Trustworthy and Inclusive Identity Management for Applications in Social Media

Till Halbach Røssvoll and Lothar Fritsch

Norwegian Computing Center (Norsk Regnesentral)
Gaustadalléen 23, 0314 Oslo, Norway
{Till.Halbach.Rossvoll,Lothar.Fritsch}@nr.no

Abstract. We describe a prototype for inclusive and secure identity management regarding a bill sharing application in social media. Beginning with the principals of universal design, and involving groups of users with impairments, we designed a set of alternative authentication methods based on OpenID. This work explains the scenario and the particularities of designing a trust, security, and privacy infrastructure with a high degree of usability for diverse user groups, and which is aligned with the requirements from regulatory frameworks. The user trials show that several authentication alternatives in multiple modalities are welcomed by impaired users, but many have restrictions when it comes to payments in the context of social media.

Keywords: Authentication, Authorization, OpenID, Identity Management, Social Media, Payment, Accessibility, Usability, E-Inclusion.

1 Introduction

Online payment applications naturally require a high level of trust by the user. This applies in particular to payment services inside social media, which are, as of today, typically viewed as being insecure and open, in contrast to for instance secure and privacy respecting internet banking [1].

The e-Me project [2] focuses on this trust and aims at providing accessible, multimodal, and 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.

So far, the trust issue has been discussed in the HCI community broadly with respect to usable privacy and security, risk and online trust, considering different objects of trust, e.g., websites, companies, and individuals [3–7]. Furthermore, trust has been discussed generally as a factor as a part of the user experience, e.g., [8, 9], and as part of trust evaluation strategies [10]. This work places the term trust inside a particular case, a payment application for social media and links it to identity management in terms of authentication and authorization. Parts of this work have been presented at previous occasions: [11] briefly introduces

M. Kurosu (Ed.): Human-Computer Interaction, Part III, HCII 2013, LNCS 8006, pp. 68–77, 2013.

the PayShare application mentioned further below, and [12] extends the topic with more details on the e-Me project and a detailed discussion of security and privacy measures [13] of the PayShare application. The novel contribution of this paper is an in-depth description of the accessible OpenID server and a thorough discussion of trust aspects of the entire solution.

The work is structured as follows: After the problem description and a brief overview of the provided solutions, trust considerations are discussed in detail. Then, best practices for design for trust are presented, before giving a detailed description of the OpenID server and the description of conducted user trials. Finally, the conclusion is drawn.

This work is funded by the Research Council of Norway through the VERDIKT program under contract no. 201554.

2 Problem Analysis

The formulation of the objective and constraints of the prototypes was put forward in the description of the Norwegian research project e-Me [2]. The solutions should be suitable for real-life use, including the context of social media, be applicable to authentication and authorization likewise, they should be accessible and offer a high degree of usability, and they should avoid to compromise privacy, security [13], and to offend legal frameworks. Additional constraints regarding the honoring of universal-design and legal frameworks are summarized in [14] and [15], respectively.

Prior to any development, a number of key challenges was identified that had been pointed out as open challenges in related research work [16]:

1. The majority of users is suffering from having to handle too many user names and passwords for authentication.
2. Poor accessibility and usability compromise security and privacy and hereby trust.
3. The majority of current authentication mechanisms is not accessible to users with impairments.
4. Users have different requirements and preferences for privacy and security in electronic solutions.
5. Users experience multiple authentication processes in case of frequent authorization as cumbersome.
6. 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.
7. When using universal design rather than the legal framework or the established traditions of information technology, and in designing for security and privacy, their incorporation becomes substantially different both in terms of legal compliance as well as on the level of software engineering, information security engineering, and privacy by design.
   - Provide security and privacy mechanisms that adapt to various skills;

- Communication, such as privacy policies, instruction, and terms and conditions must be understandable for persons with a variety of backgrounds;
- Interactions should be rather deterministic, intuitive, and memorable;
- The security infrastructure should be open to special peripheral devices such as audio readers, braille terminals, or interaction interfaces.

Many conflicts between the project's goals turned up. The prioritization of usability and inclusion over security methods created tension both on the technical and on the legal level. By using particular flavors of accessible IDM, at the same time security and DP might become weaker for the users of these methods and the system as a whole. Prioritization between advanced security policies and accessibility had to be done as well as the compilation of a portfolio of alternative authentication methods with focus on accessibility, not on equal security levels. As a consequence, the prototype can accommodate various skill levels, but at the price of very distinct levels of robustness of the security measures. In turn, this approach will make the job of risk assessment and security management of an information security management systems, e.g. according to the ISO 27000 family, more challenging.

Answering these challenges, two main services were developed: An OpenID provider, and an application to share bills among friends and to manage joint payments inside social media, named PayShare. Combined, they have the following properties:

1. OpenID cuts down the numbers of service accounts to remember for the user. In addition, the seamless authentication experience based on a persistent, personally adapted authentication channel matching the users' skills through several services reduce complexity for the users.
2. Full-scale accessibility and a high degree of usability increase the user's trust.
3. Improved accessibility by authentication adaptation in terms of several login alternatives: password, pictures, sounds, pattern, personal questions, additional one-time password (two-factor over separate channel/SMS).
4. User defined threshold for the application of more frequent authentications.
5. Validity of a person's authentication for a user defined time span.
6. OpenID as an authentication means to authorize payments in an financial application inside a social medium.

In the subsequent sections, these contributions are discussed in detail.

3 Considerations Regarding User Trust

Trust is strongly influenced by a service's security measures and privacy awareness. Trustworthy online services require a certain standard regarding user identification, authentication, authorization, role management, and information security and privacy [17]. This applies particularly to a financial application with a virtual wallet like the bill sharing service PayShare, which can be treated

like an internet bank. As a precondition for trust creation, the security mechanisms need to add to the total experience and not get into the way, as often felt by users [18]. From our user groups we learned that identity management concepts and especially authentication are the first major hindrance in participation on social media and other services, as nearly all authentication channels potentially exclude certain user groups [15]. We decided therefore to offer a variety of alternative authentication channels.

The portfolio of authentication methods made the design of security and privacy properties more difficult. The major challenge is the variety of mechanisms with distinct security properties and divergent privacy properties. Depending on a user's choice of mechanisms, the overall security, privacy, and trust framework can differ as compared to other users, and other use cases. Mechanisms may also be changed at any time due to a changing life situation or context. Therefore, it can be difficult to establish a risk management system with static risk assessment. On the other hand, when evaluating the total system security, the strength of the weakest authentication channel must be assumed.

Further issues arise from the identity management unification. By using the OpenID provider as a universal mechanism, PayShare establishes itself as a powerful 3rd party with observation capabilities both towards the social media platform and towards the payment system. In addition, an identification chain from the social media to the PayShare application is established, which continues to 'friends' and to an associated bank. Hence, pseudonymous social media participation is no longer possible. Further issues in trustworthiness are found in the underlying authentication mechanisms, where audio-visual information may leak out to other persons, dependent on the usage situation. It appears that usability and inclusion requirements are in strong tension with security, privacy, and data protection regulation.

Concerning e-inclusion aspects, the requirement of universal design implies a high degree of accessibility and usability of all involved parts of the solutions [14]. The e-Me project considered target groups consisting of users with various impairments, and elderly. Acknowledged impairments were cognitive challenges such as dyslexia, dyscalculi, orientation, learning, and memory problems, sensory challenges like sight and hearing reduction, and motor challenges like trembling hands. Elderly users sometimes have a combination of impairments. However, apart from these groups, the solutions were required to be universally designed, i.e., to be be able to use by virtually all persons.

3.1 Design Measures for Trust

The following design recommendation have been developed and were applied in PayShare to increase the user's trust into the service. They are deliberately held as generic as possible to make them applicable for electronic services in general. They compound both security and privacy aspects, as well as usability best practices.

- Require extra authorization before critical actions. Example: An extra check box has to be marked before for instance claim deletion

- Show concise and comprehensive system messages that explain the general context (what the user is about to do), the concrete task at hand, the requirements needed, and the concrete instructions. Ex.: Instructive messages like "XY has sent you a payment claim", "You are about to reject the claim", "You may need an OpenID address", "Fill in all input fields below, then press .." are shown
- Show brief and comprehensive error messages with both concrete and general help information, and directions to a human contact. Ex: "The system couldn't contact your OpenID provider. It could be caused by .. Please check .. in your settings. If you do not succeed after several trials, please contact .. (link to assistance)"
- Offer a dashboard view to ease overview gaining. Ex.: Showing the status quo, history of events, link to Terms, and link to settings
- Offer multiple easy-to-find links to the profile settings
- Offer several easy-to-find links to Terms&Conditions
- Make all user settings non-mandatory. Ex.: It is not required by the user during the service registration to specify the amount threshold for the additional authentication; instead, the most secure default is chosen (here: additional authentication is needed always), and the user can change this setting later on
- Use safe defaults for all user profile settings
- Only expose particular profile settings on demand. Ex.: Link to the setting "Change the authentication threshold" from the claim payment page, in order for the user to get rid of the "An additional authorization is needed" messages
- Offer several easy-to-find possibilities to delete the user/profile Ex.: Links to the deletion of the user account from at least the settings and the Terms
- Make as many user actions as possible reversible. Ex.: Give particular events a short time span where they can be reverted
- Offer multiple possibilities to delete user data. Ex.: It should be possible for a user to delete all own user entered data
- Anonymize all user data that are impossible to delete. Ex.: In case of an interest conflict regarding the deletion of data, undeletable data should be anonymized. Data minimization is advisable.
- Only show information relevant in a specific situation. Ex.: Do not let the user change the settings when nothing has be changed
- Offer an archive with previous events and actions, comparable to a system log
- Offer a multitude of authentication methods. Ex.: Offer authentication that accounts for sensor, motor, and cognition impairments.
- Hold the design of an OpenID server different from the design of the service to illustrate the mechanisms invoked during an OpenID authentication
- Honor accessibility and usability standards. Ex.: As a minimum, follow the HTML, CSS, WCAG 2, and WAI-ARIA recommendations.
- Run risk assessment concerning the actual strength of the authentication mechanisms versus the value-at-risk in the connected applications. Loss of personal information should be treated as one of the risks.

To wrap up, the user's trust can first of all be created by empowering the user / giving the user access. Second, user trust can be increased by adaptation, where a service provider really "sees" the user and tailors the system according to her needs and preferences. Third, trust can be increased by setting the user in control in terms of informing the user about what is going on, letting the user interact with the system (for verification purposes), and by making the service as transparent, predictable, and reliable/credible as possible. Finally, trust can be increased by smart user support, i.e., by helping the user in case of confusion, insecurity, and system failure.

4 Verification of Considerations

As already mentioned, two prototypes were developed to verify the above considerations: The social-media application PayShare (presented and discussed in [12]), and an OpenID provider. The latter service is the key authentication party and developed with a high degree of accessibility and usability. It is used for login into the social media, registration with the payment application, and for the authorization of payments. To cope with a variety of possible user impairments and preferences, it offers authentication by means of six different login methods, as illustrated in Figure 1 on the following page:

- Password memorizing,
- recognition a series of pictures,
- recognition of a series of sounds (see Figure 2 on page 75),
- pattern drawing,
- knowing the answer to a series of personal questions, and
- a PIN code calculator as a smartphone application.

A good password choice is supported by a password strength calculator detailing the use of lower and capital letters, symbols, and digits. The visual choice is made by picking a sequence (here: five) of pictures out of a set of pictures grouped in categories, such as animals, clothes, and food. Upon login, five different sets of images are presented to the user in sequence, who then has to identify the one correct image from each set. The size of the set of elements (pictures) to pick from and the number of elements the user has to chose can be set as a parameter depending on considerations regarding the number of permutations (in case the order matters) or combinations (when order does not matter) required by a specific application. As an additional security mechanism, a user's account is suspended after four bad trials. The same principle applies to the audio choice, though with sounds and music, and to personal question-answer pairs. With the latter alternative, the user can either choose from the preset collection of questions or formulate own questions. The pattern is drawn by mouse or keyboard on an 8x8 array of points, where between five and 34 points have to be marked. Finally, the PIN code calculator presents a two-channel authentication

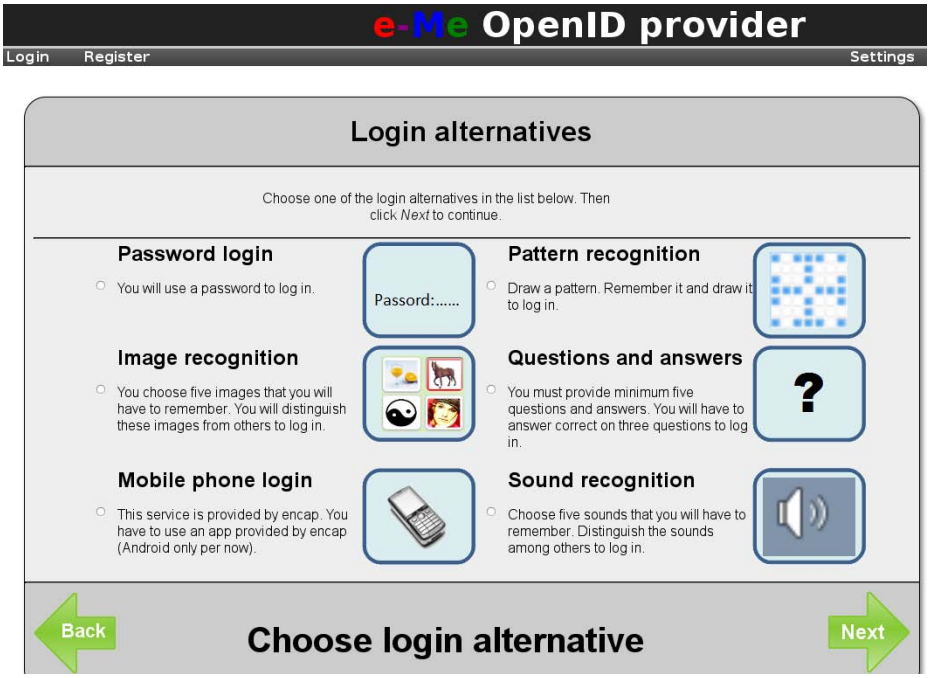

Fig. 1. Screenshot of six login alternatives shown during the OpenID registration

alternative in scenarios where this is required by the service provider (e.g., a bank). It outputs a 6-digit PIN code, which also can be read out load to the user, and which must be typed instead of the user's password. The PIN code is calculated based on a one-time password, which is sent to the phone from the server, and a device identifier.

The user can fill additional data into the OpenID profile, such as birth date, home address, etc. besides the mandatory full name and mail address. More importantly, the prototype also shows that it is possible to personalize the profile by a dedicated settings for the color scheme / contrast, which can easily be extended to other parameters such as font family, font size, and other parameters. Upon authentication, a service may ask OpenID server for all parameters, but it is up to the user to decide which parameters the OpenID server may share with the application. In case a service supports the aforementioned accessibility parameters, the service's design is altered immediately according to the parameter's values when the user returns from the authentication process at the OpenID server. This allows for a "specified once, personalize anywhere" strategy of electronic services. However, in turn, accumulated profile information in OpenID attributes can reveal individual disabilities, and thereby create privacy issues. Disability information might establish processing of medical information, which is regulated strong with respect to data protection in many countries.

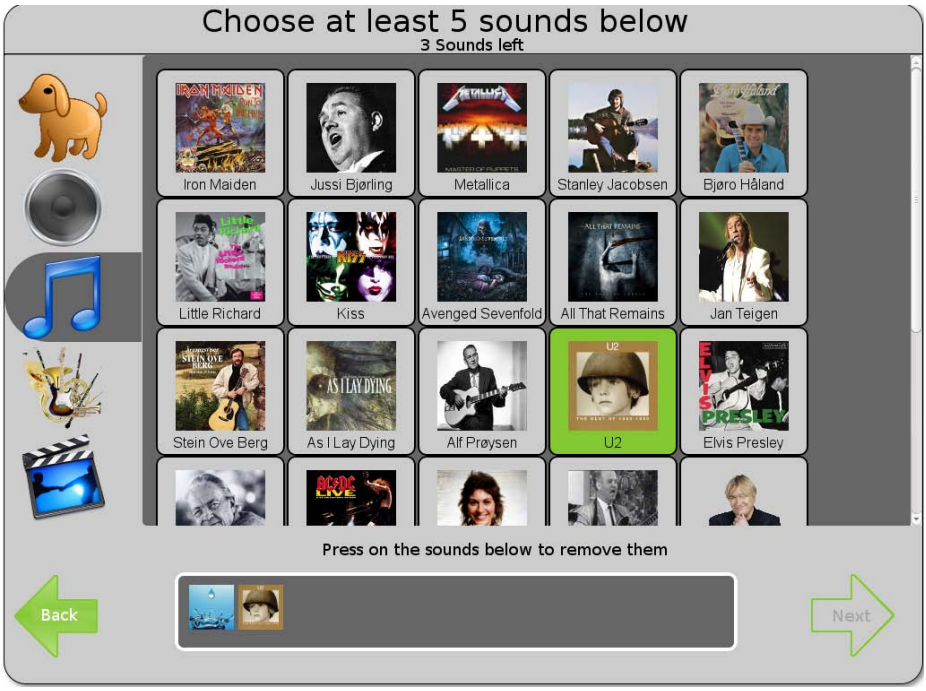

Fig. 2. Screenshot of sound based authentication

4.1 User Trials

In the user trials, eight participants tried out PayShare in combination with the OpenID server. The participants were organized in four groups of two persons and consisted mostly of elderly individuals, some with of them with visual impairments, and some with dyslexia. The groups had first to generate an OpenID account each before it was used for authentication and authorization with the payment sharing application. In the beginning, they were instructed about the situation ("you are NN, have been out eating with XY, you paid the entire bill, and now you claim your money back"), and they were given the names of the other virtual persons. All groups logged in to the given social networking site, which looked very similar to Facebook to provide the proper setting, and after that they were self-driven and only observed by the test leaders. One group filled in a claim, the other groups were notified automatically and had to pay their debt. This "game" quickly lead to new claims forth and back. Once the groups were finished, the participants had to fill out a brief questionnaire.

The first finding is that the deployment of the OpenID server was well accepted, even though none of the participants was familiar with this concept. Only two of the groups, those with sight impaired and dyslectic individuals, chose images as authentication method ("useful", "want that for my token calculator"), the others went for the password alternative ("familiar"). Some of the

sight impaired tried out pattern authentication but soon gave up ("not accessible for us"). It was also commented on the visibility of the pattern and images to others as compared to the concealed password input field. This naturally applies to audio and question-answer pairs as well.

The PayShare service was in general viewed as useful, but the majority had restrictions to make when it comes to trust, mentioning that financial services and social media were in their opinion not compatible. Some of the participants read parts of the $\tilde{2}$00-word Terms&Conditions, while nobody had a look at the 300-word privacy text. None of the participants visited their settings, underlining the importance of secure and sensible defaults.

5 Conclusion

We presented a prototype for inclusive and trustworthy authentication and authorization in the context of a bill sharing application in social media. The OpenID server offers a high degree of universal design in terms of six different login mechanisms, each of which based on different modalities. We also discussed how security, privacy, and universal design can increase trust.

A number of key factors is vital to achieve a high degree of trust of the user in the service: Accessibility, adaptation, usability, user control, information availability, interaction, verifiability, transparency, predictability, and reliability/credibility. Accessibility is the most crucial factor as it empowers users in certain situations to use the respective service at all. The other factors increase the 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, as it is widely recognized that e-inclusion measures for particular focus groups generally increase the service's usability for everybody [19].

References

1. Johnson, M., Egelman, S., Bellovin, S.M.: Facebook and privacy: It's complicated. In: Symposium on Usable Privacy and Security (SOUPS), pp. 24–29 (2012)
2. e-Me Consortium: Inclusive Identity Management in New Social Media, VERDIKT research project no. 201554, Research Council of Norway (2011), http://www.nr.no/pages/dart/project_flyer_e-me
3. Hochheiser, H., Feng, J., Lazar, J.: Challenges in universally usable privacy and security. In: Symposium on Usable Privacy and Security (SOUPS), vol. 2008 (2008)
4. Birge, C.: Enhancing research into usable privacy and security. In: Proceedings of the 27th ACM International Conference on Design of Communication, pp. 221–226. ACM (2009)
5. Dhamija, R., Dusseault, L.: The seven flaws of identity management: Usability and security challenges. IEEE Security & Privacy 6(2), 24–29 (2008)
6. Karat, C., Brodie, C., Karat, J.: Usable privacy and security for personal information management. Communications of the ACM 49(1), 56–57 (2006)
7. Cranor, L.F., Garfinkel, S.: Security and Usablity: Designing secure systems that people can use. Theory in practice. O'Reilly, Sebastopol (2005)

8. Schade, A., Nielsen, J.: Trust and Credibility, 2nd edn. E-Commerce User Experience, vol. 9. Nielsen Norman Group (2000)
9. Corbitt, B., Thanasankit, T., Yi, H.: Trust and e-commerce: a study of consumer perceptions. Electronic Commerce Research and Applications 2(3), 203–215 (2003)
10. Fritsch, L., Groven, A.-K., Schulz, T.: On the Internet of Things, Trust is Relative (chapter 9). In: Wichert, R., Van Laerhoven, K., Gelissen, J. (eds.) AmI 2011. CCIS, vol. 277, pp. 267–273. Springer, Heidelberg (2012)
11. Røssvoll, T.H.: Trust implications for universal design of social-networking applications. In: User-Centered Trust in Interactive Systems Workshop at NordiCHI (2012)
12. Røssvoll, T.H., Fritsch, L.: Reducing the user burden of identity management: A prototype based case study for a social-media payment application. In: Sixth International Conference on Advances in Computer-Human Interactions, ACHI (2013)
13. Fritsch, L.: Social media, e-id and privacy - background for the e-me project. Technical Report DART/02/2011, Norsk Regnesentral (2011)
14. Fuglerud, K.S.: Universal design in ICT services, Trondheim, Norway, 244–267 (2009)
15. Fritsch, L., Fuglerud, K.S., Solheim, I.: Towards inclusive identity management. Identity in the Information Society 3(3), 515–538 (2010)
16. Fuglerud, K.S., Røssvoll, T.H.: Usability and accessibility of personal identification management systems in electronic services. In: Proceedings of eChallenges-2011. IIMC International Information Management Corporation Ltd., Florence (2011)
17. Fritsch, L.: Privacy visualization requirements in the internet of things - a utrustit fp7 ict project note. Technical report, Norsk Regnesentral (Norwegian Computing Center) (2012)
18. Adams, A., Sasse, M.A.: Users are not the enemy: Why users compromize computer security mechanisms and how to take remedial measure. Commun. ACM 42(12), 41–46 (1999)
19. Huber, W., Vitouch, P.: Usability and accessibility on the internet: Effects of accessible web design on usability. In: Miesenberger, K., Klaus, J., Zagler, W.L., Karshmer, A.I. (eds.) ICCHP 2008. LNCS, vol. 5105, pp. 482–489. Springer, Heidelberg (2008)