Vision: Towards True User-Centric Design for Digital Identity Wallets

Yorick Last
Paderborn University, Germany
ylast@mail.upb.de

Patricia Arias-Cabarcos
Paderborn University, Germany
pac@mail.upb.de

***Abstract*—To facilitate the growing demand for a universal means of digital identification across services, while preserving user control and privacy, multiple digital identity implementations have emerged. From a technical perspective, many of these rely on established concepts within cryptography, allowing them to provide benefits in terms of security and privacy. Recent legislation also promises broader recognition and acceptance of digital identities, both in the digital world and beyond. However, research into the usability, accessibility, and user understanding of digital identities is rare. We argue that the development of *usable* digital identity wallets is vital to the successful and inclusive application of digital identities in society. In this vision paper, we describe our research plans for obtaining a better understanding of how to develop these usable digital identities wallets.**

I. Introduction

As modern society further digitalizes, the ability to identify oneself digitally in a secure and private manner is essential. Over the past decades, various forms of digital identities have been developed to meet this need, serving purposes from replacing physical identity documents to providing alternatives to current online authentication methods. Digital identity management models (§ II) have evolved alongside the internet ecosystem, transitioning from centralized systems to federated identities, and now advancing towards decentralized and self-sovereign identities [1]. In this latest paradigm, user-facing implementations are envisioned as digital identity wallets, analogous to the physical wallets people use daily [2].

Identity wallets are apps designed not only to provide decentralized identity management but also to enhance security and privacy, addressing widespread issues such as identity theft [3], [4]. Importantly, they aim at empowering users by giving them control over their digital identities while offering an easy-to-use experience [1]. Wallets are a major leap forward in user-centric identity, currently being actively promoted and developed by multiple initiatives and entities.

One of the largest identity wallet initiatives globally is the recently proposed European Digital Identity Wallet (EUDIW) [5], [6], which intends to give the more than 400 million EU citizens access to a standardized digital identity for everyday interactions by 2026. This will facilitate a universal identity for authenticating to online services, sharing and signing documents, and accessing government services [7]. Pilots are currently exploring use cases involving digital driver's licenses, passports, social security access, bank account verification, and more [8]. This trend extends globally, with initiatives such as the United States' integration of state IDs into Apple and Google Wallet [9], [10], the UK's government-backed digital ID plans [11], and Australia's Trust Exchange (TEx) platform [12] through the myGov wallet [13]. These programs reflect a global move towards digital identity wallets.

The concept of user-centric identities through wallet-based interfaces is far from new, and previous large-scale attempts—such as Microsoft CardSpace in the mid-2000s [14]—failed to gain traction, with usability often cited as a primary barrier to success [1]. The workflows and technical skills required for these systems were neither familiar nor accessible to most users and developers. At that time, human-centered security methods and user research were rarely applied in this domain, and we still see limited research on the usability of identity wallets today (§ III). Furthermore, moving control (and potential burden) to users without proper interfaces can fail to provide meaningful protection—offering only an illusion of privacy, or "privacy theater" [15], [16]. Without a practical, user-friendly implementation, current identity wallet systems risk becoming overly complex, challenging secure adoption [17]–[20], and ultimately facing the same fate as their predecessors.

In this vision paper, we argue that for digital identity wallets to succeed in their mission of providing a *widely applicable*, *usable*, and *accessible* means of digital identification and authentication, intensive user-research is required. Specifically, we contend that previous solutions have been developed based on developers' assumptions of "user-friendliness" or "ease of use", but without considering the mental models of users with regard to digital identity. Being such a loaded and ambiguous term, our aim is to start from people's understandings: *What does digital identity mean to people? What does it mean to manage an identity digitally in 2025?* Only from this starting point can we assess if, and how, wallets can support users effectively. In this paper, we outline a plan to contribute to this

Symposium on Usable Security and Privacy (USEC) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-5-9
https://dx.doi.org/10.14722/usec.2025.23001
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

vision (§ IV), with the end goal of deriving a comprehensive set of usability and accessibility guidelines for usable and secure identity wallets.

II. Background

A. Digital identity & digital identity management systems

What exactly constitutes a digital identity is often unclear. There is no universal definition of a "digital identity" and the term often lacks conceptual clarity, necessitating legal and formal definitions [21]. However, what most definitions have in common is their description of digital identity as a set of attributes about a person that uniquely represent them in a digital context or transaction. For instance, ENISA defines *digital identity* as *"a unique representation of a subject engaged in an online transaction"* and *identity* itself as *"a set of attributes related to an entity"* [21], while NIST describes it as *"an attribute or set of attributes that uniquely describes a subject within a given context"* [22]. In this paper, we adopt this general understanding of digital identity as a collection of attributes used to identify or authenticate an individual in a digital environment.

Digital identities are managed using *identity management systems*: programs or frameworks that facilitate the collection, authentication, or use of identity and information linked to identity [23]. In its most simple form, identity management systems are run by organizations for their respective service(s) in a model referred to as *centralized identity management*. In this model, a single entity (e.g., a company or government organization) is responsible for managing and storing users' digital identities and authentication credentials. Advantages of this model include its simplicity and comparative ease of implementation. However, since identities are tied to a singular service, this requires users creating and managing identities for every service they use. Furthermore, when authentication for such services rely on mechanisms with known usability issues, such as passwords [24], these issues are compounded by the need to authenticate for every service used.

Federated identity management enables the use of an identity across multiple systems. This is possible by separating roles, with the Identity Provider (IdP) handling authentication and identity verification, and Service Providers (SPs) granting access to services based on IdP-issued credentials. Federated identity can be implemented using a variety of technologies, including notably SAML (Security Assertion Markup Language), OAuth [25], and OpenID [26]. Prominent examples of a federated identity management model are single sign-on (SSO) identity providers such as Google [27], Apple [28], and Facebook/Meta [29], which enable the use of Google/Apple/Facebook accounts for logging into different services such as websites and applications (aka "social login"). While perhaps more convenient to the user, this approach also comes with various security and privacy issues, as it is mostly implemented as IdP-centric. Current deployments enable increased user profiling by IdPs [30] and create a single point of failure that increases the impact of compromised login credentials [31], [32]. Additionally, since there is no universal IdP, the issue of having to log in to multiple IdPs remains.

Ideally, users should have the ability to control and oversee which information about their identity is shared with (and across) services. This concept, referred to as *user-centric identity* [31], [33], was first introduced as an improvement to federated identity management systems [1].

A further step towards increased control and privacy is through the model of *decentralized identity*. In contrast to federated identity management, there is no reliance on a central party to provide and manage verifiable identities in this model. Instead, technologies such as blockchain and distributed ledgers can be used to achieve verifiability without a central party [1], enabling the creation of *Self-Sovereign Identities (SSI)* [34].

B. The modern identity wallet

As identity models evolve towards a user-centric approach, the *digital identity wallet* emerges as a concept applicable to both fully and partially decentralized architectures. While there is no singular definition, digital identity wallets are commonly described as a collection of identity related data, somewhat analogous to a physical wallet, possibly stored on a device such as a smartphone [2]. In essence, this is like having the IdP functionality under user control. For example, in this paradigm, an identity issuing party (e.g., government organization) can issue attributes to a user such as their name, date of birth, or social security number. These attributes are then collected and stored inside the user's identity wallet. A service, for example a website wanting to verify the user's name, can then ask for these attributes. A visualization of this flow can be seen in Figure 1.

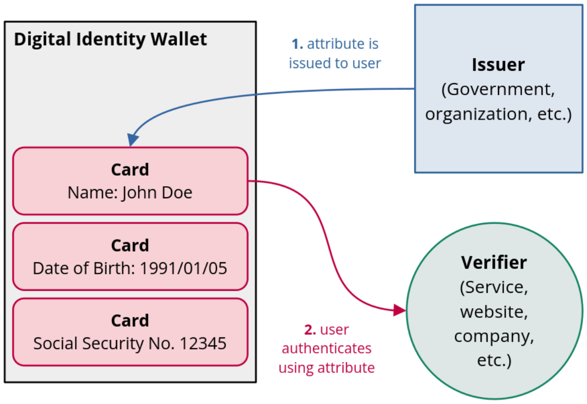
Digital Identity Wallet
1. attribute is issued to user
Issuer
(Government, organization, etc.)
Card
Name: John Doe
Card
Date of Birth: 1991/01/05
Card
Social Security No. 12345
2. user authenticates using attribute
Verifier
(Service, website, company, etc.)

Fig. 1. Example flow for a digital identity wallet. The processes of requesting identity attributes (1) and presenting identities to services (2) are independent and mediated by the user through the wallet interface.

One of the main proposed advantages of digital identity wallets is that of improved usability. By presenting identity information in a more structural, familiar manner, users should have less difficulty in understanding which identity information is contained within their wallet, and what information they share with other parties, increasing control and resulting in better privacy. However, these hypothetical usability and privacy improvements have not been proven in practice. Although identity wallets are receiving increased attention (through initiatives like the European Identity Wallet [5]), and are intended for global adoption, they are not yet widely deployed. We find important gaps in usability and accessibility research that need to be addressed for their effective deployment.

III. Related work

A. *On wallet usability*

Research into the *usability* of digital identity wallets is exceedingly rare. To our knowledge, Korir *et al.* [35] provide the first study examining the usability of an identity wallet. Through a user study of a prototype (decentralized) digital identity wallet with 30 participants, their work uncovers misunderstandings held by users about concepts such as digital identifiers. They also reveal issues with their setup reliant on QR-codes and multiple devices. Furthermore, they confirm the dominance of paper/card-based means of identity verification online, and issues that users have with such means (time needed to obtain/replace documents, likelihood of oversharing, etc.). This illustrates that digital identities indeed offer some real-world advantages compared to the current system. However, participants had mixed perceptions of the decentralized identity systems' security. Hence, a proper user understanding of the benefits and limitations is another point that should be addressed by (future) digital identity wallets.

Misunderstandings of digital identities and adjacent concepts can have a real impact on users security and privacy. In a recent study, Last *et al.* [19] develop and evaluate a prototype application for digitally signing documents using an identity wallet, one of the use cases for the EUDIW. The authors demonstrate that users' misunderstandings in such identity-based signatures can result in negative outcomes in terms of security. Here, participants choose to trust a digital signature based on a misunderstanding of the signature's guarantees and implications. This highlights the risk of identity wallets becoming a security theater, i.e., something that gives users the feeling of security without actually providing that (a term originally coined by Schneier [36]). This also applies to privacy [37], [38], where identity wallets could be (mis)used to give users a misplaced sense of privacy.

Surveys in both the United States and Europe have shown that users value their privacy and are concerned about the level of control over their data [39]–[42]. However, users also seem willing to sacrifice their privacy for relatively small gains, a phenomenon dubbed the "privacy paradox" [43], [44]. Teuschel *et al.* [45] present a study on designing privacy-preserving user interfaces for SSI wallets, showing users' tendency to trade personal data for convenience or other benefits. As the authors state, this could lead to a situation where identity wallets lead to users sharing more data than they would have without. This further highlights the importance of designing user interfaces that make users aware of the data being shared and the impact this may have on their privacy.

Designing user interfaces for identity wallets requires a trade-off between complexity and user understanding and control. For example, users can be given full control over what data is shared in each interaction (maximizing control), or only be presented with the data requested and asked for approval (maximizing simplicity). Presenting the user with an overwhelming number of controls may also cause further confusion, similar to the NASCAR problem seen in many SSO login UIs [46].

One approach (also referred to by Last *et al.* [19] and Teuschel *et al.* [45]) to getting users to adapt more secure behavior is through *security-enhancing friction*, a concept introduced by Distler *et al.* [47]. This involves moments of negative UX to slow down users and nudge them into making decisions better for security. Identity wallets could apply security-enhancing friction to encourage decisions that are better for security and privacy.

Current identity wallets (including pilots and prototypes) are generally designed for mobile devices and desktop/laptop computers. However, the emergence of new environments such as Virtual Reality (VR) and Augmented Reality (AR) may pose unique challenges for the adaptation of digital identity wallets for such platforms. Unlike conventional input methods, such as mouse/keyboard or touchscreen input, VR/AR may rely on motion controllers or gestures. This necessitates user interfaces that are intuitive and accessible for such platforms, which requires adherence to both general heuristics [48], and heuristics specific to VR/AR [49], [50]. If designed appropriately, identity wallets may be a more suitable alternative for identification and authentication in VR/AR than methods such as passwords which work best with traditional input methods.

B. *On wallet accessibility*

The lack of (consideration for) accessibility in software systems has been a long-standing problem, that has been given considerable attention in research. Such accessibility issues can stem from systems not providing a proper means of interaction for individuals with physical or cognitive disabilities, making such systems more difficult or impossible to use. While some strides have been made in improving usability for physical disabilities such as visual or auditory impairment, for example in use of devices such as smartphones [51], [52], these solutions are often far from perfect and aim to mitigate usability issues instead of pushing for the design of truly accessible technologies. Accessibility issues due to cognitive impairments have received less attention, although some accessibility tools [53] for cognitive impairments exist. This trend can also be observed in research, where most work focuses on visual impairments [54].

Although not assessing a digital *identity* wallet, but a crypto wallet, Zhou *et al.* [55] provides one of the first and few insights on the usability of such a wallet for those with visual impairments. The authors stress the connection between accessibility, usability, and security and the disproportionate impact that usability issues can have on users with a disability. Wallets that are inaccessible leave blind users prone to security misconceptions and vulnerabilities that stem from those misconceptions. Their work aims to gather experiences of blind users with current crypto wallets, and how such wallets can be made more accessible to blind users. The authors make use of user reviews and a usability study, and featured a redesign of an existing wallet based on gained insights. The authors find various accessibility issues in the existing wallet, such as unlabeled UI elements (buttons, input fields, etc.), lack of confirmations, and incompatibility with screen readers. Many of these issues were resolved through following best practices for accessible design, an approach that digital identity wallets should also take for this same reason.

For digital identity wallets to be truly universal, they need to be inclusive. Heath and Coles-Kemp [56] present a study of digital identity use by marginalized and underserved communities in the United Kingdom. More specifically, they explore the insecurities arising from pressure caused by digital exclusion when accessing digital services. Their method involves a thematic analysis of drawings made by researchers (referred to as "visual thematic mapping" by the authors) in online focus group settings. While the focus of their work is mostly on the development and (further) application of their methodology, they also identify worries concerning matters such as the management of digital identities on behalf of others (e.g., younger family member for older family members), and the sharing of identities among family members. This illustrates the need to look at digital identities from other perspectives than just the default use-case, and to consider ways in which assistance can be given to those that need it.

As we continue to push towards further digitalization of society, a growing number of individuals will be at risk of not fully being able to participate in society because of a lack of access certain technologies. This phenomenon is also referred to as *"digital exclusion"*. Especially in many societies that face aging populations (and thus an increased number of individuals with age-related disabilities), lacking accessibility of technologies vital to participation in society is likely to be an ever more pressing issue.

IV. Research Questions and Expected Contributions

As previously mentioned, our goal is to help pave the way for *usable* digital identities. Our research questions, and our expected contributions, are detailed in this section. A visualization of each research question, the methodology we plan on applying, and the expected contributions, can be found in figure 2.

A. (RQ1) How do users view and understand digital identities?

In order to design digital identity wallets that allow users to understand the information contained within, the details and consequences of the data shared during use, and the potential benefits and limitations, we first need to understand the extent to which users understand the concept of a digital identity. Our aim is to look into user understanding and underlying mental models [57] of both the concepts surrounding digital identity wallets, and the implementations thereof (notably, that of digital identity wallets such as those proposed as part of the EUDI). This also includes examining the extent to which the current concept of digital identity (as used by current implementations of identity wallets) corresponds to that of actual users. We also want to consider the social aspect of digital identities: how does this work in social groups such as families where identities (or at least credentials) need to be shared, or where older or younger family members may need assistance with managing their online identity.

	RQ1	RQ2
Description	How do users **view** and **understand** digital identities?	How can digital identity wallets be **designed** for **usability** and **accessibility**?
Methodology	• Surveys/questionnaires • Interviews • Focus groups	• Prototyping • User research
Contribution	Insights into: • **meaning** of digital identity to users • understanding of **benefits** and **limitations** • user **values**, **trust**, and **concerns** • **mental models** surrounding digital identity	• Design guidelines for **usable** digital identity wallets • **Usability assessments** of digital identity wallet products, prototypes, and pilots

Fig. 2. Visualization of research questions, methodology, and contributions.

In addition, our aim is to explore the current state of acceptance within the general population for digital identities. For example, what are potential users attitudes towards the (further) deployment of such technologies in society? What type of identity data is considered appropriate for storing, sharing, etc., and in which contexts? In which situations do users trust/distrust these technologies? Better understanding the values, viewpoints, and potential worries when it comes to digital identities may help create strategies to increase adoption once these technologies become more widely available.

We plan on employing a mix of qualitative and quantitative methods, and gathering data using surveys/questionnaires, interviews, and focus groups. All three of these revolve around gathering insights from different groups on the concept, use, values, and concerns surrounding digital identity wallets. Examples of such groups include general population users, groups of users with various disabilities, and groups (at risk of) facing digital exclusion. In regard to mental models, we plan on using semi-structured interviews combined with drawing techniques similar to other work on mental models. In short, participants will be asked to visualize concepts by means of drawings. These drawings are then analyzed by the researchers using, for example, thematic analysis or other qualitative research methods.

Answering this research question would not only result in some of the first research on user understanding of identity wallets, but will also help us shape guidelines on how to effectively communicate the process of storing, managing, and sharing digital identity data. Identity wallets that more effectively communicate the concepts, surrounding processes, and implications of digital identities can then allow users to make more informed decisions on (the sharing of) their digital identity.

B. (RQ2) How can digital identity wallets be designed for usability and accessibility?

Our second research question focuses on the design of *usable* and *accessible* of digital identity wallets. RQ1 serves as a basis for creating guidelines to design digital identity wallets that users can understand, which will be extended with research on usability in the form of prototyping and user studies. Answering this research question starts by exploring (existing) usability challenges in digital identity wallets, and how these can be overcome through better user interface design. Besides the design of the wallet itself, the interface used by issuers of attributes (e.g., a government organization issuing a name or date of birth), or services verifying attributes (e.g., a service verifying one's name and age) should be taken into consideration. This requires performing users studies with both the wallets themselves and such interfaces that facilitate their usage.

For *accessibility*, we plan to follow a similar approach. This again starts by exploring any accessibility challenges for digital identities through prototyping and user studies. As we have argued before, for a technology that is positioned to take an ever more prominent role in society it is vital that said technology is usable by all members of society. Given the broad nature of accessibility, our focus will lie mainly on the usability of hardware and software used in digital identity wallets, for those with physical and cognitive disabilities. Therefore, our goal is to include participants with such disabilities, including (but not limited to) individuals with visual impairments, disabilities that prevent typical use of devices such as smartphones, and age-related cognitive decline.

Prototypes will be developed using an iterative approach, making use of expert reviews (e.g., in the form of heuristic evaluations by external experts) and using participatory design (e.g., in the form of co-design). By following this approach, we are able to develop and validate our recommendations based on real-world, practical findings. Unlike a solely theoretical approach, this also allows us to optimize the process of developing (applications for) a digital identity wallets using our guidelines.

Our research will be among the first works to explore the accessibility of digital identity wallets. While guidelines for designing accessible software in general are not new, guidelines specific to accessible digital identity wallets do not yet exist. We expect a large portion of these guidelines for software in general to also apply to digital identity wallets. Our work combines existing guidelines with new, verified, insights on the specific accessibility challenges for digital identities to better address them.

V. Conclusion

In this vision paper, we introduced our research plans for *usable digital identity wallets*. We detailed the history and current state of digital identities and digital identity wallets, and described their increase in prevalence due to various regulations and initiatives across multiple regions. However, we also noted the current lack of research into the usability and accessibility of digital identity wallets. Usability and accessibility issues arising from this gap may have negative consequences for the security and privacy offered by identity wallets. We've identified various usability and accessibility challenges that digital identities need to overcome. Our research aims not only to address these challenges, but also to provide a path towards secure, usable, and truly user-centric digital identity management. We believe such *usable* digital identity wallets have the potential to solve many usability issues surrounding current means of digital identity management, and empower users to make better informed decisions in regard to their digital identity.

Our contribution to this end consists of two parts. Firstly, our research will be among the first studies into usability, accessibility, and user understanding of digital identity wallets. Secondly, by developing comprehensive guidelines for the development of *usable* and *accessible* digital identities, we will be providing a clear and practical path for developers of digital identity wallets to ensure usability and accessibility. Our objective is to make security, privacy, usability, and accessibility integral parts of the development of identity wallets. In addition, we aim to provide feedback based on our work to relevant stakeholders.

With this vision paper, we hope to spark discussion with the usable privacy and security community on the challenges we have outlined, and the research we are proposing to better address them. We invite others to share their insights and perspectives, and look forward to the community's feedback.

References

[1] O. Avellaneda, A. Bachmann, A. Barbir, *et al.*, "Decentralized identity: Where did it come from and where is it going?" *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, 2019. DOI: 10.1109/MCOMSTD.2019.9031542.

[2] B. Podgorelec, L. Alber, and T. Zefferer, "What is a (digital) identity wallet? a systematic literature review," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2022, pp. 809–818. DOI: 10.1109/COMPSAC54236.2022.00131.

[3] P. Security, *31 alarming identity theft statistics for 2024*, Accessed: 2024-11-08, 2024. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/identity-theft-statistics/.

[4] OWASP Foundation, *Owasp top ten*, Accessed: 2024-11-08, 2021. [Online]. Available: https://owasp.org/www-project-top-ten/.

[5] European Commission. “EU digital identity wallet.” (), [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home (visited on 10/25/2024).

[6] European Commission. “European Digital Identity.” (), [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity%5C_en (visited on 08/28/2024).

[7] European Commission. “What is the wallet — EU digital identity wallet.” (), [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+wallet (visited on 11/06/2024).

[8] European Commission. “The many use cases of the EU digital identity wallet — EU digital identity wallet.” (), [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+many+use+cases+of+the+EU+Digital+Identity+Wallet (visited on 11/06/2024).

[9] Apple. “Apple brings California driver’s licenses and state IDs to Apple Wallet,” Apple Newsroom. (Sep. 19, 2024), [Online]. Available: https://www.apple.com/newsroom/2024/09/apple-brings-california-drivers-licenses-and-state-ids-to-apple-wallet/ (visited on 11/14/2024).

[10] Google. “Store Your Digital ID on Your Phone — Google Wallet,” Google Wallet: Carry more with Google Wallet. (), [Online]. Available: https://wallet.google/digitalid/ (visited on 11/14/2024).

[11] Office for Digital Identities and Attributes and Department for Science, Innovation and Technology. “Enabling the use of digital identities in the UK,” GOV.UK. (Nov. 1, 2024), [Online]. Available: https://www.gov.uk/guidance/digital-identity (visited on 11/14/2024).

[12] Oliver Gordon, “How the government’s proposed ’trust exchange’ digital ID scheme would work,” *ABC News*, Aug. 13, 2024. [Online]. Available: https://www.abc.net.au/news/2024-08-13/trust-exchange-digital-identity-how-does-it-work/104218958 (visited on 11/14/2024).

[13] Australian Government. “Using the myGov app,” myGov. (), [Online]. Available: https://my.gov.au:443/content/mygov/en/about/help/mygov-app/using-the-mygov-app.html (visited on 11/14/2024).

[14] V. Bertocci, G. Serack, and C. Baker, *Understanding Windows CardSpace: An Introduction to the Concepts and Challenges of Digital Identities*. Upper Saddle River, NJ: Addison-Wesley Professional, 2008, ISBN: 978-0321496843.

[15] M. A. Smart, D. Sood, and K. Vaccaro, “Understanding risks of privacy theater with differential privacy,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, pp. 1–24, 2022.

[16] M. Fassl, L. T. Gröber, and K. Krombholz, “Stop the consent theater,” in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–7.

[17] A. Whitten and J. D. Tygar, *Usability of security: A case study*, 1998.

[18] K.-P. Yee, “Aligning security and usability,” *IEEE Security & Privacy*, vol. 2, no. 5, pp. 48–55, Sep. 2004, Conference Name: IEEE Security & Privacy, ISSN: 1558-4046. DOI: 10.1109/MSP.2004.64. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1341409.

[19] Y. Last, J. Geels, and H. Schraffenberger, “Digital dotted lines: Design and evaluation of a prototype for digitally signing documents using identity wallets,” in *Extended Abstracts of the 2024 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA ’24, New York, NY, USA: Association for Computing Machinery, 2024, ISBN: 9798400703317. DOI: 10.1145/3613905.3650977. [Online]. Available: https://doi.org/10.1145/3613905.3650977.

[20] Z. Zhou, T. Sharma, L. Emano, S. Das, and Y. Wang, “Iterative design of an accessible crypto wallet for blind users,” presented at the Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), 2023, pp. 381–398, ISBN: 978-1-939133-36-6. [Online]. Available: https://www.usenix.org/conference/soups2023/presentation/zhou.

[21] European Union Agency for Cybersecurity, I. Alamillo, S. Mouille, *et al.*, *Digital identity standards – Analysis of standardisation requirements in support of cybersecurity policy – July 2023*. European Union Agency for Cybersecurity, 2023. DOI: doi/10.2824/28598.

[22] D. Temoshok, D. Proud-Madruga, Y.-Y. Choong, *et al.*, “Digital identity guidelines,” National Institute of Standards and Technology, NIST Special Publication (SP) 800-63-4 (Draft), Aug. 21, 2024. DOI: 10.6028/NIST.SP.800-63-4.2pd. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/63/4/2pd (visited on 10/23/2024).

[23] M. Hansen, A. Schwartz, and A. Cooper, “Privacy and identity management,” *IEEE Security & Privacy*, vol. 6, no. 2, pp. 38–45, 2008. DOI: 10.1109/MSP.2008.41.

[24] M. Yıldırım and I. Mackie, “Encouraging users to improve password security and memorability,” *International Journal of Information Security*, vol. 18, no. 6, pp. 741–759, Dec. 1, 2019, ISSN: 1615-5270. DOI: 10.1007/s10207-019-00429-y. [Online]. Available: https://doi.org/10.1007/s10207-019-00429-y.

[25] “OAuth 2.0 — OAuth.” (), [Online]. Available: https://oauth.net/2/ (visited on 10/23/2024).

[26] OpenID Foundation. “OpenID.” (), [Online]. Available: https://openid.net/ (visited on 10/23/2024).

[27] Google. “Google identity,” Google for Developers. (), [Online]. Available: https://developers.google.com/identity (visited on 10/23/2024).

[28] Apple. “Sign in with apple,” Apple Developer. (), [Online]. Available: https://developer.apple.com/sign-in-with-apple/ (visited on 10/23/2024).

[29] Meta. “Overview - facebook login - documentation,” Meta for Developers. (), [Online]. Available: https://developers.facebook.com/docs/facebook-login/overview/ (visited on 10/23/2024).

[30] F. Karegar, N. Gerber, M. Volkamer, and S. Fischer-Hübner, “Helping john to make informed decisions on using social login,” in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, ser. SAC ’18, New York, NY, USA: Association for Computing Machinery, Apr. 9, 2018, pp. 1165–1174, ISBN: 978-1-4503-5191-1. DOI: 10.1145/3167132.3167259. [Online]. Available: https://dl.acm.org/doi/10.1145/3167132.3167259.

[31] E. Maler and D. Reed, “The venn of identity: Options and issues in federated identity management,” *IEEE Security & Privacy*, vol. 6, no. 2, pp. 16–23, Mar. 2008, Conference Name: IEEE Security & Privacy, ISSN: 1558-4046. DOI: 10.1109/MSP.2008.50. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4489845 (visited on 10/23/2024).

[32] Y. Dimova, T. Van Goethem, and W. Joosen, “Everybody’s looking for ssomething: A large-scale evaluation on the privacy of oauth authentication on the web,” *Proceedings on Privacy Enhancing Technologies*, 2023.

[33] D. Recordon and D. Reed, “OpenID 2.0: A platform for user-centric identity management,” in *Proceedings of the second ACM workshop on Digital identity management*, ser. DIM ’06, New York, NY, USA: Association for Computing Machinery, Nov. 3, 2006, pp. 11–16, ISBN: 978-1-59593-547-2. DOI: 10.1145/1179529.1179532. [Online]. Available: https://dl.acm.org/doi/10.1145/1179529.1179532.

[34] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, “A survey on essential components of a self-sovereign identity,” *Computer Science Review*, vol. 30, pp. 80–86, Nov. 1, 2018, ISSN: 1574-0137. DOI: 10.1016/j.cosrev.2018.10.002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013718301217.

[35] M. Korir, S. Parkin, and P. Dunphy, “An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control,” in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston, MA: USENIX Association, Aug. 2022, pp. 195–211, ISBN: 978-1-939133-30-4. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/korir.

[36] B. Schneier, *Beyond fear : thinking sensibly about security in an uncertain world*. New York, NY : Copernicus Books, 2003, ISBN: 0387026207.

[37] G. Edelman. “Google and the age of privacy theater.” (), [Online]. Available: https://www.wired.com/story/google-floc-age-privacy-theater/ (visited on 11/18/2024).

[38] M. A. Smart, D. Sood, and K. Vaccaro, “Understanding risks of privacy theater with differential privacy,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, pp. 1–24, CSCW2 Nov. 7, 2022, ISSN: 2573-0142. DOI: 10.1145/3555762. [Online]. Available: https://dl.acm.org/doi/10.1145/3555762 (visited on 11/18/2024).

[39] M. Madden. “Public perceptions of privacy and security in the post-snowden era,” Pew Research Center. (Nov. 12, 2014), [Online]. Available: https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/ (visited on 11/20/2024).

[40] B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Turner. “Americans and privacy: Concerned, confused and feeling lack of control over their personal information,” Pew Research Center. (Nov. 15, 2019), [Online]. Available: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-

feeling-lack-of-control-over-their-personal-information/ (visited on 11/20/2024).

[41] C. McClain, M. Faverio, M. Anderson, and E. Park. “How americans view data privacy,” Pew Research Center. (Oct. 18, 2023), [Online]. Available: https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ (visited on 11/20/2024).

[42] European Union Agency for Fundamental Rights., *Your rights matter: data protection and privacy : fundamental rights survey.* LU: Publications Office, 2020. [Online]. Available: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection (visited on 11/20/2024).

[43] P. A. Norberg, D. R. Horne, and D. A. Horne, “The privacy paradox: Personal information disclosure intentions versus behaviors,” *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007, ISSN: 1745-6606. DOI: 10.1111/j.1745-6606.2006.00070.x. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2006.00070.x (visited on 11/20/2024).

[44] N. Gerber, P. Gerber, and M. Volkamer, “Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior,” *Computers & Security*, vol. 77, pp. 226–261, Aug. 1, 2018, ISSN: 0167-4048. DOI: 10.1016/j.cose.2018.04.002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404818303031 (visited on 11/20/2024).

[45] M. Teuschel, D. Pöhn, M. Grabatin, F. Dietz, W. Hommel, and F. Alt, “'don't annoy me with privacy decisions!' — designing privacy-preserving user interfaces for SSI wallets on smartphones,” *IEEE Access*, vol. 11, pp. 131 814–131 835, 2023, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2023.3334908. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10323303 (visited on 11/20/2024).

[46] “NASCAR problem,” IndieWeb. (), [Online]. Available: https://indieweb.org/NASCAR_problem (visited on 11/20/2024).

[47] V. Distler, G. Lenzini, C. Lallemand, and V. Koenig, “The framework of security-enhancing friction: How UX can help users behave more securely,” in *Proceedings of the New Security Paradigms Workshop 2020*, ser. NSPW '20, New York, NY, USA: Association for Computing Machinery, Jan. 28, 2021, pp. 45–58, ISBN: 978-1-4503-8995-2. DOI: 10.1145/3442167.3442173. [Online]. Available: https://dl.acm.org/doi/10.1145/3442167.3442173 (visited on 11/21/2024).

[48] A. Joyce. “10 usability heuristics applied to virtual reality,” Nielsen Norman Group. (), [Online]. Available: https://www.nngroup.com/articles/usability-heuristics-virtual-reality/ (visited on 11/21/2024).

[49] S. M. Ko, W. S. Chang, and Y. G. Ji, “Usability principles for augmented reality applications in a smartphone environment,” *International Journal of Human–Computer Interaction*, vol. 29, no. 8, pp. 501–515, Aug. 3, 2013, ISSN: 1044-7318. DOI: 10.1080/10447318.2012.722466. [Online]. Available: https://doi.org/10.1080/10447318.2012.722466 (visited on 11/21/2024).

[50] R. Murtza, S. Monroe, and R. J. Youmans, “Heuristic evaluation for virtual reality systems,” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 61, no. 1, pp. 2067–2071, Sep. 1, 2017, Publisher: SAGE Publications Inc, ISSN: 1071-1813. DOI: 10.1177/1541931213602000. [Online]. Available: https://doi.org/10.1177/1541931213602000 (visited on 11/21/2024).

[51] Apple. “Accessibility.” (), [Online]. Available: https://www.apple.com/accessibility/ (visited on 11/12/2024).

[52] Google. “Android accessibility.” (), [Online]. Available: https://www.android.com/accessibility/ (visited on 11/12/2024).

[53] Apple. “Accessibility — cognitive.” (), [Online]. Available: https://www.apple.com/accessibility/cognitive/ (visited on 11/12/2024).

[54] D. M. B. Paiva, A. P. Freire, and R. P. de Mattos Fortes, “Accessibility and software engineering processes: A systematic literature review,” *Journal of Systems and Software*, vol. 171, p. 110 819, Jan. 1, 2021, ISSN: 0164-1212. DOI: 10.1016/j.jss.2020.110819. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0164121220302168 (visited on 11/13/2024).

[55] Z. Zhou, T. Sharma, L. Emano, S. Das, and Y. Wang, “Iterative design of an accessible crypto wallet for blind users,” in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, Anaheim, CA: USENIX Association, Aug. 2023, pp. 381–398, ISBN: 978-1-939133-36-6. [Online]. Available: https://www.usenix.org/conference/soups2023/presentation/zhou.

[56] C. P. R. Heath and L. Coles-Kemp, “Drawing out the everyday hyper-[in]securities of digital identity,” in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI '22, New Orleans, LA, USA: Association for Computing Machinery, 2022, ISBN: 9781450391573. DOI: 10.1145/3491102.3501961. [Online]. Available: https://doi.org/10.1145/3491102.3501961.

[57] D. Jonassen and Y. H. Cho, “Externalizing mental models with mindtools,” *Understanding models for learning and instruction*, pp. 145–159, 2008.