Entwurfsversion, veröffentlicht als: Lorenz, A., & Borcea-Pfitzmann, K. (2010). Role management in a privacy-enhanced collaborative environment. In P. Kommers, & P. Isaías (Eds.) *Proceedings of the IADIS International Conference e-Society 2010*, (pp. 3–10). International Association for Development of the Information Society (IADIS), Porto: IADIS Press. URL: http://www.iadisportal.org/digital-library/role-management-in-a-privacy-enhanced-collaborative-environment, Slides: http://www.slideshare.net/anjalorenz/role-management-in-privacyenhanced-collaborative-environment (Stand: 06.01. 2012)

**Full Paper**

# Role Management in a Privacy-Enhanced Collaborative Environment

Anja Lorenz* Katrin Borcea-Pfitzmann†

Nowadays, social software is in demand in very different settings. Managing relationships (e.g., social networking sites) and content sharing (e.g., photo sharing), but also collaborative working via the Internet became a widely accepted part of the social lives of people. Especially, collaborative environments provide platforms supporting users in creating and exchanging new ideas, material, and conducting discussions, but also in representing themselves by allowing for according profile management etc., cf. [KR07].

Supporting the users' privacy in such interactive environments stands in sharp contrast to the objectives of collaboration. However, previous work has shown that different approaches may overcome this ostensible contradiction. One further approach is subject of this paper and consists of a differentiated role management. Accordingly, this paper describes the particular settings of applications shaping *Privacy-Enhanced Collaborative Environments (PECE)*, for which a comprehensive role management has to be realized. The paper discusses the implications on the role concept resulting from the privacy-related settings and introduces a three-dimensional approach for roles in a collaborative environment.

*Chair of Business Information Systems, University of Technology Chemnitz, Germany
†Chair of Privacy and Data Security, University of Technology Dresden, Germany

# 1 Motivation

Collaborative applications became widely accepted, not least since the hype around the Wikipedia platform. With collaborative applications, users get comprehensive tool support to work together with other persons, to create and assess ideas as well as to collaboratively produce new content. That content can be shared amongst selected persons or even with the public, in general. Forums, wikis, or weblogs (also known as blogs) are well-established instances of social software. More special software such as groupware or collaborative eLearning platforms features very similar characteristics. These are, in the first line, connecting different users and providing comprehensive support for communication, collaboration, and, in some cases, even for coordination. However, these possibilities, which are obviously very useful in the indicated application areas, encompass privacy threats, as well. Thereby, the concept of privacy is defined as a person's control over her personal data, i.e., it „describe[s] and demand[s] limits on the appropriation of others' peaceful seclusion, personal information, intimate choices, and identities" [Sta07].

Current popular discussions all concerning the issue of privacy in the Internet focus on protecting people from being observed by institutions for different reasons (e.g., distribution of selective advertising, support of decisions regarding employment, etc.). Technical means (such as anonymization of communication channels, encryption of communication contents or using pseudonyms instead of real names) available to protect one's privacy, in turn, typically focus on the traditional perception of interactions: sender-recipient relationships, i.e., transaction-oriented scenarios between a service provider (e.g., an e-shop) and a user (customer).

When turning to social software and, in particular, to collaborative applications, however, more demanding requirements need to be considered. Social interactions between several users typically do not follow pre-defined protocols, but are rather the result of ad-hoc decisions and according activities. Further, the traditional assumptions restrict technically supported interactions to the involvement of only two parties whereby one of these is an organization. This narrowed assumption still triggers the developments of privacy-enhancing technologies (PETs). Especially, David Chaum, which is one of the leading scientists in this field, saw the surrounding of each person uniformly untrusted [Cha85]. This, however, cannot be applied to social software platforms where interaction is a strongly wanted feature that would not work in a fully untrusted environment.

this context, this paper discusses particular issues and solutions related to roles and their management in a *privacy-enhanced collaborative environment (PECE)* supplemented by privacy-enhancing identity management. Accordingly, the paper is structured as follows: After a description of the particular characteristics of PECEs, an overview of the objectives of roles in collaborative settings will be given whereby we argue the specific „role" of roles within PECEs. After this, we describe our integrative approach of an efficient role management within PECEs by splitting

them into three dimensions. Issues related to the interplay of role management and particular privacy-enhancing mechanisms are pointed out. The paper concludes by discussing the solution and presents an outlook on further work.

## 2 Privacy-Enhanced Collaborative Environments

Even if the scientific community has become more and more aware of the problems connected to privacy in high-interactional application environments, several means or, to be more specific, mechanisms already exist that are useful to overcome privacy-related threats.

One of the most popular approaches is privacy-enhancing identity management, which, in comparison to traditional ways of identity management (which primarily follow the single-sign-on concept, e.g., Microsoft CardSpace, Liberty Alliance), puts *user control* in the focus. This means, that the primary identity-related management functions reside on the users' trusted environments, e.g., at their personal computers. Systems realizing privacy-enhancing identity management focus on the management of different partial identities a user may possess (the concept of partial identities had been introduced in [PH08]). User control, in this relation, refers to the possibility of users self-determining which personal data is disclosed to whom and in which application context.

### 2.1 PRIME and PrimeLife: Research Projects on Privacy-Enhanced Identity

Research in the field of privacy-enhancing identity management as well as the development of according prototypes had been in the focus of several projects, e.g., PRIME funded by the EU (`https://www.primeproject.eu/`) and project PrimeLife (`http://www.primelife.eu/`). In the frame of those projects, several related articles were published coping with privacy in community-based environments. While Borcea-Pfitzmann et al. [BPHL+06] discusses the specifics of privacy management in communities, in general, Borcea-Pfitzmann and Liesebach [BPLP05] as well as Borcea et al. [BDF+05b] describe the approach of integrating privacy-enhancing identity management into a particular collaborative e-Learning environment, namely BluES'n, which serves as framework for the discussion of this paper, as well.

### 2.2 BluES'n: A PECE for Learning

BluES'n (to pronounce: BluES enhanced) represents the privacy-enhanced adaptation of the collaborative eLearning platform BluES (which is an abbreviation of *BluES like universal eEducation System*). BluES has been developed to allow users

- interacting with the *system* in a *self-determined* way as well as

- interacting with *other users* in a *democratic* manner.

Learning and working in BluES is not restricted by strong hierarchical structures, but the system itself fosters vital communication and collaboration among the users of the eLearning environment. Accordingly, the architecture of the system follows the paradigm of flexible modularization whereby a small core application integrates all functionality of the system by plugging in individual modules. That way, the BluES system allows for a very generic system design that can easily be adapted to the users' needs. Specified building blocks reflect that system philosophy, on the one hand, and provide a conceptual structure of the overall system to its users, on the other hand. In the following, the core building blocks having effect on the role management described in this paper are presented.

The central building block supporting the work of the users is the *workspace*. It is used to separate context-dependent, objective-, and task-oriented processes. Workspaces are represented not only by the content, which is elaborated on within the workspaces' frames, and the utilities used to manipulate the content, but workspaces are also characterized by particular properties. These are, e.g., maximum of participants in the workspace, duration of the workspace being active, permissions and available roles.

Another important building block comprises the concept of *functional modules*. These are software components, which encapsulate task-related functionalities; they are reusable and configurable according to the corresponding requirements. Functional modules represent the central items of the workspaces. Examples for functional modules are tools for communication (chat), coordination (calendar), collaboration (wiki or creativity techniques), or for content creation and presentation.

For the sake of completeness, it should be mentioned that the core BluES platform comprises further building blocks related to data management. But, since data handling is not required to describe the concepts of this paper, we will not go into detail regarding those building blocks. Further information on this issue can be retrieved by conferring [BP08].

## 2.3 Privacy and Security Mechanisms in BluES'n

With respect to privacy and security, we distinguish between building blocks for identity management and for access control. Thereby, pseudonyms and partial identities are concepts of the former building block. Pseudonyms are used to realize addressability and moreover, they serve as identifiers of the partial identities used to represent the user in certain contexts. A partial identity is a subset of attributes, whereby the union of all partial identities of an individual is his/her complete identity [PH08]. Thus, the concepts of pseudonyms and partial identities allow to actively control the degree of privacy of a user. This strongly depends on how frequently a

user selects one and the same partial identity and on how fine-grained the partial identities are defined.

An exceptional characteristic of BluES'n consists in a twofold approach of providing authentication and authorization (i.e., access control): Parallel to the well-known ACL-based approach implying that each user registers with the system, BluES'n allows also for an account-less access control approach. This is based on certified properties – so called anonymous credentials [Cha85] – that are issued to the users. Such a credential attests the users their rights to access resources in a given way. Beforehand, policies are being attached to the resources. A policy indicates which credential a user has to show to get access to the corresponding resource. To conclude, users do not need to sign in and to maintain a profile in the system. Instead, they authenticate only on the layer of interaction between the users without involving system protocols. Such kind of authentication is required not for the reason of authorizations, but to give others an idea with whom they are interacting. The main advantage of this approach is that users can self-specify particular context boundaries, within which they act presenting one specific partial identity of themselves.

The eLearning platform BluES'n comprises other approaches, which all are used to cope with the dilemma related to social interaction and privacy requirements. To indicate but a selection: controlled transmitting and using according awareness information, cf., e.g. [BDF+05b], privacy-respecting reputation [Ste06], and intra-application partitioning [BDF+05a].

## 3 Overview of Roles in Collaborative Settings

The motivation of integrating roles into a collaborative environment is quite simple: they do already exist there anyway – at least in an implied way. When users work together, each of them will take over a certain position within the group to set up the working scenario. Zhu [Zhu03] states, that „without roles, there would be no collaboration". A survey of related scientific literature revealed different interpretations of the concept of roles. According to this, roles can be classified in four main categories:

1. **Positions**. Also referred to as *status* or *function*, roles can be used to describe a collection of rights, duties [Lin36], and expectations [Luh84].

2. **Groups**. Roles are also used to categorize users by similarity. In this way a role shows the *kind* of user [Zna65].

3. **Behavior**. Roles can be used to assign activities to users [Ger71], e.g., *reader* or *reviewer*.

4. **Relations**. Finally, roles can describe different kinds of relationship, cf. [Mea67], [Gof74], or [CJR02]. In that case, the role of a user can differ depending on the individual interaction partners, e.g., a secretary is a workmate towards other secretaries, but an employee towards the director.

Based on this variety of understandings, there are different approaches of integrating roles into collaborative learning environments: from simple role management systems that distinguish between owner and participant roles, e.g. CommSy (http://www.commsy.net) or Bildungsportal Sachsen (https://bildungsportal.sachsen.de/), via systems to realize role-based access control on materials or functionalities (cf. [Edw96], Moodle (http://www.moodle.de/), up to environments providing a free and universal role management system for complex scenarios ([KR04], Saba (http://www.saba.com/)). The prime aim, which all the approaches strive for, consists in gaining particular benefit for users of the applications by reducing management complexity, i.e., similar actions can be applied to a group of users at once instead of to each user individually (whereby the group is determined by the according role uniting the persons). With help of roles, it is possible to generate a certain work setting [Dil99], to ease access control [NO94], and to assign a set of duties and expectations to a user group [KR04]. By showing the role of a user to another, they can get a better understanding of their relation in the current work setting [Bel04].

Integrating roles in PECEs helps to maintain the focus of the tasks. In particular with regard to users heavily using different partial identities, role profiles and descriptions can remind of their aims, duties, or relationships. However, roles are information about a user and can be put on one level with personal data like surnames or ages. Thus, roles imply privacy threats. Especially, if just a few holders of one and the same role exist within the environment, that could enable non-authorized persons to link the partial identities indicating that role to each other. In cases where each user is aware of the existence of only one role holder, e.g., a working group has exactly one team leader, every partial identity showing this role can be associated with the one person known from the physical world.

## 4 Concept of Role Management in PECEs

This section describes the approach of role management developed for integration in a PECE. It had to face up a proof-of-concept validation by applying it in BluES'n (cf. section 2). Accordingly, the development of role management had to meet the specifics of the e-Learning platform BluES. This particularly means that the traditional approach of pre-determined role assignment to user accounts cannot be followed. As introduced, the users perform all activities within workspaces. Basically, all users have the same options of participation and initiation of learning scenarios due to the prime paradigm of BluES „Each user is allowed to do anything – within the frame of generally agreed rules and directives". In fact, roles are not needed outside

of workspaces except for the role denoted to users administrating the platform. Within workspaces, a flexible role management is required that can be adapted to the learning scenarios, e.g., addressing autocratic, democratic and autonomic settings. Since tasks, authorizations, and team constellations may instantly change during collaborative work, the roles in a workspace have to be adjustable to such conditions.

## 4.1 A Role Concept for a Democratic Collaborative Environment

By integrating roles into a PECE, the facilitation of as many tasks related to user management as possible is intended. In this context, the following understanding of roles evolved: Roles describe stereotypes of users, which abstract a group of actors with equal rights and duties. Certain expectations are placed in users of a specific stereotype addressing the way the users should act like. Further, assignments of roles shall also help the interaction partner to range in a user's position within the collaborative work.

To develop a highly flexible system that meets the requirements of privacy-preservation, we distinguish the following three dimensions of roles that comply with their management tasks:

1. **Administrative roles** are used to manage users' rights and to realize role-based access control in workspaces, e.g., *owner* or *participant*;
2. **Functional roles** are used to manage users' tasks by defining particular privileges, duties, and expectations, e.g., *teacher* or *author*;
3. **Group-dynamic roles** are used to identify a user's abilities within a group, e.g., *expert* or *problem solver*.

To simplify the general access, every user holds only one administrative role per workspace. Either, he is the *owner* possessing all administrative responsibilities concerning the respective workspace, or he is a *participant* who is actively involved in given tasks. Finally, the user may passively attend the work in a workspace as *guest*. With respect to the variety of possible working scenarios and flexible adjustments, functional roles may be defined by the (workspace) owner without restrictions by a set of predefined role definitions. Unlike the administrative roles, a user may hold more than one functional role. This approach corresponds to situations of the physical world where people also have to manage more than just one position within particular contexts. Thus, the set of tasks, duties, or responsibilities of a user is formed by his individual combination of roles that are much easier to manage than a wide division of highly sophisticated role definitions, like, e.g., an *author with reviewing tasks* in contrast to an *author with reviewing and teaching tasks*. Group-dynamic roles used within a particular group base on calculations of

the role holders' reputations. This implies that the users' performances are assessed regarding certain abilities and corresponding reputation values are calculated. With respect to the determination of group-dynamic roles of users, the reputation values of all group members are compared whereby the results define the assignments of the particular group-dynamic role to the according users. For more information about the concept of flexible roles in BluES, see [Lor09] and [BP08]. By realizing a combination of these three role dimensions, we developed a role management that is not only able to be adjusted by several role attributes, like duties, access rights, or expectations, but also by the specific combinations of roles for users, that makes it usable for a wide range of working scenarios.

### 4.2 Benefits Regarding Privacy Issues

The described approach of role management in PECEs does not only benefit from the possibility of flexible role definitions. Integrating roles also opens the possibility to shift the conditions for provided rights and functionalities from users to roles. That means that the policies of resources as well as of functional modules indicate roles instead of users denoting them as entities authorized to access the resource or functional module, respectively. E.g., writing access to a document is allowed for all users possessing the role *author*. So, it is no longer necessary to know the particular users having writing access, but they have to prove the possession of the author credential. In comparison to the well-known role-based access control mechanism, our approach does not require a list of users assigned to a role, centrally managed by the application server. Instead, privacy is provided by externalizing that list in form of de-centralization of user-role assignment.

Additionally, users can distribute their roles to different partial identities. By separating roles onto different partial identities, interaction partners do not get to know that the roles and the partial identities belong to a particular person. For instance, a user may act as an *author* using a partial identity with the pseudonym „John". When being a *reviewer*, one and the same user presents himself as „Michael". Since users have the possibility to appear in different contexts using different partial identities towards their interaction partners, the roles-related risk of linkability of partial identities decreases to a minimum.

A further advantage addresses the independent evaluation of the reputation of a user in different contexts. With help of roles, the quality of a user's work can independently be evaluated. This way, e.g., a poor reputation value of an *author's* work would not influence his standing as *reviewer*. That way, the person is also not identifiably by his reputation value(s).

## 5 Discussion of the Concept

With the role management developed for the PECEs, users may distribute their roles on several partial identities to minimize linkability of personal data to a complete identity. Although we provide possibilities to distribute role attributes to several roles according to the management tasks and to use those roles with different partial identities, users have to be careful concerning the granularity of their data distribution, nevertheless. If they use only few partial identities, it is relatively easy to create links between them. This is especially true when the same role sets are used with two or more partial identities. In BluES'n, a decision suggestion module (DSM) has been integrated to support users with selecting the appropriate partial identity according to the corresponding context. To enhance the DSM support for managing roles, we analyzed which context can be important for using a role and in which situations do the users switch to another partial identity, cf. Table 1. For this, we devolved the pseudonym classification of [PH08].

| **Kind of pseudonym** | **Changing pseudonym per** | | | **Example** |
|---|---|---|---|---|
| | **Role** | **Interaction partner** | **Transaction** | |
| Person pseudonym | – | – | – | Identity card or national insurance number |
| Role pseudonym | • | – | – | Different login names in online shops and platforms |
| Relationship pseudonym | – | • | – | Different customer IDs for airline and insurance for the same flight |
| Role-relationship pseudonym | • | • | – | Contract numbers |
| Transaction pseudonym | (•) | (•) | • | TAN numbers for bank transfers |

Tabelle 1: Classification of pseudonyms based on interaction partners, roles and transactions, cf. [Lor09]

In accordance to these contexts, we determined possibilities for selection rules of partial identities that can be performed by the DSM. Afterwards, we evaluated the ability of the rule to protect users' privacy:

- With **transaction pseudonyms**, the highest degree of privacy can be reached, because every partial identity is used only once and will not be reused in future. In collaborative environments, recognitions of interaction partners and shared experiences are indispensable for reasonable group work. Therefore, an automatic creation of a new partial identity each time a transaction is performed is not an adequate solution.
- **Role**, **relationship** and **role-relationship pseudonyms** solve the problem of recognizability, but limit the free choice of disclosure of personal data by the user. To give an example, in case of a partial identity created towards a particular interaction partner, the user has to disclose that personal data (encapsulated within this partial identity) that will be needed in transactions covered by this relationship or role. Thus, an automatic selection of the proper partial identity based on a certain role, a certain relationship, or a role-relationship relation is problematic with respect to privacy, as well.
- The option of creating **only one partial identity (person pseudonym)**, which would imply all of a user's personal data, corresponds to the traditional account-based approach. It would eliminate all privacy-enhancing benefits. This again is not an acceptable way for role management in PECEs.

As a result, we appoint that there is no default way to realize an automated selection of partial identities according to the chosen roles the users act with. The DSM may only give advices to the user, which corresponds to the user's preferences, e.g., a user strictly distinguishes between trusted workspaces in contrast to open ones when selection partial identities.

## 6 Conclusion and Outlook

In PECEs, technologies of privacy-enhancing identity management are used to protect the users' privacy. This way, the user's personal data are distributed onto several partial identities. To prevent unauthorized collections of personal data by service providers as well as by other users, PECEs provide means for usercontrolled disclosure of personal data, i.e., users may decide by themselves, which information can be accessed by whom and in which application context.

Displaying roles to the interaction partners of a user means to reveal a hint, which could be used to link the user's partial identities and to create a detailed profile about that user from the collected data. With the help of a flexible and decoupled role management, the roles of a user may be distributed onto several partial identities. Thus, every partial identity of a user holds a different set of roles. That way, the risk for the users' privacy can be reduced. The analysis of options for self-acting selections of partial identities by the DSM of BluES'n has shown that there is no

standard way for selecting the right partial identity. The DSM only can make proposals based on the user preferences and on his previous behavior. Finally, the users have to decide on the right distribution of their personal data. A privacy-enhancing identity management may help them with this task. A standard solution for choosing the proper granularity of partial identities does not exist.

The work documented in this paper is well elaborated with respect to developing the concept and discussing privacy issues related to the concept. Its technical realizability has been proved by a first implementation and integration into BluES'n. Our future work will take up the integration work, which needs to be finalized, as well as to focus on experimental evaluation, e.g., conducting an according study with real users.

## Literaturverzeichnis


[BDF+05a] Katrin Borcea, Hilko Donker, Elke Franz, Katja Liesebach, Andreas Pfitzmann, and Hagen Wahrig. Intra-application partitioning of personal data. In Alfred Kobsa and Lorrie Cranor, editors, *Proceedings of the Workshop on Privacy-Enhanced Personalization (PEP'05)*, pages 67–72. UC Irvine Institute for Software Research (ISR), Edinburgh, UK, June 2005. URL `http://www.isr.uci.edu/pep05/papers/borcea-pep.pdf`.

[BDF+05b] Katrin Borcea, Hilko Donker, Elke Franz, Andreas Pfitzmann, and Hagen Wahrig. Privacy-aware elearning: Why and how. In Piet Kommers and Griff Richards, editors, *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2005*, pages 1466 – 1473. Association for the Advancement of Computing in Education (AACE), Chesapeake, VA, 2005. URL `http://www.editlib.org/p/20284`.

[Bel04] Raymond Meredith Belbin. *Management teams: why they succeed or fail*, volume 2. Oxford, 2004. ISBN 0-7506-5910-6. URL `http://books.google.de/books?id=PYYtYhOeEyMC`.

[BP08] Katrin Borcea-Pfitzmann. Framework für die entwicklung einer universellen kollaborativen elearning-plattform. Phd thesis, Technische Universität Dresden, Fakultät Informatik, Dresden, September 2008. URL `http://nbn-resolving.de/urn:nbn:de:bsz:14-ds-1237287991632-27077`.

[BPHL+06] Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann, and Sandra Steinbrecher. What user-controlled identity management should learn from communities. *Information Security Techni-*

*cal Report*, 11(3):119–128, 2006. URL http://linkinghub.elsevier.com/retrieve/pii/S1363412706000343.

[BPLP05] Katrin Borcea-Pfitzmann, Katja Liesbach, and Andreas Pfitzmann. Establishing a privacy-aware collaborative elearning environment. In *Proceedings of the EADTU Working Conference 2005*, volume 2005, pages 10–11. EADTU, Rome, Italy, November 2005. URL http://www.eadtu.nl/proceedings/2005/papers/KatrinBorcea-Pfitzmann.pdf.

[Cha85] David Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985. URL http://dx.doi.org/10.1145/4372.4373.

[CJR02] Angela Carell, Isa Jahnke, and Natalja Reiband. Computergestütztes kollaboratives lernen: Die bedeutung von partizipation, wissensintegration und einfluss von rollen. *Journal Hochschuldidaktik*, 13(2):26–35, September 2002. ISSN 0949-2429. URL http://www.sociotech-lit.de/CaJR02-CkL.pdf.

[Dil99] Pierre Dillenbourg. What do you mean by collaborative learning? In Pierre Dillenbourg, editor, *Collaborative-learning: Cognitive and Computational Approaches*, pages 1–19. Elsevier, Oxford, 1999.

[Edw96] W. Keith Edwards. Policies and roles in collaborative applications. In *Proceedings of the 1996 ACM conference on Computer supported cooperative work - CSCW '96*, pages 11–20. ACM Press, New York, USA, November 1996. ISBN 0-89791-765-0. URL http://dx.doi.org/10.1145/240080.240175.

[Ger71] Uta Gerhardt. *Rollenanalyse als kritische Soziologie: Ein konzeptueller Rahmen zur empirischen und methodologischen Begründung einer Theorie der Vergesellschaftung*. Number 72 in Soziologische Texte. Luchterhand, Neuwied, Berlin, 1971.

[Gof74] E. Goffman. *Rollenkonzepte und Rollendistanz*. Hoffmann und Campe Verlag, Hamburg, 1974. ISBN 978-3455091182.

[KR04] Andrea Kienle and Carsten Ritterskamp. Rollenbasierte kooperationsunterstützung in cscl-umgebungen. In Gregor Engels and Silke Seehusen, editors, *Proceedings of DeLFI 2004, Die 2.e-Learning Fachtagung Informatik*, Lecture Notes in Informatics, pages 223–224. Springer, Bonn, 2004. URL http://www.sociotech-lit.de/KiRi04-RKi.pdf.

[KR07] Michael Koch and Alexander Richter. Social software – status quo und zukunft. Technical Report 2007-01, Universitaet der Bun-

deswehr Muenchen, Fakultaet fuer Informatik, Neubiberg, February 2007. URL http://www.kooperationssysteme.de/docs/pubs/RichterKoch2007-bericht-socialsoftware.pdf.

[Lin36] Ralph Linton. *The study of man: an introduction*. Appleton Century Crofts, Inc., New York, USA, 1936. ISBN 978-0138589691.

[Lor09] Anja Lorenz. *Rollenmanagement trifft Privatsphäre: Problempunkte und Konsequenzen*. VDM-Verlag, Saarbrücken, 2009.

[Luh84] Niklas Luhmann. *Soziale Systeme. Grundriß einer allgemeinen Theorie*. Suhrkamp Verlag, Frankfurt, 1984. ISBN 351857700X.

[Mea67] George Herbert Mead. *Mind, Self and Society*. University of Chicago Press, Chicago, 3 edition, 1967.

[NO94] Matunda Nyanchama and Sylvia L. Osborn. Access rights administration in role-based security systems. In *Proceedings of the IFIP WG11.3 Working Conference on Database Security VII*, pages 37–56. North-Holland Publishing Co., Amsterdam, The Netherlands, The Netherlands, 1994. ISBN 0-444-81976-2. URL http://dl.acm.org/citation.cfm?id=679923.

[PH08] Andreas Pfitzmann and Marit Hansen. Anonymity, unlinkability, undetectability, unobservability, pseudonomity and identity management – a consolidated proposal for terminology. Draft, Version 0.31, Februar 2008. URL http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

[Sta07] William G. Staples. *Encyclopedia of Privacy: A-M*, volume 1 of *Encyclopedia of Privacy*. Greenwood Publishing Group, Westport (Connecticut); London, 2007. ISBN 0313334773. URL http://books.google.de/books?id=sFv1ZltBhR0C.

[Ste06] Sandra Steinbrecher. Design options for privacy-respecting reputation systems within centralised internet communities. In Simone Fischer-Hübner, Kai Rannenberg, Louise Yngström, and Stefan Lindskog, editors, *Security and Privacy in Dynamic Environments: Proceedings of the IFIP TC-1 1 2 1st International Information Security Conference (SEC 2006)*, volume 201 of *IFIP*, pages 123–134. Springer, Boston, 2006. ISBN 0-387-33405-X. ISSN 1861-2288. URL http://www.springerlink.com/content/9423773p13q287k6/.

[Zhu03] Haibin Zhu. Some issues of role-based collaboration. In Guy Oliver, Samuel Pierre, and Vijay KEditors Sood, editors, *Proceedings of Canadian Conference on Electrical and Computer Engineering 2003 (IEEE*

*CCECE 2003)*, volume 2, pages 687–690. IEEE Computer Society, Montreal, Canada, 2003. URL http://dx.doi.org/10.1109/CCECE.2003.1225988.

[Zna65] Florian Znaniecki. *Social relations and social roles: the unfinished systematic sociology*. Chandler publications in anthropology and sociology. Chandler Pub. Co., San Francisco, CA, 1965.