Entwurfsversion, veröffentlicht als: Lorenz, A., & Borcea-Pfitzmann, K. (2010). Role management in a privacy-enhanced collaborative environment. *Interactive Technology and Smart Education*, 7 (2), 102–112. URL: http://dx.doi.org/10.1108/17415651011071037 (Stand: 08. 01. 2012)

Research Paper

Role Management in a Privacy-Enhanced Collaborative Environment[*]

Anja Lorenz[†] Katrin Borcea-Pfitzmann[‡]

Abstract

Purpose

Facing the dilemma between collaboration and privacy is a continual challenge for users. In this setting, this paper discusses issues of a highly flexible role management integrated in a privacy-enhanced collaborative environment.

Design/methodology/approach

The general framework was provided by former findings of several research projects, i.e., collaborative platform BluES and projects of privacy and identity management PRIME and PrimeLife. The role management concept bases on a literature survey and has been proofed by integration into the privacy-enhanced environment BluES'n.

Findings

A three-dimensional role management concept was developed describing users' rights, tasks, and positions. A discussion on how to fulfill privacy requirements yielded that a semi-automated decision making regarding

[*] This paper originated at the IADIS e-Society Conference, Porto, Portugal, 18-21 March, 2010

[†] Chair of Business Information Systems, University of Technology Chemnitz, Germany

[‡] Chair of Privacy and Data Security, University of Technology Dresden, Germany

the use of roles with different identities is reasonable to support users' control of their privacy when interacting with others.

Research limitations/implications
The concept of flexible role management complies with the requirements of privacy-enhanced collaborative environments. However, a fully automated approach of rule-based information disclosure is not possible as such decisions depend on personal and situational aspects.

Practical implications
Using the example of a flexible role management concept, research described in this paper demonstrates that privacy and interaction concerns can be balanced and should be considered in application design processes.

Social implications
Concepts of privacy-enhanced collaborative environments allow respecting privacy-related attitudes and could improve the quality of service consumption.

Originality/value
The paper demonstrates contrasts between collaboration and privacy attitudes and presents solutions for the integration of role management to overcome this initially supposed contradiction.

Keywords
Role management, privacy, collaborative environments, social software, BluES'n

1 Introduction

Collaborative applications are nowadays an integral part of many working groups. These tools deliver their users comprehensive support for communication, collaboration and coordination of the tasks within a working group. This way, co-workers are enabled to easily create and assess ideas as well as to collaboratively produce new content, which can be shared among group members. Forums, wikis, or weblogs (also known as blogs) are well-established instances of collaborative applications. More special software such as groupware or collaborative eLearning platforms features very similar characteristics.

However, these possibilities, which are naturally very useful in the indicated application areas, encompass privacy threats, as well.[1] Obviously, collaborative applications tempt the users not only to indicate factual statements but also to disclose personal opinions and attitudes as described in Pötzsch and Borcea-Pfitzmann [PBP10]. Technical means (such as anonymization of communication channels, encryption of communication contents, or using pseudonyms instead of real names) are first-step approaches to cope with privacy problems caused by the use of provided functionality of the applications.

Nevertheless, those instruments imply two issues, which are not to be underestimated: First, privacy-enhancing technologies (PETs) are typically not provided together with the actual application. Instead, they are independent tools, the use of which makes only sense if the user or the application, respectively, does not invade the user's privacy, e.g., by sending a unique identifier with each message. Second, the focus of the privacy-enhancing tools is rather 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 collaborative applications (which are to be understood as a particular type of social software), 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. Traditional models of computer communication refer to a clear separation of human beings and the computers they use In the course of Web 2.0 developments, this assumption has to be revised in such a way that human beings not only use computers but they also become parts of the digital world. Further, the development of privacy-enhancing technologies is still triggered by the narrowed assumption that the surrounding of each person is 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. Consequently, privacy-respecting applications need to be designed in such a way that the privacy-enhancing technologies have to be integrated within the applications and they have to regard the specifics of the applications functionality.

In this context, this paper discusses particular issues and solutions related to the specific topic of roles and their management, which are important building blocks of collaborative applications, 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

[1] Thereby, the concept of privacy is defined as „the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.“ [Wes70]

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 is still hesitating in developing adjusted means to overcome the problems connected to privacy in high-interactional application environments, several mechanisms already exist that can be used.

One of the most promising approaches is *privacy-enhancing identity management*, which, in comparison to traditional ways of identity management (primarily following the single-sign-on concept, e.g., Microsoft CardSpace, Liberty Alliance), puts the *user into control* of his/her personal data. This means, that the primary identity-related management functions reside on the users. trusted environments, e.g., at their computers. Systems realizing privacy-enhancing identity management focus on the management of different partial identities a user creates and possesses (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 in which application context and to what extent.

Research in the field of privacy-enhancing identity management and the development of according prototypes had been in the focus of several projects, e.g., PRIME (https://www.prime-project.eu/) and PrimeLife (http://www.primelife.eu/), both of them funded by the EU. In the frame of these 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. [FLBP06] 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.

2.1 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*). The initial system BluES has been developed in accordance of the prime paradigm „Each user is allowed to do anything – within the frame of generally agreed rules and directives“. This particularly means that users are enabled

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

- to interact 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 and provide a conceptual structure of the overall system to its users. 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 also building blocks related to data management and further information on this issue can be found in [BP08].

2.2 Privacy and Security Mechanisms in BluES'n

As indicated, the core system BluES has been enhanced with specific modules allowing to preserve the users' privacy when working with the collaborative application. Thus with respect to privacy and security, we distinguish between building blocks for *identity management* and for *access control*. Thereby, pseudonyms and partial identities (pIDs) are concepts of the former building block. Pseudonyms are used to realize addressability of the users in the collaborative environment. They prevent linkability to the real identity of a user by substituting account names and are generated by cryptographic means. Moreover, pseudonyms serve as identifiers of pIDs, which in turn are used to represent the user in certain contexts. A pID is a subset of attributes, whereby the union of all pIDs of an individual is her complete identity [PH08]. In a privacy-enhanced environment, users are enabled to present themselves using several pseudonyms towards other users as well as towards the system. This allows a user to actively control the degree of his/her privacy depending on how frequently the user selects one and the same pID and on how fine-grained the pIDs 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. The credential attests the users their rights to access resources in an indicated way. Beforehand, so called access control policies are being attached to the resources. The policy indicates which credential(s) 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 (recognition of pseudonyms) 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 pID of themselves.

The eLearning platform BluES'n comprises further approaches, all of which are used to cope with the dilemma related to the wish of social interaction and the privacy attitudes of the users. To indicate but a selection: controlled transmitting and using according awareness information, cf. e.g. [FLBP06], privacy-respecting reputation [Ste06], and intra-application partitioning [BDF+05].

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 [Mea67] [Gof74][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`) via systems to realize role-based access control on materials or functionalities [Edw96] up to environments providing a universal role management system for complex scenarios [KR04]. 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].

In addition to the benefits for access management, integrating roles in PECEs helps to maintain the focus of the users' tasks. In particular, with regard to users heavily using different pIDs, role profiles and descriptions can remind of their aims, duties, or relationships.

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, it had to meet the specifics of the e-Learning platform BluES. This particularly means that 1) the traditional approach of pre-determined role assignment to user accounts cannot be followed; 2) the users perform all activities within workspaces; 3) all users have the same options of participation and initiation of learning scenarios.

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* and their according role attributes, like role title, duties, permissions, maximum number of role holders etc., 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 a particular context. Thus, the set of tasks, duties, or responsibilities of a user is formed by his/her individual combination of roles, which 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 are used within a particular group and base on calculations of contextual reputations. This implies that the users' performances are assessed regarding certain abilities and corresponding contextual 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 access control 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. For example, 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 (RBAC), our approach does not require a list of users assigned to a role, centrally managed by the application server. Instead, that list is being de-centralized by issuance of credentials indicating the according role to the respective users. This way, the users maintain control over displaying the role to others, which again contributes to the ambition of preserving the users' privacy.

Additionally, users can distribute their roles to different pIDs. Thereby, interaction partners do not get to know that the roles and the pIDs belong to one particular person. For instance, a user may act as an *author* using a pID with the pseudonym „Joana“. When switching to the functional role *reviewer*, one and the same user presents herself as „Hanna“. Since users have the possibility to appear in different contexts using different pIDs towards their interaction partners, the roles-related risk of linkability of pIDs decreases to a minimum.

A further advantage addresses the independent evaluation of the reputation of a user in different contexts (contextual reputation). With the aid 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/her standing as *reviewer*. Or even more specific since contextual reputations are the basis for group-dynamic roles: A person can gain high reputation as a *team leader* while not really asserting himself/herself in conflicting situations as *mediator*. That way, reputation-related assessments of the user by others will not bias each other. Obviously, privacy can only be really preserved if the user applies distinct pseudonyms for the different contexts denoting her as team leader and mediator.

5 Discussion of the Concept

With the described concept of role management developed for PECEs, users may distribute their roles onto several pIDs to minimize linkability between different activities and linkability to the physical identity of themselves. In result, it reduces the risk of linking disclosed 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 pIDs, users have to be careful concerning the granularity of their data distribution, nevertheless. If they use only few pIDs, it is relatively easy to create links between them. In such a case, the attributes of the pIDs would be very similar and parts of the personal data used within the individual pIDs could overlap. This may lead to situations where other users could associate those pIDs of the user, based on same identity attributes.

In BluES'n, a decision suggestion module (DSM) has been integrated to support users with selecting the appropriate pID 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 pID, cf. Table 1. For this, we devolve the pseudonym classification of Pfitzmann and Hansen [PH08].

	Changing pseudonym per			
Kind of pseudonym	**Role**	**Interaction partner**	**Trans-action**	**Example**
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 pIDs that can be performed by the DSM. Afterwards, we evaluated the ability of the rule to protect the users' privacy:

- With **transaction pseudonyms**, the highest degree of privacy can be reached, because every pID 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 pID 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 pID created towards a particular interaction partner, the user has to disclose all those personal data (encapsulated within this pID) that will be needed in transactions covered by this relationship or role. Thus, an automatic selection of the proper pID 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 **just one pID (person pseudonym)**, which would imply all of a user's personal data required for any transaction within the collaborative environment, 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 automatic selection of pIDs 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 selecting pIDs.

An additional argument needs to be considered referring to roles being information about a user. Thus, roles may also imply privacy threats. Especially, if just a few holders of one and the same role exist within the environment, it could enable non-authorized persons to link the pIDs 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 pID showing this role can be associated with the one person known from the physical world.

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 pIDs. To prevent unauthorized collections of personal data by service providers as well as by other users, PECEs provide means for user-controlled disclosure of personal data, i.e., users may decide by themselves, which information can be accessed by whom in which application context and to what extent.

Displaying roles to the interaction partners of a user means to reveal a hint, which could be used to link the user's pIDs 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 pIDs. Thus, every pID 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 pIDs by the DSM of BluES.n has shown that there is no standard way for selecting the right pID. The DSM only can make proposals based on the user preferences and on her previous behavior. Finally, the users have to decide on the appropriate distribution of their personal data. A privacy-enhancing identity management may help them with this task albeit a standard solution for choosing the proper granularity of pIDs 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 of administrative and functional roles into BluES'n. Also, a module has been developed specifically addressing the assessment of the users performance and the calculation of reputation values. 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.

Acknowledgement

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 216483.

Literaturverzeichnis

[BDF⁺05] 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.

[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 Technical 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`.

[FLBP06] Elke Franz, Katja Liesbach, and Katrin Borcea-Pfitzmann. Privacy-aware user interfaces within collaborative environments. In Kristijan

Mihalic, editor, *Proceedings of the international workshop in conjunciton with AVI 2006 on Context in advanced interfaces – AVI '06*, pages 45–48. ACM Press, New York, USA, 2006. URL http://dx.doi.org/10.1145/1145706.1145715.

[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.

[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.

[PBP10] Stefanie Pötzsch and Katrin Borcea-Pfitzmann. Privacy-respecting access control in collaborative workspaces. In Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, and Ge Zhang, editors, *Privacy and Identity, IFIP AICT 320*, volume 320/2010 of *IFIP Advances in Information and Communication Technology*, pages 102–111. Springer, Boston, 2010. ISBN 978-3-642-14281-9. URL http://dx.doi.org/10.1007/978-3-642-14282-6_8.

[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`.

[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/`.

[Wes70] Alan Westin. *Privacy and Freedom*. Atheneum, New York, 1970.

[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.