Towards Usable Interfaces for Proof Based Access Rights on Mobile Devices

Marcel Heupel, Dogan Kesdogan

Towards usable interfaces for proof based access rights on mobile devices

Marcel Heupel and Dogan Kesdogan
University of Siegen, Germany
Chair for IT Security Management

[1] heupel@wiwi.uni-siegen.de
[2] kesdogan@uni-siegen.de

Abstract. Access rights management is in the middle of many collaboration forms such as group formation or sharing of information in different kinds of scenarios. There are some strong mechanisms to achieve this, like anonymous credential systems. However in general their usage is not very intuitive for lay users. In this paper we show the potential of using proof-based credential systems like Idemix to enhance the usability of privacy-respecting social interaction in different collaborative settings. For instance transparently performing authorization without any user intervention at the level of the user interface becomes possible. In order to improve the usability, we complement this by introducing a mental model for intuitive management of digital identities. The approach should also empower users to define their own access restrictions when sharing data, by building custom proof specifications on the fly. We show this exemplary with a developed prototype application for supporting collaborative scenarios on a mobile device. We also present first evaluation results of an early prototype and address current as well as future work.

1 Introduction

For quite some time, a major trend in our information society is the increasing use and disclosure of personal information in private and in business life. The recent massive propagation of mobile devices and mobile applications gains strength from leveraging efficient, secure and privacy-respecting interaction as well as communication patterns between individuals and communities that are seamlessly supported with mobile devices in term of enjoyable user experience [4].

On the one hand security and privacy are one of the most-cited criticism for pervasive and ubiquitous computing [15]. On the other hand usability is a prerequisite for security and privacy. Therefore, it is part of a major effort to balance and improve security and privacy design of mobile applications by considering usability aspects especially due to the limitations and capabilities of mobile devices (e.g. screen size, limited memory, computation capabilities and ease of localization). One of the most disregarded and critical topics of computer security has been and still is, the understanding of the interplay between

usability and security [9]. In social and collaborative interaction settings, advantages such as enhancing social contacts, personalizing services and products compromise with notable security and privacy risks arising from the user's loss of control over their personal data and digital footprints [10]. From the usability perspective, large amounts of scattered personal data lead to information overload, disorientation and loss of efficiency. This often results in not using security options offered by the application.

One of the means for enhancing privacy in communication to individuals and services is to allow for the usage of partial identities or digital faces, i.e. user data selected to be disclosed for a particular purpose and context. Privacy-enhancing technical systems and applications supporting collaborative users activities have to allow for user-controlled identity management (IdM). Furthermore, such an IdM system has to be deployable on mobile platforms by providing good performance in terms of response time as a quality of service factor for usability [20] and also as part of the security protection goal availability [5]. Poor response times lead to end-user frustration and negatively affect the usage of the applications especially when no adequate help or feedback is provided. With respect to the different capabilities and restrictions of modern mobile devices (e.g. smartphones and tablet PCs), addressing security and usability aspects becomes crucial. Experts from various research communities believe that there are inherent trade-offs between security and usability to be considered [6,9,21]. These general requirements are based on the objectives of the EU FP7 project di.me [10].

One of the most powerful and future promising IdM systems is IBM's "Identity Mixer" (Idemix) [7], which is also able to run on smart cards [2]. Due to the strong cryptographic algorithms, proving of powerful and complex statements (like e.g. inequality of attributes) needs quite some computation time [8,23] and thereby influences the performance of the whole application. This is especially true if only devices with relatively weak computation power, like mobile phones, are used. However, since the newest generation of smartphones and tablets come with really strong processors a new evaluation of the capability of those devices seems reasonable.

In a user controlled IdM the user needs to have the capability to define the access rights by himself. Therefore a good and usable interface is essential. Lab tests with some early prototypes showed, that many users had problems with defining complex proof based access rights. Therefore we aim to implement and evaluate a mental model for the representation of partial identities in the user interface (UI), which is strong oriented on real world observation, where the identity of the user stays the same and only the view of participating third parties can vary.

In this paper, we present our current work to enhance the usability of end-user controlled access rights management in privacy-respecting mobile collaborative settings.

The reminder of this paper is organized as follows. An overview on the state-of-the-art is given in Section 2. In section 3 we present the derived requirements primarily based on Di.Me. Next, section 4 presents our approach. Finally, we

conclude with a presentation and discussion of our evaluation results in Section 5 and present our conclusions and outline ongoing and future work in Section 6.

2 State of the art

Access control means in general controlling access to resources, which are e.g. made available through applications. It entails making a decision on whether a user is allowed to access a given resource or not. This is mostly done by many techniques like comparing the resources access attributes with the users granted authorities. For access control, the authentication of the *who* is the process of verifying a principals [3] identity whereas the authorization is the process of granting authorities to an authenticated user so that this user is allowed to access particular resources. Therefore, the authorization process is mostly be performed after the authentication process. Often, IdMs are responsible for authentication. There is a lot of work about Idm an access control in the literature. A good overview of the field of user centric identity management is given by Jøsang and Pope [16] and also by El Maliki and Seigneur [12].

With respect to the different capabilities and restrictions of modern mobile devices (e.g. smart-phones and tablet PCs), addressing authentication, authorization and usability aspects becomes crucial. Often, the complexity of authentication and authorization is reflected in UI which is critical for mobile applications deployed on mobile devices with limitations in the screen space. A contribution from the usability field to enhance authentication is e.g. the usage of graphical passwords. An example is the usage of pass-faces for graphical authentication in Android smart-phones to unlock the main screen. However also those approaches have been proven to be not secure enough e.g. due to the smudge traces that can emerge on the screen surface. A recent publication showed that is really easy to guess the right pattern and break such authentication system [1]. Biometrics also allows for enhancing authentication but are still "classified as unreliable because human beings are, by their very nature, variable" [9,17]. Related to authorization, most systems need the interaction of the end-users at least in form of confirmations. The challenges increase if (lay) users are asked to set access rights for others, delegate rights, or manage their own security and privacy preferences. In the context of this work, the EU Project PICOS (Privacy and Identity Management for Community Services) represents a good and current example. The *2010 First Community Prototype Lab and Field Test Report D7.2a* [19] cites that users had problems to use the PICOS privacy manager on mobile devices (Nokia MusicExpress 5800). Notifications and (automatic) advisory might lead to actions which the user finds intrusive or annoying in some cases (such as in the well-known case of Windows pop-ups or MSWord's paper-clip). Especially in collaborative applications as socio-technical systems, this will affect the psychological acceptance of the application which leads to not using security and privacy mechanisms. This mostly results in expensive change requirements affecting the technical realization of mobile applications [9, 18]. Indeed, people involvement

[3] A principal can be a user, a device, or a system, but most typically it means a user.

varies and the usage can range from occasional to frequent according to a given setting and circumstances.

For both, authentication and authorization, cryptography is an established used mechanism for increasing confidentiality and integrity of exchanged data. However, a total security or privacy provision is an illusion [15] because current approaches are not able to avoid at least threats and attacks e.g. emerging from loosing devices or based on physical access to them [11]. Approaches mostly only focus on hindering such attacks or making them difficult.Trade-os between security and other (non-)functional requirements such as usability and cognitive mental models supporting interaction design are well-described in tremendous lot of classical literature in the corresponding research communities, e.g. Computer-Supported Collaborative Work (CSCW), Human-Computer Interaction (HCI), psychological, and sociological sciences etc. Nevertheless, the current state of the art leaves room for considerable improvement how such systems can support an usable and secure user experience. Security and usability research for developing usable (psychologically acceptable) security mechanisms and mental models is a young research field which depends on the context in which those mechanisms have to be used [9]. Researchers especially from the CSCW and HCI research fields generally agree on that security and privacy issues arise due to the way systems are designed, implemented, and deployed for a specific usage scenario [6, 9, 21]. Because of this and many facts cited above, we argue that security and privacy design by considering usability is specific to the project context. Thus we analyze user-controlled access rights management related requirements in this paper based on concrete Di.Me requirements by considering security and usability along with performance in our initial design and architecture. Furthermore, many related work is focusing on improving collaborative interaction related to access rights in general. For instance, the recently opened social networking platform Google plus [13] proposed a similar approach in some points. They also emphasized to focus on real world behaviors and introduced an promising approach with their circles concept, which is oriented on the real world circle of friends. However, the room for improvements still needs further work as we intend to reach with the work presented in this paper.

3 Requirements

Our approach is based on the usage of the proof-based anonymous credential system Idemix. The gathered requirements related to usability result from using Idemix for our first prototype of a mobile application for Android devices to support complex mobile collaborative scenarios. Further requirements were derived from the scenario are based on our work at the EU FP7 project digital.me. In contrast to related work, we used the latest reference implementation of the Idemix specification released on June 2011 and provided first performance evaluation for non-atomic Idemix operations.

3.1 Requirements derived from the scenario

In our scenario, Alice is attending on a business conference. Therefore she activates her business profile on her mobile device, selects some of the attributes she likes to reveal (like her last name, or her occupation) and broadcasts them. Other conference participants can now find her by browsing broadcasted contact information and can send her a contact request. Alice also adds some additional information about selected ongoing projects. This information can only be obtained by invitees, who are also sharing their profile and are working as engineer in the automotive sector. In our use case, Bob, another participant of the conference, is browsing the profile information. When he comes across Alices' profile, he likes to read the additional project papers. By requesting the information, Bobs device receives a challenge, stating that he has to prove that he fulfills certain conditions (e.g. that he is working as an engineer in the automotive sector). This is automatically carried out by the devices in the background. After Alice is convinced that Bob is actually working as an engineer and grants him access to the requested documents. The whole protocol is automatically carried out by the devices in the background without disturbing Alice. She can review at a later time, who requested her documents. If she likes, she could activate a notification about requests for her information and also manually grant or prohibit access. Figure 2 illustrates the main scenario as an interaction diagram.

Publishing data with individual access rights: The attendees of the conference should be enabled to create and publish individual profiles and publish them on the conference platform. Other attendees can log in to the conference server and browse the list of profiles. Because there are different kinds of profile attributes, like e.g. affiliation, interests, real name, and the users probably do not want to publish all of them to everyone. The users might want to publish selected attributes, like for example project papers or the real name only to selected individuals. This finer access rights are even more important for dynamic attributes like location, current activity or reachability.

Creation of partial identities In order to publish different sets of information, maybe by also using different pseudonyms, we have the need for multiple partial identities. Together with the definition of fine grained access rights, this also gives the possibility to define multiple values for profile attributes. This would be very useful concerning the availability or reachability, because when in a meeting, the user might still want to be available for members of his family in case of emergency, while being not available for everyone else.

From the described scenario we could derive the following important requirements:

R1 The user can use partial identities
R2 The user can browse data published by others
R3 Fine grained access rights for published data can be defined
R4 Capability to prove attribute values (Idemix + Certificate Authority (CA))

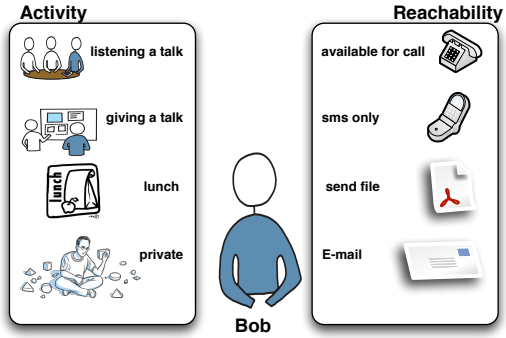

Fig. 1. Reachability management

3.2 Non-functional requirements

Based on our experiences from the early evaluation of our first prototype and derived from requirements from the di.me project we defined several major non-functional requirements which will be explained in the following.

Minimization of user interaction: The main goal is to balance and also improve the security and privacy in our scenario with the usability of the prototype. Therefor an important step, especially on mobile devices with limited screen size and interaction capabilities, is the minimization of user interaction in general. Besides this main non-functional requirement, we have further functional requirements derived from the scenario described above.

New concept for partial identities: A central point of our approach should be to make the UI as intuitive as possible. Therefore we are trying to implement a new mental model for (partial) digital identities, which is strongly oriented on the real world observations. The point we are addressing in our approach is the fact, that it is not intuitive for human beings, to have multiple identities as it is common practice in the digital world. Most people definitely act different when they are interacting with different people, but this happens almost unconscious. People will not actively switch identities like embodying a different person, they will stay the same person. What we try to implement in our approach, is a new concept, where we have no names or avatars for digital faces, profiles, identities etc. in the UI. Instead the different partial identities of the user will be represented as a picture of the contacts this identity is used for. The identity of the user stays the same, only the view of others can vary. The mental model for the UI will visually represent the faces with pictures of the people this face is used to interact with.

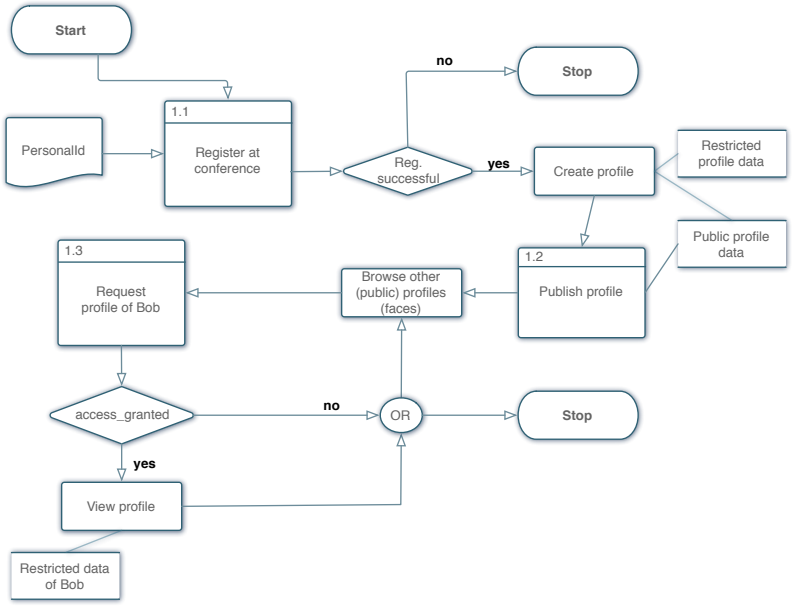

Fig. 2. Interaction flow of the scenario

Context sensitivity An important added value due to the use of modern smart-phones, is the availability of additional sensor data. This opens new possibilities for access and reachability management. The system can e.g. automatically mute the phone when attending a talk, or give access to information depending on the proximity to the requesting person.

NFR1 Minimization of user interaction
NFR2 Intuitive representation of partial identities
NFR3 Context sensitive access rights

4 Approach

To verify our prototype and evaluate the UI concepts in a running application we extended the Android-based prototype used in previous lab trials as well as the shared (collaborative) conference server. We provided various user interfaces (UIs) for creating digital faces and credentials as well as their attributes, formulating proofs, selecting attributes to be disclosed in a given context and certifying them with the help of an Idemix CA. Figure 7 illustrates the implemented architecture. Since the first prototype used XML-RPC, the mobile client application is now able to perform the main protocols of Idemix (e.g. *Get Credential* or *Show Proof*) also via XMPP. This Section should give a short overview about the implementation details and also present the developed interfaces.

4.1 Implementation of the scenario (R2, R4)

We provided various user interfaces (UIs) for creating digital faces and credentials as well as their attributes, formulating proofs, selecting attributes to be disclosed in a given context and certifying them with the help of an Idemix CA. In contrary to our first prototype, which purpose was more to test the feasibility and performance of Idemix on a modern smartphone [14], we did not integrate an additional Tor client in our approach. This significantly increased the overall response times and is only a small trade-off concerning privacy. Since we are using a XMPP server for communication, the IP addresses are not that easily traceable and moreover our scenario takes place in a more or less closed environment, the conference. Most people will be in the same network anyway. However, if users still like to hide their IPs to the XMPP server, they can still easily install a separate Tor client like Orbot [22] on their smartphone and obfuscate the network traffic. In order to publish data we build a server, where people can upload their profiles and also request a list of profiles previously published by other users.

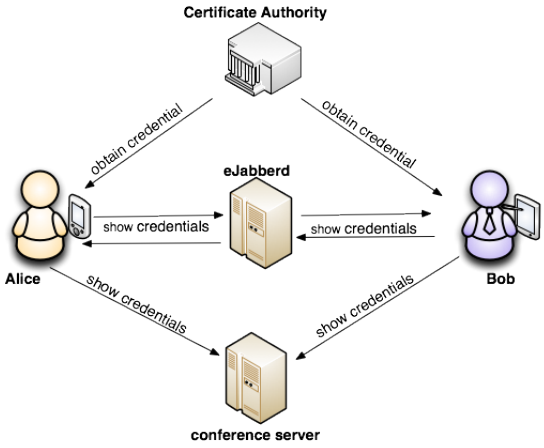

Fig. 3. Architecture of the implemented scenario

Automated proof generation in the background (NFR1) Besides the possibility to create customized proof statements, our approach also supports automatic proof generation in the background, without the need for user interaction. Like stated in the scenario, users have the option to publish information or documents with custom restrictions. When a user is trying to access that restricted data, a challenge is sent by the data provider to the user, that certain predicates need to be proven in order to gain access to the data. For instance the user can be asked to prove that he is working in the automotive industry. If

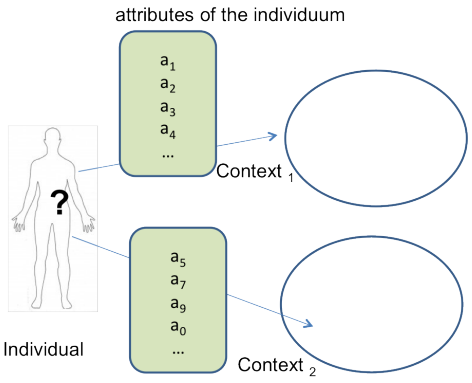

Fig. 4. Identity management becomes context management

the necessary credential is available, a proof containing the required predicate, is computed automatically in the background and sent back to data provider.

4.2 The Interface (NFR1)

In order to ease the interaction by on the one hand make it very intuitive and on the other hand minimize the entering of data. Once the user has registered for the conference and received the initial credential from the conference CA, an initial root profile is created automatically. Profiles are called *digital faces* or just *faces* in our context. The default digital face contains the attributes that have been certified in the registration process. If the user wished to create a new digital face, he/she can use this default face as a starting point and add or remove attributes.

4.3 Context dependent identity management (R1, NFR2, NFR3)

During the creation of a digital face it is possible to define the *context variables*, when this face is to be used. The context is defined mainly by the people the user is interacting with, but can be further extended by also taking the current activity or location into account. As an example, if Alice creates a face with her name, affiliation, and current activity and decides to use this in the context of *work*, she would set that this face is automatically used when interacting with persons from the group *colleagues*. Now she could also define exceptions, in which another face (e.g. *private*) is used, for example by setting an individual rule for her colleague Bob, or by making it also dependent on her current location (e.g. only show her phone number while in the office). Figure 4 shows an abstract illustration of the concept. for each different context, a different subset of all attributes is disclosed.

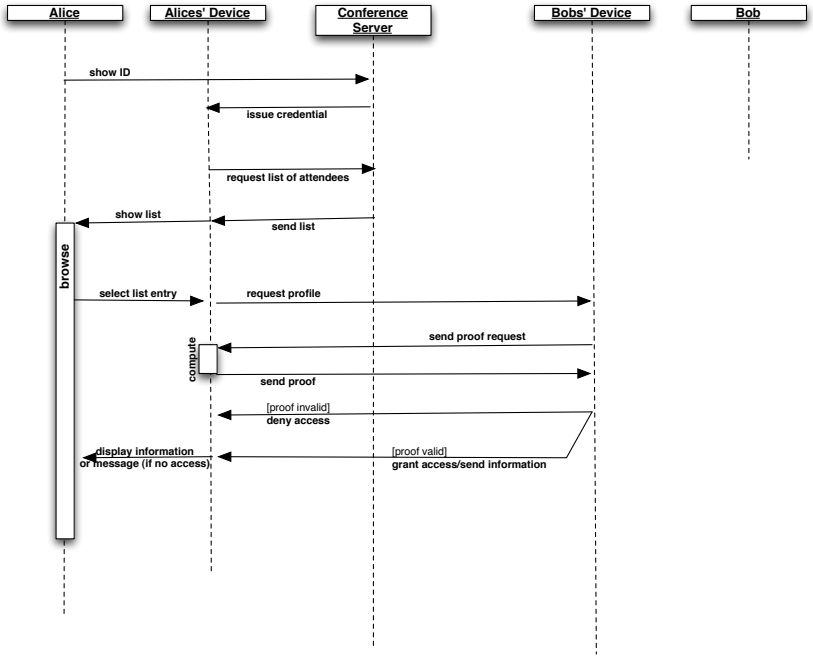

Fig. 5. Sequence diagram for accessing restricted information

Definition of fine-grained acces rights with intuitive user interfaces (R3) We build a UI that eases the complex process of proof generation with Idemix, even for lay users. In addition to the context dependent disclosure of digital faces, the user can define individual conditions that another person has to fulfill in order to access selected information of files. To to this, the user just clicks on the attribute of interest and a dialog will show up, where a statement like *affiliation* = *xyz*, or *age* >*30* can be defined with a few clicks, similar to the a building block concept.

5 Experiences and Discussion

According to our first experiences based on empirical evaluations of our prototype, end-users are able to use our approach. In the following, we describe how we carried out first lab testes and observed the users by the usage of our prototype.

To organize the development and evaluation process of the prototype, we followed the AFFINE methodology [3], which is an agile framework to enforce the consideration of non-functional requirements like e.g. usability and security. The lab tests were carried out periodically considering the provided feedback in each test iteration. For this, we followed as mentioned before an agile framework for

(a) List of digital faces (b) Managing groups of contacts (c) Select a person

Fig. 6. Selected GUI masks of the prototype

integrating non-functional requirements earlier in the development process while considering end-users' as well as developers needs. Since the adopted AFFINE framework described in [3] is Scrum based, we provided continuously running prototypes granting so fast feedback loops. We split up the evaluation of the new user interface in two phases. In the first phase, we have conducted functional unit tests. For this, we extended the provided unit tests in the original Java Idemix implementation to check new functionalities related to R4. These functional tests concentrated on validating the intended interaction possibilities.

In the second phase, we evaluated the developed UIs of our system in different lab tests carrying out different tasks within the implemented "Conference Scenario". Different members from various departments in our university were invited to use the prototype in a simulated conference situation. The persons who contributed in our lab tests had different background in using collaborative systems and social software and had no knowledge about proof-based credential systems. Thus we provided an introduction to the essentials of Idemix from the usage perspective as we described it above in the corresponding Section. We observed that the positive resonance with respect to Idemix functionality generated some kind of curiosity which motivated the testers. Latter was very interested in knowing how they can generate attributes especially those one with vague assessments (e.g. "I m older than 18" etc.). However, this was a first indicator that the performance of the developed system has to fit the worst cases of a real usage scenario. The main issue thereby is that Idemix bases in its computation on data represented in the XML format which is expensive in terms of resources especially on mobile devices.

End-users enjoyed the transparent access rights management that was carried out in the background in general. However, many users wished to be able to view

the access protocol and asked for new UIs in order to view detailed logs at a later time. Protocoling access at the level of the mobile device will surely represent a new performance challenge over the time.

The visualization of the digital faces by representatives of the persons that face is shown found good acceptance in the group of testers. However, some questions arose about how to decide which of the persons in a group should be the representative, or if a merged picture would be better. Some users also brought up the suggestion, to also include symbolic graphics chosen by the user, which can also be associated to a specific context. This could be especially useful when no pictures are available of the person or the group.

6 Conclusion and future work

With our approach we presented a way to represent a very strong and complex concept for fine grained access control to personal information with the anonymous credential system Idemix and an unconventional mental model for the representation of partial identities supported by context-dependent identity management. With the extended prototype we were able to perform first usability and performance tests which gave us promising results. We built and evaluated various prototypes for checking the feasibility of our approach. First evaluations showed this feasibility and beyond good initial acceptance we got valuable feedback for future improvements. Currently we are fine-tuning the prototype as a preparation for widespread user tests in order to get valuable data about user acceptance and behavior pattern when dealing with partial identities. It will be also targeted to look deeper into the behavior patterns of users dealing with partial identities and to evaluate them.

References

1. A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. 2010.
2. P. Bichsel, J. Camenisch, T. Gross, and V. Shoup. Anonymous credentials on a standard java card. In *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 600–610, New York, NY, USA, 2009. ACM.
3. M. Bourimi, T. Barth, J. M. Haake, B. Ueberschär, and D. Kesdogan. Affine for enforcing earlier consideration of nfrs and human factors when building socio-technical systems following agile methodologies. In *Proceedings of the 3rd Human-Centered Software Engineering Conference*, Reykjavik, Iceland, 2010.
4. M. Bourimi, J. M. Haake, M. Heupel, B. Ueberschär, T. Barth, and D. Kesdogan. Enhancing privacy in mobile collaborative applications by enabling end-user tailoring of the distributed architecture. *International Journal for Infonomics (IJI)*, 3(4):563–572, December 2011.
5. M. Bourimi, J. Ossowski, Abou-Tair, S. Berlik, and D. Abu-Saymeh. Towards Usable Client-Centric Privacy Advisory for Mobile Collaborative Applications Based on BDDs. pages 1–6, Feb. 2011.

6. M. Boyle, C. Neustaedter, and S. Greenberg. Privacy factors in video-based media spaces. In S. Harrision, editor, *n Media Space: 20+ Years of Mediated Life*, pages 99–124. Springer, 2008.
7. J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation, 2001.
8. J. Camenisch and E. Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 21–30, New York, NY, USA, 2002. ACM.
9. L. Cranor and S. Garfinkel. *Security and Usability*. O'Reilly Media, Inc., 2005.
10. T. di.me project. di.me - integrated digital.me userware, 2011.
11. H. Dwivedi, C. Clark, and D. Thiel. *Mobile Application Security*. The McGraw-Hill Companies, 2010.
12. T. El Maliki and J.-M. Seigneur. A survey of user-centric identity management technologies. In *Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on*, pages 12 –17, oct. 2007.
13. Google Inc. The google+ project.
14. M. Heupel. Porting and evaluating the performance of idemix and tor anonymity on modern smartphones. Master's thesis, University of Siegen, December 2010.
15. J. I. Hong and J. A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 177–189, New York, NY, USA, 2004. ACM.
16. A. Jøsang and S. Pope. User centric identity management. In *Proceedings of AusCERT*, 2005.
17. K. Kryszczuk and A. Drygajlo. Credence estimation and error prediction in biometric identity verification. *Signal Process.*, 88(4):916–925, 2008.
18. V. Lee, H. Schneider, and R. Schell. *Mobile Applications: Architecture, Design, and Development*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2007.
19. PICOS TEAM. PICOS Public Deliverables Site. http://picos-project.eu/Public-Deliverables.29.0.html, January 2010.
20. B. Shneiderman and C. Plaisant. *Designing the User Interface: Strategies for Effective Human-Computer Interaction (4th Edition)*. Pearson Addison Wesley, 2005.
21. B. Shneiderman, C. Plaisant, M. Cohen, and S. Jacobs. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. Shneiderman, 5 edition, March 2009.
22. The Tor Project. Tor on android. http://www.torproject.org/docs/android, 2010.
23. K. Verslype, J. Lapon, P. Verhaeghe, V. Naessens, and B. De Decker. Petanon: A privacy-preserving e-petition system based on idemix. *Report CW522*, Oktober 2008.