Research on User Experience for Digital Identity Wallets: State-of-the-Art and Recommendations

Rachelle Sellung[1], Michael Kubach[1]

Abstract: Digital identity wallets are central components for Decentralised and Self-Sovereign Identity (SSI) approaches. They are the interface for users to manage their identities and gain access to services. Hence, the usability and user experience of these wallets is pivotal for the adoption of those popular and privacy friendly identity management concepts. As research on the user experience of wallets is still in its infancy, this paper aims to provide a first overview of recent research – published and from completed and ongoing research projects. Findings are summarized and recommendations for developers are derived.

Keywords: digital identity; IdM; identity management; digital wallet, digital identity wallet; user experience, usability; privacy; security, self-sovereign identity; ssi.

1 Introduction

Identity Management (IdM) is being transformed by Decentralized Identity and Self-Sovereign Identities (SSI), which rely on digital identity wallets controlled by users to manage their identity information and access services. Many initiatives, organizations, and projects are embracing this approach, with the EU Digital Identity Wallet [Eu22] as only one very prominent example. The aim is to provide wide-scale trustworthy and privacy-friendly digital identification. While pilot projects have proven the feasibility of IdM solutions, the challenge remains in widespread adoption. Technical functionality and high levels of security alone are insufficient adoption factors (cf. Attribute Based Credentials, German eID, PGP, etc.), as privacy-friendly solutions that lack explicit user consideration can result in unusable technology, hindering adoption and leading to misunderstandings as well as potential security or privacy issues. Oftentimes the solutions are not attractive to the user and therefore not adopted at all, as they are complicated to use and offer, albeit being privacy friendly, no other benefits.

Most users are lacking an intrinsic motivation to deal with security and privacy enhancing technologies [WT05], as they only seem to hinder them in their main goals which are usually to achieve a specific goal by using a service: buy new shoes, connect with friends, find the best Ramen restaurant in town, etc. Interaction patterns like login via Facebook (or similar) to access services are well-established, and apparently the perceived benefits for users outweigh the perceived risks, which can be observed from the huge success of such non-privacy friendly solutions. Digital identity wallets promise an easy way to have

[1] Fraunhofer IAO, Nobelstr. 12, Stuttgart, 70569, firstname.lastname@iao.fraunhofer.de

cbe doi: 10.18420/OID2023_03

a privacy preserving solution to identity management. However, if such alternative, privacy friendly solutions, require lots of work, learning of new interaction patterns or provide little perceived benefits, user will not adopt it. This is a major challenge that wallet bases solutions are facing today. Over the past years, we have conducted several studies and reviewed the literature, analyzing and evaluating the wallet-based identity approaches currently in development towards their practicality for end users. This paper summarizes our findings and gives an overview of the progress towards user-friendly digital identity wallets that balance security, privacy, and trust to foster trust and privacy relationships with other users or services. The goal is to enable the development of wallets that actually find widespread adoption as they cater to the needs of the users.

The remainder of the paper is structured as follows. In section two we present an overview of the state-of-the-art of the research on user experience of digital identity wallets. Following, we have identified several illustrative best and worst practices that are presented in section three. The findings of our analyses are compiled into design guidelines for digital identity wallets of the fourth section, five is a conclusion.

2 State-of-the-Art of User Experience Research

Overall, there is still limited research been published on the usability and user experience of identity management solutions. This is despite many solutions claiming to be user friendly and providing user centric solutions. However, usability and user experience has recently benefited from more user centric approaches, especially when it comes to digital wallets and digital governmental services. This section gives an overview of recent work.

2.1 Related Project Work

In the last few years, the authors have conducted user experience and usability research on digital identity wallets in various EU (e.g. DECIDE, MGOV4EU) and German National Projects (e.g. ONCE). First, the DECIDE project was funded by the EU Horizon 2020 NGI Trust Open Call[2]. Its goal was to conduct a study that analyzed and evaluated decentralized identity management technologies and their user experience for end users and service providers. In addition, a user-friendly prototype of a digital identity wallet was developed to enable users to make informed decisions considering security, privacy and trust, thus establishing trust and privacy relationships with other users or services. Throughout the wallet analysis, the development of a prototype, and various user tests, design guidelines were established for wallet solution developers and derive recommendations making decentralized identity management technologies valuable for service providers. Some of the results of this project have already been published at [Kh22].

[2] https://www.ngi.eu/funded_solution/ngi_trust1-48/

Second, the mGov4EU project[3] is funded by the EU Horizon 2020 program. It is a project focusing on creating a user centric solution for improving mobile governmental services in regard to eIDAS, SDG, and cross border scenarios. The project work that the authors conducted focused on qualitative work with end-users of mobile governmental services and digital wallets. In addition, the work included constructing usability and user experience requirements to be considered throughout the development of the project pilots. After conducting desk research and qualitative research, good practices were developed and published under [SHB22].

Lastly, the ONCE project[4] is funded by the German Federal Ministry for Economic Affairs and Climate Action and is one of the German Showcase Secure Digital Identities ("Schaufenster Sichere Digitale Identitäten") projects develop German digital identity solutions and various use cases for wallets. The project work conducted in this project by the authors include a focus on user experience research for the wallet and concrete private and public sector use cases. The research includes both qualitative and quantitative research with various types of users to gain greater insights on the necessary user experience and usability guidelines needed for digital wallets.

2.2 Relevant User Experience Studies

In the last couple of years there has been a few usability or user experience studies evaluating various digital identity wallets. This section highlights five of recent user studies. It emphasizes the methods used and their key findings.

[Sa22] presents a mixed methods approach of 60 interviews split between 4 SSI wallets, where they had users go through three different tasks. They discovered that participants scored the wallets low for novelty and stimulation. Further, participants demonstrated problems with the terminology used in the SSI wallets. From a privacy and security feature standpoint, the results show that users may not have realized that the wallet data is saved only on their phones. Lastly, users did not really understand what SSI was and therefore could possibly not judge or "appreciate the advantages".

[Kh22] completed a usability evaluation of 3 wallets that were chosen from a pool of 23 pre reviewed wallets that were decentralized identity solutions. The three wallets that were chosen were Connect.me, Jolocom, and uPortID. Applying a mixed methods approach 18 people were interviewed that had to complete 8 different tasks with the wallets. They find that end users are having challenges understanding the concept and the practical purpose of the technology. Moreover, lacking usability could hinder end users from experiencing and understanding the privacy and security benefits it would have.

[KP22] conducted a qualitative analysis with semi-structured interviews of 30 participants on topics of usability, privacy, and security. An own prototype was developed, and

[3] https://www.mgov4.eu
[4] https://once-identity.de

evaluated by the participants, after reviewing wallets by Connect.Me, uPort, Lissi, ShoCard, and SelfKey. Their main findings were that end users had problems understanding what "DIDs" are and related terminology. Furthermore, participants found QR codes (a key aspect of most wallet tasks) confusing. In addition, they suggest that when providing user error messages, having the messages in a simplified or less technical manner could lead to greater understanding. Overall, their self-proclaimed tech savvy participants stated that they are worried that there is still a learning curve for the current perception of a wallet. Regarding wallet backups, participants expected that the recovery of the wallet would be an automated basic feature. For privacy features, participants stated that they had a higher perception of privacy in situations where they were given the choice of which data to disclose or not. This was more so in comparison to when they were informed on technical components that improved their privacy.

[Za21] presents a usability assessment of the wallets by Connect.me, Jolocom, ShoCard, Trinsic, and uPort that finds two key issues. First, QR codes could lead to confusion or problems with end users. Second, they found the backup and recovery methods for the wallets to be a usability issue. Particularly the use of a seed phrase was a challenge.

[KP22] presents results of two user studies with a total of 16 participants that tested an operating wallet prototype. The participants completed 6 different tasks following the think aloud method. Participants found benefits in simplifying administrative processes and understood the ID process in the study. The results also showcase that user appreciated a simplistic design of the wallet prototype and found it easily understandable. Regarding data protection, approximately one third would do an extra step for increased data protection. Finally, users had concerns about losing their "wallet key" and the damage associated with losing control over their data and accounts managed though the wallet.

3 User Experience Best and Worst Practices

The following section aggregates the findings of the aforementioned literature and projects on user experience for digital identity wallets. In several projects over the last years we had performed user experience tests. There, we evaluated digital identity wallets available in smartphone app stores as well as prototypes with end users and experts. The derived best practices illustrate how certain challenges for digital identity wallets can be elegantly solved, while worst practices give concrete examples of pitfalls and how certain features should not be implemented. This is certainly not a complete list. A more comprehensive guideline follows then in section 4.

3.1 Five best practices in the design of digital wallets

The best practices may conflict with other requirements (privacy, security, interoperability, scalability, etc.) and must be weighed against them in the respective application scenario. Best practices present an ideal case while the technical state of the

art might restrict the ability to currently implement them. Hence, not all of they have been already implemented in wallets that are available in smartphone app stores.

1 **Automatic backup:** Regular backups should be performed once there have been changes made to the credentials stored in the wallet. Those are performed without the user having to initiate them each time manually – after he has enabled this function in the beginning. This enables restoration of credentials and accounts in case of lost or broken devices. It also frees users from mental load. The least would be frequent and visible reminders to perform a backup.

2 **User-friendly securing of the wallet and functions:** The wallet handles highly sensitive personal data and is the key to services that are important for the users. Reminding (or even forcing) the user to secure it via a sufficiently long passcode, ideally in combination with secure and user-friendly biometrics against unauthorized access, is a fundamental security requirement. Moreover, it emphasises towards the user the fact that it is important to protect the data and to be careful when handling it. As PIN-codes and passphrases are not particularly user-friendly, they should be complemented by biometrics. Moreover, a layered model of protection makes sense. Opening the wallet might be only protected by device biometrics while particularly sensitive functions, like resetting the wallet or displaying key phrases should be protected by wallet PIN.

3 **Simplistic and modern design:** The user studies showed that most users do not really care about identity management. They just want to access their services and get through the identity management process as quick as possible. A simplistic and modern design gives the user the impression that they are using a secure and modern tool that does what it should. It does not distract them; functions are easily reachable and recognizable.

4 **Quick launch of the application and overall responsiveness:** A wallet is "just" a tool that is standing between the users and the access to the services they want to actually use. Thus, launching the application navigating inside the application and performing actions with it should take as little time as possible. Delays annoy users as they keep them from reaching their actual goal. This is also related to "Simplistic and modern design" but must be emphasised.

5 **Tutorials or demos to educate users on the specifics of wallet-based identities:** The use of digital identity wallets with actions like the scanning of QR-codes to identify for digital services is new to users and differs from well-known interaction models like logging in with Facebook for websites. Hence, user should be made familiar with the wallet-based concept as well as the specific application and features through real world use cases presented in demos. Demo scenarios offered by the wallets engage users by relating to simplifying moments of their everyday life. However, user studies also made clear that only a smaller percentage of users take note of tutorials. The basic wallet functions should ideally be self-explanatory for users.

3.2 Seven worst practices in the design of digital wallets

The worst practices were found in wallet applications that were at a certain point of time available in the smartphone app stores and the respective wallets were marketed as "ready to use". It is certainly possible that these points have been resolved in the meantime by the vendors. Still, the worst practices are listed here in order to enable learning by others' mistakes.

1 **Use of technical language:** Credentials, Claims, DIDs and Seed Phrases are concepts that are not familiar for technically non-interested users and not understood by many average people. If there is both a backup and a recovery function offered – what is the difference between them? This would have to be explained. Many wallets display DIDs as issuers of credentials or in the history of interactions – but this is just some cryptic text for average users. The use of new terms and concepts can complicate the new digital wallet concept even further, discourage adoption and could even lead to user errors that might destroy the trust in a technically sound solution.

2 **Structuring the app according to the DID concept and not the established mental models of users:** Users are not (yet) familiar with the concept of Verifiable Credentials and the decentralized triangle of trust between issuers – users – verifiers. Some wallets have been hiding the credentials of users behind the "connections" from where those Verifiable Credentials originated. In theory, based on the SSI concept, this might make sense. It should not a big problem in practical use as credentials usually do not have to be manually found in the wallet in order to fulfil a claim. Still, this is not intuitive for users that open their wallet to look for their credentials. Moreover, some wallets are not offering a way to delete credentials. This does not create trust and made users in wallet studies think that their data might still be somewhere out there.

3 **Non-transparency - No explicit information for users on storage of data:** Even if the applications follow the SSI concept, sometimes data might be stored on central or cloud servers (e.g. for backups). However, solutions often not make this transparent. Some follow strictly the SSI concept and store everything only in the local wallet application. This confuses average users that are not sure where their data is actually saved and where they can/have to delete it if they want to. One wallet, for instance, gives information on whether the identity was backed up or not without providing necessary information on how and where it was backed up and how the user can manage her backed-up data.

4 **Little support to users:** The concept of SSI and wallet applications of this kind are new for must users. Only offering a brief tutorial at the first start of the app (that cannot be relaunched later), none or only brief descriptions in dialogues and menus as well as missing help sections / FAQs in the applications leaves users alone in a new field, leading to frustrations.

5 **No recoverability:** Most users expect that if they come into any problems (e.g., lose/break their phone), they can recover their digital credentials in a logical and easy

manner. Hence, users should be provided with a simple and familiar recovery process. In addition, users should have the choice between varying security and convenient options of recovery/ back up based on their preferences. If this is not possible, it must be made explicitly clear to the users. Offering recovery methods unfamiliar to users can be confusing and lead to further complications and errors in the use of the application. An example is the use of 12-word mnemonic phrases that were found to confuse many average users.

6 **No portability:** No wallet know to us has so far implemented an option for users to conveniently transfer all accounts and credentials to other wallets (neither on other phones for the same wallet or to wallets from other vendors). This is inconvenient and creates a lock-in that the SSI concept originally claimed to avoid.

7 **Backup[5] methods insufficiently implemented:** This point is related to the previous two points. Wallets are often not highlighting the importance of creating a backup. Moreover, an understanding of the different forms and functionalities, advantages, and disadvantages of types of backups (mnemonic phrase, cloud backup, local file etc.) is not created. In addition, in some wallets the only backup options were limited and not familiar to the user (mnemonic phrases). This could lead to users hesitating over the use of a backup or having feelings of confusion of where it was stored and how it works or why it is important. In the end, users don't feel confident that they can restore their account in case of loss.

4 Derived Design Guidelines

Building off the work presented in the previous sections, design guidelines for digital identity wallets were derived. The guidelines were developed in two iterations. First, a draft guideline was compiled, and the recommendations implemented in in a prototypical wallet in the DECIDE. Second, this wallet was tested in a user test to critically validate the guidelines. They were then developed further to incorporate the results of the user studies performed in the ONCE project to arrive at the final guidelines presented below.

The guidelines span four categories: User Experience, Security and Privacy, Identity Data Management, and User Interface. Alongside each guideline, there is a defined importance level following RFC2119 [Br97] given to reference the prioritization of the guideline.

[5] Digital wallets may choose to not include a backup or restore function by design (e.g. for security reasons), at the cost of potentially hindering user experience and adoption.

User Experience Design Guidelines		
No.	*Title*	*Description*
DG1	User Onboarding	Introduction to the basic concept and functionalities of a digital identity wallet or particularly important tasks (e.g., setting up a secret phrase) for users SHOULD be explained through a text and ideally a tutorial at the first start is included. It MUST be possible to skip the tutorial at the first start for experienced users. Moreover, this information (e.g., in the form of tutorial or a section that answers FAQs) SHOULD be accessible to users at any given time of using the application, e.g., in the form of a help button. Tutorial and/or FAQ-section SHOULD contain explanations of at least the following potentially new features (if available) to an average user: Backup function, Storage of personal data, Account elimination, Account restoration, Information about SSI/wallet concept, Secret Phrase
DG2	Use of understandable terms	Digital identity wallets MUST use terms that are understandable for an average user throughout the whole interaction. All terminology (labels, buttons, messages, etc.) MUST be understandable for users with little technical understanding and new to the topic of digital identity. This good practice does not only enhance usability, but also guarantees that no user group is excluded. This is particularly important to avoid the exclusion of certain groups of users affected by the digital divide (certain demographics, minorities, other disadvantaged groups).
DG3	Use of consistent terms	Terminology (labels, buttons, messages,..) MUST be applied consistently in all wallet functions and layers. This not only enhances usability, but also avoids user errors that might endanger security or privacy. It also refers to the consistent use of buttons and symbols throughout.
DG4	Interaction patterns	Users MUST be offered repeated and consistent interaction patterns for similar tasks (e.g., obtaining credentials, backing up data).
DG5	Customizability	There SHOULD be an option to customize the appearance/order of credentials (e.g., re-arrange, delete) in wallets. I.e., one customizable feature that COULD be introduced is an option to pin different documents or credentials to the home page or the top of the credentials page, which could be the most often used or the 'favourite' credentials of the user.
DG6	Simplicity of Use	Wallets SHOULD ensure that users have as few of steps as possible to complete a task or function. This contributes to the learnability of the tasks or functions completed with the wallet for users. According to [IW18] learnability is characterized by the user being empowered to easily learn, use and remember. For wallets, learnability means that users would easily learn how to use the app, not have any difficulties using it and finally, easily remember how to use the app or service or how to find certain information within the application. Applying this guideline improves adoption in the short term and leads to greater user acceptance and avoids user errors and, hence, security and privacy threats in the long term.

DG7	Help & feedback	This good practice implies offering a "helpdesk" for users that answers any questions that may arise in the user experience. Whenever the user is not able to proceed within the application, he or she MUST be able to get assistance. This assistance can be provided, e.g., by means of simple clickable "i" or "?" that provides the user with additional information. Feedback refers to patterns that inform the users about the status of the operations they are conducting. Such patterns include for example notifications or haptic output [HB11], [DF20]. However, feedback can also mean that the user provides feedback to the developer. Both help and feedback contribute to an enhanced user-friendliness.
DG8	Error handling	Wallets MUST hinder users to make mistakes for all predictable cases. However, they SHOULD not just block an operation. Instead, it should be explained to the user why an operation is not available at the moment (e.g., transferring a credential to a potentially malicious verifier). If there is an error, or the user makes a mistake, the wallets should provide clear and understandable cause, also giving the user clear instruction on how to fix it. It shows that there is a strong interdependency between error handling and feedback and therefore, both must be ensured.
DG9	Search & filter	As in any other application, there SHOULD be a way for the user to search for certain information, data or functionality through a search engine implemented in the application (one of six interaction design patterns defined by [HB11], [DF20]). Even if all good practices are fulfilled by the developer, some users might prefer to look for data through a search function instead of using other functionalities that are already there. Another add-on that comes along with that search function is a filter. Such a filter makes it much faster for users to find what they are looking for.
DG10	Operability	The user interface MUST be adaptive, so that content is presented to users in a high-quality way adjusted to the size of the device. Operability stands for (a) suitability for the device, and (b) conformity of the device with user expectation [IW17], [IW18]. This also touches a challenge arising from the huge variety of devices available on the market. This challenge requires that wallets are operable and supported by all (relevant) mobile devices available on the market. An example is to have a quick launch and responsibility of the application. An SSI wallet is "just" a tool that is used to access other services. Thus, launching the application and performing actions should take as little time as possible, as delays would annoy people as they keep them from reaching their actual goal.
DG11	Familiarity and Relatability	Demo scenarios offered by wallets SHOULD engage users by relating to moments of their everyday life and how a wallet could improve it. Thus, users understand and see the purpose of the digital wallets quickly.

Table 1:User Experience Design Guidelines

Security and Privacy Design Guidelines		
No.	*Title*	*Description*
DG12	Transparent information on data storage	Wallets MUST provide transparent and straightforward information of how and where the personal data of users is stored; who has the access to the data; how the data is encrypted and how it can be deleted.

DG13	Properly securing the wallet and functions	Wallets handle sensitive data and are the key to important services. Hence, they MUST remind (maybe even force) users to protect them via secure passcode/biometrics. This adds security: It emphasizes that it is important to protect the data stored in and managed through wallets and to be careful when handling it, sharing data and using other sensitive functions.

Table 2: Security and Privacy Design Guidelines

Identity Data Management Design Guidelines		
No.	*Title*	*Description*
DG14	User-friendly and transparent backup options	There MUST be several user-friendly options for backup and explanations of the implications of each form of backup. Moreover, wallets SHOULD include a certain flexibility and user control in regard to the backup function: e.g., keeping the 5 most recent automatic backups, manually deleting backups. The users MUST be educated by the wallet regarding the advantages and disadvantages of these different options.
DG15	Automatic Backup	One backup option MAY be an automatic backup function. Automatic backups SHOULD be performed once there have been changes to the credentials – without the user having to initiate them manually. This enables restoration of credentials and accounts in case of lost or broken devices. It also frees users from mental load.
DG16	Visible reminders to back up data	In case an automatic backup function is not active, users SHOULD receive frequent and visible reminders to use the backup function including explanation of its importance. If the reminders are deactivated, a warning with explanation SHOULD be displayed. There COULD be the option to customise the interval of reminders.
DG17	Portability of data across digital wallets	The backup function MAY also be combined with an "Export and Transfer" function to transfer credentials to other devices and wallets of other vendors (the latter would require a commonly accepted standard format). This would cover the important lack of portability of current solutions and fulfil a basic SSI claim. However realized, a convenient way to export and import data MUST be included in digital wallets. This could also be regarded a GDPR requirement.
DG18	Account elimination option	Wallets MUST include the option to delete an account in a straight-forward and uncomplicated manner explain to the user comprehensibly how her personal data and account can be deleted (e.g., by deleting all credentials and/or backups).
DG19	Adoption of user-friendly account recovery options	Wallets MUST offer user-friendly account recovery options that follow users' mental models. Digital wallets SHOULD explain to their users the importance of the recovery function in a clear manner.

Table 3: Identity Data Management Design Guidelines

User Interface Design Guidelines		
No.	*Title*	*Description*
DG20	Accessibility	The size of text MUST be adjustable. Wallets SHOULD have high contrast colors to allow good readability/accessibility for all users. Pictures, buttons, and icons used SHOULD be minimalistic and avoid misinterpretation or potential confusion.

DG21	Minimalistic and simple design	The wallet SHOULD have a minimalistic and simple design that allows users to focus on the important functions of services. Simplicity automatically increases accessibility, which means that no user groups are excluded because they lack certain capabilities. A simplistic and modern design signals to the users that they are using a secure and modern tool that does what it should. It does not distract them; functions are easily reachable; it is potentially even fun to use.
DG22	Placement of information	Users MUST always be clearly directed to the most important functionalities. the right placement of information within the application. It has been shown that a straight-forward layout and arrangement of instructions and functionalities is crucial for the usability of the service. Moreover, overlaps and replications of text and generally, large quantities of text should be avoided [KR19] [IW18], [DF20], [IW17], [CLH20].
DG23	Use of colors and icons	The "look and feel" of the application for the user MUST be as appealing as possible. Not only the wrong choice of colors can negatively impact users, but also the inconsistent use of logos or a corporate identity. Moreover, icons play an important role in the user experience. Well-designed and well-placed icons are beneficial. This is reflected in these empirical studies with citizens [IW18], [CLH20], [SHB18].

Table 4: User Interface Design Guidelines

5 Conclusion

Based on recent project work and published research on the user experience of digital identity wallets we have identified best and worst practices as well as derived user design guidelines. These results will play an important role for our ongoing work in the projects ONCE and mGOV4EU. Future work could further (re-)evaluate these best/worst practices alongside the quickly developing wallet market. This could include studies on the practices above to gain a deeper understanding of user mental models and requirements. One limitation of the current research on the user experience of digital identity wallets is that it is solely based on demo scenarios and proof of concepts. It is unclear how users really act when they handle their data in real services. Hence, with more wallets and actual real world use cases becoming available, the design guidelines could be developed further.

Bibliography

[Br97] Bradner, S.: Key words for use in RFCs to Indicate Requirement Levels. RFC Editor, 1997.

[CLH20] Chang, D.; Li, F.; Huang, L.: A User-centered Evaluation and Redesign Approach for E-Government APP: 2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE, 2020.

[DF20] da Silva, L. F.; Freire, A. P.: An Investigation on the Use of Interaction Design Patterns

in Brazilian Government Mobile Information Systems. Brazil, 2020.

[Eu22] European Commission: European Digital Identity. https://commission.europa.eu/strategy-and-policy/priorities-2019-024/europe-fit-digital-age/european-digital-identity_en, accessed 19 Aug 2022.

[HB11] Hoober, S.; Berkman, E.: Designing mobile interfaces: patterns for interaction design. 2011.

[IW17] Isagah, T.; Wimmer, M. A.: Mobile Government Applications: Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance. ACM, New York, NY, USA, 2017.

[IW18] Isagah, T.; Wimmer, M. A.: Addressing Requirements of M-Government Services. In (Kankanhalli, A.; Ojo, A.; Soares, D. Eds.): Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance. ACM, New York, NY, USA, pp. 599–608, 2018.

[Kh22] Khayretdinova, A. et al.: Conducting a Usability Evaluation of Decentralized Identity Management Solutions. In (Friedewald, M.; Kreutzer, M.; Hansen, M. Eds.): Selbstbestimmung, Privatheit und Datenschutz. Springer Fachmedien Wiesbaden, Wiesbaden, pp. 389–406, 2022.

[KP22] Kostic, S.; Poikela, M.: Do Users Want To Use Digital Identities? A Study Of A Concept Of An Identity Wallet. Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). USENIX Association, Boston, MA, pp. 195–211, 2022.

[KPD22] Korir, M.; Parkin, S.; Dunphy, P.: An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control. Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). USENIX Association, Boston, MA, pp. 195–211, 2022.

[KR19] Kureerung, P.; Ramingwong, L.: A Framework for Usability Design to Promote Awareness of Information Disseminated via Mobile Government Applications: 2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST). IEEE, 2019.

[Sa22] Sartor, S. et al.: Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets. 30th European Conference on Information Systems (ECIS), 2022.

[SHB18] Sellung, R.; Hölscher, M.; Burgstaller-Hochenwarter, L.: Good Practices of User Experience and Design Research for Mobile and Electronic Governmental Services. Springer, Cham, pp. 138–149, 2022.

[SHB22] Sellung, R.; Hölscher, M.; Burgstaller-Hochenwarter, L.: Good Practices of User Experience and Design Research for Mobile and Electronic Governmental Services. In (Kő, A. et al. Eds.): Electronic Government and the Information Systems Perspective. Springer International Publishing, Cham, pp. 138–149, 2022.

[WT05] Whitten, A.; Tygar, J. D.: "Why Johnny Can't Encrypt". Security, Nr. 1999, pp. 679–702, 2005.

[Za21] Zaeem, R. N. et al.: On the Usability of Self Sovereign Identity Solutions“, University of Texas at Austin Center for Identity, UTCID 21–02, 2021.