Sicherheit und Benutzbarkeit durch Identitätsmanagement

Sven Wohlgemuth, Uwe Jendricke, Daniela Gerd tom Markotten, Felix Dorner, Günter Müller

Institut für Informatik und Gesellschaft, Abt. Telematik
Albert-Ludwigs-Universität Freiburg
Friedrichstraße 50, 79098 Freiburg im Breisgau
{wohlgemuth, uwe, dany, dorner, mueller}@iig.uni-freiburg.de

Abstract: Mit dem zunehmenden Einsatz von IT- und Kommunikationstechnologie und der Verlagerung von wirtschaftlichen Aktivitäten in Rechnernetze gewinnt IT-Sicherheit mehr und mehr an Bedeutung. Der Einsatz von sicheren IT-Systemen bildet die Grundlage für den Nutzer, seine Privatsphäre zu schützen, d.h. sein Recht auf informationelle Selbstbestimmung zu wahren. Nutzer können jedoch nur sicher arbeiten und ihre Privatsphäre schützen, wenn die verwendeten Systeme für sie benutzbar sind. In diesem Beitrag wird mit dem Identitätsmanagement eine Sicherheitsanwendung vorgestellt, die den Nutzer bei der Durchsetzung seiner Sicherheitsbedürfnisse unterstützt und ihm ein situationsabhängiges Handeln unter verschiedenen Rollen ermöglicht. Mit dem Identitätsmanager wird ein Prototyp für den Einsatz auf einem Endgerät des Nutzers vorgestellt.

1 Einleitung

In den letzten Jahren hat der Einfluss vernetzter IT-Systeme stark zugenommen. Trotz dieser Entwicklung sind viele Nutzer nicht bereit, IT-Systeme für sicherheitskritische Transaktionen, wie beispielsweise den elektronischen Einkauf, zu benutzen. So hat eine Studie des britischen National Consumer Council ergeben, dass 55 % aller Internet-Nutzer das Einkaufen im Internet für die gefährlichste Art des Einkaufens halten [Nat00]. Diese Vorbehalte gegen den E-Commerce können jedoch nicht durch das Fehlen von sicheren Anwendungen motiviert sein, da inzwischen eine Vielzahl von Sicherheitsanwendungen existiert. Es hat sich jedoch gezeigt, dass Nutzer mit den derzeit verfügbaren Anwendungen nicht arbeiten können oder wollen [Whi99, Wai98, Jen00, Ger03b]. Die Gründe für die geringe Akzeptanz von Sicherheitsanwendungen sind in den Bereichen IT-Sicherheit, Privatheit und Benutzbarkeit zu identifizieren.

1.1 IT-Sicherheit

IT-Sicherheit ist für die Akzeptanz des E-Commerce ein Schlüsselfaktor für den Kunden [Sch99]. Es müssen die folgenden Sicherheitsfunktionen realisiert werden, damit im E-Commerce mindestens dasselbe Maß an Sicherheit wie im konventionellen Handel erreicht wird:

- **Selbstbestimmte Identifikation des Kunden:** Der Kunde muss sich unterschiedlich gegenüber Händlern identifizieren können. Insbesondere muss er die

gleichen Möglichkeiten wie im konventionellen Handel haben, anonym zu handeln.

- **Verkettbarkeit von Transaktionen:** Der Kunde muss im Rahmen seiner Möglichkeiten entscheiden können, ob verschiedene von ihm durchgeführte Transaktionen verkettbar sein sollen. Technische Vorgaben können die Entscheidung einschränken: Muss der Kunde beispielsweise mit Kreditkarte bezahlen, dann kann er eine Verkettung über die Kreditkartennummer nicht vermeiden.

- **Zurechenbarkeit des Händlers:** Bestimmte Aktionen des Händlers müssen für den Kunden zurechenbar sein. Schickt der Händler dem Kunden beispielsweise eine Auftragsbestätigung, dann muss der Kunde auch gegenüber Dritten beweisen können, dass diese Auftragsbestätigung von diesem Händler stammt.

- **Zurechenbarkeit des Kunden:** Bestimmte Aktionen des Kunden müssen für den Händler zurechenbar sein. So muss der Händler beispielsweise gegenüber Dritten beweisen können, dass eine Bestellung einem bestimmten Kunden zurechenbar ist.

IT-Sicherheit die Gesamtheit der technischen Maßnahmen und Werkzeuge zur Durchsetzung der Schutzziele der mehrseitigen Sicherheit [Ran97], d.h. dass alle Beteiligten die aus ihrer Sicht wünschenswerte Sicherheit selbst festlegen können und diese vom IT-System gewährleistet wird. In den heutigen Anwendungen ist IT-Sicherheit sehr unterschiedlich implementiert, so dass verschiedene Sicherheitsstufen erreicht werden. Möchte der Nutzer sicher arbeiten, dann muss er jede Anwendung für seine individuellen Sicherheitsinteressen konfigurieren und eventuell zusätzliche Sicherheitskomponenten integrieren. Dabei ist IT-Sicherheit jedoch für den Nutzer ein Sekundärziel, d.h. Nutzer wollen vorrangig ihre Aufgaben mit einem IT-System erledigen und sich nicht mit der Absicherung ihrer Systeme beschäftigen.

1.2 Privatheit

Privatheit (engl. *privacy*) ist ein Kunstwort und wird synonym mit dem Recht auf informationelle Selbstbestimmung verwendet. Das Recht auf informationelle Selbstbestimmung ist als die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen“ definiert [Bun83]. Im Teledienstedatenschutzgesetz ist dazu festgeschrieben, dass das anonyme Auftreten des Nutzers von Diensteanbietern nicht behindert werden darf [Tel97]. Alan F. Westin definiert Privatheit als „the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others, …“ [Wes67]. In diesem Beitrag wird Privatheit nur im Bezug auf IT-Systeme betrachtet. Dabei ist vor allem die Verarbeitung und Weitergabe von personenbezogenen Daten relevant.

Viele Anwendungen ermöglichen es dem Nutzer jedoch nicht, die Herausgabe seiner Daten zu kontrollieren und nachzuvollziehen. So geben Systeme oft vom Nutzer unbemerkt Systemdaten (MAC-Adresse, IP-Adresse, Ortsinformation, …) preis, die bereits eine Verkettung von Aktionen des Nutzers ermöglichen. Nutzer haben jedoch ein großes

Interesse am Schutz ihrer Daten. So haben beispielsweise 84 % der Internetnutzer in der Studie „Trust and Privacy Online“ [Fox00] angegeben, dass sie besorgt sind und dass unbekannte Personen oder Firmen personenbezogene Daten über sie erhalten können. Wünscht der Nutzer jedoch eine speziell auf ihn angepasste Ansprache und Produktindividualisierung durch einen Händler (One-to-One Marketing), die der Händler nur anhand von Informationen über den Kunden generieren kann [Pep97], so sollte ihm die selbstbestimmte Freigabe seiner personenbezogenen Daten ermöglicht werden.

1.3 Benutzbarkeit von Sicherheitsanwendungen

Die Benutzbarkeit von Sicherheitsanwendungen ist derzeit in vielen Fällen nicht gegeben [Whi99, Wai98, Jen00, Ger03b]. Dabei bestimmt weniger die ergonomische Aufbereitung der Oberflächen die Benutzbarkeit. Vielmehr ist die dem Nutzer oft unverständliche Präsentation der vorhandenen Sicherheitsmechanismen für die Nichtnutzung verantwortlich [Mul98, Ger00, Ger03b]. Der Nutzer wird auf der Benutzungsoberfläche oft mit komplexen Sicherheitskonzepten konfrontiert, die insbesondere für den Sicherheitslaien nur schwer zu verstehen sind. Beispielsweise konnten bei der Evaluation der Signiersoftware SignTrust Mail der Deutschen Post AG 120 Benutzbarkeitsprobleme identifiziert werden [Ger03b], wobei 75% der identifizierten Probleme die Sicherheit des Systems negativ beeinflusst haben. Zudem verfügt jede Anwendung über individuell gestaltete Benutzungsoberflächen, so dass der Nutzer für jede Anwendung den Umgang mit der Sicherheitsfunktionalität neu erlernen muss.

Die Aspekte IT-Sicherheit, Privatheit und Benutzbarkeit adressiert das im Folgenden vorgestellte Identitätsmanagement. Dazu bildet Identitätsmanagement ein natürliches Verhalten des Menschen auf IT-Systeme ab: Jeder Mensch tritt gegenüber anderen Menschen unterschiedlich auf. Identitätsmanagement unterstützt den Nutzer bei dieser Verhaltensweise, indem es ihm ein nachvollziehbares und individuelles Auftreten gegenüber seinen Kommunikationspartnern ermöglicht und gleichzeitig seine Kommunikation vor Dritten schützt.

2 Die Teil-Identität

Jede Person hat eine Identität. Diese Identität beinhaltet die Rollen, die eine Person einnimmt. So ist man beispielsweise beim Einkaufen annähernd anonym, beim Besuch bei Freunden jedoch sehr gut bekannt. Dieser (oft unbewusste) Wechsel der offenbarten Identität wird durch den Wechsel von situationsabhängigen Rollen modelliert, die Teil-Identitäten genannt werden. Eine Teil-Identität ist eine Menge von persönlichen Daten eines Benutzers, wobei jeder Benutzer über mehrere Teil-Identitäten verfügen kann. Ähnlich wie in der realen Welt wechselt der Benutzer in Rechnernetzen seine Teil-Identität, wodurch er sich – je nach Situation und Rolle – im Spektrum zwischen Anonymität und Identifikation bewegt. Auf diese Art schützen Nutzer ihre Privatsphäre und ermöglichen so zum anderen einen Reputationsaufbau gegenüber einem Kommunikationspartner unter der verwendeten Rolle. Die Teil-Identität wurde 1993 das erste Mal von Roger Clarke eingeführt; jedoch wird sie von ihm nicht für Identitätsmanagement verwendet, sondern zur Überwachung von Personen [Cla93].

In der folgenden Abbildung tritt der Nutzer namens *Willi Weber* je nach Situation unter vier Teil-Identitäten auf. Verwendet er die Teil-Identität *Einkaufen*, so gibt er seine personenbezogenen Daten wie sein Name, die Angaben zu seiner Kreditkarte und seine Adresse zur Veröffentlichung an den Kommunikationspartner frei. Damit ist er unter Verwendung dieser Teil-Identität identifizierbar und seine Handlungen können ihm zugerechnet werden. Tritt er hingegen unter seiner Teil-Identität *Freizeit* auf, so tritt er unter dem Namen *Webster* auf und zeigt seine Zugehörigkeit zu einem Verein. Die Handlungen, die er unter dieser Teil-Identität durchführt, können nicht zu seiner Identifizierung führen, solange keine Beziehung zwischen dieser Teil-Identität und einem ihn identifizierendem Datum hergestellt werden kann. Unter der Teil-Identität *Anonym* werden keine personenbezogenen Daten an den Kommunikationspartner weitergegeben.

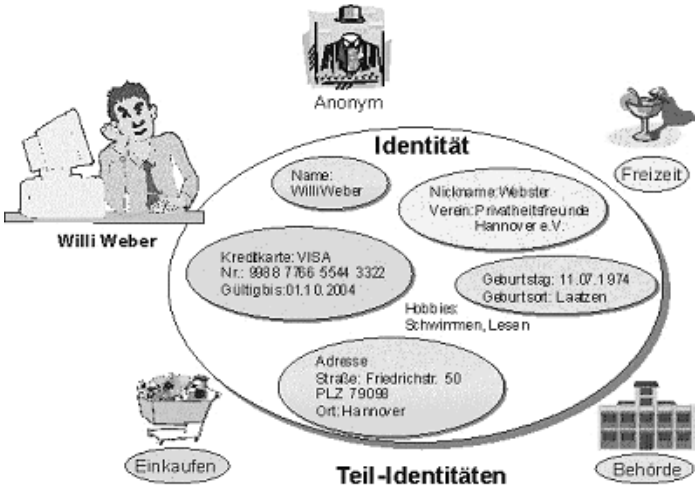

Abbildung 2.1: Die Identität und Teil-Identitäten des beispielhaften Nutzers *Willi Weber*

2.1 Datentypen einer Teil-Identität

Eine Teil-Identität setzt sich aus einer Menge von Tupeln zusammen. Jedes Tupel beinhaltet die Beschreibung des persönlichen Datums (Bezeichner) und das persönliche Datum selbst:

- **Persönliches Datum (Pseudonym)**: Mit einem persönlichen Datum, wie *Willi Weber* oder einem öffentlichen kryptographischen Schlüssel, kann der Nutzer sich mehr oder weniger eindeutig identifizieren. In Abhängigkeit des gewünschten Auftretens im Spektrum zwischen Anonymität und Identifizierung, kann der Nutzer unterschiedliche Typen von Pseudonymen verwenden [Pfi00]. Beispielsweise ermöglichen Transaktionspseudonyme, wie z.B. eine eindeutige Transaktionsnummer, eine Verkettung der einzelnen Schritte einer Transaktion mit dem Nutzer, ohne die Anonymität des Nutzers aufzuheben. Dahingegen ermöglichen Personenpseudonyme, wie z.B. eine Telefonnummer, eine Identifizierung des Inhabers.

- **Bezeichner**: Jedes persönliche Datum wird durch einen Bezeichner referenziert, z.B. „personname.given“ (vgl. [Cra02]).

- **Schlüssel-Bezeichner** verweisen auf Daten, die eindeutig sind wie bspw. ein privater kryptographischer Schlüssel.

- **Identifizierende Schlüssel-Bezeichner** verweisen auf Daten, mit denen eine Person eindeutig identifiziert werden kann wie bspw. die Personalausweisnummer.

- **Schablone**: Die Schablone einer Teil-Identität ist die Menge der Bezeichner einer Teil-Identität, enthält aber keine persönlichen Daten. Schablonen können dem Nutzer daher als Muster für Teil-Identitäten zur Verfügung gestellt werden.

Mit der Abbildung der Teil-Identitäten in ein IT-System werden die personenbezogenen Daten und die Einstellungen zur Zurechenbarkeit des Nutzers in dem System gespeichert. Der Nutzer wird mehrere Teil-Identitäten auf seinem System speichern, die er mit einem Identitätsmanagement-System verwaltet.

3 Identitätsmanagement

Tritt ein Nutzer gegenüber Kommunikationspartnern mit unterschiedlichen Teil-Identitäten auf, dann betreibt er Identitätsmanagement. Identitätsmanagement ermöglicht es dem Nutzer, sicher zu kommunizieren und sein Recht auf informationelle Selbstbestimmung zu wahren. Das in diesem Beitrag vorgestellte Identitätsmanagement basiert auf verschiedenen früheren Ansätzen, die teilweise durch die Entwicklung der hier vorliegenden Arbeit entstanden sind [Jen00, Ger01a, Jen01, Ger01b, Jen02]. Die Arbeiten fremder Autoren beschäftigen sich mit technischen Details und politischen sowie rechtlichen Aspekten des Identitätsmanagements. Nicht oder erst später wurde in ihnen die theoretische Fundierung des Konzeptes Identitätsmanagement, dessen Erprobung in der Praxis sowie dessen Benutzbarkeit behandelt. Im Folgenden wird auf bestehende Identitätsmanagementsysteme eingegangen und die Komponenten eines generischen Identitätsmanagements beschrieben.

3.1 Verwandte Arbeiten zu Identitätsmanagement

Bereits im Jahr 1985 wurden erste Ideen zu einem Identitätsmanagement veröffentlicht, ohne jedoch diesen Begriff zu verwenden: In [Cha85] wird die Identifikation von Nutzers mittels digitaler Pseudonyme beschrieben. Die Generierung und Speicherung dieser Pseudonyme wird beim Nutzer propagiert, um die Verkettbarkeit zu reduzieren. Dazu wird ein mobiles, persönliches Endgerät (PDA) vorgeschlagen.

Mit dem *Identity Protector* wurde 1995 das erste Identitätsmanagementsystem zum Schutz der Anonymität des Nutzers vorgeschlagen [Ros95]. Es sollte dem Nutzer ermöglichen, seine Identität hinter sogenannten Pseudo-Identitäten, die den Teil-Identitäten ähneln, zu verbergen. Es werden verschiedene Systemarchitekturen vorgeschlagen: In-

tegration und Betrieb als Teilsystem in das eigene System oder in das System von vertrauenswürdigen Dritten. Allerdings wurde der *Identity-Protector* bisher nicht implementiert.

Die erste Implementierung einzelner Funktionen eines Identitätsmanagementsystems wurde im *Erreichbarkeitsmanager* realisiert [Dam95]. Ein Nutzer identifiziert sich gegenüber seinem Kommunikationspartner mit einem Pseudonym, das die vom Nutzer gewählten personenbezogenen Daten und kryptographische Schlüssel enthalten kann und zur Wiederverwendung in späteren Transaktionen mit dem Kommunikationspartner verknüpft wird. Bei der Implementierung dieser Funktionen wurde auf deren Benutzbarkeit geachtet: Die Pseudonyme wurden als Ausweise und Visitenkarten auf einem mobilen Endgerät visualisiert, um eine verständliche Interaktionen mit ihnen durch den Einsatz vertrauter Objekte zu erzielen.

Eine erste Implementierung von Funktionen eines Identitätsmanagement für das WWW wurde 1997 in den Bell Laboratories vorgenommen [Gab97]. Der *Janus Personalized Web Anonymize*r (später *Lucent Personalized Web Assistant, LPWA*) bietet Funktionen, um anonym WWW-Seiten aufzurufen und um personalisierte WWW-Seiten mit vorher definierten Pseudonymen zu nutzen. Dieses System setzt voraus, dass der Nutzer dem LPWA-Betreiber vertraut.

Das bisher umfassendste kommerzielle Identitätsmanagementsystem war der *Freedom*-Dienst der Firma Zero-Knowledge, der von 1998 bis 2001 betrieben wurde [Gol99]. Dieser Dienst ermöglicht dem Nutzer, unter verschiedenen Rollen (*Nyms*) aufzutreten, die den Teil-Identitäten ähneln. Dabei ist der Dienst nicht auf das WWW beschränkt, sondern unterstützt neben dem Protokoll HTTP auch die Protokolle SMTP, POP, SSL, IRC, Telnet und NNTP. Ähnlich wie der LPWA besteht auch *Freedom* aus einem Anonymitätsnetzwerk und mehreren Servern, die die benötigten Dienste (z.B. E-Mail) anbieten.

Die so genannten *Infomediaries* [Cra99] sollen dem (WWW-)Nutzer bei der Verwaltung seiner personenbezogenen Daten helfen. Der Nutzer speichert diese Daten an einer zentralen Stelle. Das System unterstützt den Nutzer bei der kontrollierten Freigabe seiner personenbezogenen Daten. Einige *Infomediaries* bieten die Verwaltung von verschiedenen Identitäten an, die aus Teilmengen der personenbezogenen Daten bestehen. Durch die zentrale Datenhaltung beim Betreiber eines solchen Dienstes wird ihm die Erstellung von umfassenden Nutzerprofilen ermöglicht und gefährdet die Privatsphäre des Nutzers.

Das im Jahr 1999 von Microsoft eingeführte *Passport*-System [Mic03] kann nicht als Identitätsmanagementdienst bezeichnet werden, da der Nutzer dabei nicht über Teil-Identitäten verfügt. Durch die zentrale Speicherung der personenbezogenen Daten beim Passport-Betreiber und aufgrund der ungenügenden Datenschutzpolitik, wie bspw. der fehlenden Berücksichtigung regionaler Datenschutzrichtlinien und der fehlenden expliziten Information des Nutzers zum Zeitpunkt der Datenweitergabe an Dritte, ist dieser Dienst nicht geeignet, die Datenschutzansprüche des Nutzers zu befriedigen.

Eine Verbesserung stellt der Identitätsmanagementdienst der Liberty Alliance dar [Lib03]. In dem Konsortium Liberty Alliance arbeiten mehr als 150 Firmen an der Spezifikation eines verteilten Identitätsmanagementdienstes, d.h. die personenbezogenen

Daten des Nutzers können durch mehrere Anbieter des Identitätsmanagementdienstes verteilt verwaltet werden. Dem Nutzer wird das rollenbasierte Auftreten unter Pseudonymen ermöglicht. Eine Verkettung der personenbezogenen Daten ist somit nur möglich, wenn sie bei allen Anbietern des Identitätsmanagementdienstes unter demselben Pseudonym verwaltet werden [Zeh02]; d.h. der Nutzer muss den Identitätsprovidern vertrauen.

Rechtliche Hintergründe des Identitätsmanagement, Anforderungen an ein generisches Identitätsmanagement im Endgerät des Nutzers sowie dessen Ziele sind in [Köh00a] beschrieben. [Köh00b] formuliert einige Anforderungen der Nutzer an ein Identitätsmanagementsystem: Das System muss den Nutzer über die Weitergabe seiner personenbezogenen Daten informieren, es muss vertrauenswürdig sein, es muss „einfach zu bedienen“ und kostengünstig verfügbar sein.

In [Cla01] wird die Verbindung von Teilidentitäten und Rechten mittels Attributzertifikaten, so genannten Credentials, beschrieben. Der Schwerpunkt liegt dabei auf einer Infrastruktur für die pseudonyme Nutzung von Credentials. An der TU Dresden wurde ein auf dieser Arbeit basierender Prototyp eines Identitätsmanagers für das beispielhafte Szenario *Einkaufen im Internet* implementiert [Kri02].

In [Koc01] wird beschrieben, wie Identitätsmanagement das Auftreten in verschiedenen Communities des Internet (z.B. Chaträume, Rollenspiele, …) erleichtern kann. Die Arbeit konzentriert sich auf die Mobilität der Daten und schlägt dazu eine zentrale Datenbank vor, die der Nutzer mit verschiedenen Anwendungen aus dem Internet erreichen kann.

IBM stellt mit dem *idemix*-System ein Identitätsmanagementsystem für die anonyme Nutzung von Credentials vor [Cam02]. Der Nutzer kann gegenüber einem Diensteanbieter mittels eines Credentials nachweisen, dass er für die Nutzung eines Dienstes berechtigt ist, ohne dass der Diensteanbieter die Aktionen des Nutzers verketten und somit ein Profil des Nutzers erstellen kann. Im Falle eines Missbrauchs ist jedoch die Identifikation des Nutzers durch eine vertrauenswürdige dritte Partei möglich.

3.2 Komponenten eines generischen Identitätsmanagements

Die ständige Weiterentwicklung der Technologie verlangt eine modulare Architektur, um zu vermeiden, dass für jedes System im software-technischen Sinne ein neues Konzept für Identitätsmanagement entwickelt werden muss. Aufbauend auf der Sicherheitsplattform mit den erforderlichen Sicherheitsmechanismen zum Schutz der Privatsphäre des Nutzers bauen die Komponenten zur Identitätskonfiguration, zur Identitätsaushandlung und zur Handlungsbestätigung auf

Die *Benutzungsoberfläche* muss entsprechend dem Modell der Teil-Identität adaptiv an das Benutzerwissen anpassbar sein [Ger00]. Von ihrer Gestaltung hängt die Akzeptanz des Sicherheitswerkzeugs hauptsächlich ab. Die Benutzungsoberfläche muss die Sicherheit des Identitätsmanagers in verständlicher Weise widerspiegeln, da Sicherheitslaien die Sicherheitsmechanismen des Identitätsmanagers nicht überprüfen und einschätzen können. Sicherheitskritische Teile der Benutzungsoberfläche, wie beispielsweise das

Signierwerkzeug, müssen im persönlichen Vertrauensbereich des Benutzers lokalisiert sein [Pfi99].

In [Ger01b] konnte durch eine Implikation der Schutzziele der mehrseitigen Sicherheit gezeigt werden, dass die Schutzziele teilweise vom System kontrolliert werden können. Dies führt zu einer Komplexitätsreduzierung auf der Benutzungsoberfläche. Die verbleibenden Schutzziele *Anonymität* und *Zurechenbarkeit* müssen jedoch vom Nutzer direkt konfiguriert werden. Dies ist jedoch eine schwierige Aufgabe [Cla99], die Fachwissen und Zeit vom Nutzer verlangt und daher nicht zumutbar ist. Diese Komplexität kann reduziert werden, indem die nutzerkontrollierten Schutzziele dem Nutzer als Teil-Identität(en) dargestellt werden.

Die *Identitätskonfiguration* ermöglicht dem Benutzer, situationsgerecht eine Teil-Identität auszuwählen und zu erstellen, mit der er sich seinem Kommunikationspartner gegenüber zeigen möchte. Dieser Auswahlvorgang ist größtenteils automatisierbar, da das System eine erneute Kommunikation mit einem schon bekannten Partner erkennen und die früher mit diesem Partner genutzte Teil-Identität auswählen kann. Das System hat die Möglichkeit, Kontextinformationen wie Ortswechsel, Zeit oder Nutzeraktionen auszuwerten, um einen Situationswechsel zu erkennen. Wechselt der Benutzer nachträglich innerhalb dieser Situation die Teil-Identität, so muss das System prüfen, ob der Grad der Anonymität der neuen Teil-Identität noch erreichbar ist. Da man gegenüber einem Partner seinen Grad der Anonymität nicht nachträglich erhöhen kann (Monotonie der Anonymität [Wol00]), ist die Teil-Identität innerhalb einer Situation nicht beliebig wechselbar.

Eine *Identitätsaushandlung* ist dann notwendig, wenn ein Teilnehmer über seinen Kommunikationspartner mehr wissen möchte, als dieser anfangs preiszugeben bereit ist oder ein Konflikt über den Grad der Verbindlichkeit dieser Kommunikation besteht. Deshalb muss den Kommunikationspartnern die Möglichkeit gegeben werden, die Teil-Identitäten untereinander auszuhandeln. Dabei müssen drei verschiedenen Arten der Aushandlung berücksichtigt werden:

- **Mensch-Mensch:** Zwei Kommunikationspartner müssen sich über die auszutauschenden Teil-Identitäten einigen. Es kann eine mehrstufige Aushandlung stattfinden.

- **Mensch-Maschine:** Diese Situation findet sich häufig im Bereich des E-Commerce. Der Nutzer muss dem Server persönliche Daten wie Name, Adresse oder Finanzdaten bekannt geben. Oft werden weitere Daten verlangt. Hier kann eine Aushandlung stattfinden, wobei beispielsweise eine Übertragung von Bezahlinformationen von weiteren Daten durch den Server abhängen kann.

- **Maschine-Maschine:** In vielen Situationen ist eine automatische Aushandlung ohne direkte Benutzerbeteiligung möglich. So wird beispielsweise im Erreichbarkeitsmanagement zwischen dem angerufenen und dem anrufenden Gerät ausgehandelt, ob und wie der Anruf signalisiert werden soll.

Handlungsbestätigung: Der Benutzer muss für jede Teil-Identität bestimmen können, ob seine Handlungen oder die Handlungen seines Partners zurechenbar sein sollen. Dabei

müssen die vier Fälle der Zurechenbarkeit [Jen00] berücksichtigt werden (z.B. für eine Kommunikation zwischen Alice und Bob):

- Alice signiert.
- Bob signiert.
- Alice schickt eine Empfangsbestätigung.
- Bob schickt eine Empfangsbestätigung.

Die Einheit Handlungsbestätigung stellt dafür die nötigen Werkzeuge wie ein Signierwerkzeug und einen Ortsstempeldienst [Zug01] zur Verfügung.

Die *Sicherheitsplattform* beinhaltet die Schnittstelle zu kryptographischen Primitiven (z.B. Signatur- und Verschlüsselungsverfahren) und zu einem Anonymitätsnetzwerk, die Verwaltung der Verbindungen zu den Kommunikationspartnern und eine gesicherte Datenbank für die geschützte Verwaltung der Teil-Identitäten. Alle zuvor genannten Bestandteile bauen auf dieser modularen Sicherheitsplattform auf, da sie die erforderlichen Sicherheitsfunktionalitäten zur Verfügung stellt und die vom Benutzer ausgewählten Sicherheitseinstellungen garantieren kann. Das Anonymitätsnetzwerk ist die Grundlage des Identitätsmanagements. Es garantiert dem Benutzer ein anonymes Auftreten im Netz, wobei sich der Benutzer gegenüber seinem Kommunikationspartner durch die Auswahl von Teil-Identitäten nach Wunsch identifizieren kann.

4 Der Identitätsmanager

Zur Evaluierung des vorgestellten Identitätsmanagements wurde ein Identitätsmanager-Prototyp für mobile Endgeräte entwickelt, der auf der CeBIT 2003 ausgestellt wurde. Der Identitätsmanager ist in ein sicheres Gesamtsystem integriert, das auf einem Compaq iPAQ H3870 implementiert ist. Im WWW steht zudem ein Demonstrator des Prototypen zur Verfügung, der sich an den Anwendungsfällen des zugrunde liegenden Szenarios orientiert.[1] Im Folgenden wird der Entwurf des Prototypen und dessen Einsatz in einem beispielhaften Szenario beschrieben.

4.1 Szenario: Kauf und Kontrolle einer digitalen Zugfahrkarte

Das Szenario, in dem die Funktionsweise des Identitätsmanagers demonstriert wird, bezieht sich auf den Kauf einer digitalen Zugfahrkarte mit dem mobilen Endgerät des Nutzers und deren Kontrolle durch das Zugpersonal. Dazu verfügt das mobile Endgerät neben dem Identitätsmanager und verschiedene Anwendungen, u.a. eine elektronische Geldbörse, einen WWW-Browser und eine E-Ticketanwendung.

[1] http://tserv.iig.uni-freiburg.de/telematik/forschung/projekte/kom_technik/atus/idm-demo/index.html

Der Nutzer lädt sich zu Beginn elektronische Münzen in seine elektronische Geldbörse. Bei dieser Transaktion mit seiner Bank muss er sich authentifizieren, damit die Bank das Konto des Nutzers entsprechend belasten kann. Dazu tritt der Nutzer unter der Teil-Identität *Bank* auf. Für die anschließende Fahrplanauskunft nutzt der Kunde über den Identitätsmanager die anonyme Teil-Identität. Der Kunde kauft seine Fahrkarte erst im Zug, die dort über einen funkbasierten virtuellen Fahrkartenautomaten bezogen werden kann. Der Kunde bezahlt anonym mit den elektronischen Münzen und erhält ein elektronisches Ticket. Ein Zugbegleiter kann das Ticket überprüfen, wobei der Kunde mit einem Einmalpseudonym (z.B. mit einer Teilidentität *Reisen*) auftritt. Dieses dient der Zurechnung des Tickets zum Kunden, die durch einen Vergleich der angezeigten Daten des Zugbegleiter-PDAs mit dem Kunden-PDA vorgenommen werden kann. Der ökonomische Wert einer Teil-Identität wird durch die Aushandlung personenbezogenen Daten gegen den Erhalt von Prämienpunkten beim Kauf einer digitalen Zugfahrkarte veranschaulicht. Das Szenario und die damit verbundenen Sicherheitsanforderungen an die eingesetzten IT-Systeme sind detailliert in [Ger03] beschrieben. Das Szenario war Gegenstand der Ausstellung des Schwerpunktprogramms 1079 „Sicherheit in der Informations- und Kommunikationstechnik“ der DFG auf der CeBIT 2003.

4.2 Architektur des Identitätsmanagers für mobile Endgeräte

Der Identitätsmanager ist das zentrale Sicherheitswerkzeugs des mobilen Endgerätes. Er stellt sowohl die Schnittstelle der Sicherheitsmechanismen des Systems zum Nutzer als auch zu den Anwendungen des Systems dar. Der Zugang zu den personenbezogenen Daten und zu den kryptographischen Schlüsseln des Nutzers erfolgt ausschließlich über den Identitätsmanager. Die Anfrage einer Anwendung nach diesen Daten wird vom Identitätsmanager daraufhin geprüft, ob der Nutzer die angefragten Daten in der momentanen Situation freigegeben hat. Die folgende Abbildung zeigt die Architektur des Identitätsmanagers. Eine ausführliche Beschreibung der Systemarchitektur für das mobile Endgerät und den zugehörigen Sicherheitsmechanismen und Anwendungen findet sich in [Ger03].

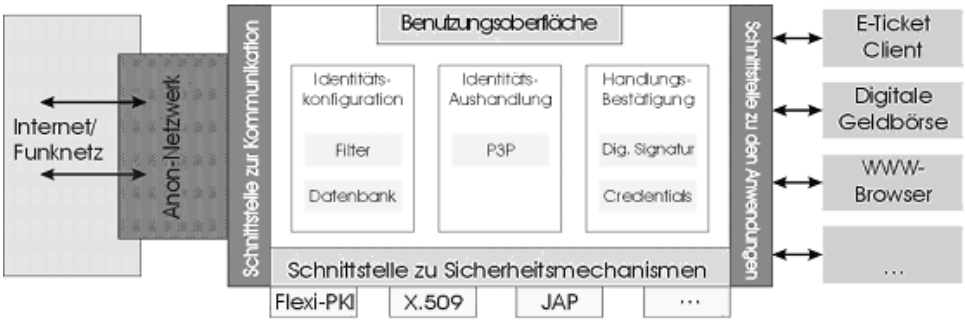

Abbildung 4.1 Architektur des Identitätsmanagers für mobile Endgeräte

Die Akzeptanz des Identitätsmanagers ist wesentlich von dessen *Benutzungsoberfläche* abhängig. Bei der Gestaltung wurde deshalb großer Wert auf die intuitive Bedienbarkeit gelegt, um Unsicherheiten und eine mögliche Fehlbedienung bereits im Vorfeld weitgehend auszuschließen. Deshalb wurde bereits zu Beginn der Entwicklung dessen Zielgruppe (Sicherheitslaien) miteinbezogen. Die Benutzungsoberfläche zeigt dem Nutzer die aktuelle Identität mit den betreffenden personenbezogenen Daten an. Die folgende Abbildung stellt die Integration des Identitätsmanagers in die Benutzungsoberfläche des mobilen Endgerätes dar. Der Nutzer kann jederzeit seine Identität überprüfen, ohne die Benutzungsoberfläche der primären Anwendung zu behindern. Die Benutzungsoberfläche wurde während der Entwicklung iterativ in Benutzertests evaluiert. Die Ergebnisse der Tests gingen in die weitere Implementierung ein [Ger03b].

Abbildung 4.2 Integration des Identitätsmanagers in die Benutzungsoberfläche des mobilen Endgerätes

Die *Identitätskonfiguration* beinhaltet die Funktionen zur Verwaltung und Auswahl von Teil-Identitäten, die gesicherte Datenbank und die Situationserkennung. Die gesicherte Datenbank speichert die Teil-Identitäten, die personenbezogenen Daten des Nutzers sowie die Regeln für den situationsabhängigen Umgang mit den Teil-Identitäten. Für diesen Prototyp wird eine Situation u.a. durch den Kommunikationspartner, die aktuelle Anwendung und die vorliegende Teil-Identität bestimmt [Jen02]. Ein Filter überprüft den Datenstrom des mobilen Endgerätes nach personenbezogenen Daten des Nutzers. So kann er beispielsweise Felder eines WWW-Formulars erkennen, falls sie sich an den P3P-Standard richten, und die dort geforderten Daten einfügen, soweit sie in der aktuellen Teil-Identität freigegeben sind.

Mit der *Identitätsaushandlung* können Konflikte zwischen dem Nutzer und einem Kommunikationspartner ausgehandelt werden, die sich auf die Menge der angeforderten personenbezogenen Daten und die Art der Zurechenbarkeit beziehen. Durch die Implementierung von P3P zur Darstellung der personenbezogenen Daten ist eine begrenzte Aushandlung möglich, wenn das System des Nutzers die Datenschutzrichtlinie des Nutzers mit der des Kommunikationspartners vergleicht. Im Fall eines Konfliktes kann der Identitätsmanager den Nutzer auf diesen Konflikt aufmerksam machen und ihm Lösungen zur Auflösung des Konfliktes vorschlagen. In der folgenden Abbildung wird eine solche Interaktion des Identitätsmanagers mit dem Nutzer dargestellt: Der Nutzer möchte

beim Kauf einer digitalen Zugfahrkarte Prämienpunkte erhalten, muss dafür aber bestimmte personenbezogene Daten an den Betreiber des Fahrkartenautomaten freigeben. Der Identitätsmanager schlägt ihm dazu u.a. eine passende Teil-Identität für diese Situation vor.

Abbildung 4.3 Aushandlung eines Konfliktes

Zur *Handlungsbestätigung* und zur Durchsetzung des Schutzzieles *Zurechenbarkeit* wurde ein Signierwerkzeug integriert. Es wird von einer Anwendung aufgerufen, sobald diese eine digitale Signatur benötigt. Zum Erstellen einer digitalen Signatur muss sich der Anwender mit seiner handschriftlichen Unterschrift authentifizieren, wodurch ihm die Handlung „Unterschreiben“ und die damit verbundene Willenserklärung verdeutlicht werden. Die Schlüsselverwaltung wird vor dem Anwender so weit wie möglich verdeckt. So erfolgt beispielsweise die Auswahl des Signaturschlüssels implizit über die Auswahl einer Teilidentität. Die Ergebnisse der Systemtests zeigten, dass die handschriftliche Unterschrift für den Nutzer verständlich und den anderen genutzten Präsentationsmethoden überlegen [Ger01a], wenn auch hardwareintensiver ist. Das Credential-Werkzeug des Identitätsmanagers ermöglicht das Erstellen, Einsehen, Prüfen und Weitergeben von Credentials.

Mit den Schnittstellen zu den Sicherheitsmechanismen des mobilen Endgerätes wird die *Sicherheitsplattform* für den Identitätsmanager realisiert. Um das Schutzziel *Anonymität* zu erreichen, werden die Sicherheitsmechanismen JAP [Ber00] zur anonymen Nutzung der Dienste des WWW, die kryptographischen Primitive zur Verschlüsselung und digitalen Signatur und ihr Einsatz im Rahmen der FlexiPKI [Buc99] und die Sicherheitsmechanismen der Bibliothek zur spontanen Vernetzung, zur vertraulichen und zurechenbaren Kommunikation über Funktechnologien [Sed01] konfiguriert und eingesetzt.

Mit diesem mobilen Identitätsmanager wurde gezeigt, dass ein Nutzer sein Auftreten gegenüber verschiedenen Kommunikationspartnern über Teil-Identitäten situationsabhängig steuern und seine personenbezogenen Daten kontrollieren kann. In Nutzertests wurde gezeigt, dass das Konzept des Identitätsmanagements für Sicherheitslaien verständlich ist und eine adäquate Abstraktion von den zugrunde liegenden Sicherheitsmechanismen ist.

5 Zusammenfassung und Ausblick

Nutzer verlangen nach sicherer Kommunikation, ihre primären Ziele sind jedoch andere, wie bspw. das Versenden von E-Mails oder die Nutzung von mobilen Anwendungen. Aus diesem Grund dürfen Nutzer nicht mit Sicherheitsfunktionen „belästigt“ werden. Mit dem Identitätsmanagement wurde ein Sicherheitswerkzeug für den Sicherheitslaien entwickelt, mit dem sein Nutzer das rollenabhängige Auftreten und die situationsabhängige Veröffentlichung seiner personenbezogenen Daten kontrollieren und steuern kann. Gleichzeitig übernimmt das System die Konfiguration der meisten Schutzziele, ohne den Nutzer dabei zu entmündigen. Jedoch werden die individuellen Erwartungen und Fähigkeiten seiner Nutzer nicht berücksichtigt. Für die adaptive Gestaltung von Benutzungsschnittstellen erweist sich die bisherige undifferenzierte Einteilung in Experten, Normalnutzer und Laien in der HCI [Kob99] als unzureichend. Seit Januar 2003 wird diesbezüglich eine Befragung durchgeführt [Kai03]. Die zu prüfenden Hypothesen beziehen sich auf Eigenschaften wie „Bereitschaft zur Nutzung von Sicherheitsmechanismen“, „Sicherheitsbewusstsein“ und „Sicherheitskompetenz“. Die Daten sowohl dieser Befragung als auch die Ergebnisse der Systemtests dienen als Input zu einer differenzierten Nutzermodellierung und damit als Voraussetzung für eine adaptive Benutzungsschnittstelle von Sicherheitswerkzeugen. Zudem müssen für ein weit verbreitetes Identitätsmanagement geeignete Protokolle entwickelt werden, damit die Übertragung von Reputationen von Teil-Identitäten des Nutzers auf eine andere Teil-Identität des Nutzers ohne Beeinträchtigung seiner informationellen Selbstbestimmung, die anwendungsunabhängige Integration in IT-Systeme und die damit verbundene systemübergreifende Aushandlung von Identitäten möglich ist.

6 Danksagung

Der vorliegende Beitrag entstand im Rahmen des DFG-Schwerpunktprogramms 1079 „Sicherheit in der Informations- und Kommunikationstechnik“ gefördert wird.

7 Literaturverzeichnis

[Ber00] Berthold, O, Federrath, H. und Köhntopp, M. Project 'Anonymity and Unobservability in the Internet'. In *Workshop on Freedom and Privacy by Design / Conference on Freedom and Privacy 2000*, S. 57-65, Toronto/Canada, April 2000.

[Buc99] Buchmann, J., Ruppert, M. und Tak, M.. *FlexiPKI - Realisierung einer flexiblen Public-Key-Infrastruktur*. Technischer Bericht der TU Darmstadt, Dezember 1999.

[Bun83] Bundesverfassungsgericht. Volkszählungsurteil. In *Entscheidungen des Bundesverfassungsgerichts*, Band 65, Seite 1 ff. 1983. Urteil vom 15.12.1983; Az.: 1 BvR 209/83; NJW 84, 419.

[Cam02] Camenisch, J. und Van Herreweghen, E. Design and Implementation of the idemix Anonymous Credential System. In *9th ACM Conference on Computer and Communications Security*, S. 21-30. ACM Press, November 2002.

[Cha85] Chaum, D. Security without Identification: Transaction Systems to make Big Brother Obsolete. *Communications of the ACM*, 28(10):1030-1044, Oktober 1985.

[Cla93] Clarke, R. Computer Matching and Digital Identity. In *Proceedings of the Computers, Freedom & Privacy Conference*, San Francisco, 1993.

[Cla99] Clarke, R. Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice. In *Proceedings of the User Identification and Privacy Protection Conference*, Juni 1999.

[Cla01] Clauß, S. und Köhntopp, M. Identity management and its support of multilateral security. *Computer Networks*, 37(2):205-219, Oktober 2001.

[Cra99] Cranor. L.F. Agents of Choice: Tools that Facilitate Notice and Choice about Web Site Data Practices. In *Proceedings of the 21st International Conference on Privacy and Personal Data Protection*, S. 19-25, September 1999.

[Cra02] Lorrie Cranor, Mark Langheinrich, M. Massimo, M. Presler-Marshall, and J. Reagle. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. http://www.w3.org/TR/P3P/, April 2002.

[Dam95] Damker, H., Rannenberg, K. und Müller, G. Erreichbarkeitsmanagement und mehrseitige Sicherheit aus Benutzersicht. In *Fachvorträge auf dem 4. deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik*, BSI-Druckschrift 7165, Mai 1995.

[Fox00] Fox, S. Trust and Privacy Online: Why Americans Want to Rewrite the Rules. Technical report, The Pew Internet & American Life Projekt, August 2000.

[Gab97] Gabber, E., Gibbons, P.B. Matias, Y. und Mayer, A.. How to Make Personalized Web Browsing Simple, Secure, and Anonymous. In *Proceedings of Financial Cryptography 97*, LNCS 1318. Springer Verlag, Februar 1997.

[Ger00] Gerd tom Markotten, D. und Kaiser, J. Benutzbare Sicherheit - Herausforderungen und Modell für E-Commerce-Systeme. *Wirtschaftsinformatik*, 42(6):531-538, Dezember 2000.

[Ger01a] Gerd tom Markotten, D., Jendricke, U. und Müller, G. Benutzbare Sicherheit - Der Identitätsmanager als universelles Sicherheitswerkzeug. In Günter Müller und Martin Reichenbach (Eds.), *Sicherheitskonzepte für das Internet*, Kapitel 7, S. 135-146. Springer-Verlag Berlin, Mai 2001.

[Ger01b] Gerd tom Markotten, D. und Jendricke, U. Identitätsmanagement im E-Commerce. *it+ti Informationstechnik und Technische Informatik*, 43(5):236-245, Oktober 2001.

[Ger03a] Gerd tom Markotten, D., Wohlgemuth, S. und Müller, G. Mit Sicherheit zukunftsfähig. PIK Sonderheft Sicherheit 2003, 26(1):5-14, 2003

[Ger03b] Gerd tom Markotten, D.,: Benutzbare Sicherheit für informationstechnische Systeme, Dissertation an der Albert-Ludwigs-Universität Freiburg, 2003.

[Gol99] Goldberg, I. und Shostack, A.. The Freedom Network Architecture. In *Proceedings of the IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology ICCST'99*, S. 298-303, Oktober 1999.

[Keu97] Keupp, H. und Höfer, R. (Hrsg.). *Identitätsarbeit heute*. Suhrkamp. 1997.

[Kai03] Kaiser, J.: Besteht eine Beziehung zwischen Nutzbarkeit und Sicherheit? - Entwurf einer Empirie zur Nutzung heutiger Sicherheitsmechanismen in IT-Anwendungen, in: PIK Sonderheft „Sicherheit 2003“, 2003.

[Koc01] Koch, M. und Wörndl, W.. Community Support and Identity Management. In *Proc. Europ. Conference on Computer-Supported Cooperative Work (ECSCW2001)*, Bonn, September 2001.

[Köh00a] Köhntopp, M. Generisches Identitätsmanagement im Endgerät. In *Materialien zum GI-Workshop 'Sicherheit und Electronic Commerce - WSSEC 2000'*, März 2000.

[Köh00b] Köhntopp, M.. Identitätsmanagement - Anforderungen aus Nutzersicht. In *Workshop 'Datenschutz und Anonymität' des NRW-Forschungsverbundes Datensicherheit*, Düsseldorf, März 2000.

[Kob99] Kobsa, A., Wahlster, W. (Hrsg.): User Models in Dialog Systems, Springer Verlag, Berlin, 1989.

[Jen00] Jendricke, U. und Gerd tom Markotten, D. Usability meets Security - The Identity-Manager as your Personal Security Assistant for the Internet. In *Proceedings of the 16th Annual Computer Security Applications Conference*, pages 344-353, Dezember 2000.

[Jen01] Jendricke, U. und Gerd tom Markotten, D. Identitätsmanagement: Einheiten und Systemarchitektur. In Dirk Fox, Marit Köhntopp, and Andreas Pfitzmann (Hrsg.), *Verlässliche IT-Systeme - Sicherheit in komplexen Infrastrukturen*, S. 77-85. Vieweg, Wiesbaden, September 2001.

[Jen02] Jendricke, U., Kreutzer, M. und Zugenmaier, A. Mobile Identity Management. Technical Report 178, Institut für Informatik, Universität Freiburg, Oktober 2002. Workshop on Security in Ubiquitous Computing, UBICOMP 2002.

[Kri02] Kriegelstein, T. Entwurf und Implementierung eines Identitätsmanagements anhand eines Beispielszenarios, Februar 2002. Diplomarbeit.

[Lib03] Liberty Alliance Project. Specifications Version 1.1. http://www.projectliberty.org/specs/archive/v1_1/liberty-specifications-v1.1.zip, Januar 2003.

[Mul98] Müller, G. und Stapf, K.-H. (Hrsg.). *Erwartung, Akzeptanz, Nutzung*, *Mehrseitige Sicherheit in der Kommunikationstechnik*, Band 2, Addison Wesley Longman Verlag GmbH. 1998.

[Mic03] Microsoft Corporation. Microsoft .NET Passport Review Guide. http://www.microsoft.com/net/services/passport/review_guide.asp, Juni 2003.

[Nat00] National Consumer Council. E-commerce and consumer protection. A report by the National Consumer Council, August 2000.

[Pep97] Peppers, D. und Rogers, M. *Enterprise One to One: Tools for Competing in the Interactive Age*. Doubleday. Februar 1997.

[Pfi199] Pfitzmann, A., Pfitzmann B., Schunter M. und Waidner, M. Trustworthy User Devices. In Günter Müller und Kai Rannenberg (Hrsg.), *Technology, Infrastructure, Economy*, Volume 3 of *Multilateral Security in Communications*, S. 137-156. Addison Wesley Longman Verlag GmbH, 1999.

[Pfi00] Pfitzmann, B., Waidner, M. und Pfitzmann, A. Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity. Technical Report RZ 3232 (93278) 05/22/00, IBM Research Division, Zürich, Mai 2000.

[Ran97] Rannenberg, K., Pfitzmann, A. und Müller, G. Sicherheit, insbesondere mehrseitige IT-Sicherheit. In Günter Müller und Andreas Pfitzmann (Hrsg.), *Mehrseitige Sicherheit in der Kommunikationstechnik*, S. 21-29. Addison-Wesley Longman Verlag GmbH, 1997.

[Ros95] van Rossum, H., Gardeniers, H. und Borking, J. et. al. Privacy-Enhancing Technologies: The Path to Anonymity, August 1995.

[Sed01] Sedov, I., Haase, M., Cap, C. und Timmermann, D. *Hardware Security Concept for Spontaneous Network Integration of Mobile Devices*. In Proceedings of the International Workshop "Innovative Internet Computing Systems", Ilmenau, Juni 2001.

[Sch99] Schoder, D. und Müller, G.. Potentiale und Hürden des Electronic Commerce: Eine Momentaufnahme. *Informatik Spektrum*, 22(4):252-260, 1999.

[Tel97] Teledienstedatenschutzgesetz, July 1997. Artikel 2 G 9020-6/1 v. 22.7.1997 I 1870 (IuKDG).

[Wai98] Waidner, M. Open Issues in Secure Electronic Commerce. Technical report, IBM Research Division, Zürich, Oktober 1998.

[Wes67] Westin, A.F. *Privacy and Freedom*. Atheneum, New York, NY. 1967.

[Whi99] Whitten, A. und Tygar, J.D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, August 1999.

[Wol00] Wolf, G. und Pfitzmann, A. Properties of protection goals and their integration into a user interface. *Computer Networks*, 32:685-699, 2000.

[Zeh02] Zehentner, J.. Privatheit bei Anwendungen für Identitätsmanagement im Internet, Dezember 2002.

[Zug01] Zugenmaier, A., Kreutzer und Kabatnik, M. Enhancing Applications with Approved Location Stamps. In *2001 IEEE Intelligent network workshop proceedings*, 2001.