# IDENTITY MANAGEMENT FOR SELF -PORTRAYAL

Toby Baier,[1] and Christian P. Kunze,[2]

[1]*Distributed Systems Group - VSIS, University of Hamburg, Vogt-Kölln-Straße 30, 22527 Hamburg, Germany*

[2]*Distributed Systems Group - VSIS, University of Hamburg, Hamburg (Germany)*
{baier,kunze}@informatik.uni-hamburg.de

**Abstract** Identity management systems help users to organise their digital profiles in order to communicate parts of them, whenever needed and wanted, to communication partners like internet services or personal contacts. Most current identity management research tries to achieve the highest possible degree of data hiding for best privacy. After sketching some of these projects, this paper presents a different approach where users are assumed to be interested in presenting themselves to selected online communities or internet services for better personalisation, to achieve a consistent reputation, or to establish an application- and service-independent internet society. It thereby stresses the aspect of privacy that persons have the option for self-portrayal. To support this thesis, a survey is presented which shows that many users who actively participate in Internet communities would make high use of such a system. Finally, the project "onefC" is presented which prototypically realises this approach.

**Keywords:** Digital Identity, Identity Management, Self-Determination, Digital Citizen, Online Communities

## 1. INTRODUCTION

Many Internet services require personal data of the users to be personalised, optimised or to function at all. Any personalised service obviously needs the identification of the user, most require authentication also. To offer a service which is specifically adjusted to a certain users demands, additional personal information about this user is needed. This is not specific to the Internet, it applies in real life as well: no bank office will grant access to an account without the clients authentication. And in a bookstore, the shop assistant will ask for the customers preferences to offer a personalised selection of books. But while this identity management is familiar in real life, it is hard to be done online. Internet

users need to keep track of their login data to any service they use, they need to decide what information they show to communication partners and afterwards remember who knows what about them.

The problem of identity management arises not only during the use of Internet services, but also applies to self-presentation in online communities. People are complex social beings, and the Internet has become an important medium for communication and collaboration. There are many possibilities to coact on the Internet, including simple mailing lists, USENET newsgroups, online blackboards, or sophisticated online portals with several possibilities of interaction. All these subsume to online communities. In each community, the members are presenting themselves by some degree to the other members, otherwise only few interaction would be possible. But if a user has presented herself to one community, she must do it again for every other community she would join. The image one has created can not be transferred, including relations to other members and reputation.

There are two faces of online identity management: one is privacy, the other is self-portrayal. The former is needed to protect personal data from the public or specific third parties, the latter is wanted for convenient use of the Internet and building a consistent, service- and community independent personality. These two objectives should be reached in conjunction, because one does not make sense without the other. A privacy and security oriented identity management system would restrict the users too much in their Internet experience, while a self-portrayal one which disregards security issues is a too great danger to privacy and data protection.

The self-portrayal functionality of an identity management system must offer the following: in a communication session, selected parts of the own identity attributes can be shown either automatically or with user confirmation to the communication partners. The attributes should be transferred in a standard format and with metadata describing the attributes. The system should automatically generate pseudonyms for new contacts who shall not see one of the already existing pseudonyms. These pseudonyms are like identity-parts and can be associated with arbitrary attributes. Short-term or even one-time pseudonyms must be inactivated and archived after use.

Security for identity management means, that others can only see those parts of an identity which they are authorised to. Unauthorised access to any identity data must be prohibited, including unauthorised access to the identity manager itself to prevent identity theft. This also includes the protection during transmission: any data sent over networks must be encrypted. To enhance privacy further, anonymiser networks could be used to prevent third parties to recognise that identity data was transmitted.

The next section briefly introduces some identity management systems or projects which provide some of the identity management functionality. Section 3

explains the motivation for a self-portrayal driven identity management solution in greater detail. After that, the results of a survey about the need of identity management is presented in section 4. Finally, the onefC system developed at University of Hamburg is introduced, followed by a general conclusion.

## 2. HISTORY AND STATE OF THE ART OF IDENTITY MANAGEMENT SYSTEMS

The beginning of digital identity management (abbreviated as IDM) was set with David Chaums article about ”Security without identification” [Chaum, 1985]. Chaum proposes the use of different pseudonyms for different situations, including one-time-pseudonyms and long term pseudonyms for ongoing relationships. The unlinkability of the pseudonyms plays a major role, so that the privacy of the pseudonym holder is not violated. Also, anonymous communication is important, so that the use of the pseudonyms can not be watched.

Since then, identity management systems were seen as privacy enhancing technologies (PET). Accordingly, most active identity management projects have the increase of privacy as their main goal. Mainly commercial IDM approaches have ease of use and personalisation as their targets. In the following, some IDM systems will be presented and explained.

### 2.1 Commercial projects

There are several commercial projects in the context of identity management. Most aim for single sign-on with internet services. Microsoft’s .NET passport and the Liberty Alliance’s Project Liberty will be presented hereafter, other projects include Novell’s DigitalMe and XNS.org.

**2.1.1 Microsoft .NET passport.** While .NET passport is not an identity management system in the sense that Chaum predicted it, it is the largest IDM system currently deployed. This is due to the fact that Microsoft forces all 1.5 million users of their free web mail service Hotmail to use .NET passport for authentication. The system aims mainly at single sign-on (authenticate once, use several different services), but also offers to reveal additional personal information to the services. This includes the propagation of credit card numbers for online purchases. All data is stored centrally on a Microsoft server, which makes it vulnerable as a single point of failure and violability. There have already been several cases of system breakdowns and flaws, in which users were authenticated as someone else, reading foreign mail[1]. Next to these security flaws, the coarse data model is the most profound drawback.

[1] see http://www.epic.org/privacy/consumer/microsoft

**2.1.2 Project Liberty.** The Project Liberty is an initiative of many companies and non-commercial organisations to establish an infrastructure for online exchange of personal data. The main aspect of it is the concept of "federations". Federations are built between different service providers, which have the possibility of directly sharing user information after the user's consent. User profile information is stored decentrally at the service providers, only in later versions users can manage their data themselves. Direct user to user communication is not in the scope of the project, but due to very sophisticated protocol definitions likely possible.

## 2.2 Research projects

As mentioned, most research activity on the field of identity management goes into privacy concerns. Only the IDRepository developed at Technische Universität München has community support as a motivation.

**2.2.1 DRIM - Dresden Identity Management.** The Dresden Identity Management project[2] is an important part of a EU funded integrated project called PRIME (Privacy and Identity Management for Europe). It provides an identity manager (IDMAN) which uses several standard security mechanisms like SSONET for secure connections, AN.ON as an anonymising network adapter, X.509 [3] and XML signatures, and P3P [4] for privacy rule negotiation [Clauß and Köhntopp, 2001]. P3P is also used for actual attribute transfer, although it needed to be extended outside of specification for this.

Security, data-hiding and anonymity services are the main features of DRIM, and the functionality is not hidden from the users, which makes it hard to use for non-security-experts. Also, DRIM concentrates on usage of services on the web, direct user to user communication is not covered yet.

**2.2.2 iManager.** The iManager is part of the ATUS project[5] at University of Freiburg and considers usability to be a most important aspect of privacy enhancing technologies. If the users can not use these tools properly, they will most likely be more hazardous to privacy and security than they help to preserve it. Even more: if PET software does not meet usability standards, people will not use the software at all. Usability aspects of current privacy software like PGP are considered as very confusing. Jendricke states that identity management could be a way to make privacy enhancing technologies more usable and therefore

[2] http://drim.inf.tu-dresden.de
[3] http://www.ietf.org/html.charters/pkix-charter.html
[4] http://www.w3.org/P3P
[5] http://www.iig.uni-freiburg.de/telematik/atus

more secure. The iManager tries to provide an easily usable interface [Jendricke and tom Markotten, 2000].

**2.2.3 IDRepository (Cobricks).** The Cobricks project[6] at Technical University of Munich contains an own implementation of an identity manager [Koch and Wörndl, 2001]. This is the only current identity management project which has community support as a main aspect. It is designed to help users to join and maintain community affiliations. The IDRepository stores all personal information and is kept decentrally, although the authors suggest to keep it at a trusted third party.

# 3. MOTIVATION FOR SELF-PORTRAYAL-ORIENTED IDENTITY MANAGEMENT

Since the advent of identity management in 1985, using the Internet has changed dramatically, not alone because far more people have access to it. Latest research shows that two thirds of all US citizens have Internet access [Madden, 2003]. This transformed the Internet from an academic place, which was used only by a few specialists, to a public place where all kinds of communication is done: e-commerce has evolved to an important part of business to business (b2b) transactions, but also for end customers to have a better choice (b2c). Lately, the success of online market places like eBay [7] has led to an even more popular customer to customer (c2c) business. But doing business is of course not the only application for the Internet: just like it was meant to be used in the beginning for academics, the World Wide Web has evolved to a place for exchange of information for everybody. Online communities develop from plain text USENET newsgroups to highly sophisticated blackboards, where every user can have a detailed private or public profile to store personal information, or with which usage information is associated by the backboard system. Blackboard communities can easily be created using dedicated services[8] or elaborate server components[9] which can be installed on own web servers. Since these communities can be easily joined and left, many have a problem of high user fluctuation. But users who join and leave communities quickly have the disadvantage of earning little or no reputation, since online reputation can not be transferred between communities yet, due to the missing identity representation. Of course, travelling through the space of online communities unknown might be wanted by some users for privacy, secrecy, or negative intentions like

[6] http://www.cobricks.de
[7] http://www.ebay.com
[8] for example http://groups.yahoo.com
[9] for example http://www.phpbb.com

fraud or deceit. But many online users put a lot of effort into their online self-portrayal, trying to build a good reputation. The huge number of personal web homepages is a good sign for this [Döring, 1999]. People on the Internet want to be seen, they want to be known.

Peer to peer journalism is a form of information distribution where all users can commit news items. For this it is obvious that reputation and trust plays a major role: the more reputation an author has, and the more people trust in the quality of this authors competency, the more people will actually want to read these news. But since trust and reputation are always bound to persons, it is clear that a definite identification of the users is needed. The onefC project tries to achieve this through identity management.

Privacy is often seen as the protection of personal data from other people or organisations. Then, privacy enhancing technologies (PET) are "a coherent system of information and communication technology measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system" [Borking and Raab, 2001]. But what is the functionality of the Internet? This can not be reduced to the fact that users can send electronic mail over the Internet – the social collaboration factor offers much more. Here the problem can be seen as a trade-off: "the more I show about myself, the better functionality I get, but also the more people can see my personal data". This includes the possibility that the user is not so much afraid of others seeing their personal data, but very eager to get the best functionality available. So privacy is not only about hiding data, it is also about making the user able to show his data in a reasonable way.

Another important aspect of digital self-portrayal is the fact, that the communication partner receives a portrait or image of the user. Classical identity management systems do not cover this side, because the aim is to hold these images as sparsely detailed as possible. Since self-portrayal identity management enforces user to user (u2u) communication, the management of communication partner images is not only about data mining. This part of identity management can be seen as a semiautomatic addressbook, which stores not only addresses but arbitrary personal information about communication partners in the same way that own personal information is stored.

## 4. INTERNET USAGE AND SELF-PORTRAYAL SURVEY

As a demonstration that self-portrayal-oriented identity management is a real need of internet users, an exploratory, non-representative survey was done using

a web-based questionaire[10]. The link to the questionaire was published on the homepage of the VSIS (distributed and information systems) research group at the University of Hamburg and distributed to many online blackboards. Thus, mainly the target group of the onefC project was reached: long-term Internet users, who spend considerable amounts of their social life and spare time on the Internet. Among the 240 participants 223 make daily use of the Internet, only 9 since less than a year. More than the half (124) have their own web site. Moreover, many of the participants are active in online communities: over 50% write articles in online blackboards more than once a week, 35% even almost daily. 111 of the participants are active in three or more blackboards, only 20 do not use blackboards at all. Three quarters state that they have made personal contacts on the internet. The average age of the participants is 29 years, while the youngest is 14 years old, the eldest 54 years. All in all, this surely does not represent the whole Internet community, but it represents the part of it which may be interested to gain a consistent Internet identity for self-portrayal.

The main part of the questionnaire was a selection of fourteen personal attributes plus two extra fields for self-selected attributes, for which each participant was asked to say whether they would reveal it to more than one but not all internet services or communication partners. If they would not reveal them at all or just to one partner, there would be no need for an identity manager and conventional methods of information management would suffice. If the attributes would be shown to anyone, they could as well be published on a personal web site, also here no identity management is needed. The main advantage of identity management is the selective revealing of personal attributes, and the survey was designed to find out for how many of the very active Internet users such a mechanism would be useful.

To get a representative overview, it was made sure that the selection of the fourteen given attributes was spread from very personal and private ones (like the postal address) to rather public ones (like a pseudonym). The variation can be seen in figure 1, ordered from left to right concerning positive votes. It can be seen that only four of fourteen attributes would be shared to selected communication partners by more than 50% of the participants, but only two attributes would be shared by less than 20%. No attribute would be shared by all nor by none of the participants. This reflects the personal and flexible utilisation of the system: anyone should be able to share whatever attributes she or he wants, there should be no fixed default attributes which can not be extended by users or new services and applications.

[10]The questionaire is available at http://vsis-www.informatik.uni-hamburg.de/projects/onefc/umfrage/fragebogen-e.phtml (in english, german version is also linked). Any input will be not be considered anymore, though.

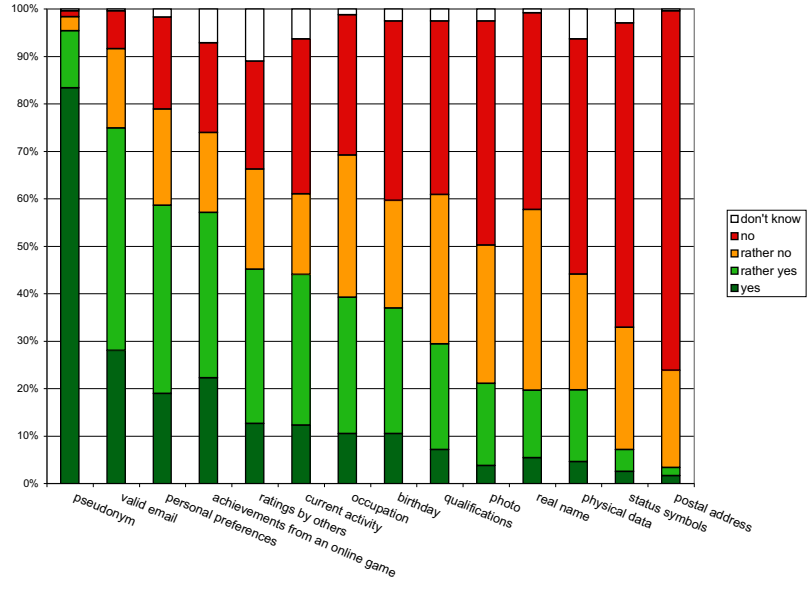


*Figure 1.* How many participants would reveal each attribute?

The survey revealed that the attributes are more likely to be shared when they have their origin or main functionality on the Internet. This reflects the reluctance of users to reveal real-world attributes of the own identity. Still, some of the real identity would be shown under certain circumstances, presumably to increase trust or to enable real-world interaction like delivery of goods. The disposition to reveal Internet related identity information offers sufficient ground for identity management, though.

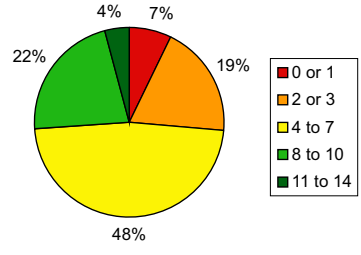


*Figure 2.* How many attributes would the participants use in an identity management system?

To find out if the participants would actually make use of an identity management system, we analysed how many times each of them said ”yes” or ”rather

yes" to the question whether they would share the given attribute to selected communication partners. The result is shown in figure 2. It can be seen that 26% of the participants would make high use of the system and manage more than the half (8 to 14 of 14) of their attributes with the identity management system. 48% would use such a system for 4 to 7 out of 14 of their attributes, which is still a sensible extent. Our thesis is that for these 74% of the participants, an identity management system would make life on the Internet a lot easier to manage. The remaining 26% would not make much use of such a system.

Another question on the questionaire was "How much are you concerned about your privacy when giving out personal data over the Internet?". While the majority of participants (62%) said to be very or rather concerned about their privacy, these people were almost equally distributed to those who would share many attributes and those who would share rather few attributes. This means that fear about privacy violations was a minor factor for the decisions taken in the main part of the survey: the revealing of the given attributes. Remembering the fact that many people would like to reveal attributes from the online world, and realising now that they are equally afraid of losing their privacy, it is clear that there is a real need for identity management.

The attributes entered into the user specified boxes (attribute 15 and 16) were quite interesting too: one participant chose "bank balance" and answered "rather yes". Apparently, she or he saw that if one trusted a system so much as to manage large parts of their identity, one could also enter critical data and be assured that no unauthorised access would be possible.

It needs to be noted that the complex matter of identity management was not explained in detail on the questionaire. Rather, certain situations were explained in which the procedure of identity management was sketched (reveal personal attributes to several selected online communication partners). Maybe the answers would have been different if the participants knew how identity management actually works, including automatically generated short-lived pseudonyms and transparent encryption.

## 5. PROJECT onefC: AN APPROACH TO AN IDENTITY-ENRICHED SESSION INFRASTRUCTURE

The project "open net environment for Citizens" (onefC) is developing a concept and realisation of an identity-enriched session infrastructure on the basis of self-portrayal. This section presents an overview of the main components of the onefC-architecture. They can be divided roughly into the concept of a digital identity and the management components which assist the user to achieve his needs and goals.

## 5.1 Representing Users Identities

As the project onefC has the aim to make it possible to be someone on the net, the developed concept of a digital identity covers many aspects of the interpersonal comprehension of identities. [Baier et al., 2003] This comprehension consists of aspects of philosophy, psychology and sociology.

One of the main tasks of the identity is to reliably identify an object or person. This is formalised in the philosophic and mathematic definition of the identity as a binary relation which links any object just to itself. This means it is a special or marginal case of equity. To decide whether the inspected object is in this relation or not, the philosophical term of the moderate numerical identity can be used. It accepts the identity of objects if consecutive characteristics remain even while their state is changing or the object maintains in a continuous but not total change. [Brockhaus, 1989][Henrisch, 1976][Mittelstraß, 1984]

Another aspect of identities is the construction of the single individual with its characteristic attributes. Thereby the identity develops in interactive experiences and relationships in adopted roles in different social contexts. The understanding of being an individual and having the control directs to the unconscious behaviour of presenting the own identity in parts of different size, adapted to the actual figured role and social context. This tends to a newer psychological concept of an identity, which regards it as a complex structure with multiple sets of elements. Every set represents one or more group, role, body or task drawn identity-parts. These parts are organised in a so called "identity patchwork" and are flexibly activated or deactivated depending on the actual context. Each part consists of attributes which contain objective and subjective characteristics of the corresponding person. The objective attributes are similar to entries in a passport - they are more or less verifiable facts like size, age, gender or the appearance as well as achieved skills. The subjective content can cover capabilities in comparison to others, the social appearance, sentiments and moods. [Döring, 1999][Resch, 1998][Suler, 1996][Turkle, 1999]

The developed identity model maps the "identity patchwork" to a self-referencing data-tree (see figure 3). Each node of the tree represents one identity-part, which is associated with one or more social contexts. These contexts represent common and shared backgrounds of experience in which the corresponding identity node is activated and used for communication. As a consecutive element a unique identifier ties all nodes together. This results in the possibility to identify users across different contexts. Together with the context the unique identifier directs to the part of the identity which has to be activated and thus both imply the presented attributes.

Mapping the identity to a data-tree offers the possibility to use its hierarchical structure for simplifying the construction of the single identity-part. At first the onefC model defines a concept of inheritance to reuse attributes. Each node

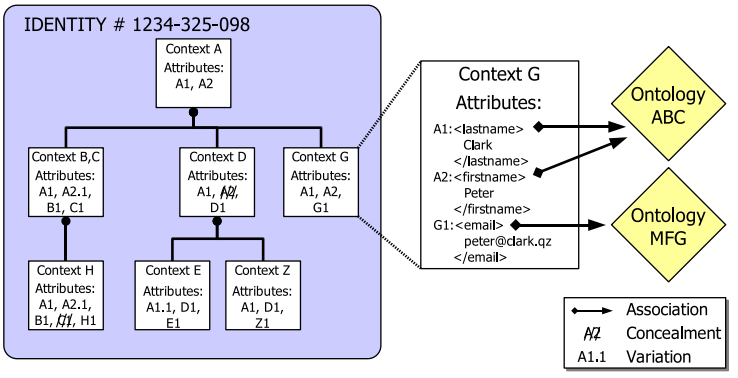


*Figure 3.* The Identity Model of the Project onefC

inherits the attributes of its superior and extends it by adding new one. As it is not always eligible to integrate all characteristics of the superior node, the possibility to conceal particular parts of it is needed. To adapt inherited attributes to the demand of the actual node context, a concept of visibility is introduced. This makes it possible to overwrite the content of characteristics instead of redefining them.

As discussed in section 4, there should be no predefined set of attributes, because the needed ones depend on the actual communication context and the user's aims. To cope this, the used attribute model derives from the container concept. It combines meta-data and the explicit content in so called "profile attributes". One of the most important information of the meta-data is the association with an ontology. This makes it possible to use a semiautomatic process to help the user to construct identity-parts for new contexts. To integrate one important aspect of community support, onefC defines the special attribute type of "social-identity attributes". Attributes of this type represent the feeling of being a member of a certain group. With this information the identity-part is banded together with other to a virtual and higher construct: a social identity for this group.

To store and communicate the identity the data-tree is transformed in an XML[11] representation. This leads to the possibility to use the onefC identity model as an exchange format in an open environment.

## 5.2 Self-Portrayal-Oriented Identity Management

As the term self-portrayal oriented identity management suggests, the onefC architecture is inspired by the social behaviour of presenting the personal identi-

[11] eXtensible Markup Language, see http://www.w3.org/XML

ty in accordance with the actual context, role, or situation. It should aid the user to enforce his or her needs and aims. To achieve this, the architecture integrates different core components to a session and identity management system (see figure 4).

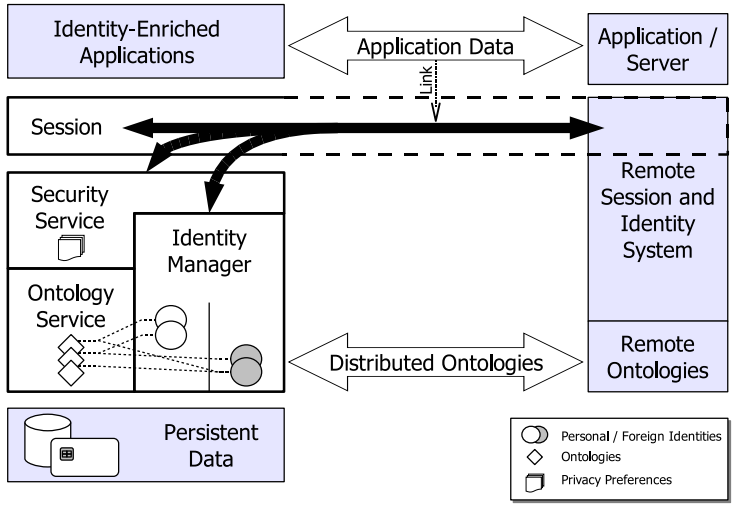


*Figure 4.* The onefC Identity-Enriched Session Infrastructure

The core identity management system consists of the central identity manager and the services the manager uses to provide its functionality. It has been implemented prototypically already [Kunze, 2004]. The management component encapsulates the identities of the user and his communication partners. As the foreign identities are build up from the information provided by the remote identity management systems, they just represent the image the partner has shown in the past and actual communication acts. To enforce the needs and preferences of the identity owner, the identity management component reverts to a security service. This module is based on P3P[12] and APPLE[13] to specify and negotiate privacy aspects before exchanging identity data. While preparing the response to a request the security service has to agree to send any single attribute. This provides the possibility to the user to define as fine grained access rights as he or she needs. This service has also the task to establish safety and trust to a communication act. This is done by using classic techniques like data encryption and signing.

As described in the subsection above, the attributes stored in the identities are associated with ontologies. The management of them is performed by the

[12]http://www.w3.org/P3P/
[13]http://www.w3.org/TR/P3P-preferences/

ontology service which bases on a concept of distributed ontologies. The additional semantic information of the attributes is used in a semiautomatic process to build up new identity-parts for unknown contexts or requested attributes.

Identity Management is no end in itself. Since all identity information exchange is done to enrich other communication, a modern session concept was introduced to the onefC architecture. A session is an abstract construct which comprises of a set of communication acts, a representation of the participants and a set of describing attributes. All communication between enabled applications is associated to a session, and sessions are managed using a session manager. The participants of a session are represented using the identities from the identity management system. Some security functionality like encryption or unobservability are handled as attributes of sessions.

## 6. CONCLUSION

It was shown that privacy is not only about hiding personal data, it includes the option to present oneself to selected communication partners. Identity management is a good solution to support both sides of privacy, data protection on the one hand side, self-portrayal on the other. The presented survey shows that for many active members of online communities, a self-portrayal oriented identity management solution would be of good use. The project ”onefC” at University of Hamburg provides a prototype of an identity management system which has self-portrayal as the main motivation. There is already a prototypical example application which uses the onefC-Infrastructure about which will be reported in an upcoming paper. It provides a collaborative filtering service which is personalised with values from onefC identities, while these identities are extended by using the service as well. It can use identity attributes not generated by itself, too.

Future steps include the further development of the onefC infrastructure: the session management component and the ontology infrastructure need to be elaborated. Also, security and privacy mechanisms like P3P and encryption must be further integrated. Large scale evaluation will show how feasible the system is, and how users will actually make use of it.

## References

[Baier et al., 2003] Baier, T., Zirpins, C., and Lamersdorf, W. (2003). Digital identity: How to be someone on the net. In *Proceedings of the IADIS International Conference of e-Society*, volume 2, pages 815–820.

[Borking and Raab, 2001] Borking, J. J. and Raab, C. D. (2001). Laws, pets and other technologies for privacy protection. *The Journal of Information, Law and Technology (JILT)*, 1.

[Brockhaus, 1989] Brockhaus, F. A. (1989). *BROCKHAUS ENZYKLOPÄDIE in vierundzwanzig Bänden: Zwölfter Band Kir – LAG*.

[Chaum, 1985] Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044.

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

[Döring, 1999] Döring, N. (1999). *Sozialpsychologie des Internet*. Hogrefe.

[Henrisch, 1976] Henrisch, D. (1976). Identität und Objektivität: eine Untersuchung über Kants transzendentale Deduktion. In *Sitzungsberichte der Heidelberger Akademie der Wissenschaften – Philosophisch-Historische Klasse*, volume 1, page 54 et sqq. Winter.

[Jendricke and tom Markotten, 2000] Jendricke, U. and tom Markotten, D. G. (2000). 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.

[Koch and Wörndl, 2001] Koch, M. and Wörndl, W. (2001). Community support and identity management. In *Proc. European Conf. on Computer Supported Cooperative Work (ECSCW 2001)*, pages 319–338. Bonn, Germany.

[Kunze, 2004] Kunze, C. P. (2004). Digitale Identität und Identitäts-Management. *Informatiktage 2003*.

[Madden, 2003] Madden, M. (2003). America's online pursuits: The changing picture of who is online and what they do. http://www.pewinternet.org.

[Mittelstraß, 1984] Mittelstraß, J. (1984). *Enzyklopädie Philosophie und Wissenschaftstheorie 2*. Wissenschaftsverlag.

[Resch, 1998] Resch, F. (1998). Zur präpsychotischen Persönlichkeitsentwicklung in der Adoleszenz. *Psychotherapeut*, 43(2):111–116.

[Suler, 1996] Suler, J. (1996). Identity Management in Cyberspace. web-site. *http://www.rider.edu/users/suler/psycyber/identitymanage.html*, Abruf am 06.10.2002.

[Turkle, 1999] Turkle, S. (1999). *Leben im Netz: Identität in Zeiten des Internet*. Rohwolt Taschenbuch Verlag.