PRIME – Ein europäisches Projekt für nutzerbestimmtes Identitätsmanagement

PRIME – A European Project for Privacy-Enhancing Identity Management

Marit Hansen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Katrin Borcea-Pfitzmann, Andreas Pfitzmann, Technische Universität Dresden

Zusammenfassung Neue Konzepte für datenschutzförderndes Identitätsmanagement stehen im Mittelpunkt des Projekts „PRIME – Privacy and Identity Management for Europe". Das Projekt hat am 1. März 2004 begonnen und läuft gefördert im 6. EU-Rahmenprogramm für vier Jahre. Ziel ist, Lösungen zu erforschen und zu entwickeln, die es Menschen ermöglichen, die Kontrolle über ihre Privatsphäre im Cyberspace in die eigene Hand zu nehmen. Dieser Artikel beschreibt die Schwerpunkte der Forschung in PRIME.

►►► **Summary** New concepts establishing Privacy-Enhancing Identity Management are the central points of the project "PRIME – Privacy and Identity Management for Europe". The project was launched on March 1, 2004, and is funded by the 6th EU Framework Programme for four years. The primary objectives are research and development of solutions enabling the users to keep their privacy in cyberspace under their own control. This article describes the main focuses of research in PRIME.

KEYWORDS K.4.1 [Public Policy Issues] privacy, identity management, multilateral security, privacy, informational self-determination, pseudonym

1 Identitätsmanagement in der Informationsgesellschaft

Das Internet gehört mittlerweile zum alltäglichen Umgang und immer mehr Online-Anwendungen erleichtern das Leben der Menschen. Aber während etliche Nutzer ihre persönlichen Daten eher widerwillig und nur deswegen preisgeben, weil ihnen keine Alternative angeboten wird, gehen andere Nutzer sorglos mit ihnen um, ohne im Grunde zu wissen, was mit den Daten geschieht.

Das Hinterlassen von auswertbaren Datenspuren und Identity Theft (Identitätsdiebstahl) in der Online-Welt sind heute ständige Begleiterscheinungen geworden. Eine effektive Gegenmaßnahme wäre technisch unterstützte informationelle Selbstbestimmung[1] auf der Basis von nutzerbestimmtem Identitätsmanagement (siehe [7; 9]).

Im Gegensatz zu den bekannten Identitätsmanagement-Ansätzen von Microsoft .NET Passport[2] und der Liberty Alliance[3] [17] zielt PRIME (*Privacy and Identity Management for Europe* – Datenschutz- und Identitätsmanagement für Europa) auf die Entwicklung eines Identitätsmanagementsystems, das informationelle Selbstbestimmung in den Mittelpunkt stellt. Dies bedeutet, dass dem Nutzer in Übereinstimmung mit den europäischen Datenschutzbestimmungen[4] die Möglichkeit der Entscheidungen über seine persönlichen Daten auf der Basis von maximaler Datentransparenz gegeben wird.

Vorarbeiten zu Teilen dieses umfassenden Ansatzes, der in den folgenden Abschnitten weiter ausgeführt wird, sind bereits in anderen

[1] Volkszählungsurteil, BVerfGE 65, S. 1 ff., 1983.
[2] http://www.passport.net/.
[3] http://www.projectliberty.org/.
[4] http://europa.eu.int/comm/justice_home/fsj/privacy/.

Forschungs- und Entwicklungsprojekten realisiert worden:

- Mit P3P – *Platform for Privacy Preferences*[5] gibt es einen vom W3C standardisierten Mechanismus, um technisch gestützt die Privacy Policy des Anbieters zu interpretieren und den Kontakt zu dessen Angebot nur dann zu erlauben, wenn die Privacy Policy nicht im Widerspruch zu den Vorstellungen des Nutzers steht.
- Anonymisierungsdienste wie AN.ON[6] oder TOR[7] bieten dem Nutzer Anonymität auf Netzebene und schützen dort seine Identität. Die Anwendungsebene, auf der je nach Situation alle Facetten zwischen Anonymität und Identifizierung sinnvoll sein können, wird von diesen Diensten nicht adressiert.
- DataJournals [2] protokollieren welche persönlichen Daten wann an welchen Dienst gegeben wurden und welche Bedingungen mit der Datenherausgabe verbunden waren. Dadurch kann der Nutzer nachvollziehen, was seine Interaktionspartner über ihn wissen.
- Der iManager als Teil des Projektes ATUS – *A Toolkit for Usable Security*[8] [8] unterstützt die Nutzer in ihrem Identitätsmanagement, insbesondere auch beim mobilen Einsatz. Das Konzept konzentriert sich auf die Realisierung im Client; eine Unterstützung durch Interaktionspartner oder externe Dienste ist nicht vorgesehen.
- In DRIM – *Dresden Identity Management*[9] [6] wird Identitätsmanagement auf der Basis von digitalen Pseudonymen und Rollen umgesetzt. Das Konzept sieht unter Anderem die Einbindung von Treuhändern vor. DRIM ist ein Vorläufer des PRIME-Prototyps.
- idemix (*identity mixer*)[10] ist ein anonymes Credential-System (siehe Abschnitt 3.4), das ebenfalls mit Pseudonymen arbeitet. Es wird innerhalb von PRIME verwendet und weiterentwickelt.

[5] http://www.w3.org/P3P/.
[6] http://www.anon-online.de/.
[7] http://tor.eff.org/.
[8] http://www.iig.uni-freiburg.de/telematik/atus/.
[9] http://drim.inf.tu-dresden.de/.

2 Das Projekt PRIME

Im Mittelpunkt des Forschungsprojekts „*PRIME – Privacy and Identity Management for Europe*“ („Datenschutz- und Identitätsmanagement für Europa“) stehen die Entwicklung und Umsetzung neuer Konzepte für datenschutzförderndes Identitätsmanagement. Das Projekt wurde am 1. März 2004 gestartet und wird über den Zeitraum von vier Jahren vom 6. EU-Rahmenprogramm, Bereich „*Information Society Technologies (IST)*“, und dem Schweizer Bundesamt für Bildung und Wissenschaft gefördert.

2.1 Ziele

Ziel des Projektes ist es, Lösungen zu erforschen und zu entwickeln, die es den Menschen ermöglichen, selbst die Kontrolle über ihre Privatsphäre im Cyberspace zu übernehmen.

Während der Begriff „Identity Management“ von Werbestrategen mittlerweile überall dort verwendet wird, wo es auch nur ansatzweise um eine wie auch immer geartete Verarbeitung personenbezogener Daten geht, adressiert PRIME vor allem das selbst bestimmte Verwalten der eigenen so genannten „digitalen Identitäten“ oder genauer „digitalen Teilidentitäten“: Jeder Nutzer hat eine Vielzahl solcher digitaler Teilidentitäten, d. h. Benutzerkonten und Datensätze, die in den verschiedenen Rollen und Interaktionskontexten in der digitalen Welt von Bedeutung sind. So soll etwa das unterschiedliche Auftreten der Nutzer in verschiedenen Rollen wie z. B. als Arbeitnehmer, als Verbraucher, als Bürger, als Patient, als Reisender oder als Privatperson auch online unterschiedlich sein können.

Personenbezogene Daten, die in dem einen Kontext enthüllt werden, sollen nicht notwendigerweise mit denen in anderen Kontexten in Beziehung gesetzt werden können – es sei denn, dies ist vom Nutzer

[10] http://www.zurich.ibm.com/security/idemix/.

[11] Aus einem PRIME-Tutorial.

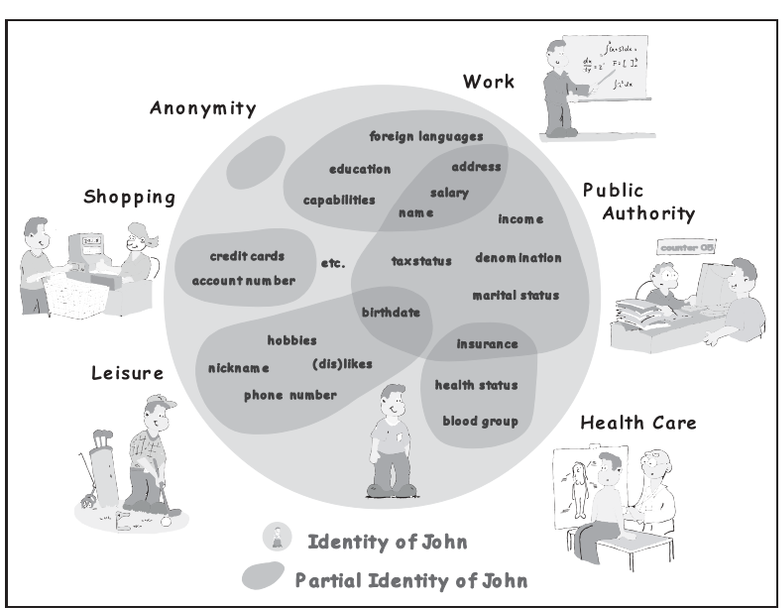

Bild 1 Johns Teilidentitäten (engl. „Partial Identities“)[11].

ausdrücklich gewollt oder gesetzlich gefordert. Dies ist Ausdruck der Grundprinzipien von PRIME, zu denen maximale Datensparsamkeit (d. h. maximale Vermeidung personenbezogener Daten), Transparenz für den Nutzer und implementierte informationelle Selbstbestimmung gehören.

Bedarf für eine derart datenschutzfreundlich gestaltete Technik ist auf jeden Fall vorhanden: Viele Menschen fühlen sich heutzutage durch Identitätsdiebstahl und Aufweichung der Persönlichkeitsrechte in ihrer Privatsphäre bedroht. In der Informationsgesellschaft möchten sie sich auf eine sichere Art und Weise miteinander austauschen und dabei gleichzeitig die Kontrolle über ihre persönlichen Daten behalten. PRIME konzentriert sich auf Lösungen für ein datenschutzförderndes Identitätsmanagement, das zur Souveränität der Nutzer über ihre Privatsphäre und zur datenschutzgerechten Datenverarbeitung von Organisationen beiträgt.

2.2 Interdisziplinarität und Praxisbezug

Eine wesentliche Voraussetzung für den Erfolg sieht PRIME in der interdisziplinären Erarbeitung der Lösungen: So wird im Projekt auf technische, rechtliche, soziale, wirtschaftliche sowie ergonomische Anforderungen besonderes Gewicht gelegt. Von entscheidender Bedeutung ist die Entwicklung von Modellen, damit die Funktionalität und die Bedienung der Datenschutz- und Identitätsmanagementkomponenten leicht handhabbar sowohl für Nutzer als auch für Diensteanbieter werden. Um eine umfangreiche Marktakzeptanz für diese Technik zu erreichen, werden neue Lösungen für die Verwaltung eigener Teilidentitäten in realen Szenarien demonstriert, z. B. in den Bereichen der Identifikation und Authentifikation in der Reiseabwicklung, bei der Nutzung von Location Based Services für mobile Endgeräte und im E-Learning. Zum Projektende wird PRIME einen Prototyp vorstellen und aufzeigen, wie damit datenschutzförderndes Identitätsmanagement in diesen Szenarien erreicht werden kann. Zudem werden die Konzepte und Entwicklungen des datenschutzfördernden Identitätsmanagements von PRIME in Form von Tutorien und E-Learning-Systemen den verschiedenen Zielgruppen näher gebracht.

Das Projektkonsortium setzt sich aus Partnern verschiedener auf dem Gebiet des Identitätsmanagements agierender Disziplinen zusammen: Während die technischen Projektinhalte (wie z. B. Identitätsmanagement, Autorisierungs- und Kryptomechanismen sowie Kommunikationsinfrastrukturen und Ontologien) im Wesentlichen von IBM (mit *IBM Frankreich* als Projektleitung und *IBM Research, Schweiz* als technische Leitung), dem *Centre National de la Recherche Scientifique/LAAS* und dem *Institut EURECOM* (beide Frankreich), der *Technischen Universität Dresden*, der *Johann Wolfgang Goethe-Universität Frankfurt am Main* und der *RWTH Aachen* (alle Deutschland), der *Karlstads Universitet* (Schweden), der *Università di Milano*, dem *Joint Research Centre/IPSC* und dem *Fondazione Centro San Raffaele del Monte Tabor* (alle Italien), von *Hewlett-Packard* (Großbritannien) und *Chaum LLC* (USA) erbracht werden, erhält das Projekt juristische Unterstützung durch die Partner *Katholieke Universiteit Leuven* (Belgien) und *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (Deutschland) sowie auf dem Gebiet der sozio-ökonomischen Konzepte durch die *Universiteit van Tilburg* und die *Erasmus Universiteit Rotterdam* (beide aus den Niederlanden). Weitere Partner, die im Projekt maßgeblich zur Anforderungsanalyse und Evaluierung der Projektergebnisse beitragen, sind die *Deutsche Lufthansa* und *T-Mobile* (Deutschland) sowie *Swisscom* (Schweiz).

2.3 Kooperationen und Kontakte

Die Arbeit von PRIME wird von einer Referenzgruppe kritisch begleitet, die Experten aus Wirtschaft, öffentlicher Verwaltung, Verbraucherschutz- und Bürgerrechtsorganisationen, Forschung & Entwicklung, Standardisierungsgremien, Datenschutzinstitutionen und Strafverfolgungsbehörden umfasst. Auch die Firma *Microsoft*, die eigene Entwicklungen im Bereich Identitätsmanagement im Zusammenhang mit neuen Betriebssystemversionen erarbeitet, ist in der Referenzgruppe vertreten.

Darüber hinaus kooperiert PRIME mit anderen EU-Projekten, die sich mit den Themen „Identity" sowie „Identity Management" beschäftigen, z. B. mit:

- dem interdisziplinären „Network of Excellence" FIDIS – *Future of Identity in the Information Society*[12],
- GUIDE – *Creating a European Identity Management Architecture for eGovernment*[13],
- DAIDALOS – *Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services*[14],
- InspireD – *Integrated secure platform for interactive Trusted Personal Device*[15].

Im Vordergrund von PRIME steht der Wille, die Projektergebnisse tatsächlich in die Praxis umzusetzen und in Standardisierungen einzubringen. So wirken mehrere PRIME-Projektpartner in Industrie- und Standardisierungsgruppen wie dem World Wide Web Consortium, OASIS, Liberty Alliance, ISO/IEC JTC 1 und der IETF mit.

2.4 Erste Ergebnisse

Erste Projektergebnisse sind auf der PRIME-Website[16] veröffentlicht.

[12] http://www.fidis.net/.
[13] http://www.guide-project.org/.
[14] http://www.ist-daidalos.org/.
[15] http://www.inspiredproject.com/.
[16] http://www.prime-project.eu.org/.

Dazu gehören z. B. die Anforderungsanalysen aus juristischer, sozio-ökonomischer und Anwendungssicht [14], Untersuchungen zu Prototypen und ihrer Usability sowie ein Architekturmodell eines datenschutzfördernden Identitätsmanagementsystems.

Ein zentrales Dokument ist das im Juli 2005 erschienene PRIME-White Paper [15], das die Vision des Projekts und Strategien zu ihrer Verwirklichung beschreibt. Mit der Veröffentlichung des White Papers will das PRIME-Konsortium die Diskussion rund um das Thema Datenschutz- und Identitätsmanagement noch stärker ins Gespräch bringen. Durch das White Paper soll nicht nur das Bewusstsein für aktuelle Datenschutzrisiken geschärft werden, sondern es zeigt auch anhand der entsprechenden PRIME-Ansätze mögliche Lösungen auf. Das PRIME-Konsortium lädt jeden ein, sich eine Meinung über die in dem Dokument vorgestellten Perspektiven und Vorschläge zu bilden und Feedback zu geben.

3 Identitätsmanagement à la PRIME

Im Vordergrund von PRIME steht das nutzerbestimmte Identitätsmanagement. Dies bedeutet, dass jeder Nutzer einschätzen und bestimmen[17] kann, welche seiner Kommunikationspartner was über ihn wissen. Genau dies fordert das Recht auf informationelle Selbstbestimmung, das 1983 im Bundesverfassungsgerichtsurteil zur Volkszählung formuliert wurde.

3.1 Verwaltung der eigenen digitalen Teilidentitäten

Das Projekt PRIME versteht unter Identitätsmanagement das nutzerbestimmte Verwalten der digitalen Teilidentitäten, die eine Person in der Online-Welt repräsentieren, wie beispielsweise Nutzerkonten oder Datensätze, die in Zusammenhang mit Situationen stehen, in denen sich der Nutzer befinden kann (Kontexte). So hängen Umfang und Art der Daten, die ein Nutzer herauszugeben bereit ist, sowohl von den jeweiligen Kommunikationspartnern ab als auch von seiner Rolle, in der er Informationen über sich kommuniziert. Beispielsweise wird ein Nutzer bei einer medizinischen Online-Beratung mit zugesicherter Vertraulichkeit andere Dinge offenbaren als etwa beim E-Shopping; die Kommunikation mit seiner Bank wird anders verlaufen als beim Filesharing in Tauschbörsen; und auch im Arbeitsleben verhält sich der Nutzer in der Regel anders als in seiner Freizeit, gerade was die Weitergabe persönlicher Daten betrifft.

3.2 Aushandlung über Datenschutzbedingungen

Die Vorstellung des Nutzers, wann er wem welche Daten unter welchen Bedingungen offenbart, soll er aus Sicht von PRIME mit Hilfe einer digitalen Policy zum Ausdruck bringen, die beim Etablieren einer Kommunikationsbeziehung mit den Angaben zur Datenverarbeitung der Gegenseite abgeglichen – und bei Bedarf ausgehandelt – wird. Das Identitätsmanagementsystem auf Nutzerseite speichert zum Zwecke einer späteren Nachvollziehbarkeit die Information ab, wann welcher Kontakt zustande gekommen ist und welche Datenschutzbedingungen ausgehandelt wurden.

3.3 Pseudonyme oder anonyme Nutzung

In vielen Konstellationen kann bei der Inanspruchnahme von Netz-Diensten auf Informationen, die den Nutzer identifizieren, verzichtet werden. Dies unterstützt das Identitätsmanagementsystem durch die Bereitstellung von Pseudonymen oder sogar anonymen Nutzungsmöglichkeiten ganz ohne Offenbarung persönlicher Daten. Ziel ist es, die Verkettbarkeit der Nutzerdaten

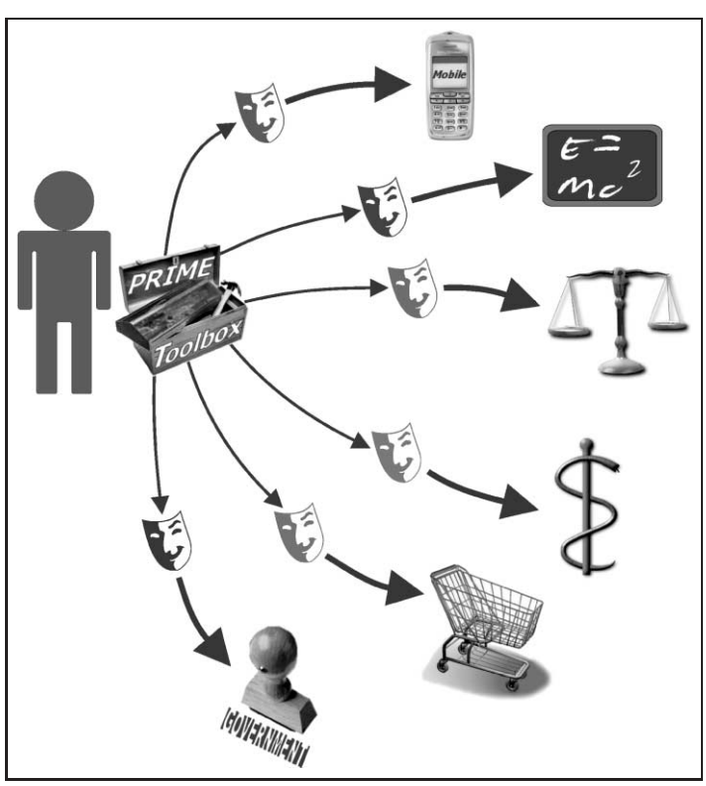

Bild 2 Nutzer treten unter kontextabhängigen Pseudonymen auf.

[17] Sofern nicht andere Einschränkungen dem entgegen stehen, z. B. im Bereich des E-Government ist häufig bereits gesetzlich festgelegt, dass der Nutzer sich mit vollem Namen identifizieren und bestimmte andere personenbezogene Daten wahrheitsgemäß angeben muss.

durch Unberechtigte verhindern zu können. Für eine möglichst weitgehende Einschränkung der Verkettungsmöglichkeit sollen Pseudonyme nicht kontextübergreifend eingesetzt werden. Natürlich steht es dem Nutzer frei, eine Verkettung explizit zuzulassen, ggf. auch über verschiedene Kontexte hinweg, wie es heutzutage z. B. bei der Verwendung von Bonus-Cards geschieht.

3.4 Credentials

Ein Mittel, um Verkettbarkeit zu verhindern, ist der Einsatz von anonymen Credentials (Berechtigungen): Ein Credential-System ist ein System, in dem Nutzer Credentials von Organisationen ausgestellt bekommen und den Besitz dieser Credentials beweisen können. Ein solches System ist anonym, wenn Transaktionen, die von ein und demselben Nutzer ausgeführt werden, nicht verkettet werden können (siehe [4; 5]). Anonyme Credential-Systeme sind geeignete Mechanismen, um Datenschutz zu gewährleisten. In PRIME spielen die anonymen Credentials eine zentrale Rolle.

3.5 PRIME als Toolbox

Ein Anliegen von PRIME ist es, Datenschutz- und Identitätsmanagement auch in existierenden Applikationen zur Verfügung zu stellen. Nicht in jedem Kontext wird die volle Identitätsmanagementfunktionalität benötigt, sondern häufig reicht das Einbeziehen einzelner Module aus. Daher werden die Arbeiten innerhalb von PRIME nicht in ein monolithisches System münden, das für sich alleine steht. Das angestrebte praktische Resultat lässt sich eher als Toolbox charakterisieren, aus der sich Entwickler, Anwender und Nutzer je nach Bedarf bedienen können.

3.6 Sensibilisierung und Training

Heutigen Nutzern ist meist gar nicht bewusst, dass sie in ihrem „normalen“ Leben jederzeit ganz instinktiv Identitätsmanagement betreiben – nämlich entscheiden, wem gegenüber sie wie auftreten. Noch weniger ist ihnen bewusst, dass ihr natürliches Identitätsmanagement in der Online-Welt durch Datenspuren und die prinzipielle Möglichkeit einer globalen Verkettung unterminiert wird.

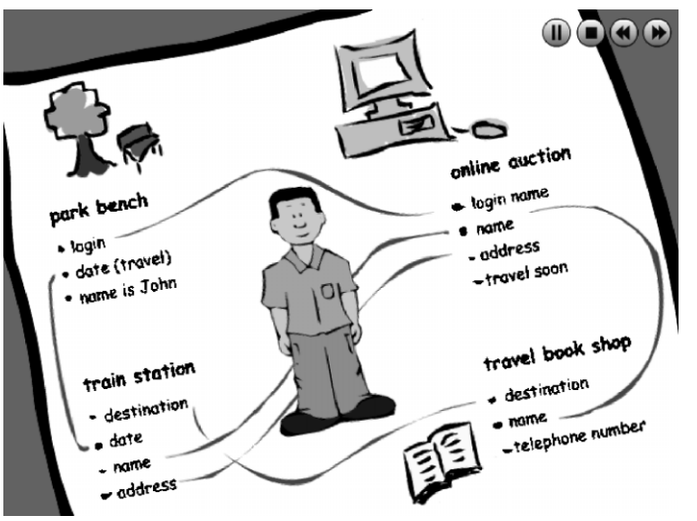

Bild 3 Darstellung von Datenspuren im PRIME-Nutzer-Tutorial.

Aus diesem Grund beschäftigt sich im Projekt PRIME ein Arbeitspaket mit der Erstellung von „Tutorials“, die Datenschutzbewusstsein schaffen und die Anwender von Lösungen schulen sollen. Neben den Nutzer-Tutorials werden spezielle Schulungsprogramme für Entwickler erarbeitet, denn sie können beim Design von IT-Systemen den Grad des Datenschutzes erheblich beeinflussen.

4 Forschungsfragen in PRIME

Allein durch die Multidisziplinarität der 20 Konsortiumsmitglieder adressiert PRIME ein weites Spektrum an Forschungsthemen rund um Datenschutz- und Identitätsmanagement. Zu den verschiedenen Forschungs- und Entwicklungsvorhaben im Projekt werden unmittelbar juristische und sozio-ökonomische Anforderungen eingesteuert, damit die Ergebnisse nicht nur technisch umgesetzt werden, sondern auch rechtskonform, sozial verträglich und ökonomisch sinnvoll und damit praxistauglich sind. Für die Prüfung der Rechtskonformität der in PRIME entwickelten Lösungen konzentriert sich das Projekt auf den EU-Rechtsrahmen. Für potentielle Diensteanbieter sind darüber hinaus insbesondere Business-Modelle interessant, die innerhalb von PRIME untersucht werden.

Ein Schwerpunkt bei der Entwicklung liegt auf der Usability der Lösungen: Gerade das komplexe Thema Identitätsmanagement muss in geeigneter Form dem Nutzer kommuniziert werden, was den Entwurf von geeigneten Benutzungsoberflächen erfordert [11].

Auch Ontologien, basierend auf einer im Projekt weiterentwickelten Terminologie zu Anonymität, Pseudonymität und Identitätsmanagement [12], werden in PRIME zur formalen Spezifikation von Konzepten und deren Beziehungen verwendet. Insbesondere für die PRIME-Architektur und speziell für die Interoperabilität zwischen verschiedenen Parteien spielen Ontologien eine entscheidende Rolle [15]. Im Bereich der Autorisierungsmodelle und -sprachen forschen die PRIME-Partner hauptsächlich an der Erweiterung der Zugriffskontrollsprache auf der Basis von Semantik-orientierten Regeln, die auf einer im Projekt entwickelten Datenschutz-Ontologie basieren [13].

Ein weiterer Projektschwerpunkt zielt auf die Entwicklung der PRIME-Plattform in Abstimmung mit Anforderungen aus der realen Praxis. Aus diesem Grund

sind Anbieter von drei verschiedenen Anwendungsbereichen (Identifikation und Authentifikation in der Reiseabwicklung, Location Based Services und E-Learning) im Projekt involviert. Zu ihrem Aufgabenfeld gehören neben der Integration der PRIME-Komponenten in die entsprechende Anwendung auch die Aufdeckung von Konflikten und Synergien zwischen Anonymität und Datenschutz einerseits und den Anwendungszielen andererseits. Außerdem wirken sie mit an der Erforschung neuer Möglichkeiten für die Anwendungen durch die Anbindung von Identitätsmanagementfunktionalität.

In PRIME beschäftigen sich fünf Arbeitspakete primär mit Forschung und Entwicklung:

- Nutzerseitiges Identitätsmanagement
- Services-seitiges Identitätsmanagement
- Autorisierungsmodelle
- Kryptographische Mechanismen
- Kommunikationsinfrastruktur

Im Folgenden werden exemplarisch relevante Forschungsfragen der genannten Arbeitspakete vorgestellt.

4.1 Nutzerseitiges Identitätsmanagement

Da PRIME den Fokus auf die Selbstbestimmung des Nutzers legt, kommt dem Arbeitspaket „Nutzerseitiges Identitätsmanagement" eine große Bedeutung zu. Hier ist wesentlich, wie man dem Nutzer veranschaulichen kann, was die Herausgabe von Daten für seine Privatsphäre bedeutet. Dies betrifft nicht nur die Gestaltung von Benutzungsoberflächen, sondern auch Möglichkeiten der Berechnung und Modellierung der Verkettbarkeit digitaler Teilidentitäten über mehrere Transaktionen eines Nutzers.

Um den Nutzer bei der (Wieder-)Verwendung von Pseudonymen zu unterstützen, wird an der Identifizierung von möglichst „kleinen" Kontexten samt den sich daraus ergebenden Konsequenzen geforscht [1]. Da zu „große" Kontexte wie auch ein kontextübergreifender Einsatz von Pseudonymen die Verkettbarkeit fördern und damit den Datenschutz schwächen, muss insbesondere auf nahtlose Kontextübergänge reagiert werden können.

Zusätzlich spielen (pseudonyme) Reputationssysteme eine Rolle, um Kommunikationspartner besser einschätzen zu können.

4.2 Services-seitiges Identitätsmanagement

Das nutzerseitige Identitätsmanagement kann sich erst dann vollständig entfalten, wenn es durch den Kommunikationspartner und/oder vertrauenswürdige Dritte unterstützt wird, z. B. Certification Authorities der PKI, Identitätstreuhänder, Wertetreuhänder, Lieferdienste (o. ä.).

Ein Schwerpunkt der Forschung hier liegt auf den Privacy Policies der Server-Seite, die Datenschutzregelungen in Unternehmen ausdrücken – und durchgesetzt werden sollen. Interessant ist das Konzept der „Sticky Policies" [10], die beim Transfer an die personenbezogenen Daten gebunden bleiben und die auch dann noch – nach Verlassen des ursprünglichen Herrschaftsbereiches – die definierten Datenschutzregelungen durchsetzen sollen.

Im Zuge des Trust Management wird über den Einsatz von Trusted Computing und manipulationssicherer Hardware geforscht.

4.3 Autorisierungsmodelle

Traditionelle Zugriffskontrollsysteme basieren auf Regelsystemen (Policies), die festlegen, wer welche Aktionen mit welchen Ressourcen ausführen (oder auch nicht ausführen) darf. „Access Control Policies" in der heutigen Form reichen jedoch nicht aus, um die Vielfalt der möglichen Datenschutzfragen zu adressieren. Beispielsweise basieren diese Policies in der Regel auf der Identifikation der Nutzer, doch innerhalb von PRIME sollen Nutzer auch anonym oder unter einem Pseudonym agieren können. Beispielsweise könnten Subjekte anstatt durch Identifikation des bürgerlichen Namens auch durch Eigenschaften beschrieben werden, z. B. „Europäischer Bürger, der mindestens 18 Jahre alt ist".

Eine datenschutzfördernde Zugriffskontroll-Policy enthält auf jeden Fall Angaben über den Zweck der Datenverarbeitung. Außerdem können die Zugriffsregeln Bedingungen und/oder Auflagen enthalten:

- Bedingungen („Conditions") müssen erfüllt sein, bevor der Zugriff auf die Daten erfolgt, und können durch gesetzliche Regelungen vorgegeben sein, etwa: „Vor der Datenverarbeitung zu einem bestimmten Zweck muss eine Einwilligung des Betroffenen vorliegen".
- Auflagen („Obligations") sind zusätzlich im Zusammenhang mit der Datenverarbeitung zu erfüllen, z. B. eine Protokollierung der Zugriffe oder das Löschen der Daten nach einem definierten Zeitraum.

Weitere Forschungsfragen ergeben sich aus den Aushandlungsmöglichkeiten: Welche Strategie soll verfolgt werden? Und: Welche Teile der nutzerseitigen Policy können – z. B. im Rahmen der Aushandlung – herausgegeben werden, ohne dass diese mehr Informationen über den Nutzer als beabsichtigt offenlegt? Zu diesem Zweck forscht PRIME daran, durch Filtern und Umbenennen aus der Policy des Nutzers eine bereinigte Policy („Sanitized Policy") zu generieren, die ohne erhöhtes Datenschutzrisiko an den Kommunikationspartner herausgegeben werden kann.

4.4 Kryptographische Mechanismen

Die Kryptographie bietet als technisches Herzstück viele Mechanismen, derer sich PRIME bedient, um Datenschutz- und Datensicherheitsfunktionalität zu realisieren. Dazu

gehört nicht nur die Möglichkeit der Ende-zu-Ende-Verschlüsselung oder der digitalen Signatur, sondern es kommen auch komplexere Schemata und Protokolle zum Einsatz, z. B. Gruppensignatur-Schemata oder Mehrparteienprotokolle.

In diesem Arbeitspaket werden Konstruktionsweisen für anonyme Credential-Systeme (siehe Abschnitt 3.4) entwickelt sowie Möglichkeiten zur Verbesserung der Effizienz untersucht.

Digitale Credentials und Zertifikate können leicht weitergegeben und kopiert werden. Bei nicht-anonymen Credentials kann man die Verwendung beobachten und bei Missbrauch einschreiten; dies ist bei anonymen Credentials so nicht möglich. Problematisch ist außerdem, dass Trojanische Pferde die Credentials „stehlen" und übernehmen könnten. Eine Lösungsmöglichkeit, die in PRIME erarbeitet wird, ist die Verwendung von manipulationssicherer Hardware, genauer: des *Trusted Platform Module* (TPM), wie es von der *Trusted Computing Group* spezifiziert wurde [16]. Das TPM kann verwendet werden, um sowohl anonyme als auch nicht-anonyme Credentials zu schützen. Es lässt sich beispielsweise sicherstellen, dass Credentials nur mit dem TPM verwendet werden können, an das sie herausgegeben wurden, oder nur mit TPMs desselben Nutzers.

Unter bestimmten Bedingungen, z. B. gesetzlich festgelegt, kann eine Aufhebung der Anonymität erforderlich sein, beispielsweise im Rahmen einer Strafverfolgung nach einer richterlichen Anordnung. Auch dies ist Gegenstand der Forschung: Wie lässt sich im definierten Einzelfall eine Reidentifizierung des Nutzers realisieren, ohne dass die Anonymität der Nichtbetroffenen gefährdet wird?

4.5 Anonyme Kommunikationsinfrastruktur

Wichtiges Ziel des Identitätsmanagementsystems ist es, dass nur Berechtigte auf Daten des Nutzers zugreifen können und dass ihm stets bewusst gemacht wird, wenn er Daten offenbart. Die genutzte Kommunikationsinfrastruktur darf dieses Ziel nicht dadurch konterkarieren, dass sie Nutzerinformationen beim Datentransport speichert und auswertet. Optimal wäre für ein Identitätsmanagement somit eine anonyme Kommunikationsbasis. Existierende Anonymisierungsdienste weisen jedoch Schwächen vor allem in Bedienbarkeit und Performanz auf.

Darüber hinaus ist es ein noch offenes Problem, wie auf geeignete Weise der Grad der potentiellen und aktuellen Anonymität sowie ihrer Grenzen festgestellt und dem Nutzer kommuniziert werden kann. Dabei geht es nicht nur um technische Grenzen, sondern auch um rechtliche Beschränkungen, die beispielsweise im Falle eines richterlichen Beschlusses eine Mitwirkung der Anonymisierungsdienstanbieter bei einer konkreten Strafverfolgung beinhalten können. Wie dies datenschutzgerecht und auf Einzelfälle beschränkt (d. h. bei Minimierung des Risikos einer Massenüberwachung) geschehen kann, ist ebenfalls ein wichtiges Forschungsthema von PRIME.

5 Zusammenfassung und Ausblick

Das Projekt PRIME vereint diverse Forschungs- und Entwicklungsinteressen im Bereich des nutzerbestimmten Identitätsmanagements. Die Partner engagieren sich innerhalb des Projekts sowohl in der Grundlagenforschung als auch bei der Entwicklung von Prototypen in realen Anwendungskontexten. Die primär technische Ausrichtung wird ergänzt durch eine applikationsbezogene, juristische und sozio-ökonomische Begleitforschung. Dadurch sollen sowohl die Praxistauglichkeit der Entwicklung und ihre Rechtskonformität sichergestellt als auch mögliche Business-Modelle aufgezeigt werden. Ein wesentlicher Schwerpunkt liegt auf der vertrauenswürdigen Realisierung der Lösung, was ebenso wie die erarbeiteten Usability-Konzepte zur Akzeptanz bei den Nutzern beiträgt.

PRIME adressiert nicht nur potentielle Diensteanbieter und Nutzer, sondern auch Standardisierungsgremien, um die als besonders geeignet erkannten Formate und Protokolle in offenen Standards zu spezifizieren.

Auch wenn zum Ende der Laufzeit des Forschungsprojekts noch keine marktreife Realisierung stehen wird, so werden die erarbeiteten Konzepte und Lösungen doch eine gute Basis für ein datenschutzförderndes, nutzerbestimmtes Identitätsmanagement bilden. Eine Expertenbefragung im Rahmen der Studie [IMS 2003] hat ergeben, dass bezogen auf die Marktfähigkeit solche Identitätsmanagementsysteme erst in einigen Jahren Anerkennung finden werden. Allerdings wird man auch die politischen und juristischen Entwicklungen genau verfolgen müssen, deren aktueller Trend zu einer künftigen Vorratsdatenspeicherung[18] [3] den Grundsätzen von Datenschutztechnik à la PRIME zuwiderlaufen könnte. Das PRIME-Konsortium beobachtet und evaluiert die laufenden Entwicklungen und lädt frühzeitig Vertreter aller Interessensgruppen ein, sich am Diskurs zur Notwendigkeit und Ausgestaltung von nutzerbestimmtem Identitätsmanagement zu beteiligen. Nur durch weite Beteiligung kann ein gesellschaftlicher Konsens für Lösungen à la PRIME entstehen.

Literatur

[1] K. Borcea, H. Donker, E. Franz, K. Liesebach, A. Pfitzmann und H. Wahrig: Intra-Application Partitioning of Personal Data. – In: Proc. of Workshop on Privacy-Enhanced Personalization (PEP 2005), Edinburgh, UK, 2005, S. 67–74.

[18] Stellungnahme von BDI, BITKOM und VATM zur Vorratsdatenspeicherung; 05. August 2005; http://www.bitkom.org/files/documents/Stellungnahme_BDI_BITKOM_VATM_Vorratsdatenspeicherung_DE_05_08_05.pdf.

[2] L. Brückner, J. Steffan, W. Terpstra und U. Wilhelm: Active Data Protection with Data Journals. – In: R. Grimm, H. Keller und K. Rannenberg (Hrsg): Informatik 2003 – Mit Sicherheit Informatik, GI Lecture Notes in Informatics (LNI), 2003, S. 269–280.

[3] F. Büllingen, A. Gillet, C.-I. Gries, A. Hillebrand und P. Stamm: Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich. Studie der wik-Consult für BITKOM Servicegesellschaft mbH. Bad Honnef, Oktober 2004. URL: http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf [Zugriff am 01.09. 2005].

[4] J. Camenisch und A. Lysyanskaya: Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. – In: B. Pfitzmann (Hrsg.): Advances in Cryptology – EUROCRYPT 2001, LNCS 2045, Springer, Berlin 2001, S. 93–118.

[5] D. Chaum: Security Without Identification: Transaction Systems to Make Big Brother Obsolete. – In: Communications of the ACM, Vol. 28 No. 10, Oct. 1985, S. 1030–1044. URL: http://www.chaum.com/articles/Security_Wthout_Identification.htm [Zugriff am 01.09. 2005].

[6] S. Clauß und T. Kriegelstein: Datenschutzfreundliches Identitätsmanagement. – In: DuD – Datenschutz und Datensicherheit (2003), Heft 9, Vieweg, Wiesbaden, S. 297.

[7] M. Hansen, P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann und M. Waidner: Privacy-Enhancing Identity Management. – In: Information Security Technical Report (ISTR) Vol. 9, Issue 1 (2004), Elsevier Ltd, Cambridge (UK), S. 35–44.

[8] U. Jendricke: Sichere Kommunikation zum Schutz der Privatsphäre durch Identitätsmanagement. Dissertation, Albert-Ludwigs-Universität Freiburg i.Br., Wirtschafts- und Verhaltenswissenschaftliche Fakultät, Dez. 2002. Erschienen im Rhombos Verlag, 2003.

[9] M. Köhntopp und A. Pfitzmann: Informationelle Selbstbestimmung durch Identitätsmanagement. – In: it+ti Informationstechnik und Technische Informatik 43 (2001) Nr. 5, S. 227–235.

[10] M. Casassa Mont, S. Pearson, und P. Bramhall. Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. – In: Proc. DEXA Workshops 2003, S. 377–382.

[11] J.S. Petterson, S. Fischer-Hübner, N. Danielsson, J. Nilsson, M. Bergmann, T. Kriegelstein, S. Clauß, und H. Krasemann: Making PRIME Usable. – In: Proc. of the 2005 Symposium on Usable Privacy and Security (SOUPS), ACM Int'l Conf. Proc. Series Vol. 93, S. 53–64.

[12] A. Pfitzmann und M. Hansen: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology. V 0.23, 25. Aug. 2005. URL: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml [Zugriff am 01.09. 2005].

[13] PRIME: First Annual Research Report V 1.0. Apr. 2005. URL: http://www.prime-project.eu.org/public/prime_products/deliverables/rsch/pub_del_D16.1.a_ec_wp16.1_V1_final.pdf [Zugriff am 01.09. 2005].

[14] PRIME: Framework V1. June 2005. URL: http://www.prime-project.eu.org/public/prime_products/deliverables/fmwk/pub_del_D14.1.a_ec_wp14.1_V4_final.pdf [Zugriff am 01.09. 2005].

[15] PRIME: Privacy and Identity Management for Europe – PRIME White Paper V 1.0. July 2005. URL: http://www.prime-project.eu.org/whitepaper/ [Zugriff am 01.09. 2005].

[16] Trusted Computing Group: TPM Main – Part 1 Design Principles. Specification Version 1.2, Revision 85. 13. Feb. 2005. URL: https://www.trustedcomputinggroup.org/downloads/specifications/mainP1DP_rev85.zip [Zugriff am 01.09. 2005].

[17] Unabhängiges Landeszentrums für Datenschutz, Kiel, und Studio Notarile Genghini, Milano: Identity Management Systems (IMS): Identification and Comparison Study. Studie beauftragt durch das Joint Research Centre Sevilla. Sep. 2003. URL: http://www.datenschutzzentrum.de/idmanage/ [Zugriff am 01.09. 2005].


1


2


3

1 Dipl.-Inform. Marit Hansen beschäftigt sich seit 1995 mit Datenschutztechnik und leitet den Bereich „Privacy-Enhancing Technologies" im Unabhängigen Landeszentrum für Datenschutz. Aktuelle Projekte: PRIME, FIDIS, AN.ON, ULD-i.
Adresse: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstr. 98, 24103 Kiel,
E-Mail: marit.hansen@datenschutzzentrum.de, http://www.uld-i.de

2 Dipl.-Inform. Katrin Borcea-Pfitzmann leitet und betreut seit fast 10 Jahren verschiedene Projekte im Bereich eLearning. Seit geraumer Zeit gehört dazu auch die Integration von Privacy-Enhancing Technologies, Aktuelle Projekte: PRIME, BluES, Privacy-Aware eLearning.
Adresse: Technische Universität Dresden, Fakultät Informatik, 01062 Dresden,
E-Mail: katrin.borcea@inf.tu-dresden.de, http://www.inf.tu-dresden.de/MI/?id=200

3 Prof. Dr. Andreas Pfitzmann forscht und lehrt seit mehr als 20 Jahren zu Datenschutz und mehrseitiger Sicherheit, insbesondere durch verteilte Systeme. Aktuelle Forschungsprojekte: Anonymes Web-Surfing, PRIME, FIDIS, Steganographie.
Adresse: Technische Universität Dresden, Fakultät Informatik, 01062 Dresden,
E-Mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/