IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 October 2023, accepted 12 November 2023, date of publication 20 November 2023,
date of current version 29 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3334908

RESEARCH ARTICLE

'Don't Annoy Me With Privacy Decisions!' – Designing Privacy-Preserving User Interfaces for SSI Wallets on Smartphones

MORITZ TEUSCHEL[1], DANIELA PÖHN[2], MICHAEL GRABATIN[2], FELIX DIETZ[2], WOLFGANG HOMMEL[2], AND FLORIAN ALT[2]

[1]Ludwig-Maximilians-Universität München, 80539 Munich, Germany
[2]RI CODE, University of the Bundeswehr Munich, 85579 Neubiberg, Germany

Corresponding author: Daniela Pöhn (daniela.poehn@unibw.de)

ABSTRACT Persistent digital identities allow individuals to prove who they are across the Internet. For decades, individuals have relied on large identity providers (for example, Google and Facebook). In recent years, the advent of so-called self-sovereign identities (SSI) has increasingly been approved by national governments. This decentralized approach provides users with a way to maintain control over the information associated with their identities. Yet, the design of these wallets to enable users to act in a privacy-preserving manner when sharing data with requesting services remains an open question. Based on a qualitative pre-study, we chart the design space for privacy-preserving user interfaces for SSI wallets and explore several designs to understand user adoption and decision-making processes. A qualitative user study (N=16) based on realistic scenarios revealed that while the proposed designs generally increase privacy awareness, participants trade data for convenience. Our study is complemented by guidelines for designers of future user interfaces for smartphone SSI wallets.

INDEX TERMS Awareness, data sharing, privacy, self-sovereign identity, SSI, visualization.

I. INTRODUCTION

For many decades, persistent digital identities, which are information used by individuals to prove who they are on the Internet, have been issued by large identity providers, such as Facebook (Facebook Connect) and Google (Google Sign-In) [1]. These identity providers store data on servers and manage it centrally. However, central management can lead to potential misuse, as demonstrated by the Cambridge Analytica scandal [2]. In addition, these identity providers can aggregate large amounts of data, such as which service is used and when. The concentration of only a few identity providers is also problematic if accounts are taken over by, for example, a successful phishing attack [3].

More recently, self-sovereign identities (SSI) [4], [5] have been moving into focus. Individuals thereby receive control over the information associated with their identities. Rather than using central storage, SSI implementations utilize so-called wallets [6] on smartphones or computers. This approach has rapidly gained popularity, as demonstrated by the European Union's (EU) plan for the new electronic Identification, Authentication, and trust Services (eIDAS) regulation. eIDAS 2.0 uses a digital ID wallet, allowing citizens to save their documents and personal information, including the official eID, in a wallet app. In eIDAS, the eID should be usable across all member states [7]. To apply SSI, the user, also called *holder*, receives identity information from at least one *issuer* (a home organization, such as the EU) in their wallet. These so-called *verifiable credentials (VCs)* [8] are then transmitted anonymously, or at least pseudonymously, from the holder to the *verifier*, i. e., the service provider (for example, a webshop or a local authority). Each entity within the SSI ecosystem is represented by decentralized identifiers (DIDs) with a data

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

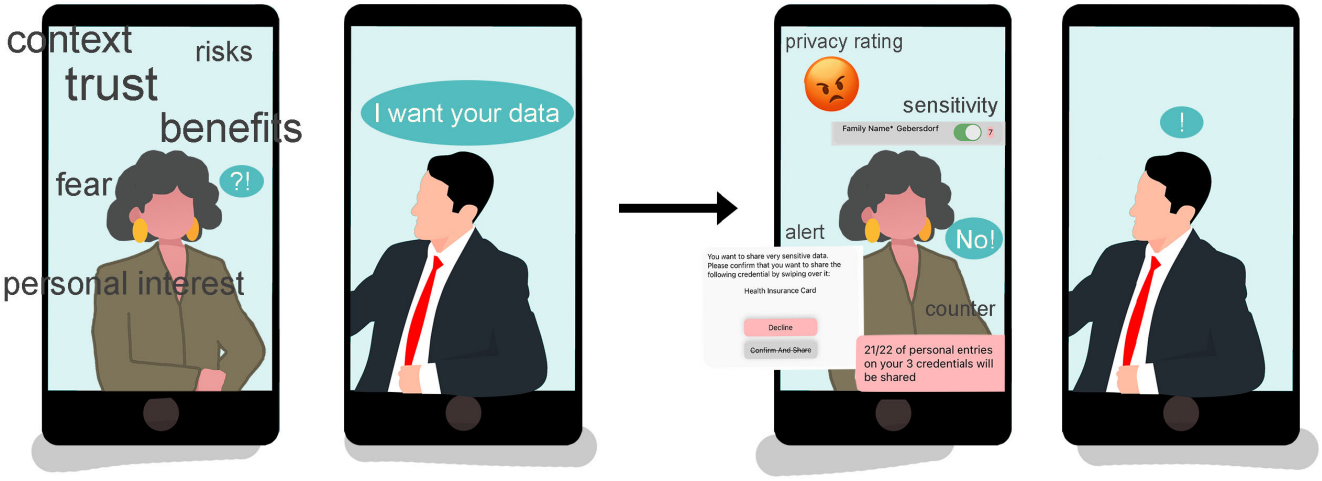


FIGURE 1. In this paper, we explore factors supporting users' decision to disclose personal data when using wallets to manage self-sovereign identities (SSI). In particular, we chart a design space for awareness designs and compare different design concepts to assist people in making privacy-preserving decisions.

set described by a DID document [9]. DID documents are typically stored in decentralized storage, such as blockchains, distributed ledgers, or decentralized networks [10].

As the complexity of the underlying structures makes it difficult for users to handle them, they are hidden by wallet implementations. At the same time, the implementations of these early-stage SSI wallets still face many unsolved challenges [11], particularly regarding the user interface. Even though they provide more convenience to users than conventional solutions, they also require high responsibility from individual users. With SSI, users must handle and manage their data instead of only consenting to its release. Therefore, it is not only the company's but also the users' responsibility to protect their privacy. Consequently, users must be aware of their data and privacy to protect them. The wallet design is essential as users use wallets to manage their data. To support the design of future user interfaces for mobile SSI wallets, our exploratory research was driven by the following five research questions.

- RQ1: Are users willing to adopt mobile SSI as a new identity management concept?
- RQ2: What is the users' understanding of the underlying SSI paradigm? How does it influence their actions?
- RQ3: How can users be supported in making responsible use of their data using mobile SSI wallets?
- RQ4: How can users be made aware of the sensitivity of their data?
- RQ5: How can the design of the mobile user interface help users make privacy-preserving decisions?

We believe that the user interface plays an important role in this regard. However, designing such an interface presents several challenges. Hence, the question is whether users will eventually be willing to spend more time controlling their shared data if this leads to more privacy. Based on the findings of a qualitative pre-study, we explore the design space of user interfaces for mobile SSI wallets that increase privacy awareness (see Fig. 1). A qualitative user study (N=16) with real-world scenarios reveals that privacy-aware designs can indeed increase the user's privacy concern and influence data-sharing behavior to some extent. Moreover, it shows that trust in the entity is essential for the participants and that other benefits, such as convenience, may be more important in some scenarios. Our work is complemented by reflecting on how the designs influence users' understanding of SSI wallets and behavior in different application scenarios.

The *contribution* of our work is threefold: First, based on related work, a study of SSI wallets, and a pre-study, we chart a design space and identify privacy-enhancing features for the design of mobile SSI wallets. Second, we implement and evaluate different wallet designs, exploring users' behavior regarding privacy-preserving data management. Third, we provide lessons learned and discuss how our findings can support designers of future user interfaces for SSI wallets.

The remainder of this article is organized as follows. We outline related work in Section II. Then, in Section III, we define the terminology applied in this article and compare different real-world SSI wallets. The research approach is described in Section IV. The research approach is used in the pre-study (see Section V) and in the main user study (see Section VII). The results of the pre-study result in the design space (see Section VI), which is applied in the user study to determine whether awareness designs can support users' decisions. Finally, we discuss our approach in Section VIII.

II. RELATED WORK

Our work draws from prior research on privacy and privacy-enhancing designs (Section II-A) and SSI (Section II-B). We briefly summarize the need for our study in Section II-C.

A. PRIVACY AND PRIVACY-ENHANCING DESIGNS

Large identity providers issue increasingly persistent digital identities while storing and managing data centrally. Although the log-in is convenient, business models based on the collection and use of data may not be in the interest of users, and central management enables misuse. According to Statista, the number of daily active Facebook users worldwide has increased yearly since 2011 despite the Cambridge Analytica scandal [12]. Furini et al. [13] argue that this may be due to users not knowing about their data being used. Another possibility is the existence of the privacy paradox. The privacy paradox [14] explains that people disclose more personal information in real scenarios than they admit. Smith et al. [15] highlight the importance of considering the privacy paradox when conducting research in information security. They argue that studies often explore users' intentions instead of their behaviors or actual outcomes. In addition, Hui et al. [16] support the theory that people make risk-benefit trade-offs for privacy.

Pötzsch [17] explains the privacy paradox, such as misconceptions and a lack of stimuli signalizing risks. She also names privacy awareness as a solution to ''remind people about their intentions to protect privacy''. Distler et al. [18] provides a collection of security-enhancing designs, including nudging, and compares them to their newly introduced term security-enhancing friction. According to Acquisti et al. [19], nudging acknowledges that users can be affected by differences in the system design. This means that nudging can influence users to take a certain action, for example, by using Gestalt principles. One difficulty in showing warnings of any kind is the so-called ''warning fatigue''. According to Mackie, warning fatigue can result from being ''over-warned'' [20]. To address this issue, information on how to protect against the threat should be included. Cranor supports this finding [21]. Warning fatigue could mitigate our attempts to support privacy-preserving decisions. Hence, using polymorphic dialogues [22] or habituation-resistant warnings [23] could be necessary. These designs are more resistant to the mentioned fatigue and maintain their effects over a longer period of time. However, Bravo-Lillo et al. also describe the usability burden that can result from such designs. According to Renaud and Dupuis [24], fear may scare people into performing certain actions. However, there is dissent on the method's effectiveness.

B. SELF-SOVEREIGN IDENTITIES AND WALLETS

Initially, the principles of SSI were identified by Allen [25]. Many of the ideas presented regarding SSI are proposals for future vision. Nonetheless, it seems the community has already agreed on many principles and developed prototypes, such as Lissi [26] or esatus [27], that adhere to those. Section III-B compares the wallets by Lissi and esatus with other wallets on the market.

Liu et al. [28] list twelve design patterns, explaining how SSI works without describing the UI and its effects. SSI and corresponding implementations in the form of wallets fulfill all seven principles of privacy by design according to Cavoukian [29]. Gürses and Pridmore [30] differentiate three different proposals to maintain privacy in systems design. One of these, preemption, can be achieved with SSI by using different DIDs for different entities and using DID rotation. Kondova and Erbguth [31] analyze existing SSI approaches on blockchain on General Data Protection Regulation (GDPR)-compliance, whereas Nokhbeh Zaeem et al. [32] compare solutions with gathered requirements.

Although several authors have analyzed and designed SSI approaches, few studies have focused on the user. The wallets in other use cases were studied in more detail. Sukaris et al. [33] and Arindy and Suzianti [34] evaluate the perception of wallets. Yong Lee et al. [35] notice an effect of enjoyment and satisfaction on impulsive buying behavior. Similarly, Voskobojnikov et al. [36] reveal shortcomings of current wallet user experiences and users' misconceptions, which could lead to financial losses. Abramova et al. [37] analyze risk perceptions and security behavior to better understand users' characteristics. Fröhlich et al. investigate custodial wallets for cryptocurrencies [38]. They found that novice users struggle with their use, as user interfaces are primarily designed for experts.

C. SUMMARY

Current SSI research is mostly theoretical, see [39], [40], [41], [42], [43], and [44]. A user-centric approach is often assumed to lead to better protection of users' privacy, but there is hardly any supporting evidence. Several privacy-enhancing designs have been proposed and tested so far, although not for SSI wallets. First insights into crypto wallets suggest that these are currently not very usable in everyday scenarios [36]. This may also be the case for mobile SSI wallets. However, this requires further research as digital identity differs from crypto money. To do so, our research explores privacy and privacy-aware designs for mobile SSI wallets, thereby shedding light on the so-far unanswered research questions RQ1–RQ5.

III. BACKGROUND ON SELF-SOVEREIGN IDENTITIES

We provide a brief background on SSI by defining the terminology applied in this article and comparing SSI wallets.

A. TERMINOLOGY OF SELF-SOVEREIGN IDENTITY

We use the following terminology based on Preukschat et al. [45] and Mühle et al. [4] in this article:

- Verifiable Credentials: A collection of metadata and claims that can be verified by a proofing mechanism.
- Claim: Statement about an attribute of an entity.
- Proof: Data that allows a verifiable credential to be verified by a verifier, that is, a digital signature.
- Wallet: Software to store private keys, verifiable credentials, and other documents.

- Verifier: Requests identity information or attributes of a holder, for example, allowing access to a service.
- Issuer: Trusted parties that verify attributes/claims of an entity.
- Subject: The entity the claims within the verifiable credentials are made about.
- Holder: Owner of the claims within a verifiable credential, and usually the same entity as the subject.

B. COMPARING SELF-SOVEREIGN IDENTITY WALLETS

The Sovrin Foundation gathered several requirements for self-sovereign privacy by design [46], which was superseded by Hyperledger Aries Requests for Comments (RFCs). However, their statement does not consider further malicious entities besides identity providers collecting huge amounts of data. If, for example, one service says it requires more data, then it is up to the user to decide if they trust the service. One central element for self-sovereign data control is the wallet, which the user typically installs on the smartphone.

To compare different real-world SSI wallets on the market, we used the list of the European Blockchain Association [47]. We searched for the corresponding wallets in the Google Play Store using our test smartphone, Pixel 6, with the current Android OS. Thereby, we obtained the candidates Lissi Wallet [26], Verimi [48], Data Wallet by iGrant.io [49], esatus Wallet [27], VIDwallet [50], SmartWallet by Jolocom [51], and Gataca Identity [52]. Each organization offers at least one demo workflow, which we use to recognize differences. Not all organizations have a public GitHub repository with the corresponding source code. In the comparison, we focus on interfaces and design but comment on noticed issues.

1) LISSI WALLET

We tried to create a wallet with Lissi, but were unsuccessful in the first attempt. Also, later on, we encountered issues. After the wallet was finally set up, we played the demo scenarios (see Fig. 2a). By scanning the QR code, new verifiable credentials can be obtained. Self-attestation, this is, the creation of own credentials, is impossible. This is true for most of the wallets tested. When receiving a credential offer and sending proofs, the issuer or verifier is stated, and a sign about the verification is appended. If several credentials fulfill the requirements of the request, then the user can select them from a dropdown list. Finally, the user can see information about the credentials by clicking on the corresponding sign.

2) DATA WALLET

Some iGrant.io demo workflows failed immediately in the beginning because the QR codes were invalid according to their own app. In contrast with Lissi, self-verified claims are possible. The user has to simply add new claims with the corresponding values. To receive verifiable credentials, the QR code has to be scanned after choosing the type of claim. The information list about the institution can become long, as it may include the data agreement. In addition, users can create connections with organizations by scanning QR codes. We noticed that information about the verifier is difficult to find (see Fig. 2d) and the actual claims are blurred (see Fig. 2e), but can be unblurred with an additional click.

3) ESATUS WALLET

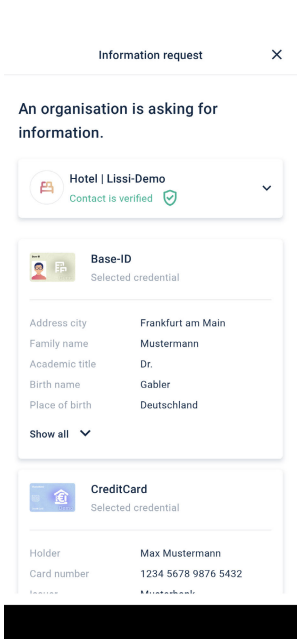
With esatus Wallet, we participated in their test network by sending a claim (see Fig. 2b) and were asked about the future behavior with this specific verifier (see Fig. 2c). The same popup appears for receiving claims. The *Ask me later* option appears in the middle is the default option. If the user chooses to click yes (the first option), they can choose to receive notifications. This option is not selected by default. Although the app was set to English, the text appeared as a mixture of English and German. After the relaunch of the app, the language was displayed properly.

4) VIDWALLET

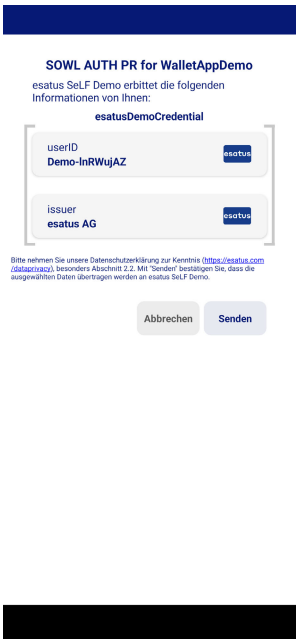
During the setup of VIDwallet, we had to accept the unformatted terms of data protection. This was the only data protection information we had to accept during the test of all wallets. Similar to the demo of the Data Wallet, we struggled to receive some credentials. Here, we received a hypertext transfer protocol (HTTP) status code 403 (forbidden). The demo provided three options for obtaining verifiable credentials: connecting phone numbers, connecting emails, or using external sources. The external sources include an ID, such as a scanned passport or identity card, the social networks Facebook and Google, and a bank. The latter redirects the user directly to PLAID, a data network and payment platform. We used two email addresses to play with the wallet: a normal email address and a throwaway account. Both are accepted, although the verifiable credential about the throwaway account only says that the user had this email address at the very moment. However, as the email address did not provide enough claims (see Fig. 2f), the workflow had to be stopped due to an error message (DID and verifiable ID credentials were required; we had DID, validated ID, and email). Here, we noticed that the user can only scan a QR code once.

5) SMARTWALLET

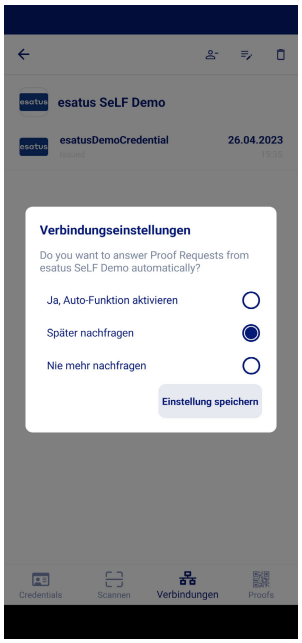
After choosing a PIN, the wallet was ready for use. We scanned a QR code using a button in the middle of the control bar and received information about the issuer and verifiable credentials. By clicking on the issuer's logo, we were forwarded to their website. However, the amount of information within the wallet regarding the issuers and verifiers is limited. Self-attested credentials are possible, for example, if insufficient claims are available. This did not always work in the demo, as shown in Fig. 2h. In addition, the QR code scanner had problems recognizing the QR codes several times. Once, we saw the service name `%{service-name}` (see Fig. 2g), which could have been caused by the demo. We could not find an option for activating biometric authentication.



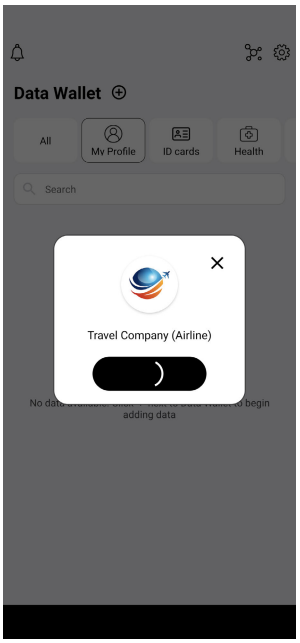
(a) Lissi Wallet receiving a request.



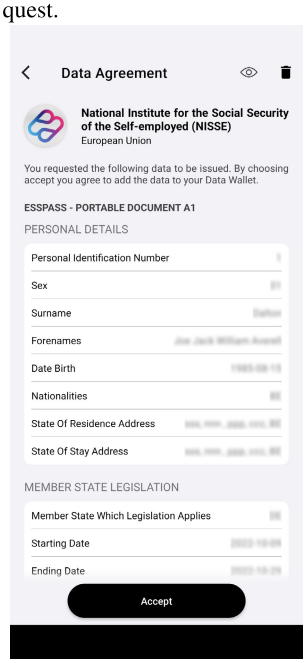
(b) esatus Wallet when the verifier requests a claim.



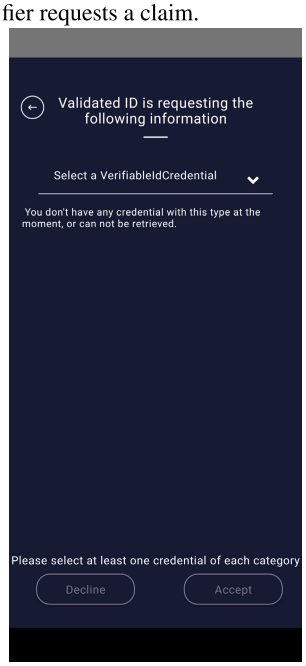
(c) esatus Wallet asking about future behavior with the verifier.



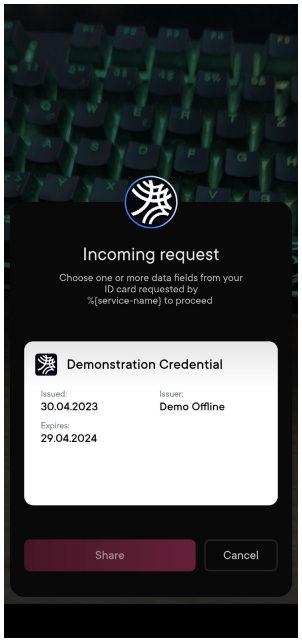
(d) iGrant.io Data Wallet receiving claims.



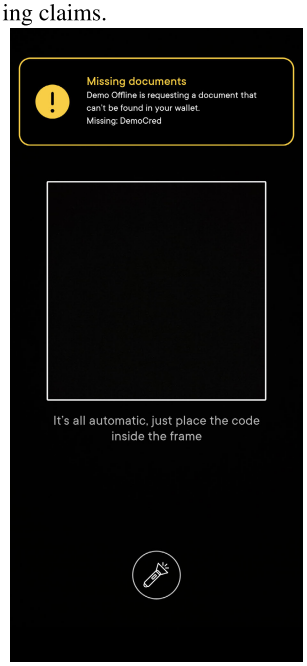
(e) iGrant.io Data Wallet receiving blurred claims.



(f) VIDwallet with issues complying with requested claims.



(g) SmartWallet with an incoming request.



(h) SmartWallet with an error.

FIGURE 2. **Screenshots of selected wallets found in the app stores.**

6) VERIMI WALLET AND GATACA IDENTITY

We could not make them work on the test smartphone and in a virtual environment.

7) SUMMARY

During our tests by trying the demo scenarios, we noticed differences in the behavior and visual elements of the wallets, but also some similarities, such as applying PINs for authentication by default, having a home screen with the most information, and a menu bar with functionalities including a QR code scanner. Only the Data Wallet applies a slightly more complicated procedure to receive verifiable credentials. Some wallets accepted self-attested claims. However, even the verified email address applied by VIDwallet has almost no validity, as throwaway accounts can be used.

Most wallets show little to no information about the issuer and verifier, except for Lissi Wallet (verified) and Data Wallet (mostly, see Data Agreement). This might make the user send verifiable credentials to a malicious organization [53]. This is even more serious if the requests are accepted by default, which is possible with esatus Wallet. The functionality may reduce the clicks the user requires and, hence, even be desired – but it can be applied by malicious verifiers simultaneously. Similarly, blurring utilized by the Data Wallet may have similar effects because the user does not have to see the claims to accept the request. However, one might argue that personal data is, similar to passwords, typically not shown in clear text. A button to show the data might be a solution.

To conclude, we found almost no design elements supporting the user in deciding whether a request is acceptable. Based on these results, the user already has to know about the sensitivity of their data or the concept of self-sovereign identity may lead to even more shared data. Our study focuses on understanding the paradigm and how to support users.

IV. RESEARCH APPROACH

In the following, we briefly explain our research approach. To recap, the research questions focus on willingness to adopt SSI (RQ1), the understanding of the underlying paradigm and the influence on actions (RQ2), support mechanisms to make responsible use (RQ3), awareness of the sensitivity of data (RQ4), and user interface design supporting privacy-preserving decisions (RQ5). To answer these research questions, we first conduct a pre-study (see Section V). We then introduce the design space and enhance our prototype accordingly (see Section VI). Finally, we conduct a user study using this new prototype (see Section VII). In the following, we briefly summarize our methodology for these three parts.

To validate the usability of the prototype design, incorporating design decisions of currently available wallets, a qualitative *pre-study* is conducted. To answer RQ1, three designs regarding users' control of their data are tested. The pre-study also provides first insights into research questions RQ2–RQ4 (i. e., by actions and questionnaire). Since the pre-study results indicate a strong tendency toward trading benefits for privacy, we explore how much (sensitive) personal data users would share.

Based on the results of the pre-study, the prototype is improved. Since the pre-study results indicate a strong tendency toward trading benefits for privacy, we explore how much (sensitive) personal data users would share to obtain different benefits. Moreover, we create a *design space* for awareness designs that lead to higher privacy awareness and test four selected designs in the user study.

In the qualitative *user study*, we choose a similar approach to the pre-study but add real-life scenarios requiring interviewees to share more data to receive certain benefits. This approach is chosen to validate our assumption from the pre-study. In addition to answering RQ1–RQ4, we investigate whether those awareness designs could lead users toward more privacy-preserving decisions (RQ5). These questions are being answered by actions and the questionnaire.

Both studies are exploratory and emphasize qualitative insights. We follow the ethical regulations of our university. As both studies align with the regulations, they do not require additional approval.

V. PRE-STUDY: CONTROL OVER SHARED DATA

Wallets already exist on the market (cf. Section II-B). One unanswered question is how well minimal data sharing is supported. This already assumes that users want to control their data. However, what if a user does not want to be bothered by such decisions? This question needs to be answered first to design a mobile SSI wallet.

Consequently, this section describes the apparatus (Section V-A), the study design (Section V-B), the procedure (Section V-C) and results and discussion (Section V-D) of the pre-study, conducted to answer RQ1–RQ4.

A. APPARATUS

The pre-study was conducted in May 2022. Eight subjects participated in this qualitative study. As we assume that mostly younger persons will use the SSI wallet as it is typically installed as a smartphone app, the participants were chosen based on age (see Section V-D1).

1) WALLET DESIGN

The design of our mobile wallet versions follows existing SSI wallets, such as Lissi and esatus [26], [27], (cf. Section III-B). We simplified it to fit the purpose of the study (see R1–R4): users can scan QR codes and receive and view VCs. The interface uses the React Native Framework [54]. The design of the prototype's home screen is shown in Fig. 3a. Lissi Wallet aligns the credentials in a grid, whereas esatus Wallet shows them individually. Users typically receive more information by selecting a credential, such as activities and data. We decided on the slide functionality to provide an easy, intuitive overview. Additional information can be obtained.

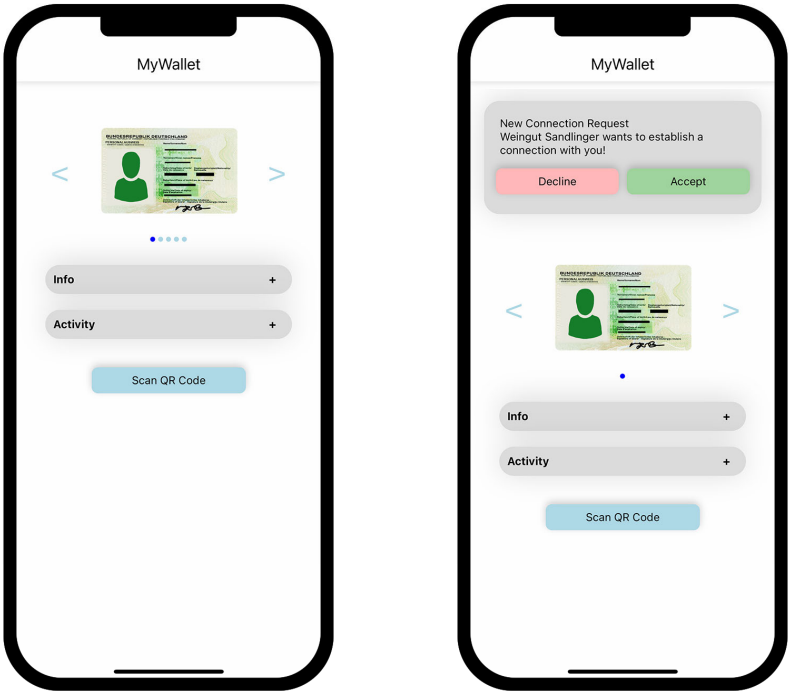
a: WALLET WORKFLOW

The workflow for scanning a QR code and accepting a request is similar to that of the existing wallets. In Lissi Wallet, users can scan QR codes by clicking a button. This functionality has its own tab in esatus Wallet. To make the functionality visible, we opted for the button. After successfully scanning a QR code, the user is prompted with a connection request at the top of the screen (Fig. 3b). Declining the request removes the notification box from the top and returns the user to the original screen. Accepting triggers a new box after two seconds.

b: WALLET VERSIONS

We created three mobile wallet versions. Fig. 4 shows the implemented designs: no-detail, detail, and selectable.

In the *no-detail design*, the user was only presented with the VCs they would share when sending the requested proofs



(a) Home screen of the prototype used in the pre-study.

(b) Connection request after scanning the QR code.

FIGURE 3. Pre-study wallet prototype design.

to the verifier, that is, the person verifying their identity. Consequently, they could not see the individual claims on the credentials requested by the verifier. When accepting the request, another notification similar to the previous one pops up after a short delay, asking the user if they want to accept the credential sent by the verifier. As a reminder, those credentials were connected to the products requested by the participants in the pre-study.

The other two designs show users a notification informing them that the verifier wants to see some proof. By clicking the "Show Request" button, users are led to a new screen that displays the required credentials. The user could click on credentials to obtain detailed information about single claims. Whereas the *detail version* only showed the required claims, the *selectable version* provided a means to approve sharing particular claims using a slider. In a real-life scenario, this could include subscribing to an optional newsletter or transmitting a birthday to receive a special gift. However, mandatory claims could not be deselected.

2) SCENARIOS

The pre-study consisted of two rounds with two scenarios each. After each round, a questionnaire (see Appendix A) was provided. Participants were given a smartphone (iPhone 13), on which the wallet was installed, already opened, and included the eID of the fictive person Nicola Gebersdorf. The scenarios were based on real-world situations. These were selected such that various use cases for SSI-Wallets are tested. The first task in round 1 with a bank introduced the SSI concept. The second task with a beverage store required the sharing of more credentials. In round 2, the wallet design was changed. The first task involved buying a concert ticket under pressure, which required all claims. This resembles a common online situation where more claims than required are requested. The second task of round 1 was repeated in round 2 to compare the results. Table 1 provides an overview of these tasks.

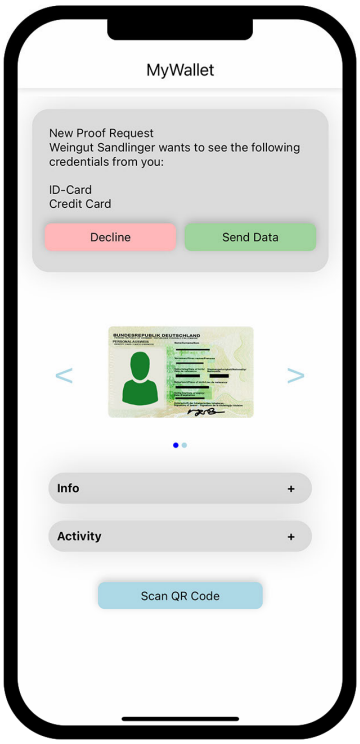
3) QUESTIONNAIRE

The questionnaire (Appendix A) contains demographic questions (7), questions about technology affinity (3), and questions on users' experiences with the wallet and their views toward personal data management (9).

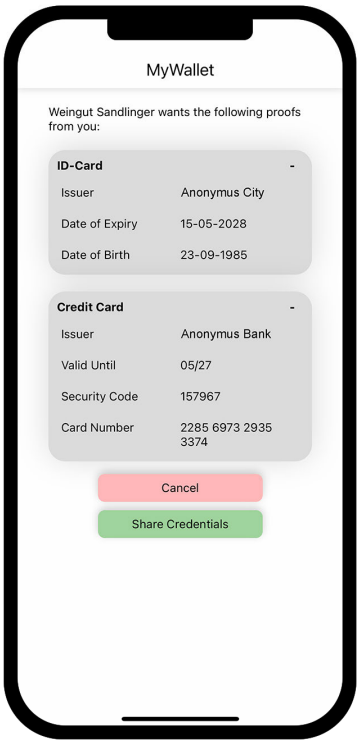
B. STUDY DESIGN

The study followed a within-subject design, in which participants were exposed in two rounds to different wallet designs. Hence, each participant was shown two out of the three designs. The wallets were presented in a counter-balanced order.

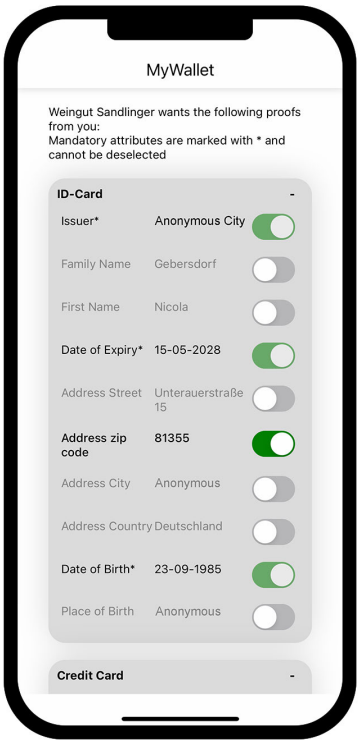
The independent variables were the wallet design (selectable, detail, and no-detail) and different tasks. The dependent variables were the user experience, participants' feelings of control and trust, privacy concerns, and sharing behavior.



(a) No-detail design version: The user is only told which verifiable credentials they provide for proof, but not which individual claims the verifier requests.



(b) Detail design version: The user can see which claims on the verifiable credentials the verifier requests.



(c) Selectable design version: The user can select additional information that they want to be transmitted to the verifier – for example, if there is an optional subscription to a newsletter.

FIGURE 4. **The three different designs used within the pre-study.**

TABLE 1. **Overview of tasks, credentials, and claims used in the pre-study.**

Task	Credential	Claims
	Round 1	
#1: City Bank	ID card	all
#2: Beverage store	ID card credit card	issuer, expiry date, birth date all except holder
	Round 2	
#3: Concerto	ID card credit card	all all
#4: Beverage store	ID card credit card	issuer, expiry date, birth date all except holder

C. PROCEDURE

The study consisted of six phases. The duration of the study was approximately 40 minutes per participant.

1) INTRODUCTION

The participants were provided with a short introduction to the topic and an overview of the study. We told them that this study tests the usability of and preferences for a wallet.

2) ROUND 1

As a first task, the participants had to scan a QR code from their City Bank to receive a digital version of their credit card. The second task involved interactions with their favorite beverage store. The beverage store offers a good beverage for a symbolic payment of 0.50 Euros if using an SSI wallet. After a successful negotiation, participants were given a drink as compensation for participating in the study.

3) QUESTIONNAIRE 1

The questionnaire (App. A) was provided for the first time.

4) ROUND 2

In round 2, which consisted of two tasks, the wallet's design was changed. The first task was to acquire concert tickets

from the ticket agency *Concerto* for their favorite band, which exclusively reserves the first ten rows for people who bought the tickets with their SSI wallets. The tickets were given out on a first-come, first-serve basis. Participants were asked to imagine a situation in which they arrived slightly late at the ticket counter and had long queues in front of them. The purpose was to create a situation where the participant is under time pressure and desires to acquire the offered goods. In the second task (still using the same design), the beverage store sold a pre-order coupon for a limited beverage edition. Participants could purchase that coupon for a symbolic sum and redeem the coupon for a beverage later. The purpose of this task was to see a direct comparison in a similar scenario with the same shared data but different wallet designs.

5) QUESTIONNAIRE 2

The questionnaire was provided again to enable comparability. The demographic and technical affinity questions were omitted, as they were already answered in round 1.

6) FINAL DISCUSSION

In the discussion, we obtained a deeper understanding of the participants' motifs, behaviors, and opinions. Additionally, participants were asked about certain behaviors and comments. Thus, insights on whether participants acted according to the privacy paradox and whether they were more likely to share data under pressure or when offered benefits were obtained. Finally, we asked for suggestions for improvement and how they liked the wallet.

D. RESULTS

1) DEMOGRAPHICS

Participants' ages ranged from 15 to 62 years (med = 35). All interviewees were German and lived in Germany at the time of the study. The highest degree was a doctorate degree (4), a master's degree (2), a bachelor's degree (1), and less than a high school diploma (1). Most participants were full-time (3/8) or self-employed (3/8) employees. None was color-blind. Most participants (5/8) were technical-savvy. All the participants used their smartphones several times per day.

2) USABILITY AND TRUST

Participants found that the wallets were generally easy to use (med = 5, biased std. dev. = 0.58) and enjoyable (med = 4, biased std. dev. = 0.93). The integrity of the wallet scored four out of five for the detail and selectable versions; for no-detail, it was slightly lower. 75% of all participants answered with a four or higher when asked if they liked the wallet more than a traditional one. Two participants who liked the wallet least compared to a traditional, physical wallet (#3 and #4) rated their technical affinity as low. All participants were able to imagine using the wallet daily. Some participants were hesitant to share data in round 1. This was confirmed and explained by interviewee #7: "In the second round, I had more trust in the app". He argued that getting used to the app increases trust.

TABLE 2. Median of answers given for each design version.

Question	no-detail	detail	selectable
Ease of Use	5	5	5
Enjoyment	4	4	5
Confusion	1.5	1	1
Trust in integrity	3.5	4	4
Control over personal data	3.5	4	5
Cumbersome transmission	2	2	1
Truly necessary information transmitted	3.5	4	4
Afraid of too much information transmitted	4	2	3
SSI wallet more liked than physical	4	4	4

3) PREFERENCES

Table 5 in Appendix B shows the allocation of study designs to participants and their preferred versions (bold). A summary of all answers can be found in Table 2. The median was computed for rounds 1 and 2 together.

Participants who were shown the no-detail version almost always preferred the version detail or selectable. The only exception was participant #4. She liked the no-detail version more because it required fewer steps. She pointed out that she had to show her whole ID card in a non-digital scenario. All other participants, except #4, chose not to have the no-detail version because they could see more details about what exactly is shared. This fits the answers regarding the workflow itself. Interviewee #4 rated her technical affinity the lowest, which might explain the answers.

4) CONTROL

According to the survey, participants felt that they had the most control when using the selectable version. However, when looking at the average rating, the difference between detail (avg.: 4.2) and selectable (avg.: 4.4) is rather small. When making participants aware of the privacy paradox and asking them if they could manage their own data, they seemed unsure but argued that they would or at least supported the idea. When asked if they would agree that wallets increased their awareness of which personal data were shared, two interviewees agreed. However, one noted that for people who do not care about their data, there would only be a slight increase in awareness of sharing practices.

5) SHARING BEHAVIOR

Since the participants did not handle their own data but played the fictitious role of Nicola, one could argue that they might behave differently in real life. However, when asked about their behavior, all participants agreed to give up their privacy for convenience. This result supports the assumption made by studying different wallet designs. To use current wallets, users have to be aware of their data and handle it carefully. Some were hesitant to share information initially, but when it came to getting something they wanted, they all shared their data. Most participants said that privacy was important to them

and that they would be careful. When asked why they shared their personal information, they admitted that, in this case, the demand was more important than the data. When looking at the answers from the survey, participants were most afraid to transmit too much information with the no-detail screen (med = 4) and least afraid with the detail version (med = 2). In general, participants felt unsure whether they transmitted only necessary information with the no-detail screen (med = 3.5) but were more sure with detail and selectable (med = 4). Several participants did not perceive the data on their ID cards to be highly confidential. Participants #2 and #3 compared them to cookies. Another comparison often made was the current situation on the Internet, for example, for shopping. Two interviewees described speed as one form of convenience. Interviewee #5 pointed out the strict privacy guidelines (GDPR) in Germany. Three participants (#1, #2, #3) said the difference with the physical ID card was that they did not have the physical card in digital form. Having the information digitally enables the verifier to store it automatically.

VI. DESIGN SOLUTIONS ABOUT PRIVACY AWARENESS

This section discusses possible design solutions to improve awareness of the importance of personal data. First, a design space is created in Section VI-A. Based on the pre-study results, related work, and the design space, possible designs are discussed in Section VI-B and selected in Section VI-C.

A. DESIGN SPACE

The design space (Fig. 5) with the following dimensions of complexity, granularity, and temporal served as the basis for creating effective design solutions. The dimensions were selected based on focus points of particular interest for this study, which will be explained in more detail in the respective paragraphs. They were chosen out of exploratory means. That being said, it will be out of the scope of this article to test the entire design space, but instead focus on a few designs to report on the first empirical results regarding awareness designs in the context of SSI. Further research can expand or build upon our ideas and test their feasibility.

- Complexity: Complexity of the information provided by the design. The continuous scale from low to high describes how difficult it is to grasp information in the respective design. ''Low'' means that the information is easy to process and understand. On the other hand, high indicates that the users need to dedicate more time to processing the information and may have difficulties understanding the design. However, information with higher complexity might potentially provide the user with more fine-grained and detailed guidance. On the one hand, users might gain a better understanding of a concept if they gain more knowledge about it. On the other hand, the user experience of SSI wallets could suffer when they are presented with too much information that requires high processing effort.
- Granularity: Layer of operation for features. The continuous scale consists of three key points: claim, VC, and wallet. If a feature is within the claim domain, it can provide information about every claim in a credential. Credential refers to information about the entire credential, but not for each claim. Wallet indicates that the design can provide an overview of transactions and proofs. This dimension was chosen to determine the effect on users' privacy awareness when they are presented with knowledge of different granularity. In some situations, it might be better to gain an overall knowledge of the concept, in others, of individual claims. Therefore, this dimension also provides designs that might be out of the scope of this paper but deliver input for further research.
- Temporal: Point in time (before, during, and after) where the design solution is visible. 'Before' means the feature will be displayed before the proof request happens. In addition, a feature can provide information 'during' the workflow, for example, while the user checks the required proofs. 'After' shows information after the proof request when the information has been sent to the verifier. This dimension was chosen to discover learning in the context of SSI. For some interactions, it may be better and increase learning if users are approached before a critical situation occurs. For others, help may be needed in a particular situation.

Based on these dimensions, state-of-the-art reviews, brainstorming techniques, and discussions were used to develop reasonable designs and their placement in the design space. Nearly all designs found in the design space already exist in some form in other implementations. For the granularity and temporal domains, the designs could be placed based on the authors' intention when including those designs. The authors used an educated guess for the complexity domain to place the designs inside the continuous scale. The user study shall then give initial insights into the validity of this guess.

B. PRIVACY AWARENESS INTERVENTIONS

The colored points represent the design solutions, described in the following in ascending order in the temporal domain.

- Awareness Notification: Messages pop up in irregular intervals showing educational information, reminding users about the sensitivity of their information. This is similar to subtle assistance [20], [23].
- Training Request: Educate people about several aspects of their privacy and behavior within an SSI wallet through requests from non-existing fraudulent entities. This is similar to one type of phishing training.
- Trust Score: Represents a rating of verifying entities. Similar to product or restaurant ratings.
- Counter: Providing a quick overview of the relative amount of shared information could serve as an indicator of whether a verifier requires more data than needed.

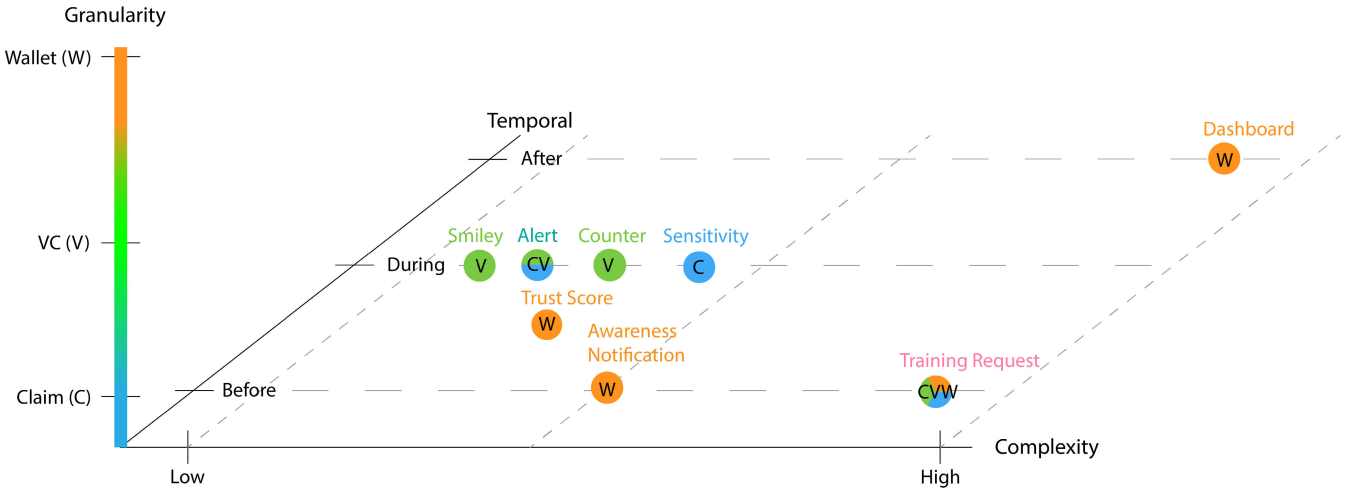


FIGURE 5. Design space for privacy awareness.

- Smiley: Indicates how sensitive the information that the user shares during a proof request is. One idea could be to let them look similar to Chernoff's faces [55].
- Alert: Confirmation popup if the user intends to share a large amount of or highly sensitive data [20], [23].
- Sensitivity: Indication of the sensitivity of data by colors, numbers, or letters for claims, similar to DuckDuckGo's browser extension Privacy Essentials [56].
- Dashboard: Overview of a user's past data transactions, similar to the privacy dashboard of Android phones [57].

The designs are not mutually exclusive. Combinations of different designs are possible in the same application. This leads to several possible combinations. However, adding too many of these designs could annoy and overwhelm users.

C. DESIGN SELECTION FOR FURTHER INVESTIGATION

To date, only designs for enhancing awareness in SSI wallets presented in the design space have been proposed, but their actual applicability or liability has not yet been evaluated. Considering the pre-study results, the question arises whether giving the user control is a good idea and, if so, how this could be achieved. Not only could they obtain an illusion of increased privacy through more control, but they could also be tempted to share more data than they would otherwise. It could be the case that without true data minimization, SSI would rather increase convenience than privacy from a user's perspective. However, users could gain a better understanding and awareness of the privacy aspects of their personal data through SSI. Nevertheless, a critical view should be maintained on whether current wallet designs for SSI actually increase users' privacy or may even harm it.

Our investigation focuses on designs with an immediate effect and leaves approaches influencing users' behavior in the long term for future work. Hence, we excluded the training requests from the evaluation, as the educational effect of this design would only become visible over time.

Furthermore, we excluded the designs of the trust scores and dashboards. This is because these designs would require a complex design process. A trust score requires the design and implementation of a scoring approach and considering how this score can be conveyed in a trustworthy manner to users. The dashboard could be a powerful means for users to make privacy-preserving decisions, yet it would need more elaboration on the information to be presented.

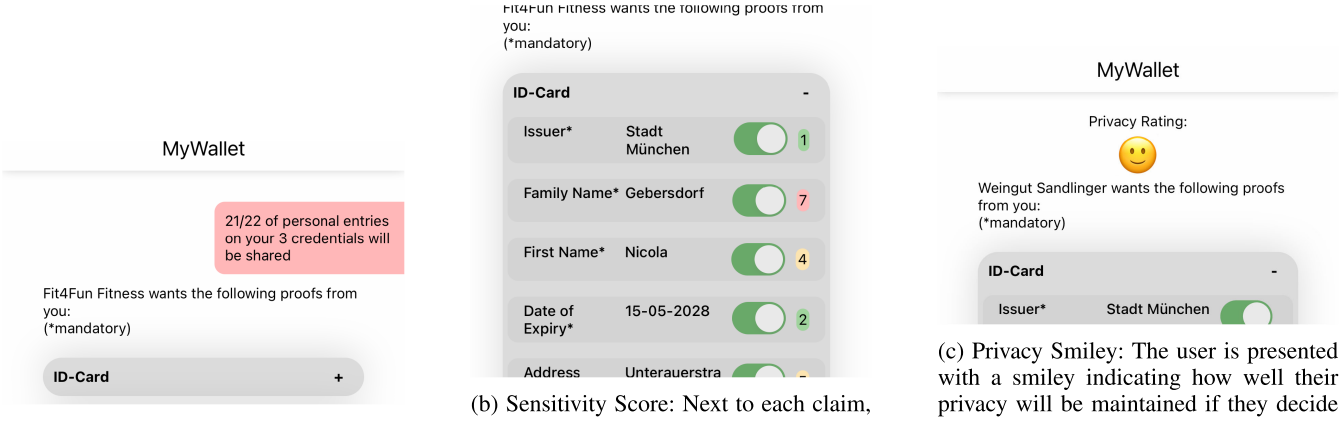
We focus our investigation on designs that are applicable during the workflow of transmitting personal data. This temporal domain was also tested in the pre-study. Therefore, the results of the pre-study and user study can be compared. All designs could be easily incorporated into the already existing prototype. Therefore, those four designs will be investigated in the user study. The following designs were refined: counter (Section VI-C1), sensitivity scores (Section VI-C2), smiley (Section VI-C3), and alert (Section VI-C4).

1) COUNTER

The counter (see Fig. 6a) shows a quantitative summary of the currently selected credentials to be shared with the verifier and is enhanced through colors (traffic lights). Thus, the counter could nudge users and receive greater attention. The background color indicates the amount of shared data (traffic lights). Hence, the information is displayed in two ways: through color and content. In the case of color blindness, the content of the counter still conveys the message. Moreover, coloring the credential has the effect of nudging the user and seeking its attention due to the Gestalt principles.

2) SENSITIVITY SCORES

The sensitivity score states the sensitivity of a claim on a scale from 1 (very low risk) to 10 (very high risk). Choosing 1 to 10 conveys to the user how critical their own data is. It is more fine-grained than the smileys described next, while still being understandable. The scores are highlighted using the



(a) Counter: The counter states how much data is currently shared.

(b) Sensitivity Score: Next to each claim, the user can see a score from 1 to 10, stating the sensitivity of this claim.

(c) Privacy Smiley: The user is presented with a smiley indicating how well their privacy will be maintained if they decide to share their data with the current settings.

FIGURE 6. Awareness designs used in the study to provide users with insights about the data they intend to share.

FIGURE 7. Five different distinct states of the privacy smiley.

corresponding numbers, as shown in Fig. 6b. Similar to the counter, the background colors change accordingly. With a color scheme, the user can quickly perceive the number of highly sensitive claims they intend to share.

3) SMILEY

The smiley is implemented using emojis. As shown in Fig. 6c, the emoji is placed on top of the screen. The smiley represents a combination of sensitivity and the amount of shared information by taking the percentage of shared credentials and putting it in relation to the sensitivity of the data. The smiley has five appearances: angry, sad, indifferent, happy, and laughing (see Fig. 7). The appearance is based on the number of shared claims and their sensitivity. The number of five smileys is selected to make the user aware of the sensitivity at a single glance.

4) ALERT

The alert (Fig. 8a) appears after the user presses the button "Share Data" on the proof request screen. This makes users aware of their intention to share sensitive data. To progress, they need to swipe, as proposed by Bravo-Lilli et al., over the name of the credential containing sensitive data. This method is more resistant to habituation, but not too difficult to dismiss. Fig. 8b shows the state after swiping.

VII. USER STUDY

Based on the pre-study in Section V-D and related work in this field, we investigate the following hypotheses.

- Users will share the personal information on their ID cards and give up privacy for convenience. They may also share personal information with higher sensitivity, such as a health insurance card, if the context is fitting. However, they will refrain from sharing this sensitive information when requested out of context. (RQ3+4)
- The designs will help the users to make decisions about sharing their data in a more privacy-oriented way. (RQ5)

First, we describe the apparatus (see Section VII-A). Section VII-B outlines the study design, which is applied in the procedure of the study (see Section VII-C). This is followed by a brief summary of the limitations of this study. Last but not least, the results are discussed in Section VII-E.

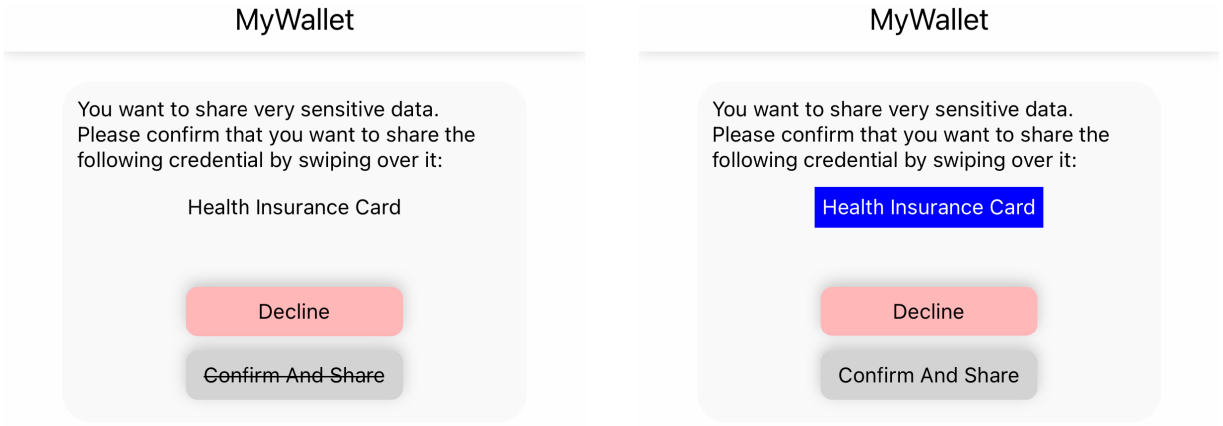
A. APPARATUS

First, the wallet design is outlined (Section VII-A1). The scenarios and their purpose are then explained (Section VII-A2). For comparability, we used the questionnaires from the pre-study (Appendix A).

1) WALLET DESIGN

According to the pre-study results (see Section V), the prototype uses the selectable design. Therefore, during the sharing process, each claim has a little slider next to it. Based on the suggestions in Section VI and participants' comments, the prototype was improved as follows.

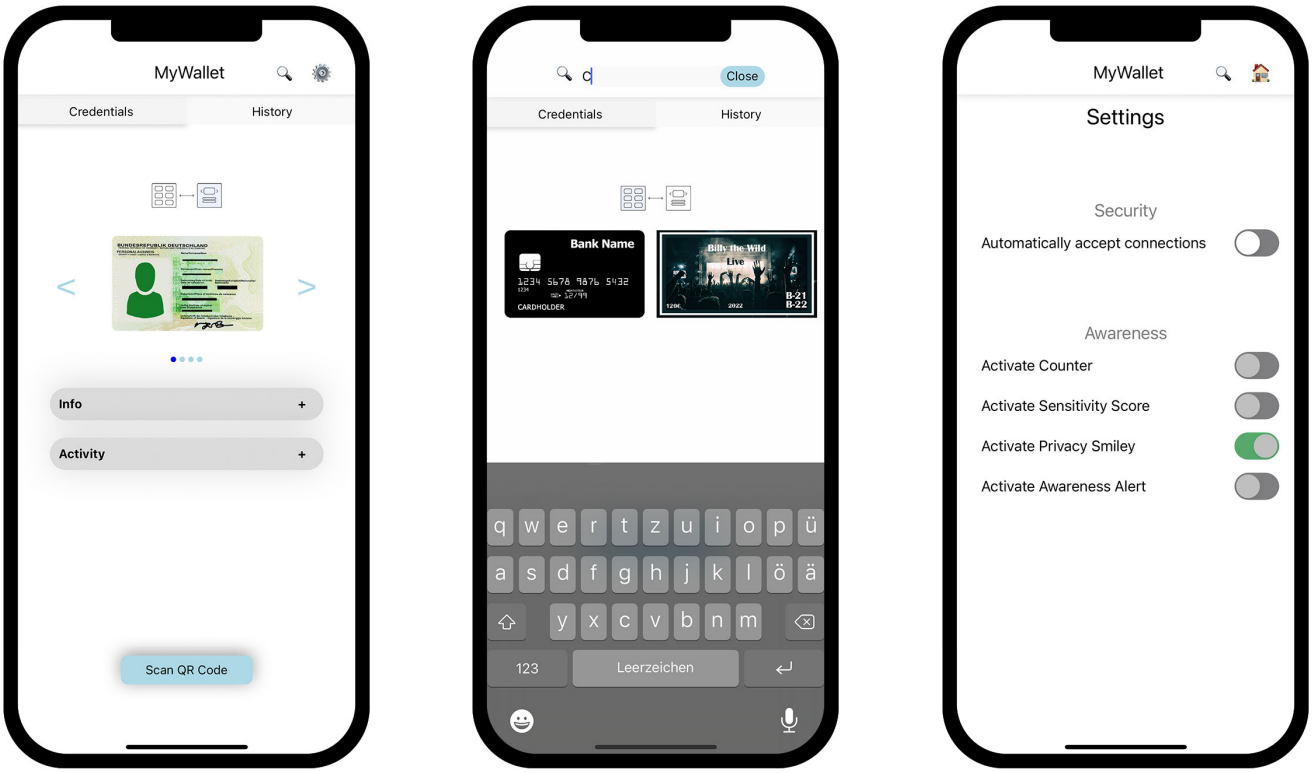
- Home Screen: At the top of the screen in Fig. 9a, we added two tabs: Credentials and History. Between the navigation bar and the picture of the current credential, another button toggles between a detail and a list view of credentials. The layout of the small boxes containing information and history underwent a visual change to adjust to the sensitivity score. Additionally, the user has the option of showing the claims previously shared. Finally, the distance between the activity and scan buttons is increased to prevent people from believing that it is connected to the credential currently selected.
- Search Field: By tapping the looking glass, a search field for credentials appears (see Fig. 9b).



(a) Alert: Warns the user that they intend to share very sensitive information.

(b) This shows the state after the user swiped over the text.

FIGURE 8. Alert that appears if health data was shared.



(a) Updated version of the home screen.

(b) Usage of the search field.

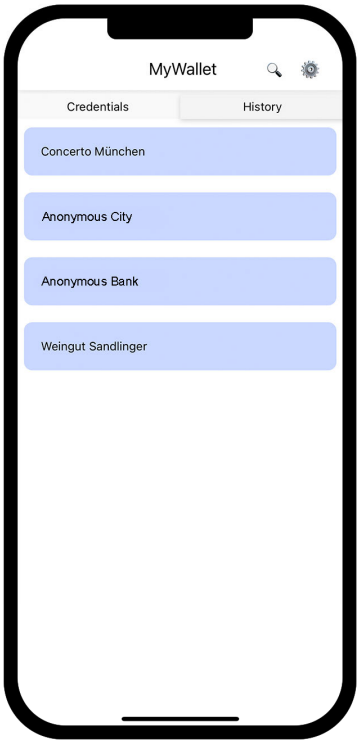
(c) Settings menu to personalize app.

FIGURE 9. Features of the updated prototype for the user study: home screen, search field, and settings menu.

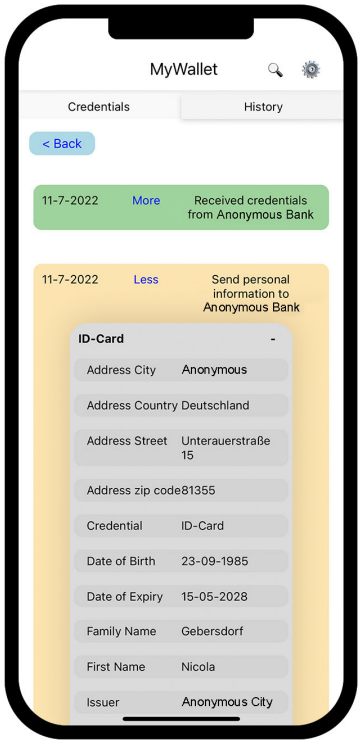
- Setting Menu: In the settings menu (see Fig. 9c), the user can individualize the appearance and behavior.
- List View: The user can switch between two different presentations: single view and list view (see Fig. 10a).
- History: The participants can see entities with whom they established a connection in the past (see Fig. 10b).
- Activity: The activity underneath the information box in the credential view can now display detailed claims.
- Pending Transactions: As shown in Fig. 11a, the message includes a spinner that indicates an ongoing process. If the user clicks on this message, the view will expand and provide more detailed information about the pending transactions (see Fig. 11b).

In general, little use of colors is made to make features clearly visible and confront users with fewer visual cues or nudges. According to the pre-study results, the prototype uses

(a) List View: Here, the credentials are ordered in a grid.

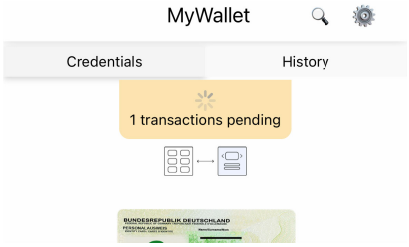


(b) History: The user can see a history of entities they interacted with.

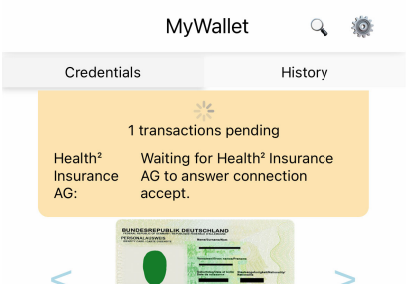


(c) By clicking on one of the history entries (see Figure 10b), the user could look up all past interactions and shared claims with the entity.

FIGURE 10. Additional features of the updated prototype for the user study: list view and history.



(a) The message shows how many transactions are pending and signalizes an ongoing process with a little spinner. It can be expanded by clicking on it.



(b) The expanded view gives more details about the pending transaction.

FIGURE 11. Transaction Pending Message: The message appears while waiting for a response by the other entity.

a selectable design. Therefore, during the sharing process, each claim has a little slider next to it. However, mandatory claims cannot be deselected.

2) SCENARIOS

The study consisted of two rounds, each with three scenarios. Round 1 repeated the tasks from pre-study round 2 for comparability. In round 2, more than the required claims were requested. Table 3 provides an overview of all tasks. Next, we present the intentions behind and expected behavior.

a: ROUND 1

In the first round, three scenarios with the same tasks as the pre-study were repeated for comparison (City Bank, beverage store, and Concerto) but with the new wallet design.

b: ROUND 2

Round two also consists of three tasks, as shown in Table 3. First, participants acquire a health insurance card from their privacy-concerned health insurance company, *Health*^{2}. Health^2 requires only claims necessary to uniquely identify a

TABLE 3. Outline of each task.

Task	Credential	Claims
	Round 1	
#1: City Bank	ID card	all
#2: Beverage store	ID card Credit card	issuer, expiry date, birth date all except Holder
#3: Concerto	ID card Credit card	all all
	Round 2	
#4: Health²	ID card	name, issuer, expiry date, birth date, birth place
#5: Fillinger Apothecary Group	ID card Credit card Health insurance card	issuer, name, expiry date all except Holder all
#6: Fit4Fun	ID card Credit card Health insurance card	all all except Holder all

customer and send them their personal insurance card. Since Nicola Gebersdorf, the virtual persona of participants during the study, is a customer of that company, they already have all the required data. Therefore, there should be no problem for participants in sharing their data with them.

The remaining two tasks test how much people are willing to exchange data for convenience. According to the pre-study results, people are willing to share all their information on their ID cards for concert cards. Would they exchange their health information for convenience?

In task 5, participants want to buy migraine medicine. However, the *Fillinger Apothecary Group* requires claims on their ID and health insurance cards. Moreover, information about the clinical condition, illness, and medication history is unnecessary when purchasing medicines. If participants ask why, the interviewer will respond that they want to avoid side effects with other medications and that the medication fits the current condition. Participants could perceive apothecaries as entities with high integrity and trustworthiness. It is expected that some participants will share their data.

The high-class fitness center *Fit4Fun* with a spa area in task 6 offers a free month of training. However, they require a credit, ID, and health insurance card and, thereby, even more information than the apothecary. If participants ask for the reason, the salesman would tell them that they possess modern training devices that can use that data. We expected most interviewees not to share sensitive health data for this.

B. STUDY DESIGN

The study was again divided into two rounds, with three tasks each. To compare awareness designs with normal wallet designs, a normal design without any privacy-awareness features was introduced. Therefore, in each round, the participants saw one of the four designs (normal, sensitivity score, counter, or privacy smiley) in a counter-balanced order. For half of the users, the alert design was also visible in round 2.

The qualitative study followed a within-subject design. The independent variables were the four different design possibilities, the appearance of an alert, and the different tasks. The dependent variables were UX, participants' feelings of control and trust, privacy concerns, and sharing behavior.

C. PROCEDURE

The study was conducted in July 2022 with 16 interviewees (six female/nine male/one prefer not to say) participating in the qualitative study. Participants (Section VII-E1) were recruited through email distribution lists at a chosen university. Participants received either a ten Euro Amazon coupon or one study point, which was needed to complete their studies.

1) INTRODUCTION

Participants were given a short introduction to the topic and course of action. Similar to the pre-study, participants were not told that the study was about data-sharing behavior.

2) ROUND 1

The first round was similar to the pre-study. As a first task, participants had to scan the QR code in a mail from their City Bank to get their credit cards into their wallets. In the second task, participants had to buy a coupon for a limited-edition beverage from their favorite beverage store for a symbolic payment. The third task involved purchasing concert cards for a popular band at Concerto. The first ten rows were reserved exclusively for SSI wallet users. However, the cards were given out on a first-come, first-served basis, and the participants arrived late at the ticket counter.

3) QUESTIONNAIRE 1

The questionnaire (App. A) was given to the participants.

4) ROUND 2

In the second round, the wallet received a design update. First, the participants had to obtain a VC of their health insurance card provided by Health[2]. The second task focused on buying migraine pills from their local apothecary, Fillinger Apothecary Group. The participants were told that they wanted to purchase medicine using the SSI wallet. The last task virtually led them to the fitness center Fit4Fun. The modern gym, including a spa with a whirlpool, offered one free month of training for users using their SSI wallets.

5) QUESTIONNAIRE 2

The questionnaire, omitting demographics and technical affinity questions, was presented.

6) DISCUSSION

The participants were asked pre-defined questions. Depending on the answers of the participants, questions were adjusted to get more insights into the perspective of the interviewee. The discussion had the purpose of answering questions that were not included in the questionnaire. Furthermore, interviewees were asked about the reasons for their behavior or opinions about certain aspects of the wallet.

D. LIMITATIONS

Our study is limited by a comparably small sample, consisting primarily of young subjects with a technical background. Yet, we expect them to belong to the main target group of SSI wallets. Design decisions for the prototype of the user study were partly based on the pre-study results, such as choosing the ''selectable'' design version. Furthermore, participants could have been more trustful in certain situations because they trusted the interviewer who played the role of the different salespersons. Finally, only four designs of the design space were tested in this study. Other awareness designs might lead to different results and should be explored in future research.

E. RESULTS

In the following, the results are presented and discussed. We focus on demographics, usability and trust, privacy-aware designs, control, and sharing behavior.

1) DEMOGRAPHICS

The ages of the participants ranged from 21 to 29 years, with an average age of 24. They had the nationalities German (8), Chinese (3), Indian (2), Spanish (2), and Russian (1). Five interviewees had a High School degree, nine had a bachelor's degree, and two had a master's degree. 75% of the participants were students (mostly media informatics or informatics), one employed full-time, one part-time, and two others. None of them had color blindness. Of the 16 interviewees, 37.5% utilize Google Pay, Apple Pay, or an equivalent. All the participants used their smartphones several times per day. In total, 87.5% of the interviewees regarded themselves as technical-savvy.

2) USABILITY AND TRUST

In both rounds, participants rated the ease of use of the wallet with 4 or more out of 5, leading to an average of 4.7 and a median of 5 (biased std. dev. $= 0.45$). The enjoyment of the wallet was rated 4.3 on average (biased std. dev. $= 0.77$). When comparing both rounds, there is only a marginal difference in ease of use and confusion. Compared to the control group, there was only a marginal difference in the ease of use of the wallet when participants had an awareness design. Enjoyment was the same for all versions, except for the counter in the second round. In the second round, the counter received a median of 3 for enjoyment (avg.: 3.5), whereas the ''normal'' version received a median of 5 (avg.: 4.33). Additionally, in the first round, confusion was one point higher in the median with the counter design (2.5) than with the normal design. In the second round, the same was true for the counter and the sensitivity score.

Participants gave a median of 4 out of 5 (average: 3.6, biased std. dev. $= 1.22$) when rating if they liked this form of wallet more than a traditional one. In the discussion, nine participants said they could imagine using this wallet daily. Four participants may use it depending on the conditions (e. g., context, advertisements, and fewer proofs). Compared with the control group, there was only a small difference in the ease of use of the wallet. Whether there was an alert or not did not influence ease of use, enjoyment, confusion, and preference over a physical wallet.

3) PRIVACY AWARE DESIGNS

When asked which of the designs the participants liked the most, none preferred the normal design over the awareness design version. When users saw the privacy smiley and sensitivity scores, two preferred the emoji and two the sensitivity score. Also, all except one participant favored the counter over other designs. Of the eight times, an alert was present in the second round, and the design in the second round was preferred six times. When there was no alert, two favored the second round, three the first, and three were indifferent. As reasons for their decision to like one design over the other, appearance was named by two participants. Two interviewees stated that the counter had provided more information. Furthermore, two participants who chose privacy smiley said they liked it because it summarized the information. One participant chose the counter over the sensitivity scores because they value quantity more than quality. When asked if the awareness designs helped them decide to share their data, six participants said no, seven said yes, and three did not answer directly. Of the seven participants who agreed, five shared their data in every task. The remaining two declined because of the privacy smiley and the additional alert. Three participants explicitly said that

TABLE 4. Percentages of participants who decided to share their data for each of the tasks.

Task	Percentage of Participants
City Bank	100
Beverage store	87.5
Concerto	93.75
Health² Insurance AG	100
Fillinger Apothecary Group	87.5
Fit4Fun Fitness	75

the privacy-aware design influenced their decision. Another three affirmed that this was not the reason for their decisions. One mentioned that in the beginning, their design was helpful, but after a certain time window, they no longer paid attention to it. Those who received the alert were asked if they thought it was helpful or disturbing. Four interviewees said that having more security features or alerts was beneficial. One participant also noted that they could imagine clicking it away and compared it to the terms and conditions that they had never read.

4) CONTROL

In the first round, control over personal information was perceived as slightly lower by participants with the normal design (med = 3.5) than by those with the awareness design (med = 4). In the second round, there was a larger difference for some of the designs. Furthermore, interviewees who saw an alert answered this question with a median of 4, whereas participants without one only gave a 2.5 median. This means that users with designs tended to feel more like they were in control than those without awareness designs.

Fig. 12a shows the differences between the first and second rounds when asked about their feelings toward control. Without an awareness design, interviewees answered the question about truly necessary transmissions with a 4 out of 5 in the median with results for counter (2), sensitivity score (3), alert, and privacy smiley (both 2.5). As shown in Fig. 12b, their fear of transmitting too much information was similar.

The fear of normal users transmitting too much data was at a median of 3, for users of the counter 5, for sensitivity scores 4, and for privacy smiley 4. We found only marginal differences between users with and without alerts.

5) SHARING BEHAVIOR

The percentage of participants who decided to share their data for each task is shown in Table 4. City Bank and Health^2 both received data from all participants. The beverage store, which required relatively little data, obtained data in 87.5% of the cases. However, Concerto, which requested much more data than the beverage store did, obtained 93.75%. Fillinger Apothecary Group and Fit4Fun required participants to share claims on their ID card, credit card, medication, hospital, and illness history, together with other data. Fillinger obtained data from 87.5% and Fit4Fun 75%. Five of the sixteen interviewees decided to decline the transmission at one point, and all at least in the second round. The privacy-aware designs involved in the first round were normal (1/3), privacy smiley (1/3), and sensitivity score (1/3). In the second round, the sensitivity score (3/5) and counter (2/5) were applied.

When asked why they shared their data, seven participants said it was because it made sense to them. Another reason often indicated was that the institution is trustworthy. Seven participants said that they wanted this service. Moreover, two participants said that they have to share their data on the Internet. Some participants did not mind whether their data was known because they thought it contained nothing important. Finally, trust in the app itself also made them believe that they could share their data securely. When asked if they think other people could use this wallet responsibly, the participants answered that with such a wallet, it is easier to share one's data than traditional means. One participant said that people "will only understand it after something [bad] happened". Eight participants agreed that they would trade privacy for convenience, and another five said that it depended on the context. Moreover, one interviewee explained that they thought they would not, but after the study, they were no longer sure.

VIII. DISCUSSION

The user study showed that participants traded highly sensitive information for their convenience or to receive the desired service or product. Designs to protect users were only partially effective. We summarize (see Section VIII-A) and discuss the findings of our user study related to the disclosure of data (see Section VIII-B), trust and sensitivity of data (see Section VIII-C), and the resulting design implications (see Section VIII-D), pointing out similarities in the literature. Additionally, we use the results to discuss the impacts on current SSI wallets in Section VIII-E. Based on this discussion, we suggest future work in Section VIII-F.

A. ANSWERS TO RESEARCH QUESTIONS

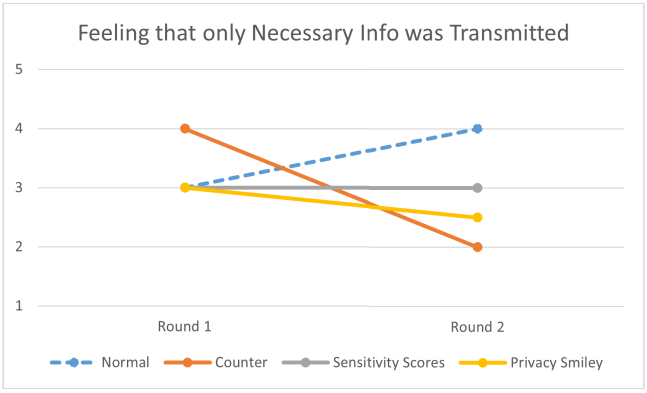
In the following, we summarize the answers to the research questions stated in Section I.

1) RQ1 – ARE USERS WILLING TO ADOPT MOBILE SSI AS THE NEW IDENTITY MANAGEMENT CONCEPT?

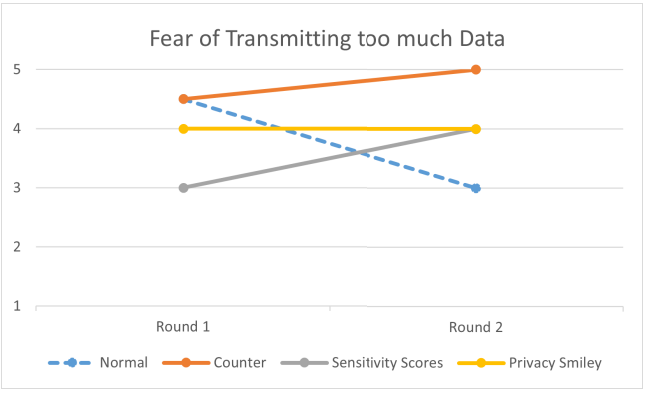
In both studies, the participants rated ease of use and enjoyment comparably high. In addition, they mainly agree on liking the mobile SSI wallet more than the physical ones. In the discussion of the user study, nine of the 16 participants stated that they could imagine using this wallet daily. The decision of four participants depended on the conditions, whereas three would not use it daily.

2) RQ2 – WHAT IS THE USERS' UNDERSTANDING OF THE UNDERLYING SSI PARADIGM, AND HOW DOES THIS INFLUENCE THEIR ACTIONS?

As shown in Table 2, the participants rated the control over personal data the highest with the selectable design. Thereby,



(a) Median of answers by participants when asked if they feel they only transmitted necessary information.



(b) Median of answers by participants when asked if they feared transmitting too much personal information.

FIGURE 12. Answers of participants to research questions about data transmission. Participants could answer on a 5-point Likert scale for both questions. The graphs compare the results from both rounds. Tasks in round 2 requested more sensitive information.

we conclude that they understand their control function, and their awareness might increase slightly.

Regarding the sharing behavior in the user study, we noticed that users generally shared sensitive data in these scenarios. This is even the case with privacy-aware designs, which help notice the request for sensitive data. Based on the discussion, the data was either not seen as important or anyway shared on today's Internet, the trust in the entity or wallet was rated high enough, or the benefits in exchange were worth the trade. Nevertheless, five of the 16 participants decided to decline the transmission at one point. Therefore, we assume that users balance their decisions and understand their rights to decline.

3) RQ3 – HOW CAN USERS BE SUPPORTED TO RESPONSIBLY USE THEIR DATA USING MOBILE SSI WALLETS?

As we saw in both studies, the willingness to disclose personal information seems to be influenced by many factors, including benefits and convenience. Thereby, privacy is less desirable than other factors for individuals. In addition, the participants noted that sharing data was easier with a wallet. With the prototype, we introduced four privacy awareness features that can support the responsible use of data in the SSI context. Further features explained in the design space should be tested in the future. Regulatory efforts to reduce the number of desired claims are another direction.

4) RQ4 – HOW CAN USERS BE MADE AWARE OF THE SENSITIVITY OF THEIR DATA?

In the interviews, participants compared their behavior to typical Internet services. Therefore, we assume that they at least partly understand the importance of their data but do not see a viable possibility to behave in a privacy-preserving manner. Regarding the designs, the counter was preferred by most participants, followed by alert, privacy smiley, and sensitivity scores. Whether the design helped make decisions had inconclusive answers. In future implementations, other ways of avoiding warning fatigue should be tested, such as varying and combining the designs.

5) RQ5 – HOW CAN THE DESIGN OF THE MOBILE USER INTERFACE HELP USERS MAKE PRIVACY-PRESERVING DECISIONS?

The designs integrated into the prototype for the user study clearly displayed if more or highly sensitive data was requested. In the interview, the participants indicated that the design with the presented features could raise awareness. It has been stated that more designs may be better. With regard to the user study (e. g., comparing Table 3 with Table 4), we noticed that although participants preferred privacy-aware designs, the decisions do not reflect this. The discussions with participants showed that other factors may be more important when making decisions. We assume that restricting the requested data and varying privacy-aware designs helps users make privacy-preserving decisions in the longer term.

B. PRIVACY DISCLOSURE BY USERS

Convenience or more general benefits seem to be correlated with willingness to disclose personal information. Laufer and Wolfe [58] describe the principle of the calculus of behavior. They state that privacy is not context-free. Culnan and Armstrong [59] introduce the term privacy calculus, which is used in related literature [60], [61], [62]. The privacy calculus explains that the customer discloses personal data if the benefits exceed the risks [59]. Similar behavior was observed in our user study.

According to Knijnenburg et al. [61], privacy disclosure is a complex topic. They describe privacy as contextualized anticipatory reflections, taking several observations into account. The term 'anticipatory' refers to the fact that participants may not be able to grasp the full variety of risks involved in their actions. Not only could users experience an illusion of increased privacy, but they could also be tempted

to share more data than they would otherwise. Privacy by design, as aimed by SSI, can help users. By requiring minimal data sharing, risks are mitigated. Minimal data sharing cannot be guaranteed if the user is in full control.

Dinev and Hart provide insights into the nature of the privacy paradox [60], stating that only because people share their data, this does not mean that they are not concerned about sharing it. The user study supports this assumption. Moreover, the awareness designs increased this concern, although this increase was only partly reflected in users' behavior.

C. THE ROLE OF TRUST AND PERCEPTION OF SENSITIVITY

According to Morosan [63], the magnitude of the relationship between privacy concerns and willingness to disclose is relatively low. Furthermore, Dinev and Hart note that trust is strongly related to the willingness to disclose. This is consistent with the findings of Agarwal et al. [64]. Moreover, Dinev and Hart refer to personal interests as an additional factor. Indeed, some users stated that their trust in the verifier or the wallet itself was the reason for sharing their data.

People in the study seemed to have a different perception of the sensitivity of their data. While some had no problems sharing their credit card information, others refused to make a transaction with their credit card. In addition, some participants did not think their health data were highly sensitive. Li [65] reasons that information may cause different perceptions of sensitivity for different users who share in different contexts. We assume that if users do not know that sharing is unnecessary, they will share more data than they should. Agarwal et al. [64] mention that salient beliefs and contextual differences are also important for understanding consumers' reactions. The beneficial effect of disclosure outweighs the negative effects and may counteract privacy measures [63]. In addition, the participants probably had previous experiences with sharing their data, which was beneficial to them but led to no visible downsides.

D. INTERFACE DESIGN IMPLICATIONS

Often, the participants did not seem aware of the risks or considered them to be lower. Moreover, some participants compared sharing data in an SSI wallet by accepting a cookie policy, terms, and conditions. Therefore, we assume that users consider the privacy choices SSI wallets provide similarly, despite the data being generally more sensitive. The willingness to disclose personal information seems influenced by many factors, including trust, fear, convenience, personal interests, benefits, and habits. Organizations have started to let users pay with their personal information, and, as Evens and Damme [66] discovered, users are willing to make that trade. This becomes problematic with a user-centered concept such as SSI. The proposed awareness designs influenced users' privacy concerns, but had a smaller influence on their sharing behavior. In the prototype, users were able to select additional information. This provided them with the possibility of sharing more information for better services. However, minimization is currently possible only if users have a minimal amount of choice.

In consequence, producing the greatest balance of benefits over harm was considered. Although users could benefit from the purpose of giving them possibilities and control, the privacy of the user is harmed in the long run by preferring other aspects to privacy. At the same time, these aspects were beneficial to the user.

E. IMPACT ON CURRENT SSI WALLETS

Comparing our awareness designs with wallets in the app stores (see Section III-B), we notice that the examples mostly provide even less information than we did at the beginning of our study. Users can view the claims and the issuer, but cannot receive a detailed view of both. The pre-study verified our assumption made by studying current SSI wallets that users already have to be aware of their data to make well-considered decisions. Hence, an issuer could claim to be another entity without any problem. In addition, users can accept all requests of one verifier, which these can take advantage of, and the data is blurred similarly to passwords. This may result in users sending more data than originally intended. Thereby, similar problems exist as in the German ID-Wallet [53], which was removed from the app stores due to vulnerabilities. However, too many requests can result in users clicking away the notifications, as used with cookie banners and other examples. Consequently, a balance must be found between convenience and security.

This demonstrates that security and usability have to be considered from the beginning when designing and implementing an SSI wallet. The implementation of the proposed awareness designs is feasible. Nonetheless, further work is required to determine the correct balance between notifications and convenience for users with varying technical expertise. This should result in the development of detailed design guidelines. Finally, existing SSI wallets and other SSI entities have to be analyzed in terms of their security.

F. FUTURE WORK

In future work, we plan to further explore the field of awareness design in the context of mobile SSI wallets. Not all designs shown in the design space were used in this study, and the study results can enhance the applied designs. We are particularly interested in measures targeting long-term behavioral changes with diverse participants (technical expertise, accessibility, etc.). Furthermore, we want to evaluate more existing SSI wallets and explore design recommendations, as well as passive privacy-preserving mechanisms. Finally, we plan to focus on the security threats of SSI wallets and their relationship to awareness design.

IX. CONCLUSION

SSI wallets promise to be the next step in identity management. By following the concept of privacy by design,

using a user-centered approach, and incorporating modern cryptographic techniques, users' privacy can be theoretically secured. To review privacy, a pre-study and the following user study with a refined mobile SSI wallet prototype were carried out. The results revealed that current wallets have good usability and can be easily adopted. However, the results also showed that users prefer to trade personal data for convenience or benefits. Therefore, four privacy awareness design solutions were tested in the user study. The awareness designs, except for the alert, increased the participants' privacy concerns. Nonetheless, most participants shared highly sensitive data to receive promised benefits. Awareness designs could protect users from revealing too much information, but could not hinder them completely. Conversely, SSI could lead to a situation that contradicts the concept's goals: users could get in a situation where they would share more data with a mobile SSI wallet than they would have without.

APPENDIX A QUESTIONNAIRE

The questionnaire was used for both the pre-study and the user study.

- Demographic Questions (open questions)
  - What is your participant ID?
  - What is your gender?
  - What is your age in years?
  - What is your nationality?
  - In which country do you live?
  - What is the highest degree or level of school you have completed?
  - What is your current employment status?
  - Do you have color blindness?
- Questions about Technological Affinity (open questions)
  - Do you use Apple Pay, Google Pay, or equivalent?
  - How often do you use your smartphone?
  - How far do you agree with the following sentence: I like to occupy myself in greater detail with technical systems.
- Questions about the SSI wallet (Likert scale)
  - It was easy to interact with the wallet.
  - I enjoy using the wallet.
  - I was confused by the wallet.
  - I had trust in the integrity of the wallet.
  - I had control over my personal data.
  - The transmission of personal information was cumbersome to achieve.
  - I have the feeling that I only transmitted personal information that was truly necessary to process my request.
  - I was afraid that I could transmit too much personal information about myself.
  - I like this form of wallet more than a traditional, physical one.

APPENDIX B PRE-STUDY

Table 5 shows the participants and the prototype design version per round.

TABLE 5. Participants and the prototype design version for each round. Two combinations (no-detail + detail, selectable + no-detail) were repeated, as two participants (#2 and #3) did not recognize the expandability of the view. Therefore, they were not able to see more details. One participant realized this when scanning the second QR code (#2) and the other was pointed to this during the final discussion (#3).

Participant	Round 1	Round 2
1	no-detail	**selectable**
2	no-detail	**detail**
3	**selectable**	no-detail
4	detail	**no-detail**
5	no-detail	**detail**
6	detail	**selectable**
7	selectable	**detail**
8	**selectable**	no-detail

REFERENCES

[1] S. Egelman, "My profile is my password, verify me!: The privacy/convenience tradeoff of Facebook connect," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst. (CHI)*. New York, NY, USA: ACM, Apr. 2013, pp. 2369–2378.

[2] J. Isaak and M. J. Hanna, "User data privacy: Facebook, Cambridge analytica, and privacy protection," *Computer*, vol. 51, no. 8, pp. 56–59, Aug. 2018.

[3] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, and E. Bursztein, "Data breaches, phishing, or malware: Understanding the risks of stolen credentials," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.* New York, NY, USA: ACM, Oct. 2017, pp. 1421–1434.

[4] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018.

[5] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*. New York, NY, USA: IEEE, Jul. 2018, pp. 1336–1342.

[6] N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in *Proc. 8th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*. New York, NY, USA: IEEE, Aug. 2020, pp. 90–95.

[7] S. Schwalm, D. Albrecht, and I. Alamillo, "eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI," in *Open Identity Summit 2022*, H. Roßnagel, C. H. Schunck, and S. Mödersheim, Eds. Bonn, Germany: GI, 2022, pp. 63–74.

[8] *Verifiable Credentials Data Model v1.1*, W3C, W3C Recommendation, Cambridge, MA, USA, Mar. 2022. Accessed: Oct. 11, 2023. [Online]. Available: https://www.w3.org/TR/2022/REC-vc-data-model-20220303/

[9] *Decentralized Identifiers (DIDs) V1.0—Core Architecture, Data Model, and Representations*, W3C, W3C Recommendation, Cambridge, MA, USA, Aug. 2021, Accessed: Oct. 11, 2023. [Online]. Available: https://www.w3.org/TR/did-core/

[10] D. Reed and M. Sporny. (2018). *A Short Primer for Decentralized Identifiers*. Accessed: Oct. 11, 2023. [Online]. Available: https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/topics-and-advance-readings/did-primer.md

[11] M. Kubach, C. H. Schunck, R. Sellung, and H. Roßnagel, "Self-sovereign and decentralized identity as the future of identity management?" in *Open Identity Summit 2020*, H. Roßnagel, C. H. Schunck, S. Mödersheim, and D. Hühnlein, Eds. Bonn, Germany: GI, 2020, pp. 35–47.

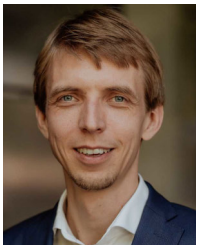
[12] Statista Research Department. (Feb. 2022). *Number of Daily Active Facebook Users Worldwide as of 4th Quarter 2021*. Accessed: Oct. 11, 2023. [Online]. Available: https://www.statista.com/statistics/346167/facebook-global-dau/

[13] M. Furini, S. Mirri, M. Montangero, and C. Prandi, "Privacy perception when using smartphone applications," *Mobile Netw. Appl.*, vol. 25, no. 3, pp. 1055–1061, Jun. 2020.
[14] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *J. Consum. Affairs*, vol. 41, no. 1, pp. 100–126, Jun. 2007.
[15] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quart.*, vol. 35, no. 4, pp. 989–1015, 2011.
[16] K.-L. Hui, H. H. Teo, and S.-Y. T. Lee, "The value of privacy assurance: An exploratory field experiment," *MIS Quart.*, vol. 31, no. 1, pp. 19–33, 2007.
[17] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?" in *The Future of Identity in the Information Society*, V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda, Eds. Berlin, Germany: Springer, 2008, pp. 226–236.
[18] V. Distler, G. Lenzini, C. Lallemand, and V. Koenig, "The framework of security-enhancing friction: How UX can help users behave more securely," in *Proc. New Secur. Paradigms Workshop (NSPW)*. New York, NY, USA: ACM, 2020, pp. 45–58.
[19] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang, and S. Wilson, "Nudges for privacy and security: Understanding and assisting Users' choices online," *ACM Comput. Surv.*, vol. 50, no. 3, pp. 1–41, May 2018.
[20] B. Mackie, "Warning fatigue: Insights from the Australian bushfire context," Ph.D. dissertation, Media Commun., UC, Canterbury, New Zealand, 2013.
[21] L. F. Cranor, "A framework for reasoning about the human in the loop," in *Proc. 1st Conf. Usability, Psychol., Secur. (UPSEC)*. Berkley, CA, USA: USENIX Association, 2008, pp. 1–15.
[22] J. C. Brustoloni and R. Villamarín-Salomón, "Improving security decisions with polymorphic and audited dialogs," in *Proc. 3rd Symp. Usable Privacy Secur. (SOUPS)*. New York, NY, USA: ACM, 2007, pp. 76–85.
[23] C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, and M. Sleeper, "Harder to ignore? Revisiting pop-up fatigue and approaches to prevent it," in *Proc. 10th Symp. Usable Privacy Secur. (SOUPS)*. Berkley, CA, USA: USENIX Association, 2014, pp. 105–111.
[24] K. Renaud and M. Dupuis, "Cyber security fear appeals: Unexpectedly complicated," in *Proc. New Secur. Paradigms Workshop*. New York, NY, USA: ACM, Sep. 2019, pp. 42–56.
[25] C. Allen. (2016). *The Path to Self-Sovereign Identity*. Accessed: Oct. 11, 2023. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html
[26] Main Incubator GmbH. (2023). *Lissi—Identity Wallet an Identity Management Solutions*. Accessed: Oct. 11, 2023. [Online]. Available: https://lissi.id/
[27] esatus AG. (2023). *Esatus AG—Enforcing Information Security*. Accessed: Oct. 11, 2023. [Online]. Available: https://esatus.com/
[28] Y. Liu, Q. Lu, H.-Y. Paik, and X. Xu, "Design patterns for blockchain-based self-sovereign identity," in *Proc. Eur. Conf. Pattern Lang. Programs (EuroPLoP)*. New York, NY, USA: ACM, Jul. 2020, pp. 1–14.
[29] A. Cavoukian, "Privacy by design," Office Inf. Privacy Commissioner, Edmonton, AB, Canada, Tech. Rep., 2009.
[30] S. Gürses and J. Pridmore, "Translating privacy into digital designs: Technical strategies to counter everyday surveillance," in *Proc. Cyber-Surveill. Everyday Life, Int. Workshop*, Toronto, ON, Canada, May 2011, p. 21.
[31] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *Proc. 35th Annu. ACM Symp. Appl. Comput. (SAC)*. New York, NY, USA: ACM, Mar. 2020, pp. 342–345.
[32] R. N. Zaeem, K. C. Chang, T.-C. Huang, D. Liau, W. Song, A. Tyagi, M. Khalil, M. Lamison, S. Pandey, and K. S. Barber, "Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI-IAT)*. New York, NY, USA: ACM, Dec. 2021, pp. 128–135.
[33] S. Sukaris, W. Renedi, M. A. Rizqi, and B. Pristyadi, "Usage behavior on digital wallet: Perspective of the theory of unification of acceptance and use of technology models," *J. Phys., Conf. Ser.*, vol. 1764, no. 1, Feb. 2021, Art. no. 012071.
[34] Arindy and A. Suzianti, "Multi-generation perception towards digital wallet in Indonesia," in *Proc. 3rd Asia–Pacific Conf. Res. Ind. Syst. Eng. (APCORISE)*. New York, NY, USA: ACM, Jun. 2020, pp. 19–24.
[35] Y. Yong Lee, C. Lay Gan, and T. Wei Liew, "Impulse Buying's antecedents and consequences: Malaysian E-wallet users perceptions," in *Proc. 5th Int. Conf. Softw. e-Bus. (ICSEB)*. New York, NY, USA: ACM, Dec. 2021, pp. 45–50.
[36] A. Voskobojnikov, O. Wiese, M. M. Koushki, V. Roth, and K. K. Beznosov, "The U in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets," in *Proc. Conf. Hum. Factors Comput. Systems (CHI)*. New York, NY, USA: ACM, 2021, pp. 1–14.
[37] S. Abramova, A. Voskobojnikov, K. Beznosov, and R. Böhme, "Bits under the mattress: Understanding different risk perceptions and security behaviors of crypto-asset users," in *Proc. Conf. Hum. Factors Comput. Syst. (CHI)*. New York, NY, USA: ACM, 2021, pp. 1–19.
[38] M. Froehlich, M. Wagenhaus, A. Schmidt, and F. Alt, "Don't stop me now! exploring challenges of first-time cryptocurrency users," in *Proc. ACM Conf. Des. Interact. Syst. (DIS)*. New York, NY, USA: ACM, 2021, pp. 138–148.
[39] C. Brunner, U. Gallersdörfer, F. Knirsch, D. Engel, and F. Matthes, "DID and VC: Untangling decentralized identifiers and verifiable credentials for the web of trust," in *Proc. 3rd Int. Conf. Blockchain Technol. Appl. (ICBTA)*. New York, NY, USA: ACM, 2020, pp. 61–66.
[40] V. Lyubashevsky, N. K. Nguyen, and G. Seiler, "Practical lattice-based zero-knowledge proofs for integer relations," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*. New York, NY, USA: ACM, 2020, pp. 1051–1070.
[41] A. Grüner, A. Mühle, and C. Meinel, "ATIB: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider," *IEEE Access*, vol. 9, pp. 138553–138570, 2021.
[42] Q. Stokkink, G. Ishmaev, D. Epema, and J. Pouwelse, "A truly self-sovereign identity system," in *Proc. 46th Conf. Local Comput. Netw. (LCN)*. New York, NY, USA: IEEE, 2021, pp. 1–8.
[43] V. Bolgouras, A. Angelogianni, I. Politis, and C. Xenakis, "Trusted and secure self-sovereign identity framework," in *Proc. 17th Int. Conf. Availability Rel. Secur. (ARES)*. New York, NY, USA: ACM, 2022, pp. 1–6.
[44] v. Čučko and M. Turkanović, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access*, vol. 9, pp. 139009–139027, 2021.
[45] A. Preukschat and D. Reed, *Self-Sovereign Identity*. Shelter Island, NY, USA: Manning Publications, Aug. 2021.
[46] D. Hardman and J. Law. (2018). *Self-Sovereign Privacy by Design*. Accessed: Oct. 11, 2023. [Online]. Available: https://github.com/sovrin-foundation/protocol/blob/master/self_sovereign_privacy_by_design_v1.md
[47] European Blockchain Associaton. (2021). *SSI Wallets*. Accessed: Oct. 11, 2023. [Online]. Available: https://europeanblockchainassociation.org/ssi-wallets/
[48] Verimi. (2023). *Verimi ID Wallet—Your Digital Wallet*. Accessed: Oct. 11, 2023. [Online]. Available: https://verimi.de/en/
[49] iGrant.io. (2023). *iGrant.io—Your Data, Your Choice*. Accessed: Oct. 11, 2023. [Online]. Available: https://igrant.io
[50] Validated ID. (2023). *Vidwallet—Regain Control of Your Digital Identity*. Accessed: Oct. 11, 2023. [Online]. Available: https://www.validatedid.com/en/vidchain/vidwallet
[51] Jolocom. (2023). *We Create Solutions for the Future of Digital Identity*. Accessed: Oct. 11, 2023. [Online]. Available: https://jolocom.io
[52] Gataca. (2023). *Trusted Digital Identities Made Easy*. Accessed: Oct. 11, 2023. [Online]. Available: https://www.gataca.io
[53] L. Wittmann. (2021). *Mit Der ID-Wallet Kannst Du Alles und Jeder Sein, Außer Du Musst Dich Ausweisen*. Accessed: Oct. 11, 2023. [Online]. Available: https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%C3%9Fer-du-musst-dich-ausweisen-829293739fa0
[54] React Native. (2023). *React Native—Website*. Accessed: Oct. 11, 2023. [Online]. Available: https://reactnative.dev/
[55] H. Chernoff, "The use of faces to represent points in k-Dimensional space graphically," *J. Amer. Stat. Assoc.*, vol. 68, no. 342, pp. 361–368, Jun. 1973.
[56] DuckDuckGo. (2023). *Privacy Essentials*. Accessed: Oct. 11, 2023. [Online]. Available: https://duckduckgo.com/app
[57] Google. (2023). *Android 12*. Accessed: Oct. 11, 2023. [Online]. Available: https://www.android.com/android-12
[58] R. S. Laufer and M. Wolfe, "Privacy as a concept and a social issue: A multidimensional developmental theory," *J. Social Issues*, vol. 33, no. 3, pp. 22–42, Jul. 1977.

[59] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Org. Sci.*, vol. 10, no. 1, pp. 104–115, Feb. 1999.
[60] T. Dinev and P. Hart, "An extended privacy calculus model for E-commerce transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, Mar. 2006.
[61] B. Knijnenburg, E. Raybourn, D. Cherry, D. Wilkinson, S. Sivakumar, and H. Sloan, "Death to the privacy calculus?" *Electron. J.*, pp. 1–8, Feb. 2017. [Online]. Available: https://adlnet.gov/publications/2017/02/death-to-the-privacy-calculus/
[62] Y. Sun, S. Fang, and Y. Hwang, "Investigating privacy and information disclosure behavior in social electronic commerce," *Sustainability*, vol. 11, no. 12, p. 3311, Jun. 2019.
[63] C. Morosan, "Disclosing facial images to create a consumer's profile: A privacy calculus perspective of hotel facial recognition systems," *Int. J. Contemp. Hospitality Manage.*, vol. 31, no. 8, pp. 3149–3172, 2019.
[64] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Inf. Syst. Res.*, vol. 15, no. 4, pp. 336–355, Dec. 2004.
[65] Y. Li, "Empirical studies on online information privacy concerns: Literature review and an integrative framework," *Commun. Assoc. Inf. Syst.*, vol. 28, no. 1, p. 28, 2011.
[66] T. Evens and K. Van Damme, "Consumers' willingness to share personal data: Implications for Newspapers' Bus. Models," *Int. J. Media Manage.*, vol. 18, no. 1, pp. 25–41, Jan. 2016.

MORITZ TEUSCHEL received the B.Sc. degree in media informatics and the M.Sc. degree in computer science from Ludwig-Maximilians-Universität München. He is a Cybersecurity Consultant in the automotive area. Additionally, he has an apprenticeship and work experience as an audiovisual media designer. His research interests include IT security, blockchain, and wallets.

DANIELA PÖHN is currently pursuing the Ph.D. degree in dynamic identity management in federations with Ludwig-Maximilians-Universität München. She is also a Senior Researcher with the Research Institute Cyber Defence and Smart Data (RI CODE), University of the Bundeswehr Munich. In her role as a Research Assistant with the Leibniz Supercomputing Centre, she was improving the global federation eduGAIN. She is also actively involved in projects related to interactive cyber training. Her research is primarily focused on identity management and social engineering.



MICHAEL GRABATIN received the B.Sc. and M.Sc. degrees in computer science from Ludwig-Maximilians-Universität München. He is currently pursuing the Ph.D. degree with the Research Institute Cyber Defence (RI CODE), University of the Bundeswehr Munich (UniBw M). His work focuses on the conception and development of technologies for federated identity management (FIM) and self-sovereign identity management (SSI) systems, including web, the Internet of Things (IoT), and government (eID) applications.

FELIX DIETZ received the B.Sc. degree in media informatics and the M.Sc. degree in human–computer interaction from Ludwig-Maximilians-Universität München (LMU). He is currently part of the Usable Security and Privacy Group, UniBw M, as a Ph.D. Student, investigating physiological reactions in security-relevant situations. Along with his studies, he was a Student Assistant with LMU, and the Institute for Applied Mathematics and Scientific Computing, UniBw M. He was a Tutor of various courses with LMU, and also a Research Associate with the Institute of Networks and Security, JKU Linz. Before his time at UniBw M, he was working in information security with InterCard/Verifone.

WOLFGANG HOMMEL is a Professor of software and data security with the University of the Bundeswehr Munich, where he is also the Executive Director of the Research Institute Cyber Defence and Smart Data (RI CODE). He has worked on the systematic design and practical implementation of identity management solutions on national and international scales in research and education networks and e-government for the past 15 years. Advancing identity management protocols and processes for identity federations and self-sovereign identity infrastructures has been the subject of numerous dissertations, student theses, and scientific publications of his research group.

FLORIAN ALT received the Diploma degree in media informatics from LMU Munich and the Ph.D. degree in human–computer interaction from the University of Stuttgart. He is a Professor of usable security and privacy with the University of the Bundeswehr Munich. In his work, he is interested in designing secure and privacy-preserving systems, that naturally blend with the way in which users interact with computing devices. His research focuses on investigating users behavior in security contexts, creating and enhancing security and privacy mechanisms based on users behavior and physiology, and understanding and mitigating threats emerging from novel ubiquitous technologies. Specific areas of application are mixed reality, smart homes, and social engineering.