Reducing the User Burden of Identity Management: A Prototype Based Case Study for a Social-Media Payment Application

Till Halbach Røssvoll, Lothar Fritsch
Norwegian Computing Center, Oslo
http://nr.no

***Abstract*—Payment applications inside social media dealing with privacy and security sensitive content require, besides trust in the involved parts like financial institutions and providers of electronic identities, in particular the trust of the users. The e-Me project focuses on this trust and aims at providing multimodal, adaptive authentication and authorization methods for social media that are usable for all users. In an integrated social-payment application connected to online banking, an OpenID provider has been developed by means of inclusive-identity management methods. The provider is used for both the social-media access control and the embedded payment service. This work describes the design decisions and eventual design made for the prototypes with considerations concerning both e-inclusion and information security and privacy.**

***Keywords*-Trust, security, privacy, identity management; e-inclusion, accessibility, usability, universal design; social media/networking applications**

I. Introduction

For architects and developers of the ever growing number of social media and electronic services, access and identity management (AIM) is a substantial part of the system design. AIM refers to techniques for determining and organizing the identity of a user in order to grant access to a service or data, also referred to as authentication, or to authorize the execution of a task [1]. In addition, electronic identities are used to organize personal data, and to provide advanced identity management systems [2].

In the context of information technology, accessibility describes the degree to which a solution is accessible for as many people as possible, in particular those with impairments, and those using assistive technology together with the product or service. Usability refers to the ease with which people can use a particular product or service. Obviously, AIM applications have to be both secure and privacy aware, and should at the same time be as accessible and usable as possible. Researchers have previously pointed out the need for inclusive access and identity management [3], as only few of these systems pay attention to accessibility and usability issues [4].

This work discusses how to design for trust, privacy, and security regarding online services and applications inside social media, while at the same time meeting the requirement for universal design. Examples of such applications are image galleries, music sharing services, online games, and news feed services. The term trust is used here in its most generic sense as the degree of reliance of one entity on another [5]. The definition of privacy in this work is based on the EU Data Protection directive [6], in the spirit of the data subject's informed participation, while security in this work bears the meaning "degree of protection to safeguard the asset, here personal data, against threats in terms of data exposure, damage, or loss".

Parts of this work have been presented on a previous occasion [7]. The novel contributions of this article are

1) an in-depth description of the prototypes, including privacy and security aspects,
2) a discussion of technical decisions regarding the universal design of the system,
3) the discussion of design considerations regarding the system's functionality for privacy and security, and
4) a discussion of the implications of the design for the user's experience of trust.

The work is organized as follows. First, the scope providing research project is introduced, followed by a description of the proof-of-concept application developed in the course of the project. Then, e-inclusion, trust, and privacy aspects are discussed, and a number of trust establishing measures is presented as a checklist before the paper concludes.

II. The e-Me project

The research project e-Me sets the context for this work [8]. The main goal of the project is to provide new knowledge to improve the usability and accessibility of access and identity management systems, including authentication mechanisms, in social media without compromising privacy and security, and without offending legal frameworks.

In the course of the project, the example application PayShare has been developed. The starting point for the development of a highly usable and accessible prototype was a literature review on the field of accessibility and usability issues of personal identification systems [9], recommending —- among others:

- an open and universally designed solution with an accessible, adaptive, and personalized multimodal user interface,

ISBN: 978-1-61208-250-9

- a minimally exposed user profile with reasonable defaults and opt-ins,
- and the application [1] of privacy-enhancing technology.

With this in mind, several hypotheses were set up:

1) The majority of users is suffering from having to handle too many user names and passwords for authentication.
2) The majority of current authentication mechanisms is not accessible to users with impairments.
3) Users have different requirements and preferences for privacy and security in electronic products.
4) Users experience multiple authentication processes in case of frequent authorization as cumbersome.
5) Authentication as used in social media can be applied to privacy and security aware applications without a degradation of the level of security or privacy.

In short, the solutions provided by PayShare are:

1) OpenID cuts down the numbers of service accounts to remember for the user.
2) Authentication adaptation by means of several OpenID login alternatives, namely password, a series of pictures, a series of sounds, pattern, and personal question, which — in total — have a higher degree of accessibility than just a single login method.
3) User defined threshold for the application of more frequent authentications.
4) Validity of a person's authentication for a user defined time span.
5) OpenID as an authentication means to authorize payments in an financial application inside a social medium.

All aspects of the solution are subsequently explained in more detail.

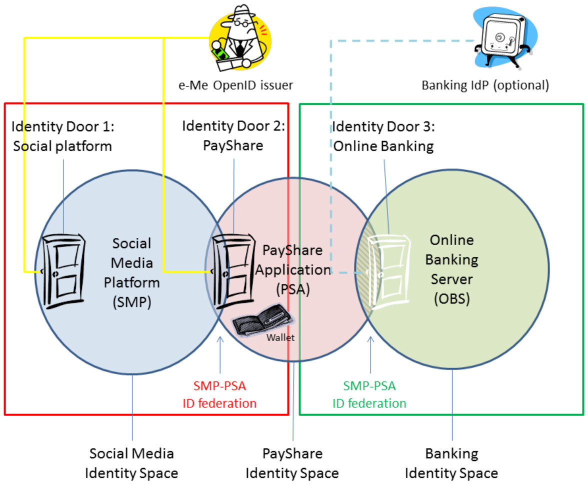

e-Me OpenID issuer
Banking IdP (optional)
Identity Door 1: Social platform
Identity Door 2: PayShare
Identity Door 3: Online Banking
Social Media Platform (SMP)
PayShare Application (PSA)
Wallet
Online Banking Server (OBS)
SMP-PSA ID federation
SMP-PSA ID federation
Social Media Identity Space
PayShare Identity Space
Banking Identity Space

Figure 1. Identity federations and identity doors in the PayShare application

III. The PayShare application

The proof-of-concept prototype PayShare is a means to test design principles, user interface, and system functionality. It can be described as an online payment service. Figure 2 shows the flow diagram of the PayShare application. The application's three entry points are "Add new claims", "View claims", and "View single claim". The user is automatically guided through the block sequence {"Read about", "View/accept terms"} before anything else can be done inside the application.

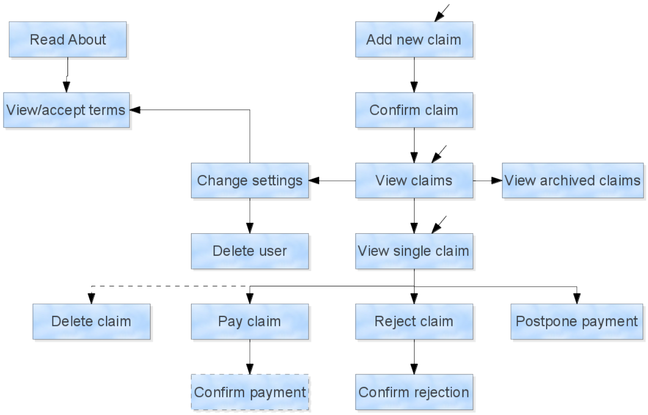


Figure 2. The flow in the PayShare application, which equals the application's pages/screens. The dashed arrow indicates a path that is only open to creditors. The dashed box refers to the external OpenID provider.

Upon registration, which basically requires the user's acceptance of the Terms&Conditions of the service, users can file payment claims for the entire group, assuming all group members are also connected through a particular social medium. For instance, consider a group of friends out to travel. One of them, here called creditor, pays for the travel tickets of the entire group and files claims against all "friends", here referred to as debtors, in PayShare. The debtors then get notifications that there are open claims that they have to pay, and the creditor can conveniently track any payment progress, i.e., see who has paid or not. Payments can be made directly in the PayShare service, meaning inside the social medium, to/from a virtual wallet in form of so-called credits, or to/from an account in a trusting bank. There is the possibility to transfer money from the bank account to the virtual wallet. PayShare in its entirety meets the requirement represented by the fifth hypothesis (Section II).

Figure 3 shows the screen shot of the "View single claim" block which is central to the application. It consists of two logical units. One unit gives all necessary claim details, such as amount, creditor, explanatory message, date, and the subclaims for all the other group members. Strictly speaking, the latter information is not mandatory for the debtor to know in order to pay the claim, but it serves as an additional explanation and justification of the claim. In the logical unit below the claim details, the debtor is asked for her choice; that is, pay the claim from the wallet, pay the claim from the bank account, reject the claim, or postpone the payment. Concerning the latter, the claim will be maintained, and a reminder about it is send to the debtor from time to the other. As mentioned, the debtor could also reject the claim, with or without a personal comment to the creditor. Before the navigation buttons are shown on the page, a brief message is displayed informing the debtor about the payment; i.e., if (and why) an additional authentication might be necessary, or — if applicable — just informing the debtor that the payment is carried out without authentication. A hyperlink to the appropriate part in the settings is given where these security preferences can be changed.

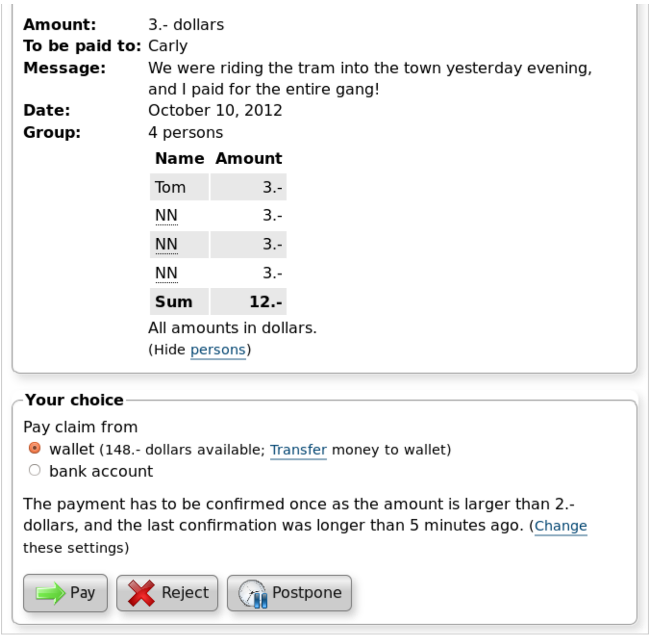
A. *Privacy & security aspects*

To solve security and privacy challenges, PayShare aims at the separation of identity spaces from each other, see Figure 1. To achieve this, electronic identities and their use have been organized in Identity Spaces. These spaces are organized with PayShare as a intermediary separating the identity spaces. We use the concept of an “Identity Door” to describe the handling of e-ID when authenticating to a service or when authorizing a transaction. In Figure 1, we show how three such identity doors are defined in PayShare:

- Door 1 is the entrance door to the social media platform that will provide the social context for PayShare.
- Door 2 is the registration to PayShare, which in general is entered from the social media platform (but can be accessed through its own user interface).
- Door 3 is the additional authorization and interface against the online banking transaction server.

Since security usability — especially of authentication mechanisms — is the primary objective of the e-Me project, compromises between the security infrastructure, privacy design, and usability had to be taken. These will be discussed further below.

Regarding other security ensuring measures, there is a user-defined threshold for the payment amount. If the amount is above the threshold, an additional OpenID authentication of the user is required to authorize payments, as illustrated in Figure 1 with Door 3. However, as the authentication mechanisms used by banks are numerous, and as an extra authentication door is perceived as a hindrance by sensitive users, PayShare acts rather as a payment intermediary. This approach allowed us to restrict Door 3 authentication to cases where the wallet is charged or discharged. As such, users are enabled to put a price at the convenience of not having to go through an authentication process for small-amount payments. Payments with an amount below the threshold are one-click payments. This measure meets the requirement represented by the third hypothesis Section II. At the same time, the OpenID provider can offer user friendly and inclusive authentication methods both on Door 1 and Door 2.



Amount: 3.- dollars
To be paid to: Carly
Message: We were riding the tram into the town yesterday evening, and I paid for the entire gang!
Date: October 10, 2012
Group: 4 persons

Name	Amount
Tom	3.-
NN	3.-
NN	3.-
NN	3.-
Sum	**12.-**

All amounts in dollars.
(Hide persons)

Your choice
Pay claim from
● wallet (148.- dollars available; Transfer money to wallet)
○ bank account

The payment has to be confirmed once as the amount is larger than 2.- dollars, and the last confirmation was longer than 5 minutes ago. (Change these settings)

Figure 3. Screenshot of the “View single claim” page in PayShare.

Authentication is delivered by an OpenID provider, which has the advantage that only a single password has to be remembered by the user, even for a variety of applications, authentication contexts, and web sites. This measure meets the requirement as formulated by the first hypothesis Section II. Theoretically, the solution works together with any OpenID provider with full support of the OpenID protocol, but in practice only a few selected providers may be found suited due to trust reasons. An own OpenID provider has been developed as one of the deliverables of the e-Me project.

Data from any authentication, be it login to the social medium or authorization of a payment, expires according to a user-defined time span for authentication validity. This measure meets the requirement put forward by the fourth hypothesis (Section II) and aims at avoiding frequent cumbersome authentications as the user’s ID is remembered for this specific time span. Consequently, an authentication process is only invoked when the payment’s amount is above the threshold, and when the time elapsed since the last authentication has exceeded the authentication validity duration. More on the reasoning for the respective design choices in Section IV-B.

IV. Discussion

In the following, it is discussed how accessibility and usability issues as well as trust, security, and privacy matters are reflected in the PayShare application.

A. *e-Inclusion*

As mentioned before, the project's focus is on inclusion aspects of the solution. Its target groups consist of users with various impairments, and the elderly. Acknowledged impairments are cognitive challenges such as dyslexia and dyscalculi, orientation, and memory problems, sensory challenges like vision and hearing reduction, and motor challenges like trembling hands. Elderly users are likely to have a combination of impairments. However, apart from these focus groups, PayShare is required to be universally designed, meaning that it can be used by virtually all persons.

To meet the requirement as formulated by the second hypothesis (Section II), the aforementioned OpenID solution offers in total five login alternatives:

- Password memorizing,
- recognition a series of pictures,
- recognition of a series of sounds,
- pattern drawing, and
- knowing the answer to a personal question.

What login method is used is up to the user to decide. Each of the alternatives aims at a particular target group (but is, of course, not restricted in use to this group): Password for user without particular login problems, picture series for the hearing impaired, sound series for the vision impaired, pattern drawing for dyslectic individuals, and personal question for users with short-/medium-term memory deficits. In total, e-Me authentication has a higher degree of accessibility than just a single login method.

Apart from login, the system's inclusiveness is met by a number of measures concerning universal design. For instance, the user interface is tailored to the needs, preferences, and context of the respective user by means of a user profile, satisfying major parts of the first requirement from the literature review.

B. *Privacy implications*

The PayShare application accounts for privacy concerns in a number of ways.

The service follows the privacy requirements [6] derived from the EU Data Protection Directive [10]. In addition, it considered the potentially harmful actions laid forth by Solove [11], and places particular attention on the handling of electronic identifiers according to the PETweb II risk taxonomy [12]. According to Solove, harmful actions on personal data are:

- Information Collection: Collection and accumulation of personal information can cause harm.
- Information Processing: Handling of collected personal data that can cause harm.
- Information Dissemination: Harms of spreading, or threat of spreading information.
- Invasion: Risks of intrusion and decision interference.

The following requirements from the uTRUSTit privacy requirement report [12] were used as the essential requirements following from the EU data protection directive [10].

- Personal data is only processed after the person gave informed consent for the processing.
- A person has the right to inquire about the own personal data stored with another party.
- A person can revoke consent for personal data processing given earlier at any time.
- The data processor can only process personal data according to the given consent (e.g. according to a privacy policy).
- The data processor makes sure that personal data is sufficiently protected from unauthorized access, manipulation, abuse or loss.
- The data processor makes sure to be able to react accordingly to consent revocation for any given personal data.

The PETweb II risk taxonomy for electronic identity management systems found a number of factors that constitute privacy risk in handling identifiers [11]. Major risks found include the possibility for identifiers to get profiled, to get stolen, and to get remotely used. In the PayShare scenario, Door1 authentication leads the users into a personalized profile. The purpose of authenticating is to access the same profile every time. The same holds for PayShare's Door 2 authentications , where personal money is administered. The risks for stolen identifiers is strongly dependent on the authentication technologies offered by the OpenID provider. In e-Me, experiments are performed with easy-to-use password replacements, and with signature strength smart card solutions [13].

A number of compromises have been made. In the given scenario – payment among a group of users registered to a social media platform, in connection to their bank account – full anonymity was nowhere possible. The social media profile, even if it should be created under pseudonym, gets through the PayShare service connected to a bank account that is connected to a verified person. In addition, pseudonymity on the social media is of limited usefulness in a scenario where friends split the dinner bill – as the identities are known between the friends anyway. The critical pieces of personal information were identified to relate to the occurrence, frequencies and destinations of payments. By inclusion into a social media, PayShare is principally able to trace a friends network's payment behavior. Repeated payments between friends can indicate closer relationships, reveal business secrets, or prove social relationships to others. The introduction of the Wallet for low-value payments loosens the connection between the bank and the social media activities. By acting as a "wallet filled with small change" up to the set threshold, the bank gets only involved into higher-value transactions. However, as ultimately, bank transactions will be used beyond Door 3, there is no way around compliance with financial market regulation, and thus full identification of sender and receiver in a bank transaction.

Regarding concrete privacy measures, there are several hyperlinks to the service's Terms such that the user can view this document also after its acceptance upon registration. In case the user does not agree with the Terms anymore, an option to delete the user account is provided. There is also a hyperlink from the settings to the deletion of the user account, as the user might find the security and privacy settings inappropriate for own needs.

As mentioned in Section III, the view of a single claim contains the display of the subclaims for group members. However, all names (except the own one, of course) are anonymized per default to honor the privacy of all involved persons. The visibility of claims can be set to "Visible to all group members" in the settings, if desired.

The deletion of a user's account includes the irreversible removal of the user's profile which in turn includes settings like bank account number, visibility of claims, OpenID address, threshold for additional authentication, and duration for storage of authentication realm. Additionally, the user's ID is removed from all open and archived claims in the database, following this policy: Where the user is a creditor and the (sub-)claim is open, the (sub-)claim is deleted. In archived (sub-)claims with the user as a creditor, the user ID is erased from the database entry. Other claims, in particular those where the respective user has been named as a debtor, are not touched.

Creditors may delete own claims, but here the restriction is that only open claims may be deleted, while archived claims cannot. In this case and in the instance of the user account deletion, the privacy of the creditor and the privacy of the debtor have to be weighted against each other. PayShare accounts for the debtor's privacy by keeping archived records, but at the same time also honors the creditor's privacy and erases her user ID from the record, as this is information provided by the creditor herself. A debtor cannot, however, delete claim records as the information concerning who is the claim's debtor has been provided by the creditor and is hence out of control for the debtor.

C. *Trust implications*

As a payment service that voluntarily relies on OpenID for authentication, and that is linked to a bank account, there are a number of trust chains. Figure 4 illustrates all paths of trust.

PayShare acts as an identity broker against the social media and the bank identity space. The bank (the trustor) has, as a minimum requirement, to trust PayShare (the trustee)

- that all virtual credits are safe and properly handled with the service,
- that all payments are correctly executed, and
- that personal data are handled in a confidential way.

The same applies to the trust chain from the user (the trustor) to PayShare (the trustee). Needless to say, the user has to trust the bank in the same way as she trusts PayShare. In addition, the user needs to trust the social medium, which provides the framework for services like PayShare, for data that PayShare and the medium have in common, like user names, and the OpenID provider, for handling authentications in a secure and privacy aware way. PayShare needs to trust the underlying social medium as well as the OpenID provider for proper and secure authentication.

Besides the robustness of the OpenID provider's authentication methods, PayShare itself must be seen as the most critical point in the privacy infrastructure. PayShare is the entity that collects and combines both information about the users' social media identity, their bank identity, and their payment requests. Therefore is the correct handling and deletion of payment requests and payment information at PayShare of utter importance. The issue of the trusted 3rd party is a well-known problem for privacy and trust research. Often, for instance when personal data is part of a business model, some form of 3rd party (e.g. intermediaries and brokers) are needed to perform the business function. These brokers can help to protect privacy by separating identity spaces and personal data between the participating stakeholders. The concept has successfully been used to anonymize location data in location-based services [14], [15]. In PayShare, the PayShare service itself handles the identity spaces with a direct mapping rather than using anonymizers [16] and advanced attribute credentials [17] due to the fact that banking transactions cannot legally be anonymized.

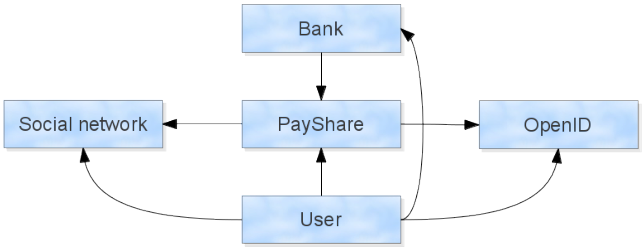


Figure 4. Chains of trust among the PayShare stakeholders.

Is is argued here that especially impaired users need particular measures to develop the same degree of trust like the average user to make up for the impairment. For instance, a blind person who is enabled to use an audio-based authentication scheme will have more trust in such a system that accounts for the user's preferences than systems that only offer visual CAPTCHAs. Similarly, a person with orientation and problem solving problems is likely to develop more trust in a system showing explaining messages about what is about to happen on the current screen than systems that do not have the same degree of usability.

All users build their trust on pieces of information, about what is about to happen, why certain things happen, what the user's choices are, etc. The picture is never entirely complete; rather, the more information the user has at a given point in time, the better in order to be able to carry out a particular task. Impaired users are likely not to get as much information as ordinary users, except when the solution is universally designed and thus accessible to virtually all.

On the other hand, too much information can result in the disorientation of the user, especially those with orientation and learning challenges [18]. The solution should therefore limit the amount of information the user is confronted with, and should also ease its processing, in terms of a weighting of the information's importance for the context the user currently is in. To sum up, it is crucial in particular for impaired users — but also for all users in general — that the system provides and makes accessible all the information the user needs in order to carry out a task by herself, not less but not more either to avoid user confusion.

V. Conclusion

User control and information are crucial to achieve a high degree of trust of the user to the service. There is a connection between e-inclusion and trust in terms of the fact that a high degree of accessibility and usability empowers the user in certain situations to use the respective service at all. In other situations, it increases the user's control or feeling of control and thereby the user's trust. The perception of increased trust is not only applicable to users with impairments but rather all users, as it is widely recognized that e-inclusion measures for particular focus groups generally increase the service's usability for everybody.

A particular challenge in the realization of PayShare was its connection to several identity spaces. Social media identities and online banking identities are different in scope, robustness, and use. PayShare had to accept the role as an identity broker or identity intermediary to bridge the respective identity spaces. The resulting privacy issues were analyzed and led to the above requirement list for PayShare.

Acknowledgment

The e-Me project is funded by the Norwegian Research Council under project no. 201554.

References

[1] K. S. Fuglerud and T. H. Røssvoll, "Usability and accessibility of personal identification management systems in electronic services," in *Proceedings of eChallenges-2011*. Florence (Italy): IIMC International Information Management Corporation Ltd., Oct. 2011. [Online]. Available: http://echallenges.org/e2011/default.asp?page=paper-repository&fltyear=all&flttheme=all&flttype=all&flttitle=&fltauthor=halbach&pagesize=100&submit=Search

[2] WP3, "Fidis Deliverable D3.1: Structured overview on prototypes and concepts of identity management systems," FIDIS Consortium, Tech. Rep., September 2005.

[3] L. Fritsch, K. S. Fuglerud, and I. Solheim, "Towards inclusive identity management," *Identity in the Information Society*, vol. 3, no. 3, pp. 515–538, 2010.

[4] G. Sauer, J. Holman, J. Lazar, H. Hochheiser, and J. Feng, "Accessible privacy and security: a universally usable human-interaction proof tool," *Universal Access in the Information Society*, vol. 9, no. 3, pp. 239–248, 2010. [Online]. Available: http://www.springerlink.com/content/j801373hw352514r/

[5] L. Fritsch, A.-K. Groven, and T. Schulz, *On the Internet of Things, Trust is Relative*, ser. Communications in Computer and Information Science. Amsterdam: Springer, 2011, vol. 277, ch. 9, pp. 267–273.

[6] European Council and Parliament, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications)," 2002.

[7] T. H. Røssvoll, "Trust implications for universal design of social-networking applications," User-Centered Trust in Interactive Systems Workshop at NordiCHI 2012, Oct. 2012. [Online]. Available: http://www.nordichi2012.org

[8] Norwegian Computing Center, "e-Me — Inclusive identity management in new social media," 2012. [Online]. Available: http://nr.no/pages/dart/project_flyer_e-me

[9] K. S. Fuglerud and T. H. Røssvoll, "Previous and related research on usability and accessibility issues of personal identification management systems," Norwegian Computing Center, Oslo (Norway), Tech. Rep. DART/10/10, Oct. 2010. [Online]. Available: http://publ.nr.no/5371

[10] L. Fritsch, "Social media, e-ID and privacy - background for the e-Me project," Norsk Regnesentral, Tech. Rep. DART/02/2011, April 2011.

[11] D. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477–564, 2006.

[12] E. Paintsil and L. Fritsch, *A Taxonomy of Privacy and Security Risks Contributing Factors*, ser. IFIP Advances in Information and Communication Technology. Springer Boston, 2011, vol. 352, pp. 52–63.

[13] L. Fritsch, "Privacy visualization requirements in the Internet of Things - a uTRUSTit FP7 ICT project note," Norwegian Computing Center, Tech. Rep., September 2012.

[14] ——, "Utprøving av Buypass e-ID og Altinn.no - resultat av smartkort-studie i e-Me-prosjekt," Norwegian Computing Center, Tech. Rep. NR Note DART/03/2011, April 2011.

[15] T. Koelsch, L. Fritsch, M. Kohlweiss, and D. Kesdogan, *Privacy for Profitable Location Based Services*. Boppard: Springer, 2005, vol. 3450, pp. 164–179.

ISBN: 978-1-61208-250-9

[16] J. Zibuschka, L. Fritsch, M. Radmacher, T. Scherner, and K. Rannenberg, "Privacy-friendly LBS: A prototype-supported case study," in *13th Americas Conference on Information Systems (AMCIS)*, P. o. t. A. C. o. I. Systems, Ed., 2007.

[17] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the Acm*, vol. 4, no. 2, pp. 84–88, 1981.

[18] T. Halbach, "Towards cognitively accessible web pages," in *Proceedings of Third International Conferences on Advances in Computer-Human Interactions (ACHI-2010)*, International Academy, Research, and Industry Association (IARIA). St. Maarten (Netherlands Antilles): IEEE Computer Society, Feb. 2010, http://www.iaria.org/conferences2010/ACHI10.html. [Online]. Available: http://publ.nr.no/5236