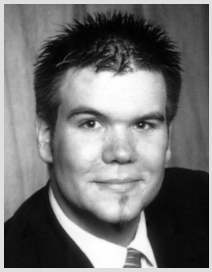
DuD
Datenschutz und Datensicherheit

Mobilität, mobile Technologie und Identität

Mobile Identitätsmanagementsysteme

Denis Royer, Kai Rannenberg

Die Beziehungen zwischen Mobilität und Identität sind nicht nur vielschichtig sondern werden mit der Berücksichtigung von Mobilität und mobiler Technologien in Identitätsmanagementsystemen auch immer wichtiger. Dieser Beitrag gibt einen Überblick über die verschiedenen Aspekte von Identität und Mobilität, wie sie im Work Package 11 von FIDIS behandelt werden und vertieft diese anhand eines Anwendungsszenarios aus dem Bereich „Mobiles Leben und Arbeiten“.



Dipl.-Wirt.-Inf. Denis Royer ist wiss. Mitarbeiter an der T-Mobile Stiftungsprofessur für Mobile Commerce und Mehrseitige Sicherheit an der Johann Wolfgang Goethe Universität, Frankfurt am Main und Koordinator des EU-Ecellenznetzes FIDIS („Future of Identity in the Information Society“, www.fidis.net).

E-Mail: Denis.Royer@M-Lehrstuhl.de

Prof. Dr. Kai Rannenberg ist Inhaber der T-Mobile Stiftungsprofessur für Mobile Commerce und Mehrseitige Sicherheit an der Johann Wolfgang Goethe-Universität, Frankfurt am Main (www.m-lehrstuhl.de) und Chefkoordinator von FIDIS.

E-Mail: Kai.Rannenberg@M-Lehrstuhl.de

1 Einleitung

Identitätsmanagementsysteme werden in der Informationsverarbeitung immer wichtiger. Ihre Funktionalitäten umfassen dabei ein ganzes Spektrum von auf der einen Seite Single-Sign-On-Systemen zur Vereinheitlichung von Nutzeridentitäten bis zu auf der anderen Seite der Verwaltung mehrerer Identitäten durch einen Nutzer, so dass er in verschiedenen Kontexten verschiedene Identitäten nutzen kann [Ra04].

Während Identitätsmanagement für das Internet intensiv in der wissenschaftlichen Literatur diskutiert wird, ist es um mobiles Identitätsmanagement eher still. Gleichzeitig ist jedoch eines der größten, wenn nicht das größte Identitätsmanagementsystem eng mit dem in der Mobilkommunikation dominierenden „*Global System for Mobile Communication*“ (GSM), das gegenwärtig 1,94 Mrd. Nutzer[1] weltweit verwaltet, verbunden.

Dieser Beitrag gibt einen Überblick über die verschiedenen Aspekte von Identität und Mobilität als Merkmale mobiler Identitätsmanagementsysteme. Dabei werden zunächst soziokulturelle, technologische und rechtliche Perspektiven berücksichtigt. Ein Anwendungsszenario aus dem Bereich „Mobiles Leben und Arbeiten“ vertieft die Betrachtung, bevor ein Ausblick auf die ökonomischen Aspekte erfolgt.

2 Mobilität und Identität

Der Themenkomplex „*Identität und Mobilität*“ liegt im Interesse einer Vielzahl verschiedener Disziplinen, die eine hohe interdisziplinäre Vernetzung haben. Dies macht insbesondere eine einfache Klassifizierung und Abgrenzung unmöglich (vgl. Abbildung 1). Deshalb wurden im Rahmen des Work Package 11 „Mobility and Identity“ des EU-Projektes FIDIS (Future of Identity in the Information Society, www.fidis.net) zunächst die soziokulturellen, technologischen und rechtlichen Aspekte und ihre Überlappungen analysiert [Ro06].

[1] Stand 2006 [GSM 2006].

2.1 Die soziokulturelle Perspektive

Einer der in FIDIS verwendeten soziokulturellen Ansätze zur Beschreibung von Mobilität ist die Aufteilung nach Idem- und Ipse-Identität, wie sie von Paul Ricoeur [Ri92] vorgestellt wurde:

- Die *Idem*-Identität, welche aus der Perspektive einer dritten Person beschreibt (Kategorisierung).
- Die *Ipse*-Identität, welche die Selbstbeschreibung einer Person aus der eigenen Sicht ist.

Werden technische und rechtliche Konzepte erstellt, adressieren, betrachten oder behandeln diese in den meisten Fällen Idem-Identitäten, die von Organisationen für ihre Mitglieder oder Klienten erstellt werden. Jedoch sollten Organisationen auch die Auswirkungen einer Idem-Kategorisierung auf die Ipse-Identität beachten, denn es funktioniert kein Geschäftsmodell ohne die Betrachtung der Ipse-Identität des Kunden: Wenn ein Kunde sich selber nicht als Adressat für ein Produkt oder eine Dienstleistung wiederfinden kann, wird er diese nicht konsumieren [Ro06].

Durch die Nutzung mobiler Technologien wird auch die Interaktion zwischen Individuen beeinflusst. So wird zwar primär über die Idem-Identität interagiert, jedoch wird durch die Kommunikation mit mobilen Endgeräten auch die Art und Weise der sozialen Interaktionen beeinflusst, wie z.B. die Kontaktaufnahme mit anderen Personen, etc. Gründe hierfür lassen sich z.B. in der dauernden Erreichbarkeit durch mobile Endgeräte und der Art und Weise finden,

wie man sich gegenüber anderen Kommunikationspartnern durch die Nutzung mobiler Endgeräte präsentiert und von ihnen wahrgenommen wird. Solche sozialen Interaktionen wirken sich schlussendlich auch auf das Selbstbild des Nutzers, also die Ipse-Identität, aus [Ro06].

Ein weiteres Konzept ist in diesem Zusammenhang das der *partiellen Identitäten*. Partielle Identitäten sind Untermengen aller beschreibenden Merkmale (Attribute) einer Identität, die je nach Kontext genutzt werden können [NaHi04]. Abbildung 2 gibt ein Beispiel, wie einzelne Attribute je nach Kommunikationskontext verschiedene partielle Identitäten bilden (siehe auch Kapitel 4).

2.2 Die technischen Herausforderungen

Besondere technische Herausforderungen ergeben sich als Konsequenzen aus der Einführung neuer mobiler Technologien, speziell mobiler Endgeräte, z.B. Mobiltelefone mit erweiterten Fähigkeiten (sog. Smartphones) oder „Personal Digital Assistants“ (PDA). Im Rahmen von FIDIS lag in einer ersten Studie der Fokus auf der Sichtweise der Nutzer solcher Geräte. In diesem Zusammenhang wurden Technologien vorgestellt, die Nutzern mobiler Endgeräte die Möglichkeit eröffnen, ihre Privatsphäre zu schützen [MüWo05]. In diesem Beitrag soll auf die drei wichtigsten Aspekte der Nutzung mobiler Endgeräte eingegangen werden:

- Die *Benutzbarkeit (Usability)* mobiler Sicherheitsmechanismen;
- Der *Schutz der Geräte und ihrer Daten* gegenüber unrechtmäßigen Besitzern;
- Die gezielte Steuerung der *Weitergabe von Identitätsmerkmalen* an andere Parteien.

2.2.1 Usability

Beim Einsatz mobiler Endgeräte ist für die meisten Nutzer die Steigerung der Produktivität das primäre Ziel. Ausgehend davon spielt Sicherheit nur eine untergeordnete Rolle, da der Einsatz von Sicherheitsmechanismen nicht unmittelbar eine höhere Produktivität zur Folge hat. Entsprechend unterschätzen viele Nutzer die Konsequenzen, die sich aus einem unzureichenden Sicherheitsbewusstsein und -handeln ergeben. Auch sind sie nur in den seltensten Fällen dazu bereit, die notwendigen Mühen in die Aktivierung und Benutzung von Sicherheitssystemen zu investieren, obwohl der unbeabsichtigte Nichtgebrauch von Sicherheitstechnologien (z.B. das Ausschalten von Passwortabfragen) Auswirkungen auf die Sicherheit eines Nutzers hat [MüWo05].

Eine Erklärung für dieses Problem lässt sich darin finden, dass die derzeit verfügbaren Sicherheitsmechanismen vielfach eine zu technische Ausrichtung haben und die Anforderungen der Nutzer, speziell die einfache Anwendbarkeit, außer Acht gelassen werden [MüWo05].

Ein Ansatz für die Lösung dieser Probleme ist der *iManager*[2]. Dieser Prototyp für ein mobiles Identitätsmanagementsystem erlaubt es auch Nichtexperten, ihre partiellen Identitäten auf mobilen Endgeräten verwalten zu können. Durch eine einfach verständliche Nutzerführung und eine anwenderfreundlichen Bedienoberfläche kann einem unbeabsichtigten Fehlgebrauch entgegengewirkt werden, und mögliche Gefahren für die Sicherheit können minimiert werden.

2.2.2 Schutz der Geräte und Daten

Mobile Engeräte speichern eine Vielzahl von Daten und Credentials, die es ihrem Nutzer z.B. erlauben, sich gegenüber Diensten ausweisen zu können. Wird nun das mobile Endgerät mit allen im Gerät gespeicherten Daten gestohlen, so hat der unrechtmäßige Besitzer die Möglichkeit, betrügerisch Aktivitäten im Namen des eigentlichen Eigentümers durchzuführen, da sich dessen digitale Identitätsmerkmale in seinem Besitz befinden (Identitätsbetrug) [Le06]. Für das Identitätskonzept in einem mobilen Umfeld ist es somit wichtig, dass das mobile Endgerät die digitalen Identitätsmerkmale mit einer real existierenden Person verknüpfen kann, um deren Authentizität zu verifizieren. Der einfachste Ansatz ist die Nutzung der PIN als Zugangskontrolle. Aber auch der Einsatz aufwendigerer Technologien, wie z.B. die Abfrage biometrischer Merkmale zur Nutzeridentifikation, ist denkbar [MüWo05].

[2] Weitere Details über den *iManager* lassen sich im Internet unter www.iig.uni-freiburg.de /telematik/atus/idm-demo nachlesen.

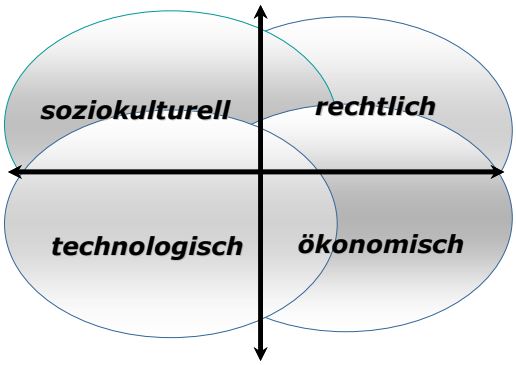


Abbildung 1: Relevante Aspekte im Bereich Mobilität und Identität

2.2.3 Weitergabe von Identitätsmerkmalen

Insbesondere mobile Dienste (etwa Location Based Services (LBS)) werden oft durch Konsortien aus z.B. Mobilfunkbetreibern und Dienstanbietern erbracht. Dabei werden (möglicherweise im Auftrag eines Nutzers) Nutzerdaten an andere Dienstanbieter (etwa Apothekenfinder) weitergeben, Wenn der Mobilfunkanbieter die Lokationsdaten jedoch ohne Berechtigung weitergibt, besteht die Gefahr, dass Nutzer gegen ihren Willen identifiziert oder lokalisiert werden können.

Deswegen muss das Risiko reduziert werden, dass Identitätsmerkmale an Parteien weitergegeben werden, die sie gegen den Willen der Identifizierten einsetzen. Aus diesem Grund müssen Nutzer die Weitergabe ihrer persönlichen Daten und Attribute gezielt steuern können und durch entsprechende Mechanismen unterstützt werden.

2.3 Die rechtlichen Rahmenbedingungen

Mit der immer weiter reichenden Verbreitung von Technologien wie RFID oder LBS und deren Vernetzung untereinander werden auch die einschlägigen rechtlichen Rahmenbedingungen immer bedeutender. Insbesondere der Schutz der Privatsphäre und die informationelle Selbstbestimmung sind essentielle Fragestellungen, die dauerhaft diskutiert werden [Ro06].

Auf europäischer Ebene wurden rechtliche Rahmenrichtlinien geschaffen, die den Schutz der Privatsphäre gewährleisten sollen. Hierzu gehören die „Datenschutz-Richtlinie“ [1995/46/EG], welche den Schutz natürlicher Personen bei der Verarbeitung von persönlichen Daten regelt, und die „Datenschutzrichtlinie für elektronische

Kommunikation“ [2002/58/EG], welche die Europäischen Mitgliedsstaaten verpflichtet, elektronische kommunikationsspezifische Regelungen zum Datenschutz zu erlassen.

Im Bereich der mobilen Kommunikation betreffen diese Richtlinien insbesondere die Handhabung der übermittelten Informationen. Neben den Nutzdaten sind dies die Verkehrs- und Lokationsdaten, welche z.B. für die Erbringung mobiler Dienste und deren Abrechnung nötig sind. So müssen beispielsweise die Verkehrsdaten nach ihrer finalen Verwendung gelöscht oder zumindest anonymisiert werden, um einen potentiellen Missbrauch verhindern zu können.

Ein weiteres Beispiel für die Regulierung der Handhabung übermittelter Informationen ist die Erstellung von Bewegungsprofilen durch einen Anbieter von LBS-Dienstleistungen. Die übermittelten Daten dürfen nur für diejenigen Dienstleistungen verwendet werden, für die der Dienstnutzer seine Einwilligung gegeben hat. Andererseits ist laut der „Richtlinie über die Vorratsspeicherung von Daten“ [2006/24/EG] eine Speicherung von sechs Monaten bis zu zwei Jahren möglich, die je nach Umsetzung dieser Direktive von Land zu Land differieren kann. Speziell die lange Speicherdauer der Daten für Vollzugsbehörden differiert dabei von den Prinzipien der „Datenschutz-Richtlinie“.

Angesichts der sich ständig weiterentwickelnder Technologien müssen auch zukünftig die rechtlichen Grundlagen immer wieder evaluiert werden, damit sichergestellt ist, dass das Recht auf Privatsphäre gewahrt bleibt.

3 Mobile Identitäten und mobile Identitätsmanagementsysteme

Im Bezug auf mobiles Identitätsmanagement lassen sich zwei große Bereiche unterscheiden: Zum einen bezieht sich das mobile Identitätsmanagement auf das *Management von Identitäten unter der Zuhilfenahme mobiler Endgeräte* (z.B. durch den i*Manager*). Zum anderen kann sich das mobile Identitätsmanagement auch auf das *Management mobiler Identitäten* beziehen. *Mobile Identitäten* sind (partielle) Idem-Identitäten von Personen, die um Ortsinformationen der identifizierten Person ergänzt sind. Die Ortsinformationen verändern sich mit der Zeit. Ein Beispiel für diese Art des mobilen Identitätsmanagements stellt GSM dar. Um Kommunikationsverbindungen, Kunden und Vertragsverhältnissen eineindeutig zuzuordnen, wurde bei GSM die „International Mobil Subscriber Identity“ (IMSI) eingeführt. Sie wird pro Vertragsverhältnis eineindeutig vergeben und ist der Schlüssel zum jeweiligen Kundendatensatz mit statischen Kundendaten (etwa Bürgerlicher Name und Postanschrift). Gleichzeitig ist die IMSI im Subscriber Identity Module (SIM), das in das jeweilige Endgerät gesteckt wird, gespeichert und personalisiert damit dieses Endgerät. Damit Kommunikationsverbindungen unabhängig vom Aufenthaltsort des Kunden geschaltet werden können, wirkt die IMSI als Schlüssel zu dem Datenbanksystem, in dem für alle eingeschalteten Endgeräte bzw.

die entsprechenden Identitäten die zugehörige Aufenthaltsinformation gespeichert wird.

Entsprechend lassen sich aus der Verknüpfung der während der Kommunikation angefallenen Daten Rückschlüsse auf den Aufenthaltsort des Kunden ziehen. Angesichts der Sensitivität dieser Daten wirken sich solche Speicherungen wiederum auf die *Ipse-Identität* eines Nutzers aus, wie z.B. die Vertrauensbeziehung zwischen einem Mobilfunkanbieter und einem Kunden.

„Erfolgsfaktoren" für die Umsetzung solcher mobiler Identitätsmanagementsysteme umfassen dabei folgende Prinzipien [RoPePa03, Ro06]:

Lokalitätsprinzip: Identitäten können je nach Kontext verschiedene oder überlappende Rollen oder Beziehungen haben. Deshalb muss der Nutzer in der Lage sein, zwischen verschiedenen Kontexten, in denen er sich befindet, differenzieren zu können.

Wechselseitigkeitsprinzip: Dieses Prinzip bezieht sich auf die Informations(a)symmetrie zwischen Nutzer und Anbieter. So kann es beispielsweise ein Nutzer für hilfreich erachten, dass seine Daten gesammelt werden, um einen von ihm genutzten Dienst besser an seine Bedürfnisse anpassen zu können. Auf der anderen Seite hat er nicht unbedingt die Kontrolle über die so gesammelten Profildaten. Er sollte deswegen wissen, welche Daten seitens des Dienstanbieters über ihn gespeichert werden, um ggf. auf diese Speicherung seiner Daten Einfluss nehmen zu können und um Informationsasymmetrien minimieren zu können.

Prinzip des Verstehens: Dieses Prinzip bezieht sich auf das gegenseitige Verständnis der involvierten Teilnehmer über ihre Identitäten und die Identitäten des Gegenübers. Im Umfeld von mobilen Diensten ist die Einhaltung dieses Prinzips notwendig, da die Wahrnehmung gegenüber der Identität eines Anbieters (z.B. empfundenes Risiko bei der Abwicklung einer Transaktion, etc.) sich direkt auf die Kaufbereitschaft des Käufers auswirkt.

4 Anwendungsszenario: Mobiles Leben und Arbeiten

Aufbauend auf den in den bisherigen Kapiteln vorgestellten Aspekten soll im Folgenden auf mobiles Arbeiten und die dazugehörigen Kommunikationskontexte eingegangen werden.

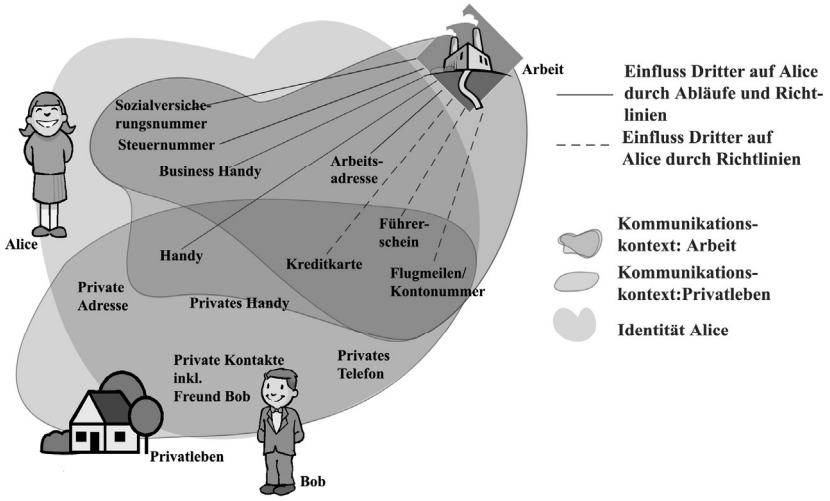


Abbildung 2: Partielle Identitäten im mobilen Arbeitsumfeld [Royer 2006]

4.1 Das mobile Arbeitsumfeld

Traditionell spielte sich der Großteil des Lebens eines durchschnittlichen Europäers in einer absehbar großen Region ab, die seinen allgemeinen Lebensmittelpunkt bildete. In den meisten Fällen waren (eher seltene) größere Ortswechsel mit dem dauerhaften Wechsel des Arbeitsplatzes und Lebensmittelpunktes an einen anderen (aber wiederum recht stabilen) Ort verbunden. „Wanderjahre" wie sie beispielsweise für Handwerker fast legendär sind, waren für Jahrhunderte eine spezielle und begrenzte Lebensphase, Mobilität war im Übrigen auf wenige Berufsgruppen (z.B. Steinmetze, Händler, Söldner) begrenzt [We05].

Heutzutage jedoch wird von arbeitenden Menschen eine weit größere Mobilität erwartet. Nicht zuletzt deswegen spielt die Mobilkommunikation eine zunehmend wichtiger werdende Rolle, um die Produktivität mobil arbeitender Personen weiter steigern zu können. Dies wird, wie eingangs bereits erwähnt, durch den Fortschritt bei den mobilen Endgeräten noch weiter forciert.

Angesichts dieser Situation müssen Organisationen, die ein mobiles Arbeitsumfeld einführen oder betreiben, folgende Kriterien im Bereich von Mobilität und Identität in ihre Überlegungen berücksichtigen [HeWe05, Ro06]:

- Flexible Arbeitszeiten;
- (IT)-Sicherheit;
- Autonomie und Flexibilität;
- Kommunikation und Kontakte;
- Privatsphäre und Datenschutzrechte.

Die Erfüllung dieser Kriterien kann dabei vielfältige Auswirkungen auf die Identität eines Nutzers haben.

4.2 Ein Fallbeispiel

Besitzt ein Mitarbeiter jeweils ein Mobilfunkgerät für das Privatleben und eines für den Beruf, so ist der Kontextwechsel zwischen Beruf und Privatleben (und den dazugehörigen partiellen Identitäten) noch relativ einfach, selbst wenn der Kontext im Zuge der fortschreitenden Flexibilisierung von Arbeitszeiten öfter wechselt als früher.

Wird jedoch vom Arbeitgeber ein mobiles Endgerät (z.B. Smartphone) zur Verfügung gestellt, das ebenfalls für private Zwecke eingesetzt werden darf, so verschwimmen Grenzen zwischen privatem und der beruflichem Kontext (siehe Abbildung 2). Auch bewegen sich partielle Identitäten und die ihnen zugeordneten Attribute (Credentials, Kontakte, etc.), die vorher nur im beruflichen Umfeld genutzt wurden, in den privaten Bereich und umgekehrt. Durch diese Entwicklung kann sich die Kontrolle der partiellen Identitäten eines Nutzers von diesem Nutzer zu anderen Organisationen, etwa der des Arbeitgebers, verschieben [Ro06].

In Bezug auf das Management der eigenen Identität eines Nutzers sind die Folgen hieraus vielschichtig: So hat etwa der Arbeitgeber die Möglichkeit, auch auf Informationen zur privaten Kommunikation zugreifen zu können (z.B. durch einen Einzelverbindungsnachweis der geführten

Gespräche) oder Bewegungsprofile zu erstellen, etwa wenn ein (ortsbasierter) Dienst genutzt wird, der dem Arbeitgeber die Position des Arbeitnehmers mitteilt, und diese Informationen in einer Datenbank zur späteren Auswertung erfasst werden. Bewegungsprofile können sich auf den privaten Kontext ausdehnen, wenn der Arbeitnehmer einen ortbasierten Dienst des Arbeitgebers innerhalb seiner Freizeit nutzt. Ein weiteres Beispiel ist die dauerhafte Erreichbarkeit für berufliche Belange, obwohl man sich im privaten Kontext befindet. In diesem Zusammenhang entstehen weitere Überlappungen der beiden Kommunikationskontexte, bzw. deren Grenzen werden vollständig aufgehoben, was sich wiederum auf die Ipse-Identität des Nutzers auswirkt (vgl. Abschnitt 2.1).

Die in den vorherigen Kapiteln angesprochenen Probleme lassen sich auch in der hier beschriebenen Fallstudie wiederfinden. So ist z.B. der Zugriff auf Daten aus dem privaten Kontext des Arbeitnehmers rechtlich nicht trivial und macht Regelungen und technische Mechanismen innerhalb der Organisation notwendig, die einen solchen Zugriff unterbinden, wenn er nicht autorisiert ist. Eine Lösung kann z.B. die Bereitstellung eines Erreichbarkeitsmanagements [RDFR97] sein, das den Nutzern erlaubt, je nach Kontext bestimmen zu können, wie, wann und wo sie erreichbar sein wollen, und eine klarere Abgrenzung der jeweiligen Kommunikationskontexte ermöglicht.

Weiterhin muss bei der Umsetzung von Identitätsmanagementsystemen dafür Sorge getragen werden, dass die Prinzipien aus Abschnitt 2.3 (Lokalität, Wechselseitigkeit und Verstehen) in den Entwicklungsprozess einfließen. Dies ist speziell der Fall für Identitätsmanagementsysteme, die mobile Identitäten verwalten [RoPePa03]: Zur Einhaltung des *Prinzips der Lokalität* muss für alle Kommunikationspartner klar sein, in welcher Rolle / Beziehung sie sich mit ihrer Identität befinden, um eine Differenzierung ihres jeweiligen Kontext ermöglichen zu können (privat, beruflich, etc.). Das *Wechselseitigkeitsprinzip* muss durch organisationsweite Regelungen zur Kontrolle der Weitergabe partieller Identitäten eines Nutzers realisiert werden, damit bekannt ist welche Daten jeweils vom Nutzer oder vom Anbieter gespeichert werden. Das *Prinzip des Verstehens* muss ebenfalls gewahrt werden, um die Identität der einzelnen Kommunikationsteilnehmer verifizieren zu können. Die einzelnen Partner müssen ihre eigene Identität und die ihres Gegenübers verstehen können. Greift der Arbeitnehmer beispielsweise auf (mobile) Dienste des Arbeitgebers zu (z.B. die Übertragung der Arbeitsergebnisse eines Außendienstmitarbeiters auf die lokale Infrastruktur des Arbeitgebers), so muss sichergestellt werden, dass es sich auch tatsächlich um einen Dienst des Arbeitgebers handelt. Durch den Einsatz von Authentifizierungsmechanismen in der Kommunikation und in den mobilen Endgeräten, ist auch dieses Prinzip umsetzbar.

Letztlich muss der Schutz der Daten auf dem Gerät gewährleistet sein, damit einem potentiellen Missbrauch (z.B. nach einem Diebstahl des Gerätes, vgl. Abschnitt 2.2) entgegengewirkt werden kann, denn ein solcher Missbrauch würde sich auch auf die privaten Bereiche auswirken [Le06, Ro06]. Beispielsweise können auf dem Gerät gespeichert private Zugangsdaten (z.B. für Online-Banking-Dienste, etc.) an unbefugte Dritte gelangen, was eine unmittelbare Gefahr darstellt.

5 Zusammenfassung und Ausblick

Der Themenkomplex Mobilität und Identität erweist sich als ein sehr umfangreiches Terrain, das vielfach noch unentdecktes Land darstellt und deshalb im Kontext von FIDIS weiter erforscht wird. Insbesondere die hohe Vernetzung der einzelnen Facetten (Technologie, Gesetzgebung, Gesellschaft, Wirtschaft, etc.) macht weitere, umfassendere Studien erforderlich.

Beispielsweise stecken relevante Technologien noch in ihren Anfangs- und Teststadien, und ihre wirtschaftlichen Aspekte (Marktteilnehmer, Geschäftsmodelle, etc.) sind noch nicht bekannt.

Ebenso sind die wirtschaftlichen und gesellschaftlichen Auswirkungen mobiler Identitätsmanagementsysteme noch nicht hinreichend untersucht worden, u.a. da sie noch kaum am Markt vertreten sind. In diesem Zusammenhang gilt es auch, die Gründe für die eher schleppende Diffusion der Systeme zu analysieren. Dazu müssen die involvierten Parteien sowie deren Interessen und Anforderungen an mobile Identitätsmanagementsysteme genauer dokumentiert und analysiert werden.

Literatur

1995/46/EG Richtlinie 1995/46/EG des Europäischen Parlaments und des Rates: Datenschutz-Richtlinie, 24.10.1995, Luxemburg, 1995.

2002/58/EG Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates: Datenschutzrichtlinie für elektronische Kommunikation, 12.07.2002, Brüssel, 2002.

2006/24/EG Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates: Richtlinie über die Vorratsspeicherung von Daten, 21.02.2006, Brüssel, 2006.

BMH05 Bauer, M., Meints, M., Hansen, M. (Hrsg.), 'D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems', FIDIS Deliverable WP 3, 2005.

GSM06 GSM Association, GSM Statistics www.gsmworld.com/news/statistics/index.shtml, besucht am 2006-07-25, 2006.

HeWe05 Hess, K., Weddige, F., Regelung und Mitbestimmung bei mobiler Arbeit, Computer Fachwissen, S. 7-11, Bund Verlag, Frankfurt a. M. 2005.

MüWo05 Müller, G., Wohlgemuth, S., (Hrsg.), Deliverable 3.3: Study on mobile identity management, FIDIS Work Package 3, 2005.

Le06 Leenes, R., Deliverable 5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research, FIDIS Work Package 5, 2006.

NaHi04 Nabeth, T., Hildebrandt, M. (Ed.), Deliverable 2.1: Inventory on Topics and Clusters, FIDIS Work Package 2, 2004.

Ra04 Rannenberg, K., Identity management in mobile cellular networks and related applications, in: Information Security Technical Report, Vol. 9, Nr. 1, 2004, S. 77-85, ISSN 1363-4127.

RDFR97 Reichenbach, M., Damker, H., Federrath, H., Rannenberg, K., Individual Management of Personal Reachability in Mobile Communication, in Louise Yngström, Jan Carlsen: Information Security in Research and Business; Proceedings of the IFIP TC11 13th International Information Security Conference (SEC '97): 14-16 May 1997, S. 163-174 Copenhagen; Chapman & Hall, London; ISBN 0-412-8178-02.

Ri92 Ricoeur, P., Oneself as another, Chicago: Chicago University Press, 1992.

RoPePa03 Roussos, G., Peterson, D, Patel, U., Mobile Identity Management: An Enacted View, Int. Jour. E-Commerce, Vol. 8, Nr. 1, S. 81-100, 2003.

Ro06 Royer, D. (Hrsg.), Deliverable D11.1: Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity, Work Package 11, 2006, www.fidis.net/fidis_del.0.html.

We05 Weiss, H., Mobil und kommunikativ, Computer Fachwissen, S. 12-13, Bund Verlag, Frankfurt a. M. 2005.