How to enhance Privacy and Identity Management for Mobile Communities: Approach and User driven Concepts of the PICOS Project

Christian Kahl, Katja Böttcher,
Markus Tschersich, Stephan Heim, Kai Rannenberg

Goethe University Frankfurt, Chair of Mobile Business & Multilateral Security
Grüneburgplatz 1
60629 Frankfurt am Main, Germany
{Christian.Kahl, Katja.Boettcher,Markus.Tschersich,
Stephan.Heim, Kai.Rannenberg, picos}@m-chair.net

Abstract. Mobility allows social communities to become a ubiquitous part of our daily lives. However, as users in such communities share huge amounts of personal data and contents, new challenges emerge with regard to privacy and trust. In this paper we motivate the necessity of advanced privacy enhancing concepts, especially for mobile communities and outline the approach of the PICOS project in order to elaborate such concepts. We explicate how we collected mobile community requirements and elaborated adequate concepts to address them. Finally, we conclude with details on how the concepts were prototypically implemented to demonstrate their feasibility, what distinguishes them from existing work, and how we intend to transfer the concepts to practice.

Keywords: Mobile Communities, Privacy, Trust, Identity Management

1 Introduction

Recent years have seen the emergence of services for professional and private on-line collaboration via the Internet. Nowadays, people spend increasing amounts of work and leisure time in on-line communities, such as online social networks (e.g. MySpace, Facebook, LinkedIn, etc.), that provide online communication services to support the activities of virtual or real world communities (cf. [1], [2], [3]). Moreover, communities based on mobile communication allow users to participate in their community not only from places where fixed-line communication is available. Mobile communication also allows the provision of services, which make use of context information (e.g., location, time), thereby enabling a deeper integration of people's virtual (mobile) and real world communities (e.g., via Loopt, Junaio, match2blue) [1].

However, when users participate in such communities, they leave private information traces they may not be aware of. The providers of community services need to handle trust and privacy in a manner that meets the participants' needs as well

[1] www.loopt.com, www.junaio.com, www.match2blue.com

as complies with regulation. On the other hand, to finance or co-finance such community services, the infrastructure often needs to be open for marketing activities of sponsors or advertisers [4]. Consequently, a new approach to identity management in community services is needed, in order to meet the stakeholders' different needs for:

- enablement of trust, by members of the community, in other members and in the service-provision infrastructure,
- privacy of community members' personal information,
- control by members of the information they share, and
- interoperability of community-supporting services between communication service providers.

The project PICOS[2] has the goal to develop such a new approach to identity management, for enhancing the trust, privacy and identity management aspects of community services and applications on the Internet and in mobile communication networks. The PICOS approach addresses the following four questions:

1. What are the trust, privacy and identity issues in new context-rich mobile communication services, especially community-supporting services?
2. How can information flows and privacy requirements be balanced in complex distributed service architectures (e.g., mash-ups)?
3. How can these issues be solved in an acceptable, trustworthy, open, scalable, manner?
4. Which supporting services and infrastructures do the stakeholders need?

In a first step to address these questions, our approach foresaw an analysis of related contemporary research and investigated the context of communities (e.g., legal, technical and economic aspects). In a next step, we gathered requirements from exemplary mobile communities in a bottom-up approach and designed a community platform architecture including concepts to address the gathered requirements and enable open, privacy-respecting identity and trust management. The architecture and concepts were prototypically implemented in a community platform and community applications, which are being tested in user trials and evaluated concerning trust, privacy, usability, ergonomics and legal issues.

This paper focuses on the process of gathering requirements (Section 2) and transforming them into adequate concepts and features for communities (Section 3), as well as on the implementation of these concepts as features in the aforementioned community platform and the first community application (Section 4). An analysis of the benefits for users and of related work follows in Section 5, a conclusion and an outlook in Section 6.

2 User-group driven requirements of mobile communities

The process of requirements gathering in PICOS was characterised by a strong user involvement and was conducted along several real-world application scenarios. The

[2] The project PICOS is receiving funding from the European Community's Seventh Framework Programme (FP7/2007-2011) under Grant Agreement n° 215056

resulting community specific requirements were then generalised, as described in the following sections.

2.1 Involvement of users in system development

The involvement of users in the development life-cycle plays an important role for the success of ICT systems [5]. Comprehensive requirements engineering depends on appropriate interactions between end users and requirements analysts to obtain a properly functioning system that reflects users‘ preferences and needs. It is recommended, that end users are involved already at the very early stages of a project in order to acquire and consolidate requirements and domain knowledge as effectively as possible (cf. [6] and [7]). Certainly, continuous interactions with users also in later phases of development processes are needed to validate the realisation of those requirements in an ICT system.

Following this approach, PICOS has a strong focus on users. Besides influencing the set of realised functionality, involving users right from the beginning has a positive effect on their attitude regarding ICT in the long run. Users also have to deal directly as well as indirectly with privacy and trust questions, which may raise their awareness in this domain. This further contributes to empowering users to handle and manage the disclosure of their personal data and the protection of their privacy – not only on a technical level but also with respect to conscious awareness. In addition, it is expected that a system, which is designed considering the advice of PICOS end users, will be accepted by comparable communities.

2.2 Requirements gathering along real-world scenarios

Today’s social communities, differ with respect to their structures, stakeholders, intentions, objectives and mobility. Accordingly, needs for trust, privacy and identity management vary between different categories of communities. For narrowing the scope of PICOS and for concretising the problem space, three exemplary focus communities, i.e., recreational angling communities, independent taxi drivers and online gamer communities have been selected to accompany the development of privacy-enhancing identity management solutions for community services. The selected groups all represent communities which benefit from mobile community services and which share a general need for trust, privacy and identity management. At the same time the groups differ by their characteristics, purposes and goals, and the specific requirements of their stakeholders (cf. [3] for more detailed information).

Recreational anglers, for example, which serve as our first focus community, are organised in various kinds of communities, e.g., angling clubs/associations, or networks of loose friends. The members of these real world communities interact in various ways, e.g., they arrange meetings, prepare angling trips, share information (e.g., pictures) about their last angling trip with friends, or just inform themselves on weather or environmental information when they are angling [8]. Within such community interactions they share more or less private information, wherefore they have an inherent need for privacy and trust.

2.3 An approach towards community generic requirements

Community-specific as well as general requirements with respect to trust, privacy and identity management have been identified by involving stakeholders of exemplary communities into the identification process. During the requirements gathering phase, the project team established close connections to representatives of the three focused communities. They were interviewed individually and in meetings to understand their attitudes and needs regarding trust, privacy, and identity management in the light of next generation community services. The complex feedback given by these community stakeholders has been categorised, explained, and backed by rationales for the stakeholders' vital interest that the requirements they stated become addressed. These community-specific requirements are mainly based upon interviews with community experts and representatives, questionnaires and observations. The requirements address trust, privacy and identity management aspects that are significant in the particular domain.

In a "top-down-bottom-up"-approach in analogy with general approaches for modelling enterprise data ([9], [10]), the PICOS consortium first designed (top-down) a high-level model identifying the core dimensions of requirements relevant for this problem space. Then the analysis of the three exemplary communities led (bottom-up) to domain-specific models of community-specific requirements.

Certainly, the community-specific requirements do not reflect the full set of requirements necessary for successfully designing an architecture suitable for all kind of communities with a mobile background. Accordingly, the community specialists of the PICOS consortium generalised these community specific requirements by merging them. This process was driven by a high-level model and by the project consortium's earlier experiences with other mobile and online communities and the respective observations. Finally, 74 generalised community requirements grouped into the five categories trust, privacy, identity management, platform and services have been identified [3]. This high number reflects the broad spectrum of current online communities that utilise mobile services to support their activities, their different use cases and the parties interacting with them.

It has to be stated clearly that only summarising and elaborating on requirements that could be transferred one by one into technical implementations was not regarded as sufficient for the success of the PICOS project. We argue that including design principles and expectations of end users, community providers and other parties (e.g., advertisers), as additional requirements, is inevitable to implement and deliver suitable solutions. Hence, the set of requirements was extended and put in relation to the high-level model. In addition, business requirements for ensuring that PICOS could easily be included into existing business processes complete the set of non-functional requirements. Using the example of advertising, we analysed which requirements have to be met by a system assuring that a community member stays in control about her data flows and how revenues could be generated while respecting users' privacy. Examples are *determining and negotiating the right set of necessary personal information* and *transparency regarding stored and processed data.* The requirements gathering process is highlighted in Figure 1.

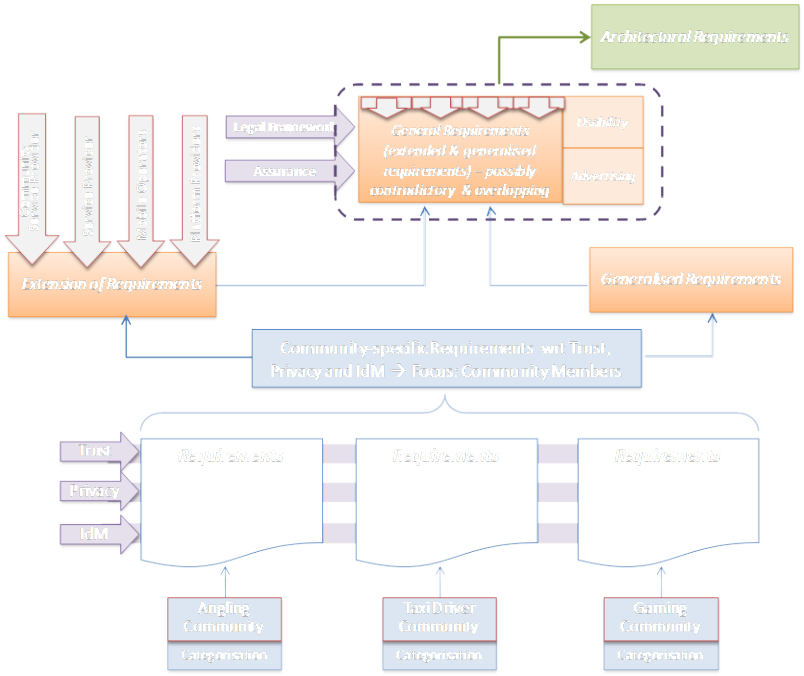

Figure 1: Requirements gathering process.

Finally, the gathered set of extended and generalised requirements was mapped to the community-specific requirements of our three exemplary communities where the specialists of the PICOS consortium together with the community representatives were able to identify that there exists a demand for the formulated requirements [3].

3 PICOS Concepts and Features

Based on the requirements gathered the PICOS community platform architecture was developed: The elaborated concepts and derived technical features and components are described in the following. For illustration a subset of these requirements is listed in Table 1 together with architectural concepts to address these requirements. These concepts can be subsumed under three different categories, which are explained in the following subsections. While the underlying requirements were gathered from communities with a mobile focus (cf. 2.2), the developed concepts may be of use for other communities also.

Table 1. Selected requirements and corresponding concepts (cf. [3]).

Requirement	Name	Addressed by
(R1.1)	Personal Trust	Partial Identities
(R2.1)	Data Minimisation	Privacy Advisor

(R2.3)	Confidentiality	Sub-Communities, Private Room
(R2.7)	Definition of Privacy Settings	Location Blurring, Policies
(R2.8)	Visibility and Reachability of Users	Location Blurring, Policies
(R2.9)	Default and Advanced Privacy Management	Policies
(R2.10)	Unlinkability	Partial Identities
(R2.11)	Fine-grained Disclosure and Sharing of Data and Information	Sub-Communities, Location Blurring, Policies, Private Room
(R2.12)	Control over Data and Information Flows	Policies
(R3.4)	Partial Identities	Partial Identities
(R3.5)	Subsequent Release of Identity Attributes	Partial Identities, Policies
(R4.4)	Policy Definition and Enforcement	Policies

3.1 Enhanced Identity Management

To enhance the identity management in mobile communities and thereby address especially the requirements with regard to the disclosure of personal information and its accessibility for other users, a number of concepts were developed or further elaborated. Based on the concept of mobile identity management [11], such concepts can support users in managing the disclosure of their current position and mobile identity in communities. Sub-communities and Partial Identities are two concepts to help users in selectively sharing personal information with others.

Sub-Communities
By founding a *Sub-Community*, users can create a restricted area, which allows the sharing of personal information among a limited group of community members. Sub-communities can be *public* or *private*. In the latter case the founder is able to decide who is allowed to be a member of that group by selecting individual members or by filtering on a set of personal profile characteristics of other members (R2.11). Information published in that Sub-Community is only accessible by its members (R2.3). Users within such a private Sub-Community can trust that published information is only accessible by other authorised members of this Sub-Community. Therefore, a user who wants to share information or resources does not need to approve access of each single user.

Partial Identities
Identity management in PICOS was designed with the goal to enable users to manage their identity-related information in a convenient way. The concept of *Partial Identities* [12] in particular allows users to create different identities for the usage in different usage contexts and different purposes. With the help of Partial Identities users are enabled to have a set of several identities in one community to decide for each identity which of their personal information they want to disclose. Each Partial Identity of a user appears to other users as a unique, individual community member. To address requirement R2.10 the relation between the different Partial Identities is only visible for the user itself and the community operator. For instance, if a user participates in different sub-communities, Partial Identities support him in hiding and revealing relations between different elements of his personal information.

Regarding the angling community example, a young unskilled angler could use one Partial Identity to be present in a Sub-Community for beginners in fly-fishing. At the same time he might express his interest in classic angling in a related Sub-Community with a 2nd Partial Identity, without the need to admit his beginners' status. The Partial Identity manager allows users to create and administer Partial Identities and to set profile information for each of them (R3.5). Considering requirement R1.1 users are not allowed to have a different gender or age in their Partial Identities. An always visible pull-down menu supports switching between Partial Identities and chosing the most appropriate one for the respective situation.

3.2 User controlled Information Flows

As the user requirements show, a balance needs to be achieved between publishing personal information in order to use functionalities of the community and keeping a certain degree of privacy. The following PICOS concepts support users in keeping their privacy while being able to use the community according to their needs.

Location Blurring
In mobile environments, especially location information is of interest, e.g., for location based services (LBS). Such services are also of interest for mobile communities, to display friends on a map or to share information about interesting spots in close vicinity. However, usually there is only the option to either show or hide completely one's own position, e.g., in the initially mentioned examples such as Loopt. The PICOS concept of *Location Blurring* is a concept which gives users the additional opportunity to hide their exact position without being completely invisible to others. It foresees the obfuscation of a user's current position or a point of interest at various levels (R2.7, R2.11). The position is displayed as a circle of a defined radius (e.g., 1, 2 or 5 km) within which users are located. Moreover, the concept allows users to specify, which other users are able to see their exact position and their blurred position (R2.8). Making use of the policies concept described below users can also differentiate their blurring configurations considering which other users get the localisation information. In the case of the PICOS angling community a user can hide the position where he is angling currently and also the exact location of a fishing spot, when this is added into a database of fishing spots on the PICOS platform.

Policies
The PICOS community prototype enables users to selectively define *Policies* in order to control who is allowed to see certain personal information (R2.7, R2.12, R4.4). These user-centred policies are based on rules, which also take context information into consideration (e.g. the current location of the user). Based on these rules a user can determine which information is available to other users in a defined situation. This can be done individually for each Partial Identity (R2.9, R3.5). It is possible to define policies for a user's presence, his location, and for selected profile information (R2.8). Thus, the PICOS policy editor enables users to manage their privacy in a very fine-grained manner (R2.11).

Private Room
Private Rooms enable users to establish a personal area for managing their private information and content. They enhance users' privacy by enabling them to store and selectively publish their private information to a certain set of other users (R2.3). Users can publish their selected private information to another user, respectively a known Partial Identity, or to a group of users in a private Sub-Community (R2.11).
In the scenario of the angling community users can manage pictures and catch diary entries in their individual private room by adding information, pictures etc. Finally, they can publish their diary entry by transferring it to a private Sub-Community, a public Sub-Community or the public community (Figure 2). Additionally, users are able to decide which of their Partial Identities will be shown as the author of their catch diary entries.

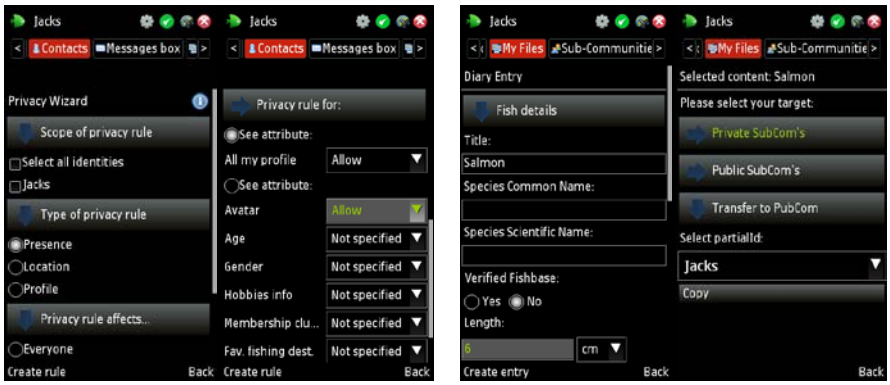

Figure 2: Screenshots of Privacy Policies (left) and Private Room (right)

3.3 Privacy Awareness Support

Managing privacy by means of Partial Identities on a mobile device might be too demanding for some users. Therefore, the concept of the *Privacy Advisor* was developed to provide guidance to users, e.g., regarding disclosure or sharing of location information. The Privacy Advisor is context sensitive and provides hints in specific situations when personal information of users is involved, e.g., registration or profile editing. It aims to warn a user in cases where the disclosure of information might be associated with risks for the user's privacy (R2.1). Thereby the Privacy Advisor will help to create awareness of privacy related aspects within mobile communities and in specific usage situations, based on the user´s actual behaviour and context.

4 Implementation into existing community platform

The PICOS architecture, including the previously explicated concepts, can be divided into two main parts, namely the *PICOS Community Platform* and the *PICOS*

Community Application (Figure 3). Both were prototypically implemented with a subset of the concepts and features the architecture contains, in order to evaluate the concepts and to demonstrate their benefits by means of our communities. In particular, we aimed to answer the question how far the concepts (Section 3) are able to address the gathered community requirements (Section 2).

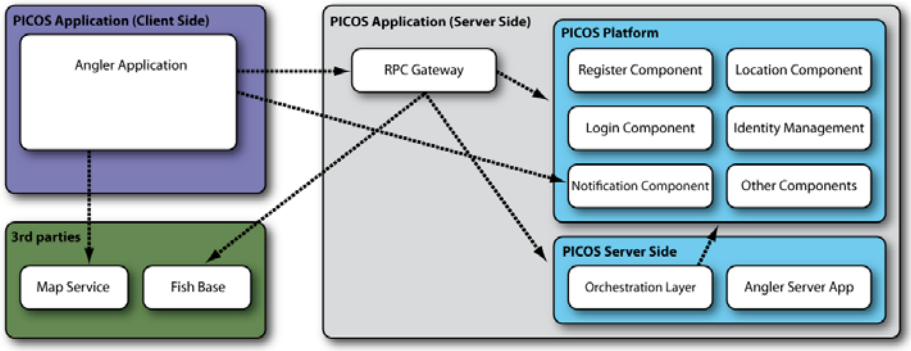

Figure 3: PICOS Implementation - Platform and Community Application

The platform is responsible for all community agnostic services, which are common for many communities, based on generalised requirements. The platform consists of a variety of components, each component with a dedicated set of features which address certain requirements directly or indirectly. For example, a *Register* component dealing with the registration process of new users, a *Login* component dealing with the session management, and a *Partial Identity Management* component.

In order to avoid the re-development of basic community functionalities from scratch the platform is partially based on the OpenCall platform[3], which provides functionalities for mobile community related communication services (e.g., chat/messaging, friend lists) and also uses elements of the open source framework ELGG[4].

The Community Application (Angler Application) is composed of a client side and a server side. The client side uses a Symbian platform[5] mobile phone and the J2ME (Java 2 Mobile Edition) environment with an installed PICOS Angler Application. It is structured in different layers as shown in Figure 3. Its design follows the model-view-controller pattern, which separates the graphical user interface from the underlying business logic and data. The server side is composed of platform components, the Community Application server side and the RPC gateway, which acts as a proxy to provide a unified access to the PICOS server side.

The PICOS implementation interfaces with 3rd party components in two different ways: The client application accesses the Fishbase database[6] via the RPC Gateway to retrieve fish species related data, whereby Fishbase is integrated into the Community Application. The client side communicates with the server side and also with a 3rd

[3] http://h20208.www2.hp.com/opencall/platforms/index.jsp
[4] http://elgg.org/
[5] www.symbian.org
[6] www.fishbase.org/home.htm

party map service, in order to realise map and location features and demonstrate related PICOS features (e.g., Location Blurring). This also underlines the openness of the platform for the integration of external services.

5 Benefits and Related Work

To be able to assess the relation to related work laid out in Subsection 5.2, first an analysis of the benefits of the PICOS work for end users is given in Subsection 5.1.

5.1 Benefits for PICOS users

With mobile communities, the work of PICOS addresses an almost unexplored domain in particular with regard to privacy, trust and identity management aspects. The PICOS concepts outlined aim to provide a significant improvement with regard to privacy, trust and identity management aspects. The PICOS users will benefit in particular from:

1. Continuous user involvement and the consideration of user requirements throughout the whole research process,
2. Innovative concepts, for improving users' privacy and providing them with new identity management tools,
3. Improvement of awareness in the public for the challenge of privacy respecting community services,
4. Aimed integration into an existing community in order to transfer the concepts to practice, and
5. Integration into an existing mobile community and communication platform.

The integrative approach, right from the start of the project is an essential and strong feature of PICOS. The PICOS platform incorporates community knowledge and delivers a technical system that can be used by network operators and application providers for application integration. Thus, it serves as a reference implementation of a state-of-the-art community supporting identity management system.

5.2 Related Work

Although there is research in the domain of communities with regard to privacy, trust and identity management, there is little, significant work that addresses the four main questions for PICOS, as listed in the introduction. By answering those four main questions, PICOS advances state-of-the-art concepts and technology in the field of trust, privacy and identity management.

In some of the areas work has already been done by projects such as PRIME[7], PrimeLife[8], PEPERS[9] and DAIDALOS[10]. The work within PRIME was focused on

[7] www.prime-project.eu
[8] www.primelife.eu
[9] www.pepers.org
[10] www.ist-daidalos.org

privacy-respecting identity management, and part of this includes the enablement and management of trust, but it did not focus on (mobile) communities. PrimeLife is working on communities, but not with regard to really established communities and specific application domains. The objective of PEPERS was to research a mobile peer-to-peer security infrastructure with the focus on decentralised trust and identity management. In contrast to PICOS, PEPERS considers individual stakeholders (e.g., journalists) and centrally managed employees, their needs (e.g., for identity management capabilities, privacy, trust, etc.) and how to balance the tensions between them. DAIDALOS concentrates on ubiquitous services provided to mobile users in a secure and privacy-friendly manner but its focus lies on the single user and not on communities and their special needs and requirements.

Besides the named research projects, the aspect of privacy in online communities is discussed intensively in the research area (cf. [13], [14], [15]), but with the focus on online communities usually not considering the special aspects of mobile communities.

6 Conclusion and Outlook

This paper outlined why there is an increasing need for privacy and identity management related enhancements in mobile communities and motivated why research is necessary in this application area. We then described how we intend to achieve such enhancements and explained how user requirements were gathered. Some of the innovative concepts, which we developed, based on such requirements, have been introduced. Finally, we described how such concepts were prototypically implemented and how the integration with an existing community platform was realised.

Each implementation of the PICOS community application prototypes is undergoing a trial with end-users of the exemplary communities. The 2nd cycle of PICOS benefits from the results of the first trials and the evaluation with anglers [17]. They will be used to improve the angler community application as well as to transfer the results to another type of community, an online gaming community.

Online games represent large communities in which players interact and collaborate. Mobile communication allows them to stay in touch with their community from wherever they are and consequently on a more continuous basis. This also allows new opportunities, e.g. for advertisers and raises new challenges with regard to privacy and trust. As a part of PICOS' second cycle especially the aspects of defining and managing policies, the Privacy Advisor and the economic potential of privacy in mobile communities will be further investigated. By this, existing privacy and identity management concepts will be enhanced and additional concepts based on the requirements of online gamers will be introduced.

Finally, we will investigate how far the results from both cycles can be generalised for further (mobile) communities. The continuous involvement of users and especially the close contact to the focused communities provide a close feedback loop to check whether the requirements have been met. The integration of industrial partners, e.g., the developers of community platforms, raises the chances, that the elaborated

concepts are finding their way into the market and to existing communities providing a sustainable benefit for the involved stakeholders.

Acknowledgments. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2011) under Grant Agreement n° 215056. The authors would like to thank in particular André Deuker for editorial remarks.

References

1. Nielsen: Critical Mass - Worldwide State of the Mobile Web. Nielsen Mobile. (2008).
2. Nielsen: Global Faces and Networked Places - A Nielsen report on Social Networking's New Global Footprint. Nielsen. (2009).
3. Liesebach, K., Scherner, T.: D2.4 Requirements. Public Deliverable of EU Project PICOS. Available at www.picos-project.eu/Public-Deliverables.29.0.html (2008).
4. Hoegg, R. et al. Overview of business models for Web 2.0 communities. In: Proceedings of Workshop 'Gemeinschaften in Neuen Medien', TUDPress, Dresden, 33 - 49 (2006).
5. Clavedetscher, C.: Point: User Involvement Key to Success. In: IEEE Software, 15(2), pp. 30, 32 (1998).
6. Rumbaugh, J.: Getting Started: Using Use Cases To Capture Requirements, Object-Oriented Programming Journal, 7(5), 8 - 12 (1994).
7. Holzblatt, K., Beyer, K.R.: Requirements gathering: the human factor. In: Communications of the ACM, 38(5), 31 - 32 (1995).
8. Arlinghaus, R, Mehner, T, Cowx, IG: Reconciling traditional inland fisheries management and sustainability in industrialized countries, with emphasis on Europe. Fish and Fisheries 3(4), 261 - 316 (2002).
9. Pin/Shan Chen, P.: The Entity Relationship Model, Toward a unified View of Data. In: ACM Transactions on Database Systems. 1 (1), 9 - 36 (1976).
10. Vernadat, F.B.: Enterprise Modeling Languages. IN: Proceedings of International Conference on Enterprise Integration Modeling Technology. Torino, Italy (1997).
11. Müller, G., Wohlgemuth, S.: Study on Mobile Identity Management, Public Deliverable of EU Project FIDIS. Available at www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.3.study_on_mobile_identity_management.pdf (2005).
12. Hansen, M., Berlich, P., Camenisch J., Clauß, S., Pfitzmann, A., Waidner, M.: Privacy-Enhancing Identity Management. Information Security Technical Report; 9(1) 35 - 44 (2004).
13. Chew, M., Balfanz, D., Laurie, B.: Undermining Privacy in Social Networks. In: Web 2.0 Security and Privacy (in conj. with IEEE Symposium on Security and Privacy) (2008).
14. Adu-Oppong, F., Gardiner, C. K.., Kapadia, A., Tsang, P. P.: Social Circles: Tackling Privacy in Social Networks, In: Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08). Pittsburgh, Pennsylvania, July 23–25 (2008).
15. Hiltz, S. R., Passerini, K.: Trust and Privacy Concern Within Social Networking Sites: A comparison of Facebook and MySpace. In: Proceedings of AMCIS 2007 (2007).
16. Boyd, D. M., Ellison, N. B.: Social Network Sites – Definition, History and Scholarship. In: Journal of Computer-Mediated Communication, 13 (2008).
17. Ganglbauer, E., Döbelt, S., Ueberschär, B.: D7.2a First Community Prototype: Lab and Field Test Report. Public Deliverable of EU Project PICOS. Available at www.picos-project.eu/Public-Deliverables.29.0.html (2010).