IDENTITY-ENRICHED SESSION MANAGEMENT

Tobias Baier and Christian P. Kunze

Distributed Systems Group - VSIS, Department of Informatics, University of Hamburg, Vogt-Kölln-Straße 30, 22527 Hamburg, Germany

Abstract: The Internet has become an important part in every day life for many users. It has changed from an instrument to exchange and link scientific data to an economical and social place, where people spend their working and spare time. But the underlying technology has not adapted to the newly risen demands of communication and collaboration. The user is almost isolated and anonymous when using the web, while still leaving traces threatening their data security and privacy. There is no global concept of "digital citizens" modern collaboration applications could base on. To overcome this lack, this paper introduces an approach of identity enriched session management. It offers the possibility to integrate different (and distinguishable!) users into meaningful relationships. This paper presents the essential concepts of identity enriched sessions and a prototypical realisation which have been developed in the "open net environment for Citizens" (onefC) project.

Key words: Digital Identity, Identity Management, Session Management, Self-Determination, Digital Citizen, Online Communities

1. INTRODUCTION

The management of user and session information in most distributed systems (for example web applications) is very complicated for users and likewise for service providers. Users need to manage their personal information for every single Internet service or communication application they use, including user-name and password but also preferences and further personal information. The situation is even worse with sessions, users have no information about sessions they have within applications and they have no power to change these sessions, for example add encryption or join the session with another application. Mostly users do not even realise that they are participating in a session, because it is not directly displayed in the client. On the other hand, service providers do have information about sessions, but problems arise when sessions need to be shared between multiple services or applications. Even more critical problems emerge when different service providers want to share sessions. Modern service composition models support the integration of organisational resources within cooperation processes that can be applied for changing participants [Zirpins et al., 2004]. To ensure the accuracy of mutual participant interactions, the concept relies on a secure exchange of session and user information. There are several approaches to achieve this, but so far they concentrate on user profile information exchange in a rudimentary way.

Identity management systems are used to manage and exchange user profile information in a reasonable way. Reasonable in this context means: automatically, purposeful, fine-grained and secure. Automatic data exchange is often wanted for insensible data or well known risk free connections. Concerning username and password this is called "Single Sign-On" and is already discussed and deployed in some places (see section 1.1). But users would not want to send their username and password to anyone, so it has to be considered to whom the information is sent to and why this communication partner needs it, therefore purposeful. Also, not everyone the user trusts should receive all identity information, so the granularity of data access should be as fine as possible. But in the end, no system which manages or even exchanges personal data makes sense without dealing with security and privacy concerns. Even if Scott McNealy says: "You have zero privacy anyway, get over it!" [Sprenger, 1999], an identity management system should provide as much privacy as possible.

It is obvious that identification, authentication and any exchange of personal data in most cases makes only sense when content bearing communication follows. Telling an online clothes shop that ones favourite colour is "blue" makes only sense when afterwards some personalised offers are made. Self-portrayal is only done with consecutive communication, whilst this communication is then identity enriched. The communication partners gain knowledge about the other side, which is used during the communication session. It follows that exchange of personal information makes most sense in a session based environment. Current trends show that more and more internet services are session based, as they combine all messages of a session and append further attributes to it. See subsection 2.3 for further details on what sessions are used for and how they are managed today. As a motivation for this paper it is enough to say that today's sessions are not application independent and are not structured in any way. Most notably they have no concept of participants and information about them, since HTTP "sessions" only have one participant (the requesting user) by default.

The idea of the project onefC (open net environment for Citizens) at University of Hamburg is to design and build a generic identity management system which is tightly integrated into an application and network independent session infrastructure. The identity management system will make it possible to store, manage and exchange personal user information. The session infrastructure will enable application independent multi-user sessions with an integrated concept for the representation and management of the users.

1.1 Related Work

There have already been several attempts in identity management. Most notably Microsoft deployed the .NET Passport system, which enables Single Sign-On on participating web services (of which eBay is the most prominent). Users can store an email address, first and last name as well as some personal data like date of birth, languages or region. They can choose whether to share nothing, only the email address, additionally their first and last name, or everything stored in their profile to passport enabled services, when they are “logged on passport”. While this is very coarsely grained, the technology is insecure and has been broken several times already.

Another commercial initiative to enable Single Sign-On was started by Sun Inc., which was joined by many major companies not only from the IT sector. The Liberty Alliance implements federated identities, which mean that services can exchange user information directly, if the users’ consents and the services are in a federation. The Liberty Alliance builds on secure standards like SAML (Security Assertion Markup Language).

There are several research projects, which attempt to build identity management systems with different emphases. Of these, the DRIM project at TU Dresden [Clauß, 2001] and the ATUS project at University of Freiburg [Jendricke et al., 2000] are the most advanced in terms of privacy support, while the IDManager of TU München [Koch, 2001] is leading in community support systems.

2. IDENTITIES AND SESSIONS

This chapter describes the concepts which have been developed for identities and sessions in the onefC infrastructure. While there has been profound research on identities, the research on sessions in this meaning is still young.

2.1 Concept of Personal Digital Identities

The question what an identity is and how it can be represented is one of the most important in identity enriched session management. As the project onefC has the aim to aid people to become someone on the net [Baier et al., 2003], a closer look on the interpersonal comprehension of identities is needed. This section shows up the complexity of the term identity by arguing aspects of philosophy, psychology and sociology. The extracted aspects build up the grounding of the used identity model.

Regarding the identity from the philosophic and mathematic point of view the ability to certainly identify an object is the focus. This is expressed by defining the identity as a binary relation which links an object just to itself. That means it is the finest relation of equivalence and can be seen as a special or marginal case of equity. This abstract definition does not help to make a precise decision about the identity of two objects. To answer this question 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]

Psychology regards the identity of a person as the construction of the single individual. The creation of the identity is based on 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 played role and social context. Thus identity is regarded as a complex structure with multiple elements, where a subset of these is activated or deactivated depending on the actual context. For this reason an identity consists of many group, role, body or task drawn identity parts and is also called "patchwork" which expands every day automatically by inserting new parts.

The second important question next to the structure of an identity is its content. Every part of an identity represents a set of attributes. These attributes 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]

As exposed the personal identity evolves in social interaction. This implies that identities influence each other. From this sociologists derivate a superior structure which is called group or social identity. This structure depends on an unordered set of people which have decided to become a member of a social group and share their more or less characteristic attributes. The link between personal and social identity is represented especially by the feeling of the affiliation to the group - the in-group relationship.

The characteristics and attributes of a social identity do not vary from the ones of a personal identity. That means a development in a group is always a development of the personal identity. [Abdelal and Herrera, 2001][Debatin, 1996][Döring, 1999][Donath, 1996]

2.2 Identity Management as Self-Portrayal

In addition to the private dimension of an identity there is also a public one - the aspects of the person which are presented to the public. This presentation of the identity is always an act of balance between social rules and the demand of the person itself. The content of the displayed attributes is chosen and possibly adjusted according to the actual played role and the pursued goals.

Thereby we always act in a manner which helps us to achieve our goals. This means we do not necessarily present us in a positive way - creating an unpleasant impression could be part of our strategy. This (mostly automatic) change of the presented identity and its attributes is called self-portrayal. [Döring, 1999][Fuchs, 2002][Jendricke et al., 2001]

2.3 Identity Enriched Sessions

The term "session" is widely used in computer systems. However, it rarely is defined or at least described: the meaning is implicitly given through the context or just assumed to be known. For the onefC project a clear definition is needed.

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.

The session contains its participants to be able to associate each communication act to its originator. The participants are represented by the identities described in subsection 2.1. Furthermore, the session attributes can have an arbitrary content, for example the type of encryption or access rules for new users to join the session. As sessions are structured in a hierarchical way, a special kind of attribute is used to assign sets of super sessions. If a session is part of other sessions it inherits any attributes of them.

In particular, our notion of sessions must not be confused with the "session" from the OSI Open Systems Interconnection Layer 5. While this session layer is absent on the Internet, it would only serve for resynchronisation of sessions on a technical layer after the communication might have been interrupted by network problems. These sessions have no further notice of participants than a TCP or UDP socket from the layer below.

On the Internet, (user-) sessions are used on the service side to track user behaviour on web sites, to store information about the user's actions (like shopping cart contents) and to gain generic information about the services effectiveness. Today's web applications use a session construct which is attached to the (historically not session based) HTTP protocol. Since the session can not be found out by the HTTP-request which a user sends, it needs to be identified using cookies, HTTP-parameters or URL-encoding [Lerner, 2000]. But it is not possible to transmit sessions between application servers, be it for intra- or even inter organisational use.

On the client side the current technology successfully hides sessions from users. In some cases it is desired that users log in or log out of the service (for example web based email systems or online banking), but most sessions are invisible to the user. We consider this a problem, since the user is not aware of certain session attributes like the (amount of) data collected on either side, type of encryption or actual session participants.

To solve these problems and to enable multi-application and multi-user sessions we propose a session infrastructure with the abstract notion of a session given above. Applications should be able to initiate or join existing sessions, users should be able to directly monitor and modify sessions. With such an infrastructure, a new generation of online services will be possible. Multi-application sessions will enable users to use several applications in one session without loosing the context. This will make it possible for services to include the functionality of more than one application into their service. The possibility to use any session enabled application also creates a choice for the user to use her favourite one. All of this increases usability. Furthermore, multi-application sessions enable online services to include functionality into their services which could not easily be integrated before.

Multi-user sessions enable a new dimension in online activities as well. So far, all sessions were only for two users. There are constructs in special applications which simulate multi-user sessions, particularly in multi-user chat systems, but while the multi-user aspect of these constructs is analogue to ours, these constructs are far from being as powerful as our sessions.

Our notion of a session is heavily inspired by real world, where people meet to discuss or negotiate. The participants of real world sessions have an image of each other, since they are able to use direct or indirect self-portrayal. All which is said within a session is implicitly associated with it. Some characteristics of the session may be negotiated beforehand, like the permission to tell non-participants about the outcome of the session. This real world concept becomes applicable to Internet sessions with the introduction of Internet identities. Without these, sessions will lack their central component.

The other way around, personal identity information may be useless for communication partners, if they can not associate any substantial statements or requests with them. Identity management and exchange of personal information rarely is an end to itself, it mostly serves other needs (for example to personalise a web service or to authenticate a user, see section 4 for more extensive examples). For these needs, the identity information must be associated with the actual communication, which is done through sessions in the onefC infrastructure.

3. THE "OPEN NET ENVIRONMENT FOR CITIZENS" (ONEFC): AN APPROACH TO REALISE IDENTITY-ENRICHED SESSIONMANAGEMENT

Demands for a digital identity model can be derived from the reflection of the interpersonal comprehension of identities. One of the central aspects is the ability to identify objects distinctly and consistently as well as the assignment of the identity in time and over different contexts. The model should allow the user to create and to activate parts of his identity in accordance with the actual context, role or situation. The contained attributes should not be restricted to any predefined data to keep the model as open as possible. In addition attributes should be reusable in and adaptable to different contexts. To integrate the concept of social identities is eligible, because the influence of the identities of other members of a group holds an opportunity of manifold appliances.

3.1 The Digital Identity Model

The onefC identity model is inspired by the presented "identity patchwork" (see subsection 2.1). It maps this concept to a data tree (see figure 1, the data tree is represented by the self reference of the Identity class). Each node of the tree represents one part of the personal identity, which can be activated in one or more contexts. As a consecutive element a unique identifier ties all nodes together. This identifier makes it possible to identify the user across different contexts. Every single context represents a common and shared background of experiences in which one part of the identity is presented. It can relate to the actual role the user presents or to the situation the communication takes place in. Together with the unique identifier the context directs to the part of the identity which is activated and thus both imply the presented attributes.

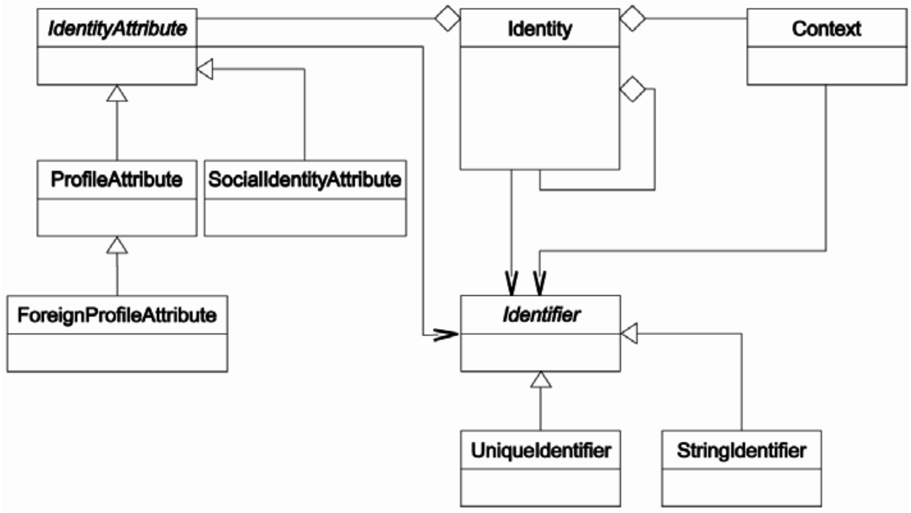

Figure 1. The onefC identity model

Using a tree as the foundation of the onefC data model has several advantages. At first the contained hierarchy is used to define an inheritance concept for the attributes of the identity. Each child node inherits all attributes from its parent. Therefore each layer of the identity tree can be seen as a refinement of the layer above. If there is a set of similar identity parts, the common attributes do not have to be defined several times. E.g. there could be a general identity part for the context "e-commerce" which contains information of the user's name, address and payment method. For each supplier this general data can easily be adapted and refined in special sub identities. A second advantage of this attribute hierarchy is the actuality of the data because every change in an attribute of higher level is passed on to the child elements.

A visibility concept is introduced to adapt attributes, which are implied by the inheritance concept to a part of the identity tree, to the actual context. This allows overwriting the value of an inherited attribute. The new local value masks the old one of the higher levels. This can be used for example if the user has several email addresses and wants to use a special one to separate the emails of single supplier.

The attribute model which is used in the identities is designed to make as little limitations to the potential content as possible. Until now there are two different basic attribute types. The first one represents the basis for all profile attributes which contain characteristics of the user. The second type stands for the "in-group" relationship of a social identity.

As mentioned above the social identity in not represented directly in the onefC model. Merely the feeling to be a member of a particular group can be expressed by the so called "SocialIdentityAttribute". To get an impression of the group identity, the attributes of the members have to be aggregated.

The second type of attributes is the profile attribute which can be used by applications to store and integrate their data. This kind of attributes is designed as a container. This container includes additional metadata about its content. Especially the information about the ontology of the data is important when sharing data between different applications.

3.2 The Identity Management Component

The social behaviour of presenting the personal identity in accordance with the actual context, role, or situation is the basis of the identity management. And therefore digital identity management can be seen as the digital equivalent of self-portrayal. While aiming mainly on digital self-portrayal, the identity manager should still be a very secure tool to increase the protection of personal data. [Berthold and Köhntopp, 2000]

The onefC identity manager which has been developed as a prototype [Kunze, 2004] provides an integrated and infrastructural service and a uniform platform to administrate own and foreign identities (see figure 2). The central management component encapsulates the access to the contained identities. It enforces the security requirements of the user. To achieve this it uses several services which are designed as modules. They are integrated into the system using defined interfaces. This allows the user to use services of his choice and trust. The most precarious service is the security service. This component performs the task to judge about the decision whether an attribute is allowed to be shared or not. It also makes a decision about using an unknown pseudonym instead of the known identifier. A prototypical sample is using the P3P[25] and APPEL[26] specification to set the rules for attribute access. Every communication about identities is done through sessions, so there is no need for identity managers to communicate directly. To keep the user track of the exchanged data the communication is logged by the monitoring service. This allows the user to inspect which data is shared and with whom. The persistence service enables the manager to store the

[25] http://www.w3.org/P3P/

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

identity data to arbitrary media. Especially the use of smart cards is ideal, because the user can carry the digital identity to any place and use it there.

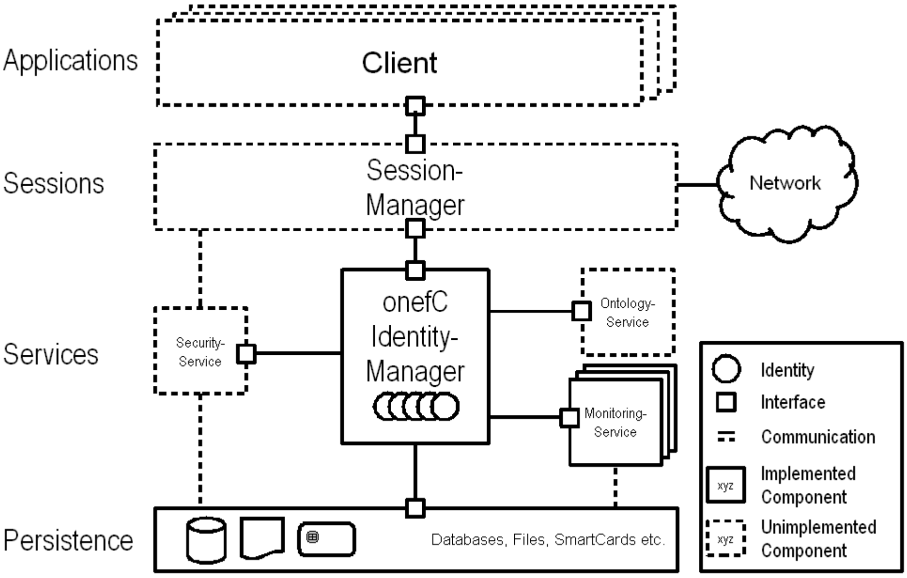

Figure 2. The components of the onefC identity manager

4. SAMPLE SCENARIOS OF ONEFC USAGE

This section presents some sample scenarios which show some of the possibilities and effects an identity enriched session infrastructure might have. As with all new technologies, it is very hard to predict what use it might be put to, just consider the World Wide Web, which ought to connect academic institutes for scientific exchange.

4.1 E-Commerce Sample Scenario

Electronic commerce transactions consist of several phases. These are often divided into information, negotiation and execution phase [Griffel et al., 1998]. During these phases different participants may join the e-commerce transaction. Also, different degrees of visibility of the participants are desired.

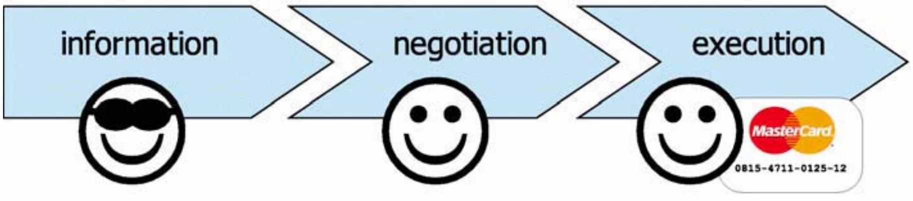

Figure 3. Degree of visibility during business transactions

During the information phase, anonymous browsing of the different offers might be wanted. Contrariwise, the offers might be personalised or even include privileges if the search is not done anonymously but with certain personal information given out to the partners. Negotiation then might already require some personal attributes, so that the service side can decide which conditions apply to this customer. In execution phase, it might be important to invite new participants to the e-commerce session, for example a financial institute which regulates payment issues. Implementing such a transaction is a complex matter, because not only transaction terms must be followed, but also security constraints must be carefully attended. Using the proposed onefC identity and session infrastructure, the development of complex e-commerce applications would be highly simplified.

4.2 E-Government Sample Scenario

The default example for E-Government is e-voting, since it requires a high degree of security and anonymity and therefore sets a high demand on the infrastructure. Although the onefC infrastructure might help to constitute a viable e-voting mechanism, it cannot solve the problem alone. Let us instead consider online registrations at the registry office. It must be assured that the person is not faking her identity by any means, but in contrary to e-voting anonymity is not required. Registration might require several steps: announcement of the former registry office (or signed registration information), server side check whether this information is valid, then the declaration of the new address. This scenario requires secure authentication, which can be reached through certificates which can be stored within the identity manager. The registry office can store digitally signed registration information within the users digital identity, so the user can show this address to other online services like online shops which need a delivery address.

During registration, session would be created to support further requests from the server side being associated to the original communication. This would enable a "wizard"-kind of question and answer dialogue with the online registration service.

4.3 E-Society Sample Scenario

While Single SignOn and easy of use for web services is one major goal of our infrastructure, the main target remains to install a possibility for an Internet society. Societies consist of individuals, and identity management enables Internet users to create Internet identities which make up individuality on the net. Consider the Internet user Alice, who is very active on various web boards. She checks Slashdot[27] often for new articles she could comment and has gained a high "Karma" on that site. This karma is a sign of reputation – it means that her comments were rated high by other SlashDot readers. Alice also writes comments on Tom's Hardware Guides Community Board (Tom's HGCB)[28], but less frequently, so she did not gain any reputation there yet. In the current Internet, she can only give the Tom's HGCB readers a web link to her Slashdot account stating her good karma there, but presumably few will take the time to check the link, since news enquiry must be fast for most Internet users. If Alice could use the same identity from an Identity Manager on both sites, other readers could automatically rate or sort articles on the one board based on reputation values the author gained on the other board. Also, a certain reader on Tom's HGCB (lets call him Bob) might have seen Alice's articles on Slashdot before. Bob liked Alice's articles very much and marked her as a trusted person for IT related information. Bob can unambiguously recognise Alice in Tom's HGCB, although she might post using a different pseudonym (username) there. This way, Alice can keep her personal reputation regardless to the application or service provider used. This is a major factor to build Internet societies. As long as Internet users can build their identity only in the small context of one service, communities will have no chance to interact and have influences on one another, which would be a main aspect of general Internet societies.

5. CONCLUSION

The "open network environment for Citizens" (onefC) project is still in development. It aims to combine identity management with session management. The main goal is to provide mechanisms for online society consti-

[27] http://slashdot.org
[28] http://www.community.tomshardware.com

tution. There is no society without individuals, and these individuals need a representation. There are several other projects leading to a similar goal, but they are motivated differently and have different emphases. The architecture of onefC is kept open and flexible so that outcomes may be used in other projects and contexts. Current status of onefC is an early prototype of the identity manager which has not been released for public review yet. There also exists a sample application which uses onefC to implement the user representation of collaborative filtering software. Future work will include the design and implementation of a session manager which fulfils the requirements described in this paper. The protocols for identity data exchange must be specified. Further, components for semantic integrity (ontology based) and privacy (P3P) are being developed.

REFERENCES

[Abdelal and Herrera, 2001] Abdelal, R. and Herrera, Y. M. (2001). treating identity as a variable: measuring the content, intensity, and contestation of identity. Technical report, Harvard Business School.

[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.

[Berthold and Köhntopp, 2000] Berthold, O. and Köhntopp, M. (2000). Identity management based on p3p. In Workshop on Design Issues in Anonymity and Unobservability.

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

[Clauß, 2001] Clauß, S. and Köhntopp, M. (2001). Identity Management and Its Support for Multilateral Security. In Computer Networks 37 (2001), special issue on electronic business systems, Elsevier, North-Holland 2001, pages 205-219.

[Debatin, 1996] Debatin, B. (1996). Elektronische Öffentlichkeiten. Über Informationsselektion und Identität in virtuellen Gemeinschaften. web-site. http://www.unileipzig.de/˜debatin/english/Articles/Fiff.htm.

[Donath, 1996] Donath, J. S. (1996). Identity and deception in virtual community. Technical report, MIT Media Lab.

[Döring, 1999] Döring, N. (1999). Sozialpsychologie des Internet. Hogrefe. Identity-Enriched Session Management 13

[Fuchs, 2002] Fuchs, T. (2002). Der Begriff der Person in der Psychiatrie. Der Nervenarzt, 73(3):239–246.

[Griffel et al., 1998] Griffel, F., Boger, M.,Weinreich, H., Lamersdorf,W., and Merz, M. (1998). Electronic contracting with cosmos - how to establish, negotiate and execute electronic contracts on the internet. In C.Kobryn, C. Atkinson, Z. M., editor, 2nd Int. Enterprise Distributed Object Computing Workshop (EDOC ’98), page 10. IEEE.

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

[Jendricke et al., 2000] Jendricke, U., Gerd tom Markotten, D. (2001). 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, 2001] Koch, M. and Wörndl, W (2001). Community Support and Identity Management. In: Proc. European Conf. on Computer Supported Cooperative Work (ECSCW 2001), Bonn, Germany, pages 319-338.

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

[Lerner, 2000] Lerner, R. M. (2000). At the forge: Session management with mason. Linux Journal, 2000(76es):24.

[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.

[Sprenger, 1999] Sprenger, P. (1999). Sun on privacy: Get over it.

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

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

[Zirpins et al., 2004] Zirpins, C., Lamersdorf,W., and Piccinelli, G. (2004). A service oriented approach to interorganisational cooperation. In M. Mendes, R. Suomi, C. P., editor, Digital Communities in a Networked Society: eCommerce, eBusiness, and eGovernment. Kluwer Academic Publishers.