Abfolge von (eingehenden und ausgehenden) Nachrichten Rückschlüsse ziehen können.

Das Umkodieren einer Nachricht in einem Mix geschieht mit Hilfe asymmetrischer Verschlüsselung, wobei jeder Mix im Netzwerk die Nachricht – bzw. dessen „äußere" Schicht – mit seinem privaten Schlüssel entschlüsselt und an den nächsten Mix weiterschickt („layered" Public-Key-Verschlüsselung). Dazu muss der Sender die zu mixende Nachricht entsprechend vorbereiten, d.h. mit den öffentlichen Schlüsseln der nachfolgenden Mixe verschlüsseln.

Falls nicht genügend Nachrichten vorhanden sind, um eine Zuordnung von eingehenden und ausgehenden Nachrichten an einem Mix zu verhindern, müssen „dummy“ Nachrichten erzeugt werden, um die Verzögerungszeit in den Mixen bzw. die Laufzeit einer Nachricht zu minimieren. Auch sollte dabei sichergestellt werden, dass alle versendeten Nachrichten gleich groß sein, damit Außenstehende durch die Größe einer Nachricht nicht auf die Entfernung zum Empfänger schließen oder eine Zuordnung von ein- und ausgehenden Nachrichten vornehmen könnten.

Die Mix-Systeme können eine Unbeobachtbarkeit und Verdecktheit bei der Kommunikation erzielen. Der Nachteil davon ist, dass die mehrfache asymmetrische Verschlüsselung jeder Nachricht sehr aufwändig ist. Es gibt einige Ausprägungen dieser Systeme mit unterschiedlichen [Kes00], so dass eine Abwägung zwischen Performance und kryptographischer Sicherheit erfolgen kann.

Das Mix-Konzept bietet einen allgemeinen und gut untersuchten Ansatz von Unbeobachtbarkeit und Verdecktheit beim Nachrichtenaustausch in offenen Umgebungen. Es könnte damit die Kommunikation zwischen Benutzerprofil- und Diensteagenten anonymisiert werden. Neben der schlechten Performance, stellt sich auch das Problem, dass einzelnen Nachrichten in den Mix-Stationen verzögert werden, was bei synchroner Kommunikation nicht immer zumutbar ist.

Zu bemerken ist auch, dass anonymisierte Kommunikation konträr zu Verschlüsselungsverfahren mit digitalen Zertifikaten ist. So hat z.B. ein E-Commerce Agent bei einer Bestellung durch eine anonymisierte Nachricht keinen Nachweis über den Auftraggeber der Bestellung mehr. Auch stellt sich die Frage, wie der Benutzer mit Anwendungen dieser Art umgehen soll, da eine grundsätzliche anonyme Kommunikation wohl nicht sinnvoll ist und somit der Benutzer auswählen muss, wie mit welchem Dienst kommuniziert wird. Dies kann z.B. nicht von der Verwendung der Daten und dem Zweck des Zugriffs abhängig gemacht werden.

5.3.4 Realisierung von Mixen

Ein Nachteil der Verfahren, die auf dem beschriebenen, „klassischen“ Mix-Konzept beruhen, ist, dass sie für Email- bzw. asynchrone Kommunikation entwickelt wurden. Daher sind sie wegen der Verzögerungszeiten in den Mixen nicht für Echtzeit-Bedingungen, wie es z.B. für Community-Unterstützungssysteme erforderlich ist, geeignet. Die meisten Realisierungen[11] des Mix-Prinzips nutzen daher ein leicht modifiziertes Konzept [FeMa98], als Beispiele seien im folgenden „Onion Routing“ und in Abschnitt 5.3.6 das Produkt „Freedom“ der kanadischen Firma Zero-Knowledge System vorgestellt.

Beim *Onion-Routing* (www.onion-router.net) [GRS99] wird zunächst eine “Onion” gesendet, die zu einem Aufbau eines anonymen Kanals zwischen Sender und Empfänger dient. Eine Onion ist dabei eine Nachricht, die mit Schichten asymmetrischer

---

[11] Eine Übersicht zu verschiedenen Systemen ist z.B. auf den Web-Seiten des Projektes „Effiziente und skalierbare Realisierung von unbeobachtbarer und anonymer Kommunikation im Internet“ der TU Dresden unter www.inf.tu-dresden.de/~hf2/anon/ zu finden

Verschlüsselung versehen ist, wie in Abschnitt 5.3.3 erläutert wurde. Die Onion enthält außerdem die Adresse des nächsten Onion-Routers, der hier die Funktion einer Mix-Station einnimmt, sowie Schlüsselmaterial, das für eine nachfolgende Etablierung eines anonymen Kanals verwendet wird.

Bei dem Lauf durch das Netz wird nun die Onion Schritt für Schritt abgebaut, d.h. im jeweiligen Onion-Router entschlüsselt, und gleichzeitig der anonyme Kanal aufgebaut. Hierzu merkt sich jeder Onion-Router, woher er eine Onion erhalten hat und wohin er die verbleibende Onion geschickt hat und zusätzlich ein Kennzeichen, eine sogenannte „Pfad-ID". Empfängt ein Onion-Router Daten für eine bestimmte ID, so verschlüsselt er die erhaltenen Daten mit einem symmetrischen Kryptosystem, dessen Schlüssel er aus dem Schlüsselmaterial der Onion gewonnen hat [FeMa98].

Mit Hilfe eines der vorgestellten Anonymisierungsverfahren kann die Kommunikation sowohl gegenüber unbefugten Dritten als auch gegenüber nicht vertrauenswürdigen Diensten anonymisiert werden. Somit kann – in Kombination mit anderen Verfahren – eine Erfüllung des Identitätsziels einer anonymen Kommunikation sowie von Vertraulichkeitszielen erreicht werden.

5.3.5 Pseudonymität

Oftmals ist eine vollständige Anonymität nicht wünschenswert, da es z.B. für Personalisierungsdienste erforderlich sein kann, dass sich Benutzer gegenüber einem Dienst identifizieren, damit einzelne Aktionen, z.B. Webzugriffe, einem Benutzer zuordnen zu können. Um diese Funktionalität zu ermöglichen, werden Pseudonyme verwendet, vergleiche dazu auch die Ausführungen in Abschnitt 2.1.2. Eine Anwendung dazu ist *Lucent Personal Web Assitant (LPWA)* [GGK+99].

Benutzer identifizieren sich an einem LPWA Proxy Server. Dieser generiert automatisch und für den Benutzer transparent einen Benutzernamen und Passwort für jede Site, die der Benutzer besucht. Damit können Web-Sites Personalisierungs-Funktionen wahrnehmen und z.B. auch Benutzerinteressen auswerten, es ist aber nicht möglich, zwischen den Pseudonymen für verschiedene Server eine Beziehung oder einen Rückschluss auf die Identität des Benutzers herzustellen. Der LPWA Proxy stellt auch einen Anonymisierungs-Dienst dar, so dass Betreiber Web-Site auch nicht aus der IP-Adresse des Clients auf die Identität des Benutzers schließen können. Die Anonymisierungs-Funktionalität ist vergleichbar zu den eher einfachen Systemen der Anonymisierungs-Proxies (vgl. Abschnitt 5.3.1) und keine Realisierung eines Mix-Konzeptes.

LPWA oder vergleichbare Pseudonymisierungs-Dienste können Beschränkungen von Anonymisierungstools aufheben, ohne eine Preisgabe der Identität des Benutzers nötig zu machen. Es wird eine Implementierung des Persona-Konzepts bereitgestellt, mit Hilfe dessen Benutzer ein Identitätsmanagement durchführen können. Es wird das Problem gelöst, dass sich Benutzer nicht selber für Dienste virtuelle Identitäten erzeugen müssen, weil bei sehr vielen Benutzerkennungen der Überblick verloren gehen kann. Als weitere Besonderheit kann durch Erzeugen einer Pseudo-Email Adresse eine Herausgabe einer

(wahren) Email-Adresse vermieden werden. Eine Email-Adresse ist oft für Dienste erforderlich, erlaubt aber meist auch (eigentlich unerwünschte) Rückschlüsse auf die Identität des Benutzers bzw. birgt die Gefahr unerwünschter Werbe-Emails.

LPWA ist auch deshalb interessant, da nicht nur eine Anonymisierung auf Kommunikations-Ebene erfolgt, sondern auch Dienst-spezifische Benutzernamen und Email-Adressen erzeugt werden können

5.3.6 Freedom

Eine interessante Anwendung ist das Produkt *Freedom* von Zero-Knowledge Systems (ZKS) [BSG00, SaHa00]. Dabei wird versucht, einen Mix-basierten Anonymisierungsansatz mit einem etwas weitergehenden Konzept für Pseudonyme als bei LPWA, zu verbinden. Jeder Freedom-Benutzer erhält dabei eine Menge von Pseudonymen, hier „Nyms“ genannt, die zur Identifizierung bei verschiedenen Diensten genutzt werden können. Solange ein Benutzer Nachrichten unter dem gleichen Pseudonym durch das Freedom-Netz schickt, sind diese verkettbar, die „wahre“ Identität des Absenders ist aber geschützt [FeBe00]. Das Haupteinsatzgebiet der Nyms dürfte das pseudonyme Senden und Empfangen von E-Mail sein [FeBe00], das Grundprinzip läßt sich allerdings auch auf andere Aspekt des Identitätsmanagement anwenden.

Bei der Erzeugung von Nyms sind auch Funktionen zur Abrechnung für den Anbieter des Freedom Anonymisierungs-Dienstes mit integriert. Der Ablauf dabei ist [SaHa00]:

- Vertraulicher Kauf einer Seriennummer, die zum Erwerb eines sogenannten „Nym-Tokens“ berechtigt
- Übermittlung der Seriennummer an einen Token-Server einer vertrauenswürdigen dritten Partei, der (nach erfolgreicher Überprüfung) ein oder mehrere Nym-Tokens an den Benutzer aushändigt
- Erstellung eines Nyms auf einem Nym-Server mit Hilfe des Nym-Tokens

Bei diesem Nym-Erzeugungsprozess sind mehrere Parteien beteiligt, damit für den Anbieter des Dienstes eine Zuordnung eines Nyms zu einer Identität (z.B. über das verwendete Zahlungsverfahren) ausgeschlossen ist, und der Benutzer nicht einer einzigen Partei vertrauen muss.

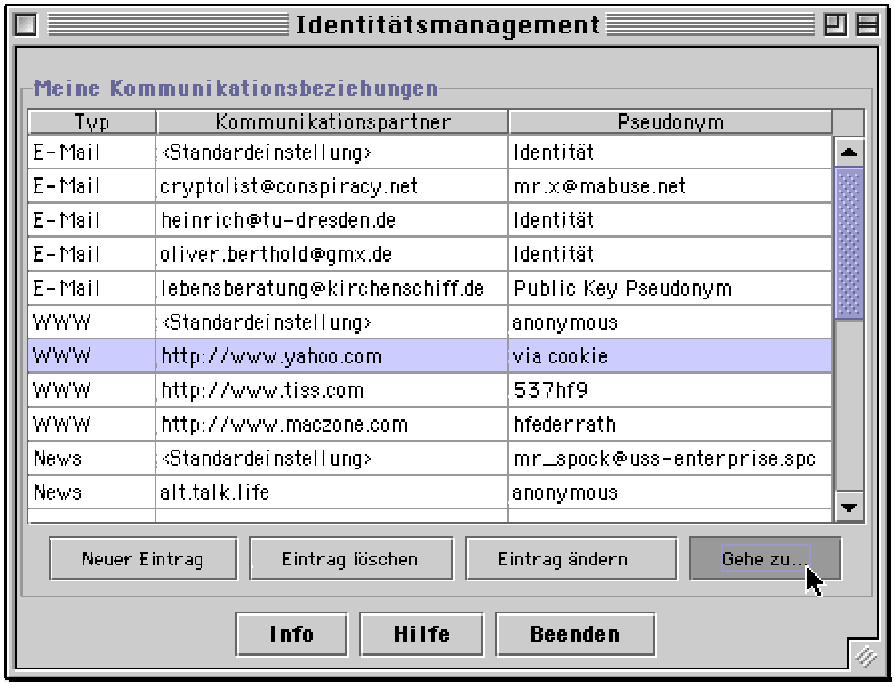

Abb. 8: Beispiel einer Oberfläche eines Identitätsmanagers

Eine Kombination von Anonymisierungsverfahren mit einem Konzept für Pseudonyme ist ein Baustein zur Realisierung von Identitäts- und Vertraulichkeitszielen. Auch ist das Verfahren zur Abwicklung des „Kaufes eines Pseudonyms“ interessant.

Ein grundsätzliches Problem ist die Handhabung der Pseudonyme, die bei Freedom, LPWA und vergleichbaren Ansätzen von den Benutzern selbst verwaltet werden müssen. Abb. 8 aus [FeBe00] zeigt dazu ein Beispiel, wie sich die Verwaltung der Pseudonyme für einen Benutzer präsentieren könnte. Es stellt sich dabei die Frage, ob eine Oberfläche dieser Art praktikabel für den (End-) Benutzer ist.

Außerdem wollen Benutzer nicht unbedingt manuell auswählen, sondern die Verwendung eines Pseudonyms oder den Zugriff auf ihre Daten soll abhängig von der Verwendungen der Daten oder den Datenschutzpraktiken eines Dienstes sein, wozu das nachfolgend behandelte „Platform for Privacy Preferences Project“ beitragen kann.

5.4 Platform for Privacy Preferences Project

„Policy Tools“ sollen Benutzer informieren, welche personenbezogenen Daten über sie gesammelt und wie diese Informationen verwendet werden und somit insbesondere auch die Transparanzziele der Anforderungen erfüllen. Als wichtigster und interessantester Vertreter dieser Art von Privacy Enhancing Technology wurde der Standard *Platform for Privacy Preferences (P3P) Project* [P3P00] vom World Wide Web Consortium (W3C) unter Beteiligung von Firmen wie AOL, IBM und Microsoft entworfen.

5.4.1 Motivation

Viele Web-Sites haben Informationen über ihre Praktiken in bezug auf Datenschutz und Privatheit in einer *Datenschutzerklärung* (engl. privacy policy) veröffentlicht. Diese Datenschutzerklärungen sind jedoch oft umfangreich und für einen Laien schwer verständlich und durchschaubar. P3P soll es Betreibern von Web-Sites ermöglichen, ihre Erklärungen in einem standardisiertem Schema in maschinen-lesbarer Form auf ihrem Server abzulegen. Die Formulierung der P3P Erklärung soll durch entsprechende Werkzeuge unterstützt werden.

Der Benutzer greift mit einem Client-seitigen Benutzeragenten, z.B. einem P3P-fähigen Web-Browser, auf eine Web-Site zu. Der Server antwortet mit seiner P3P Erklärung, die der Benutzeragent dann auswerten kann. Benutzer können damit ihre eigenen Präferenzen hinsichtlich Privatheit und Datenschutz mit den Erklärungen von Web-Sites abzugleichen, um zu entscheiden, ob die Site besucht werden soll oder nicht. Dazu werden vom Benutzer festgelegte oder ausgewählte Regeln ausgewertet.

P3P besteht aus folgenden Komponenten:

- Protokoll zum Austausch der P3P Erklärung
- Schema zur Beschreibung der Datenschutzerklärung
- Datenformat und Vokabular
- Regeln zur Auswertung der Erklärungen

Für den Austausch der P3P Erklärung gibt es zwei Möglichkeiten. Entweder es wird eine Erweiterung im HTTP Header verwendet oder der Dienstanbieter legt eine „Policy Reference“ Datei an der URL „/p3p.xml“ des Web-Servers ab. Diese Policy Reference Datei enthält dann Informationen darüber, welche P3P Datei für welchen Teil des Servers gültig ist. Eine Möglichkeit zur detaillierten Aushandlung der Datenschutzerklärung zwischen Client und Server war zwar in den ersten P3P Entwürfen angedacht, wurde aber letztendlich nicht im Standard aufgenommen, um diesen zunächst möglichst schlank zu halten.

5.4.2 Schema der Datenschutzerklärung

Eine P3P Datenschutzerklärung kann in einer XML-Form dargestellt werden, was im diesem Teilabschnitt anhand des Beispiels in Abb. 9 (nach [P3P00]) näher erläutert wird.

```
<POLICY xmlns="http://www.w3.org/2000/12/P3Pv1"
    discuri="http://www.catalog.example.com/Privacy/PrivacyPracticeShopping.html"
    opturi="http://catalog.example.com/preferences.html">
 <ENTITY>
 <DATA-GROUP>
   <DATA ref="#business.name">CatalogExample</DATA>
   <DATA ref="#business.contact-info.postal.street">4000 Lincoln Ave.</DATA>
   <DATA ref="#business.contact-info.postal.city">Birmingham</DATA>
   <DATA ref="#business.contact-info.postal.stateprov">MI</DATA>
   <DATA ref="#business.contact-info.postal.postalcode">48009</DATA>
   <DATA ref="#business.contact-info.postal.country">USA</DATA>
   <DATA ref="#business.contact-info.online.email">catalog@example.com</DATA>
  </DATA-GROUP>
 </ENTITY>
 <STATEMENT>
  <CONSEQUENCE>
    We tailor our site based on your past visits.
```

```
  </CONSEQUENCE>
  <PURPOSE><tailoring/><develop/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
   <DATA ref="#dynamic.cookies">
    <CATEGORIES><state/></CATEGORIES>
   </DATA>
   <DATA ref="#dynamic.miscdata">
    <CATEGORIES><preference/></CATEGORIES>
   </DATA>
  </DATA-GROUP>
 </STATEMENT>
<STATEMENT>
  <CONSEQUENCE>
    We use this information when you make a purchase.
  </CONSEQUENCE>
  <PURPOSE><current/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
   <DATA ref="#user.name"/>
   <DATA ref="#user.home-info.postal"/>
   <DATA ref="#user.home-info.telecom.telephone"/>
   <DATA ref="#user.home-info.online.email"/>
   <DATA ref="#dynamic.miscdata">
    <CATEGORIES><purchase/></CATEGORIES>
   </DATA>
  </DATA-GROUP>
 </STATEMENT>
 <STATEMENT>
  <CONSEQUENCE>
    At your request, we will send you carefully selected marketing
    solicitations that we think you will be interested in.
  </CONSEQUENCE>
  <PURPOSE>
   <contact required="opt-in"/>
   <customization required="opt-in"/>
   <tailoring required="opt-in"/>
  </PURPOSE>
  <RECIPIENT required="opt-in"><ours/><same/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
   <DATA ref="#user.name" optional="yes"/>
   <DATA ref="#user.business-info.postal" optional="yes"/>
   <DATA ref="#user.business-info.telecom.telephone" optional="yes"/>
  </DATA-GROUP>
 </STATEMENT>
</POLICY>
```

Abb. 9: Beispiel P3P Policy

Jede P3P Erklärung wird mit einem <POLICY> Auszeichnungselement eingeleitet. Dabei können eine natürlich-sprachliche Variante (Attribut „discuri“) der Erklärung, sowie eine URL einer Beschreibung für die Vorgehensweise für den Benutzer, um einer Datenerfassung zuzustimmen oder abzulehnen („opturi“), angegeben werden. Als nächstes wird die Entität beschrieben, die die personenbezogen Informationen sammeln und verarbeiten möchte, wozu das hierarchisch aufgebaute Datenformat von P3P zur Bezeichnung der Felder verwendet wird.

Die P3P Erklärung besteht dann aus einem oder mehreren „Statements“, die jeweils folgende Teilbereiche enthalten:

- <CONSEQUENCE>: Natürlichsprachlicher Text, der dem Benutzer angezeigt werden kann
- <PURPOSE>: Zweck der Erfassung von Benutzerprofildaten, sehr wichtig aus Sicht der Privatheit, <current/> bedeutet dabei z.B. die aktuell durchzuführende Aufgabe, die in der Regel vom Benutzer initiiert wurde, z.B. eine Suchanfrage
- <RECIPIENT>: Empfänger der Daten, z.B. auch eine dritte Partei
- <RETENTION>: Verfahrensweise bei der Einbehaltung der personenbezogenen Daten, z.B. <stated-purpose/> (nur im Sinne des angegebenen Zwecks), <indefinitely/> oder <legal-requirement/>
- <DATA-GROUP>: Bezeichnung der Profilattribute, die vom Dienst benötigt werden
- <CATEGORIES>: Hinweise für den Benutzer (bzw. dessen Agenten), wie die Daten verwendet werden

Während <PURPOSE> den grundsätzlichen, recht allgemeinen, Zweck der Datenerfassung spezifiziert, ermöglicht <CATEGORIES> eine genauere Angabe zur Unterscheidung inhaltlicher Aspekte in den Regeln. Das Beispiel in Abb. 9 enthält drei Statements. Der erste sagt aus, dass die Web-Site versucht, mit Hilfe von Cookies die Seiten zu personalisieren. Das zweite Statement spezifiziert die benötigten Informationen bei einem Kauf. Das abschließende Statement regelt die Weitergabe einiger Daten, wobei mit "required = …" angegeben werden kann, ob der Benutzer die Möglichkeit hat, diesem Zweck mittels „opt-in" oder „opt-out" zustimmen. „opt-in" bedeutet dabei, dass der Benutzer explizit einer Datenerfassung zustimmen muss, bei „opt-out" muss der Benutzer einer Verarbeitung von Daten explizit widersprechen. Diese Unterscheidung ist bei Verwaltung personenbezogener Daten grundsätzlich sehr wichtig. Aus Sicht der Privatheit wird in der Regel eine vorgegebene Einstellung im Sinne von „opt-in" gefordert.

Das P3P Datenformat bildet die wichtigsten Elemente eines Benutzerprofils ab, es stellt keine vollständige Struktur eines Benutzerprofils dar, kann aber erweitert werden, um Attribute abbilden zu können, die nicht im P3P Standard vorgesehen sind.

5.4.3 Regeln zur Auswertung

Diese Datenschutzerklärung kann von Benutzeragenten anhand von Regeln ausgewertet werden. Zur Definition der Regeln ist eine Sprache *A P3P Preferences Exchange Language (APPEL)* [APPEL01] vom W3C vorgesehen ist. In Abb. 10 (aus [APPEL01]) ist eine Beispielregel abgebildet.

```
<appel:RULE behavior="block" description="Service collects personal data
for 3rd parties">
 <p3p:POLICY>
  <p3p:STATEMENT>
    <p3p:DATA-GROUP>
     <p3p:DATA>
      <p3p:CATEGORIES appel:connective="or">
       <p3p:physical/>
       <p3p:demographic/>
```

```
        <p3p:uniqueid/>
       </p3p:CATEGORIES>
      </p3p:DATA>
    </p3p:DATA-GROUP>
    <p3p:RECIPIENT appel:connective="or">
     <p3p:same/>
     <p3p:other-recipient/>
     <p3p:public/>
     <p3p:delivery/>
     <p3p:unrelated/>
    </p3p:RECIPIENT>
   </p3p:STATEMENT>
  </p3p:POLICY>
</appel:RULE>
```

Abb. 10: Beispiel APPEL Regel

Der Wert des XML-Attributs „behavior“ legt fest, wie sich der Agent verhält, wenn die Regel zutrifft. Dies ist dann der Fall, wenn die angegebenen, mit boolschen Operatoren verknüpfbaren, Bedingungen in der auszuwertenden P3P Erklärung erfüllt sind. Es gibt in APPEL 1.0 die folgenden drei „Behaviors“, es ist dabei keine eigene Erweiterungsmöglichkeit vorgesehen:

- “request”: Die Erklärung ist in Ordnung in bezug auf die Regel, mit der Empfehlung (für den Benutzer bzw. Benutzeragenten), dass auf die betreffende URL zugegriffen werden kann
- “block”: Die Erklärung ist nicht konform zu den Regeln, die Ressource soll nicht genutzt werden
- “limited”: Die Erklärung ist teilweise annehmbar, der Benutzeragent könnte beispielsweise mit einer Warnung für den Benutzer reagieren oder beim Zugriff möglichst wenig Header Daten in der HTTP-Anfrage übertragen

Mit Hilfe einer Menge solcher Regeln können die Präferenzen hinsichtlich Privatheit des Benutzers umgesetzt werden. Die Zielsetzung ist es, sinnvolle Regelmengen von vertrauenswürdigen Organisationen bereitstellen zu lassen, da die Entwicklung eigener Regeln wohl für den durchschnittlichen Endbenutzer nicht unbedingt praktikabel erscheint.

5.4.4 Einhaltung der Datenschutzerklärungen

Eine wichtige Fragestellung bei P3P ist es, die Einhaltung der Datenschutzerklärungen zu kontrollieren, um die Anforderungen der Absicherung (vgl. Abschnitt 3.5) erfüllen zu können.

Ein Ansatz dazu ist es, die Praktiken von Unternehmen hinsichtlich Privatheit und Datenschutz von unabhängigen Institutionen untersuchen zu lassen. Im Internet gibt es dazu einige Organisationen wie TRUSTe (www.truste.org), CPA WebTrust (www.webtrust.org) oder BBB Online (www.bbbonline.org), die dieses als Dienst anbieten. Diese Organisationen überprüfen dazu die Datenschutzpraktiken von Unternehmen und stellen bei Konformität der Erklärung bzw. Einhaltung gewisser Mindestanforderungen ein *Gütesiegel* (engl. (privacy) seal) aus. Teilnehmende

Unternehmen dürfen dann durch eine entsprechende Grafik in ihren Web-Seiten auf das Gütesiegel hinweisen. Das Gütesiegel, bzw. ein Verweis darauf, kann in P3P integriert und somit Teil der Datenschutzerklärung werden (siehe Abb. 11).

```
<DISPUTES-GROUP>
  <DISPUTES resolution-type="independent"
    service="http://www.PrivacySeal.org"
    short-description="PrivacySeal.org">
   <IMG src="http://www.PrivacySeal.org/logo.gif">
   <REMEDIES><correct/></REMEDIES>
  </DISPUTES>
 </DISPUTES-GROUP>
```

Abb. 11: Gütesiegel in P3P

Das Element <correct/> im Auszeichnungselement <REMEDY> bedeutet dabei, dass bei Verstößen gegen die Erklärung Rechtsmittel durch die angegebene Organisation eingelegt werden. Auch unabhängig von Gütesiegeln kann eine Verletzung von Datenschutzerklärungen zu rechtlichen Folgen führen. Eine Integration der Prüfung von Datenschutzerklärungen ist insbesondere auch bei der Verwaltung von Benutzerprofilen sinnvoll und erforderlich.

5.4.5 P3P und Identitätsmanagement

Wie könnte jetzt P3P für das betrachtete Szenario verwendet werden? Wichtige Beiträge von P3P für eine Verwaltung von Benutzerprofilen sind unter anderem:

- Modellierung von Zweck der Datenerfassung
- Neben der Erfassung expliziter Profildaten wie Name, Email usw. werden auch dynamische Daten wie Einträge in Log-Dateien oder Cookies als Teil eines Benutzerprofils berücksichtigt
- Weitergabe von Daten an eine dritte Partei, dabei kann berücksichtigt werden, ob die dritte Partei vergleichbare Datenschutzpraktiken hat oder nicht
- Möglichkeit von “opt-in” und “opt-out" Optionen
- Möglichkeit der Verbesserung der Transparenz und Übersicht für den Benutzer durch die Auswertbarkeit von P3P Datenschutzerklärungen durch Benutzeragenten

Durch P3P ist zumindest ein Vokabular für den Austausch von Datenschutz Erklärungen und Präferenzen gegeben. Auch ist die Möglichkeit der Spezifikation von Regeln für die Formulierung von Zugriffspräferenzen vielversprechend, so dass nicht wie bei den meisten Verfahren zur Zugriffskontrolle explizite Zugriffsrechte für einzelne Dienste und Profilattribute festgelegt werden müssen.

Zur Unterstützung eines Identitätsmanagements bietet P3P weiterhin die Möglichkeit der Verwaltung verschiedener Identitäten über ein Persona-Konzept. Eine Persona wird dabei definiert als eindeutiger Identifikator für eine Menge von Werten der Datenelemente [APPEL00]. Benutzeragenten können dann verschiedene Ausprägungen von Profil-Attributen speichern und es Benutzern ermöglichen, zwischen den verschiedenen Personas bzw. Identitäten zu wechseln. Dazu kann in den APPEL-Regeln

als Attribut „persona = ...“ angegeben werden. Auf diese Weise können unterschiedliche Präferenzen beim Zugriff auf z.B. berufliche oder private Email-Adressen spezifiziert werden.

Interessant ist die Erweiterungsfähigkeit von P3P. Neben der schon erwähnten Möglichkeit, das Datenschema zu erweitern, können auch explizit eigene Elemente mit Hilfe eines <EXTENSION> Auszeichnungselements in eine P3P Erklärung eingefügt werden. Damit würden sich eventuell für Identitätsmanagement notwendige Erweiterungen ohne Verletzung der P3P Syntax realisieren lassen. Auch wäre eine Einbindung der P3P Erklärungen in einen Agenten-basierten Ansatz denkbar, da das P3P Schema getrennt und unabhängig vom Protokoll ist, so dass letzteres durch ein für Agenten-Kommunikation besser geeignetes Aushandlungs- und Koordinationsprotokoll ersetzt werden kann.

Ein P3P Benutzeragent muss nicht als selbstständige Anwendung realisiert werden. Es bietet sich insbesondere die Integration in Web-Browser an. Auch ist eine Zusammenführung eines P3P Clients mit den in Abschnitt 2.2.4 beschriebenen Infomediaries naheliegend. Leider haben die meisten kommerziellen Anbieter dies (im August 2001) noch nicht verwirklicht, sondern höchstens erst angekündigt. Ein um zusätzliche Funktionen erweiterter P3P-Client könnte in Zukunft die Rolle eines allgegenwärtigen Werkzeugs zum Identitätsmanagement einnehmen [BeKö00], insbesondere auch im Kontext mobiler Kommunikation.

Allerdings besteht dabei auch die Gefahr einer zu starken Abhängigkeit von einem Werkzeug zum Identitätsmanagement [BeKö00]. Zum Beispiel könnten durch fehlerhafte Realisierung von Sicherheitsfunktionen Angreifer die Identität des Benutzers annehmen oder „stehlen“, was wohl bei einer anderen, weniger Technik-unterstützten, Verwaltung von Benutzerinformationen nicht so leicht der Fall sein könnte. Auch könnten Benutzer durch die Bereitstellung technischer Möglichkeiten zum Schutz ihrer Privatheit verleitet werden, mehr Informationen herauszugeben als eigentlich erforderlich oder sinnvoll wäre. Dadurch würde u.a. das von den rechtlichen Rahmenbedingungen (vgl. Abschnitt 3.2) geforderte Prinzip der „Datensparsamkeit“ untergraben. Auf diese rechtlichen und sozialen Aspekte wird im folgenden nächsten Abschnitt noch etwas genauer eingegangen.

5.4.6 P3P und Datenschutz

Die Eignung von P3P zur Verbesserung von Datenschutz – insbesondere im Verbindung mit europäischen Rechtsvorschriften – wird zum Teil recht kontrovers diskutiert. Die meisten Literaturstellen [Lan00, Cra00b, GrRo00] beurteilen P3P dabei grundsätzlich positiv als geeignetes technisches Hilfsmittel zur Umsetzung bestehender Datenschutzrichtlinien:

- P3P kann eine bessere Transparenz für Benutzer erreichen
- Es lassen sich die „notice&choice“ bzw. „informed consent“ Prinzipien umsetzen (vgl. Abschnitt 3.2.3), und dadurch eine bessere Kontrolle für die Benutzer verwirklichen

- P3P ermöglicht eventuell einen „Wettbewerb von Anbietern“ in bezug auf den besten Datenschutz für Kunden, dadurch könnte eine gewisse Selbstregulierung erzielt werden [Lan00]
- Vertrauen in Online-Transaktionen insgesamt könnte wachsen, wenn Benutzern aussagekräftige Informationen und Wahlmöglichkeiten hinsichtlich des Datenschutzes von Web-Anbietern angeboten werden [Cra00b]

Allerdings wird bezweifelt, ob P3P alleine dem Nutzer ein ausreichendes Maß an Datenschutz garantieren kann [Sie01, Lan00, GrRo00]. P3P stellt dabei nur einen technischen Basisstandard zur Verfügung [Lan00]. Insbesondere werden folgende Punkte kritisiert [Epic01, Kuh01]:

- Benutzern könnte ein falsches Gefühl für Sicherheit suggestiert werden, im Endeffekt werden vielleicht mehr personenbezogene Daten herausgegeben, als es ohne P3P der Fall wäre [Epic01]
- Unsicherheit darüber was passiert, wenn Benutzer der Datenschutzerklärung nicht oder nur teilweise zustimmt [Kuh01]
- Probleme bei der Unterstützung der Kontrollrechte des Benutzers auf Auskunft, Berichtigung, Sperrung und Löschung von Daten [Kuh01], sowie der Durchsetzung der Policies [Epic01]
- Eine vermeintliche, aber nicht ausreichende Lösung könnte übergreifende gesetzliche Regelung in weite Ferne rücken lassen [Sie01]

Es erscheint klar, dass man noch ergänzende, wirksame Datenschutzkontrolle und präzise Rechtsnormen braucht [Lan00], und dass zusätzliche technische Unterstützung für die Benutzer neben P3P erforderlich ist. Der Internet Explorer 6 Web-Browser von Microsoft soll P3P Funktionen integriert haben, daher erscheint es möglich, dass P3P in Zukunft eine größere Unterstützung durch Web-Sites erfahren könnte.

5.5 Fazit

Zusammenfassend lässt sich festhalten, dass durch Verschlüsselungsmechanismen eine gesicherte Übertragung in offenen Systemen erzielt werden kann. Dies ist z.B. für den Transfer sensibler Daten zwischen einem Benutzer- und Dienst-Agenten erforderlich. Dazu ist auch eine Authentifizierung der Kommunikationspartner unerlässlich, was durch digitale Zertifikate realisiert werden kann. Andererseits dienen Anonymisierungsverfahren dazu, die Identität eines Benutzers zu verbergen und damit diesen für Privatheit wichtigen Aspekt umzusetzen. Verfahren zur Pseudonymisierung erlauben eine zur Erbringung bestimmter Dienste nötige Zuordnung einzelner Transaktionen zu einem Pseudonym ohne eine Aufdeckung weiterer Profilattribute des Benutzers. Damit können einzelne Privacy Enhancing Technologies bestimmte Aspekte der Anforderungen bei dezentraler Benutzerrprofilverwaltung erfüllen.

Ein interessanter und wichtiger Ansatz für die Modellierung von Datenschutzpraktiken und Präferenzen im Internet ist P3P, mögliche Beiträge von P3P zu einem Identitätsmanagement wurden schon im Abschnitt 5.4.5 („P3P und

Identitätsmanagement“) erläutert. Auf bestehende Probleme und Unsicherheiten von P3P in bezug auf Datenschutz wurde schon im vorausgegangenen Abschnitt 5.4.6 („P3P und Datenschutz“) eingegangen. Darüber hinaus fehlen im P3P Standard noch folgende Punkte:

- Keine Verbindung mit Anonymisierungs-Anwendungen und anderen Privacy Enhancing Technologies
- Das P3P Vokabular ist nicht ausreichend und muss erweitert werden, z.B. gibt es nur eine relativ kleine Menge pauschaler Zweckbestimmungen für die Festlegung des Zugriffszwecks [Kuh01]
- Keine vollständige Modellierung von Zugriffsrechte möglich, z.B. ist das „Schreiben in ein Benutzerprofil“ nicht abgedeckt
- Auch gibt es grundsätzlich keine Integration mit Zugriffskontrollsystemen für eine verfeinerte Festlegung von Zugriffsrechten

Ferner wurde P3P für das „Browsen von Web-Seiten“ entwickelt, d.h. für eine Benutzer-initiierte Anfrage an einen Dienst, der diese Anfrage beantwortet. Dabei wurde insbesondere auch auf die Eigenschaften von HTTP, z.B. die Berücksichtigung von Cookies, eingegangen. Es fehlt aber an Interaktions-Modellen für eine Kommunikation autonomer Komponenten, obwohl P3P schon als Basis einer Verhandlung von Diensten mit autonomen Benutzeragenten entwickelt wurde. Eine mehr auf Agenten bzw. autonome Komponenten bezogene Sichtweise ist auch bei den anderen betrachteten PET Ansätzen nötig.

Die Berücksichtigung von Verhandlung zwischen Diensteanbietern und Benutzeragenten wurde zwar nicht in den aktuellen Standard [P3P00] aufgenommen, könnte aber in zukünftigen Erweiterungen enthalten sein. Weitere interessante Aspekte, die für spätere P3P Versionen geplant sind, sind:

- Möglichkeit, eine Menge von P3P Erklärungen zur Auswahl anzubieten
- Unabstreitbarkeit von Vereinbarungen, z.B. über digitale Signaturen (bisher ist das Problem bei Personas, dass die Identitäten nicht bewiesen werden können)
- Automatischer Datentransfer

Grundsätzlich kann man zusammenfassen, dass P3P für den Bereich Identitätsmanagement und zur Unterstützung der Verwaltung von Benutzerprofilen sehr interessant ist, wobei einige Anpassungen und Erweiterungen wie beschrieben sinnvoll wären. Insbesondere ist dies dann der Fall, wenn sich dieser Standard für den Zugriff auf Web-Seiten durchsetzt und bewährt, da dabei gegebenenfalls Datenschutzerklärungen und -präferenzen übernommen werden können.

Ein wichtiger Punkt bei allen PET ist, dass die Ansätze eventuell zu kompliziert und aufwändig für durchschnittliche End-Benutzer sind. Ein Beispiel dazu ist die notwendige Vorgehensweise nur bei einer Erzeugung von Nyms im Freedom System (vgl. Abschnitt 5.3.6). Dazu kommt noch eine manuelle Verwaltung der Pseudonyme, die von einem Benutzer durchgeführen werden muss. Die Systeme müssen mehr auf die Bedürfnisse von Benutzern zugeschnitten werden, dazu gehört auch der Entwurf sinnvoller

Benutzungsschnittstellen, z.B. die Untersuchung von geeigneten graphischen Benutzeroberfläche zur Unterstützung von Privatheit.

Des weiteren muss bei den bestehenden Systemen der Benutzer die Wahl einer Identität bzw. Aktivierung einer anonymisierten Datenübertragung selbst vornehmen. Man braucht aber (auch) eine Anonymisierung der Art, dass bestimmte Profildaten automatisch anonymisiert übertragen werden. Auch ist eine technische Unterstützung von Privatheit in dem betrachteten Szenario eine Integration von Privacy Enhancing Technologies in Zugriffskontrollsysteme notwendig.

Abschließend lässt sich daher festhalten, dass weder Mechanismen zur Zugriffskontrolle noch Privacy Enhancing Technologies alleine ausreichend sind, um die Anforderungen der Gewährleistung von Privatheit bei Agenten-basierter Verwaltung von Benutzerprofilen zu erfüllen. Es ist eine Kombination der Verfahren, zusammen mit neuen Konzepten, notwendig.

6 Ausblick

Um die erläuterten Einschränkungen der diskutierten Systeme zu beheben, wird im Rahmen des Projektes Cobricks in einem Teilprojekt PACE („Privacy in Agent-based Community support and E-commerce“[12]), ein System entworfen, das die Problemstellung in dem betrachteten Szenario lösen soll[13]. Ein viel versprechender Ansatz erscheint dabei, eine Aufteilung des Zugriffskontrollverfahrens in einen flexiblen und umfassenden Mechanismus zur Bestimmung von Zugriffsrechten und einen effizient und einfach durchzuführenden Datenzugriff vorzunehmen. Ferner wird u.a. versucht, auch stärker einen Verhandlungsprozess zwischen autonomen Agenten in den Ablauf zu integrieren, sowie von vornherein eine gute Umsetzbarkeit in Benutzungsschnittstellen zu berücksichtigen.

Zu den kommerziell wichtigsten Systemen zur Verwaltung von Benutzerdaten gehören die besprochenen Infomediaries zur dezentralen Verwaltung von Profilen. Dabei ist vor allem interessant, wie sich die geplante Integration von Passport bzw. des dazugehörigen Benutzerverwaltungsdienstes „HailStorm“ [Mic01] in Microsoft's Betriebssystem Windows XP auswirken könnte. Es bleibt abzuwarten, ob die bekannten Passport-Probleme [KoRu00] hinsichtlich Sicherheit und Privatheit dabei im Sinne des Benutzers gelöst werden. Auch fehlen allgemeine Konzepte, um die erläuterten Anforderungen für die Benutzer befriedigend zu untersuchen und zu lösen.

Ein interessanter, hier nicht diskutierter, Aspekt in dem betrachteten Szenario wäre es auch, einen Abgleich von Benutzerinteressen mit Dienstanbietern in Form eines

---

12 Siehe dazu auch http://www11.in.tum.de/proj/imc/pace/

13 Ein kurzer Überblick dazu findet sich in [KoWö01]

monetären Ausgleiches herzustellen. Das bedeutet, dass Benutzer persönliche Informationen gegen Geld oder anderen Vorteilen herausgeben könnten.

Des weiterten könnten zukünftig biometrische Verfahren zur Authentifizierung von Benutzern gegenüber System-Komponenten eine wichtige Rolle spielen. Dadurch können sich wohl Verbesserungen in bezug auf Sicherheit, aber auch zusätzliche Privatheitsprobleme ergeben. Genauso könnte eine stärkere Berücksichtigung mobiler Dienste in Zukunft bedeutsam werden. Dadurch könnten neue Kategorien von Anwendungen möglich werden, z.B. die Unterstützung von (mobilen) Communities durch Auswertung ortsbezogener Benutzerinformationen. Es entstehen dabei aber auch neue, teilweise noch völlig unklare, Probleme von Privatheit [MaLa01].

Es erscheint abschließend klar, dass es noch viele ungelöste Fragestellungen in dem betrachteten Bereich von technischen Möglichkeiten zur Verbesserungen der Privatheit von Benutzerdaten in einer globalen Informationsgesellschaft gibt.

Referenzen

[ACR99] Ackerman, M.S.; Cranor, L.F.; Reagle, J.: Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In: Proc. ACM Conference on Electronic Commerce, Nov. 1999

[APPEL01] A P3P Preference Exchange Language 1.0 (APPEL 1.0). W3C Working Draft, 2001, http://www.w3.org/TR/P3P-preferences.html

[Bäu00] Bäumler, H. (Hrsg.): E-Privacy. Vieweg, 2000

[BBB+97] Bayardo, R. J.; Bohrer, W.; Brice, R.; Cichocki, A.; Fowler, J.; Helal, A.; Kashyap, V.; Ksiezyk, T.; Martin, G.; Nodine, M.; Rashid, M.; Rusinkiewicz, M.; Shea, R.; Unnikrishnan, C.; Unruh, A.; Woelk, D.: InfoSleuth: Agent-Based Semantic Integration of Information in Open and Dynamic Environments. In: Proc. ACM SIGMOD International Conference on Management of Data, Tucson AZ, 1997, S. 195-206

[BCF01] Bertino, E.; Castano, S.; Ferrari, E.: Securing XML Documents with Author-X. In: IEEE Internet Computing, Vol. 5, No. 3, May 2001, S. 21-31

[BeKö00] Berthold, O.; Köhntopp, M.: Identity Management Based On P3P. In: Workshop on Design Issues in Anonymity and Unobservability, Berkeley CA, Jul. 2000

[BeLa73] Bell, D.E.; LaPadula, L.: Secure Computer Systems: A Mathematical Model. Mitre Corp., Bedford MA, 1973

[BFK00] Berthold, O.; Federrath, H; Köhntopp, M.: Project "Anonymity and Unobservability in the Internet". In: Proc. of the Tenth Conference on Computers, Freedom & Privacy (CFP 2000), 2000, S. 57-65

[BKL+01] Borghoff, U.M.; Koch, M; Lacher, M.S.; Schlichter, J.H.; Weißer, K.: Informationsmanagement und Communities – Überblick und Darstellung zweier Projekte der IMC-Gruppe München. In: Informatik Forschung und Entwicklung, Springer, Jul. 2001, S.103-109

[BSG00] Boucher, P.; Shostack, A.; Goldberg, I.: Freedom System 2.0 Architecture. White paper, Zero-Knowledge Systems Inc., Dec. 2000

[CC98] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements. Version 15408-2 FDIS, ISO/IEC SC27 N2162, 1998

[CDGM97] Chavez, A.; Dreilinger, D.; Guttman, R.; Maes, P.: A Real-Life Experiment in Creating an Agent Market Place. In: Proc. of the Second International Conference on the Practical Application of Intelligent Agents and Multi-Agent Technology (PAAM 97), Blackpool, 1997

[Cha81] Chaum, D.: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. In: Communications of the ACM, Vol. 24, No. 2, Feb. 1981

[ChMa96] Chavez, A.; Maes, P.: Kasbah: An Agent Marketplace for Buying and Selling Goods. In: Proc. of the First International Conference on the Practical Application of Intelligent Agents and Multi-Agent Technology, London, April 1996

[Cla99] Clarke, R.: Internet Privacy Concern Confirm the Case for Intervention. In: Communications of the ACM, Vol. 42, No. 2, Feb. 1999, S. 60 – 67

[Cra99] Cranor, L.F.: Agents of Choice: Tools that Facilitate Notice and Choice about Web Site Data Practices. In: Proc. 21st Intl. Conf. on Privacy and Personal Data Protection, Hong Kong, China, Sep. 1999

[Cra00a] Cranor, L.F.: Internet Privacy and WWW. Tutorial, WWW9 Conference, May 2000, http://www.research.att.com/projects/p3p/p3p-www9.ppt

[Cra00b] Cranor, L.F.: Gateway: Platform for Privacy Preferences - P3P . In: Datenschutz und Datensicherheit, Vieweg, 2000, http://www.datenschutz-und-datensicherheit.de/ jhrg24/p3p.htm

[DGLP97] Dunn, M.; Gwertzmann, J.; Layman, A.; Partovi, H.: Privacy and Profiling on the Web. W3C Note, Jun. 1997, http://www.w3.org/TR/NOTE-Web-privacy.html

[DVPS00] Damiani, E.; Vimercati, S.D.C.; Paraboschi, S.; Samarati, P.: Securing XML Documents. In: 7th International Conference on Extending Database Technology, Lecture Notes on Computer Science, Vol. 1777, Springer, Mar. 2000

[Eck01] Eckert, C.: IT-Sicherheit. Oldenbourg, 2001

[Epic01] Electronic Privacy Information Center: Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. June 2000, http://www.epic.org/reports/prettypoorprivacy .html

[FeBe00] Federrath, H; Bertold, O: Identitätsmanagement. In: [Bäu00], S. 189 - 204

[FeKu92] Ferraiolo, D; Kuhn, R.: Role-Based Access Controls. In: Proc. 15th National Computer Security Conference, Baltimore MD, Oct. 1992

[FeMa98] Federrath, H.; Martuis, K.: Anonymität und Authentizität im World Wide Web. In: ITG-Fachbericht 153, Vorträge der ITG-Fachtagung „Internet - frischer Wind in der Telekommunikation", VDE-Verlag, 1998, S. 91-101

[FiHü01] Fischer-Hübner, S.: IT-Security and Privacy. Lecture Notes in Computer Science, Vol. 1958, Springer, 2001

[FIPA99] FIPA 99 Specification. Technical report, FIPA, 1999

[FHO98] Fischer-Hübner, S.; Ott, A.: From a Formal Privacy Model to its Implementation. In. Proc. National Information Systems Security Conference (NISSC 98), 1998

[FKK96] Freier, A.O; Karlton, P.; Kocher, P.C.: The SSL Version 3.0. Internet-Draft, Netscape Corp., 1996, http://home.netscape.com/eng/ssl3/draft302.txt

[FLM97] Finin, T.; Labrou, Y.; Mayfield, J.: KQML as an Agent Communication Language. In: Bradshaw, J.: Software Agents, MIT Press, S. 291-316

[FNS99] Fujimura, K.; Nakajima, Y.; Sekine, J.: XML Ticket: Generalized Digital Ticket Definition Language. W3C Signed XML Workshop, Apr. 1999, http://www.w3.org/DSig/signed-XML99/pp/NTT_xml_ticket.html

[For01] Forrester Research: Surviving the Privacy Revolution. Report, Feb. 2001

[FuNa98] Fujimura, K; Nakajima, Y: General-purpose Digital Ticket Framework. In: 3rd USENIX Workshop on Electronic Commerce, Aug. 1998, S. 177-186, http://www.usenix.org/publications/library/proceedings/ec98/fujimura.html

[Gar94] Garfinkel, S.L.: PGP – Pretty Good Privacy. O'Reilly, 1994

[GGK+99] Gabber, E.; Gibbons, P.B.; Kristol, D.M.; Matias, Y.; Mayer, A.: Consistent, yet Anonymous, Web Access with LPWA. In: Communications of the ACM, Vol. 42, No. 2, Feb. 1999, S. 42-47

[GGPS97] Gattung, G.; Grimm, R.; Pordesch, U.; Schneider, M. J.: Persönliche Sicherheitsmanager in der virtuellen Welt. In: Müller, G.; Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison Wesley, Bonn, Reading, 1997

[Gri01] Grimm, R.: Vertrauen in E-Commerce: Wie sicher soll E-Commerce sein? In: Müller, G.; Reichenbach, M. (Hrsg.): Sicherheitskonzepte für das Internet, Springer, 2001

[GrRo00] Grimm, R; Rossnagel, A.: P3P and the Privacy Legislation in Germany: Can P3P Help to Protect Privacy Worldwide? In Proc. ACM Multimedia, Nov. 2000, http://sit.gmd.de/~grimm/texte/P3P-Germany-e.pdf

[GRS99] Goldschlag, D.; Reed, M.; Syverson, P.: Onion Routing for Anonymous and Private Internet Connections. In: Communications of the ACM, Vol. 42, No. 2, 1999, S. 39-41

[HaSi99] Hagel, J.; Singer, M.: Net Worth: Shaping Markets When Customers Make the Rules. Harvard Business School Press, 1999

[HSD98] Howes, T.; Smith, M.; Dawson, F.: MIME Content-Type for Directory Information (vCARD Specification). RFC 2425, Sep. 1998

[Ian01] Iannella, R: Representing vCard Objects in RDF/XML. W3C Note, Feb. 2001, http://www.w3.org/TR/vcard-rdf

[Kes00] Kesdogan, D.: Privacy im Internet – Vertrauenswürdige Kommunikation in offenen Umgebungen. DuD-Fachbeiträge, Vieweg, 2000

[KLW01] Koch, M.; Lacher, M; Wörndl, W.: Das CommunityItemsTool – Interoperable Unterstützung von Interessens-Communities in der Praxis. In: Britzelmaier, B.; Geberl, S.; Weinmann, S. (Hrsg.): Proc. 3. Liechtensteinisches Wirtschaftsinformatik-Symposium, Teubner, Stuttgart, 2001, S. 147-157

[Koch00] Koch, M.: Cobricks – Eine agentenbasierte Infrastruktur für Community-Anwendungen. In: Reichwald, R.; Schlichter, J. (Hrsg.): Proc. D-CSCW 2000, Teubner Verlag, Stuttgart, München, Sep. 2000, S. 265-266

[Koch01a] Koch, M.: Kollaboratives Filtern. In: Schwabe, G.; Streitz, N.; Unland, R (Hrsg.): CSCW-Kompendium, Springer Verlag, Berlin, 2001, S. 351-357

[Koch01b] Koch, M.: Community-Support-Systeme. In: Schwabe, G.; Streitz, N.; Unland, R (Hrsg.): CSCW-Kompendium, Springer Verlag, Berlin, 2001 S. 296-296

[KoWö01] Koch, M.; Wörndl, W.: Community Support and Identity Management. In: Proc. Europ. Conference on Computer-Supported Cooperative Work (ECSCW2001), Bonn, Germany, Sep. 2001

[Köh99] Köhntopp, M: Pseudonymität – Technik und Recht. Folien für einen Kurzvortrag auf dem DASIT-Treffen in Frankfurt am 13. Dezember 1999, http://www.koehntopp.de/marit/pub/idmanage/pseudonymslides/Koehn_99PseudonymFrankfurt.pdf

[Köh00] Köhntopp, M.: Identitätsmanagement. In: Bäumler, H.; Breinlinger A.; Schrader, H.-J. (Hrsg.): Datenschutz von A-Z, Luchterhand, Neuwied, 2000

[KoRu00] Kormann, D. P.; Rubin, A. D.: Risks of the Passport Single Signon Protocol. IEEE Computer Networks, Vol. 33, 2000, http://avirubin.com/passport.html

[KuHa00a] Kudo, M.; Hada, S.: XML Access Control. Proposal, Oct. 2000, http://www.trl.ibm.com/projects/xml/xacl/xmlac-proposal.html

[KuHa00b] Kudo, M.; Hada, S.: XML Document Security Based on Provisional Authorization. In: Proc. 7th ACM Conference on Computer and Communications Security, Athens, Greece, Nov. 2000

[Kuh01] Kuhlen, R.: Privacy Sicherung in der Wirtschaft. Juni 2001, http://www.ib.hu-berlin.de/~kuhlen/VERT01/trust-v6-1-v-privacy-sicherung-wirtschaft060601.pdf

[Kyus98] Kyas, O.: Sicherheit im Internet. Internat. Thomson Publ., Bonn, 1998

[Lan00] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Neuer Standard für Online-Privacy in Deutschland vorgestellt. Pressemeldung, Aug. 2000, http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/somak/somak00/p3p_pm.htm

[Lau00] Laukka, M.: Criteria for Privacy Supporting System. In: Proceedings of NordSec2000, Reykjavik, Iceland, 2000

[Les01] Lester, T.: The Reinvention of Privacy. The Atlantic Monthly, Mar. 2001, http://www.theatlantic.com/issues/2001/03/lester-p1.htm

[LiLo98] Lin, D.; Loui, M.C.: Taking the Byte Out of Cookies: Privacy, Consent, and the Web. In: Proc. ACM Policy, Washington, May 1998

[MaLa01] Mattern, F.; Langheinrich, M.: Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge. In: Müller, G.; Reichenbach, M. (Hrsg.): Sicherheitskonzepte für das Internet, Springer, 2001

[MAIO97] Mynatt, E.D.; Adler, A.; Ito, M.; Oday, V.L.: Design for Network Communities. In: Proc. ACM SIGCHI Conf. On Human Factors in Computer Systems, 1997

[MGM99] Maes, P.; Guttman, R. H.; Moukas, A. G.: Agents that Buy and Sell. In: Communications of the ACM, Vol. 42, No. 3, Mar. 1999

[Mic01] Building User-Centric Experiences – An Introduction to Microsoft HailStorm. Microsoft white paper, Mar. 2001, http://www.microsoft.com/net/hailstorm.asp

[MuSc00] Mulligan, D.; Schwartz, A.: Your place or mine? Privacy Concerns and Solutions for Server and Client-side Storage of Personal Information. In: Proc. Computers, Freedom and Privacy, Toronto ON, Canada, Apr. 2000

[ReRu97] Reiter, M.K.; Rubin, A.D.: Crowds: Anonymity for Web Transactions. Technical Report 97-15, DIMACS, Aug. 1997

[Rös97] Röscheisen, M.: A Network-Centric Design for Relationship-based Right Management. Ph.D. Dissertation, Computer Science Department, Stanford University, 1997

[RW97a] Röscheisen, M.; Winograd, T.: A Network-Centric Design for Relationship-based Security and Access Control. In: Journal of Computer Security, Special Issue on Security in the World-Wide Web, 1997

[RW97b] Röscheisen, M.; Winograd, T.: The Stanford FIRM Framework for Interoperable Rights Management. Forum on Technology-based Intellectual Property Management, Washington DC, 1997

[OECD80] Organization for Economic Cooperation and Development (OECD): Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris, 1980, http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.HTM

[Opp97] Oppliger, R.: IT-Sicherheit. DuD-Fachbeiträge, Vieweg, 1997

[P3P00] P3P: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Candidate Recommendation, Dec. 2000, http://www.w3.org/TR/P3P/

[Pfi90] Pfitzmann, A.: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer, 1990

[PfKö01] Pfitzmann, A.; Köhntopp, M.: Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In: Federrath, H. (Hrsg.): Designing Privacy Enhancing Technologies, Proc. Workshop on Design Issues in Anonymity and Unobservability; Lecture Notes in Computer Science, Vol. 2009, Springer, 2001

[PPW88] Pfitzmann, A.; Pfitzmann, B.; Waidner, M.: Datenschutz garantierende offene Kommunikationsnetze. In: Informatik-Spektrum 11/3, 1988, S. 118-142

[PSWW00] Pfitzmann, A.; Schill, A.; Westfeld, A.; Wolf, G.: Mehrseitige Sicherheit in offenen Netzen. DuD-Fachbeiträge, Vieweg, 2000

[SaHa00] Samuels, R.; Hawco, E.: Untracable Nym Creation on the Freedom 2.0 Network. White paper, Zero-Knowledge Systems Inc., Nov. 2000

[SaSa94] Sandhu, R.; Samarati, P.: Access Control: Principles and Practice. IEEE Communications Magazine, Vol. 32, No. 9, Sep. 1994, S. 40-48

[ScEn00] Schulze, G.; Enzmann, M.: Datenschutz im Internet. In: Der GMD-Spiegel, Jan. 2000, S.42-44

[Sie01] Beschreibung Platform for Privacy Preferences Project. Mai 2001, http://www.uni-siegen.de/security/p3p.html

[SNS98] Steiner, J.G.; Neuman, C.; Schiller, J.I.: Kerberos: An Authentication Service for Open Network Systems. In: USENIX Conference Proceedings, Winter 1988.

[SoCr98] Soltysiak, S. J.; Crabtree I. B.: Knowing Me, Knowing You. Practical Issues in the Personalisation of Agent Technology. In: Proc. Third Intl. Conf. in the Practical Applications of Agents and Multi-Agent Technology (PAAM-98), Mar. 1998

[Tät00] 22. Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Landtagsdrucksache 15/10, Apr. 2000

[WaBr1890] Warren, S.D.; Brandeis, L.D.: The Right to Privacy. Harvard Law Review 193, 196, 1890

[Wag01] Wagner, M.: Shared Directories Need Shared Control. Information Week, Jul. 2001, http://www.internetweek.com/newslead01/lead072601.htm

[Wes67] Westin, A.: Privacy and Freedom. New York, 1967

[WoPf00] Wolf, G.; Pfitzmann, A.: Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen. In: Informatik Spektrum, Vol. 23, No. 3, Jun. 2000, S. 173-191

[XML00] Extensible Markup Language (XML) 1.0. W3C Recommendation (2nd Edition), Oct. 2000, http://www.w3.org/TR/REC-xml

[XPa99] XML Path Language (XPath) 1.0. W3C Recommendation, Nov. 1999, http://www.w3.org/TR/xpath

[Xrml00] XrML Specification Version 1.03. 2000, http://www.xrml.org/

[Xsig 01] XML Signature Syntax and Processing. W3C Proposed Recommendation, Aug. 2001, http://www.w3.org/TR/xmldsig-core/