# An Empirical Study of a Decentralized IdentityWallet
## Usability, Security, and Perspectives on User Control

Korir, Maina; Parkin, Simon; Dunphy, Paul

**Publication date**
2022

**Document Version**
Final published version

**Published in**
Proceedings of the 18th Symposium on Usable Privacy and Security, SOUPS 2022

**Citation (APA)**
Korir, M., Parkin, S., & Dunphy, P. (2022). An Empirical Study of a Decentralized IdentityWallet: Usability, Security, and Perspectives on User Control. In *Proceedings of the 18th Symposium on Usable Privacy and Security, SOUPS 2022* (pp. 195-211). (Proceedings of the 18th Symposium on Usable Privacy and Security, SOUPS 2022). USENIX Association.
https://www.usenix.org/conference/soups2022/presentation/korir


# An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control

Maina Korir, *University of Bedfordshire;* Simon Parkin, *TU Delft;*
Paul Dunphy, *OneSpan*

https://www.usenix.org/conference/soups2022/presentation/korir

This paper is included in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

Open access to the Proceedings of the Eighteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

# An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control

Maina Korir
*University of Bedfordshire*[*]
*maina.korir@beds.ac.uk*

Simon Parkin
*TU Delft*
*s.e.parkin@tudelft.nl*

Paul Dunphy
*OneSpan*
*paul.dunphy@onespan.com*

## Abstract

User-centric digital identity initiatives are emerging with a mission to shift control over online identity disclosures to the individual. However, there is little representation of prospective users in discussions of the merits of empowering users with new data management responsibilities and the acceptability of new technologies. We conducted a user study comprising a contextual inquiry and semi-structured interviews using a prototype *decentralized identity* wallet app with 30 online participants. Our usability analysis uncovered misunderstandings about decentralized identifiers (DIDs) and pain points relating to using QR codes and following the signposting of cross-device user journeys. In addition, the technology did not readily resolve questions about whether the user, identity provider, or relying party was in control of data at crucial moments. We also learned that users' judgments of data minimization encompass a broader scope of issues than simply the technical provision of the identity wallet. Our results contribute to understanding future user-centric identity technologies from the view of privacy and user acceptance.

## 1 Introduction

Identity fraud impacts around 10 million Americans per year [70] and costs the global economy $5 trillion per year [57]. In addition, over 90% of American consumers believe they have lost control over how their personal information is collected and used [60]. At the same time, a groundswell of new digital infrastructures [51, 75] and political initiatives are creating a renewed vigor to explore new and better ways to transact online using our identity. A common goal is to leverage user-centric identity technologies while improving access to vital services, including those provided by governments, healthcare providers, travel hubs, and financial institutions. The European Union pursues a mission to create a European Digital Identity [29]. National governments are drafting identity governance frameworks, e.g. United Kingdom [69], Canada [21], and the United States [17]. Large companies also modify their product offerings [40, 52] to accommodate privacy-friendly decentralized identity (also referred to as self-sovereign identity) [59].

One technology that is fast emerging as a cornerstone of most, if not all, future proposals for user-centric digital identity schemes is the *identity wallet*: *a tool that enables end-users to prove aspects of their identity online in a secure and privacy-respectful manner*. An identity wallet enables users to have meaningful control over the transfer and disclosure of verified personal information when identity is federated between online services. One core function of the technology is to collate cryptographic attestations of personal attributes (e.g. age, name) or entitlements (e.g. right to work) from an identity provider in a form verifiable by a second online service. German law already permits identity wallets to be legally used within anti-money laundering regulations to access financial services [22] and the federal government has already deployed its own identity wallet [6]. Private companies have also created identity wallet technologies for deployment in their products [30, 45, 46].

While the velocity of design and rollout of identity wallets is increasing, we lack knowledge about the characteristics of a successful user-centric identity wallet. We see three reasons we must further investigate these new technologies. Firstly, an identity wallet is a complex technology that integrates multiple processes that pertain to security and privacy; secondly, there is an untested assumption that the perception of enhanced control over the disclosure of personal data will drive user acceptance. Finally, while identity wallets are still in a

[*]This work was led by the first author during an internship at OneSpan


*USENIX Symposium on Usable Privacy and Security (SOUPS)* 2022.
August 7–9, 2022, Boston, MA, United States.

formative stage, there are few reported trials or experiments focused on the user experience.

In this paper, we report the results of a user study of an identity wallet prototype designed using tools for decentralized identity [59] – the most privacy-respecting vision for online user-centric identity. We conducted a user study comprised of a *contextual inquiry* and *semi-structured interview* with 30 participants recruited from the United Kingdom and the United States. Our findings cut across the domains of usability, security, and privacy. For example, while the most ambitious vision of decentralized identity requires user autonomy for identity data and credential storage, there was a dominant expectation that (at least) one trusted party provides account recovery if wallet data were lost or corrupted. The root of this finding is that participants reported not being fearful of losing an identity wallet. Also, the accuracy of user judgments about the oversight held by external parties was mixed, which is a concern if the assumed benefit of identity wallets to users is an acute understanding of data control. More generally, we learned that today, participants are dependent on paper-based methods to identify themselves to identity-critical services. However, we also found that while poor experiences onboarding with paper documents are common, participants increasingly have experiences with improved technology for document scanning, data parsing, biometric checks, etc. Therefore there appears to be an arms race between new user-centric identity methods that preserve privacy and more efficient ways to capture and parse privacy-invasive data for identity purposes. The contribution of this paper is as follows:

- We present insights into the user perceptions and acceptance of the key components of a decentralized identity wallet: decentralized identifiers (DIDs), verifiable credentials (VCs), and identity proofs. More specifically, we shed light on the perceptions of *user control* delivered by identity wallets in the context of decentralized identity, in that technically constructed privacy benefits might constitute small drivers for uptake.
- We propose a method to capture users' mental models of security and privacy in the context of identity wallets that is also applicable to other user-centric technologies. Our lightweight mental model scale prompted participants to express their intuition and understanding of the technology and geography of data. The technique informs approaches for determining how well users' understanding of user-centric services impacts acceptance, an important issue with, e.g. FIDO2 authentication [43].
- We detail usability measures and user journey challenges inherent to decentralized identity wallets. We also draw parallels to similar issues inherent to other user-centric technologies, such as FIDO [16] and FIDO2 [43], where learnability is a particular challenge for end-users. Finally, we propose improvements for identity wallet technology.

The remainder of the paper is organized as follows: Section 2 details related work, and Section 3 introduces key concepts of identity wallets and the design of our prototype. Our user study design is detailed in Section 4, followed by presentation of results (Section 5), limitations (Section 6) and discussion (Section 7). Our concluding remarks are in Section 8.

## 2 Related Work

### 2.1 Federated Identity Management

Federated Identity Management (FIM) is the technology and process to transfer trustworthy attributes from one security domain to another. FIM techniques and technologies are standard in orchestrated and closed deployments (e.g. a workplace), but it is a more significant challenge to achieve FIM on the open Internet where, back in 2001, users had an average of 16 accounts to manage [63]. In FIM deployments, the number of parties involved in an identity transaction increases from two parties to three, and we get what is known as the *trust triangle* [59] that has three roles: issuer, verifier, and holder (or, identity provider, relying party, and user).

The seven laws of identity [14] are heuristics that support the evaluation of identity schemes and are particularly relevant to FIM. Microsoft designed CardSpace around 2006 to instantiate those seven laws and create a universal identity layer for the Internet. Indeed, one claimed design priority of the Microsoft Infocard system was the user experience [15].

Landau and Moore [42] propose that FIM is a technology of great promise whose wider adoption has so far been disappointing, and also describe some of the economic *tussles* that can make or break FIM in a specific application. They propose that so far, identity providers and service providers have tussled about who controls user data rather than the provision of benefits to users. Gov.Verify is one British government system that federates citizen identity across government services. Gov.Verify is beset by privacy concerns [8] along with citizen concerns about interacting with the government via private companies [12].

### 2.2 Web Single-Sign On

Single-sign on is one critical application of FIM, and this exists on the open web, most commonly in the form of the standards-based *OpenID Connect* (OIDC), or OAuth 2.0 [1]. Google provides an OIDC compatible sign-on, but *Facebook Connect* provides a proprietary sign-on technology that leverages OAuth 2.0. While technically different, Facebook's single sign-on mechanism is conceptually similar. One significant difference is that OIDC offers a taxonomy of the attributes and data formats that an application can provide and consume, whereas OAuth 2.0 does not [18]. Facebook proposed in 2010 that there were more than 250 million users

of Facebook Connect [71], and research has expressed concern that users were not making informed consent for sharing attributes with online services [27].

A study of web single sign-on relying parties suggested Facebook followed by Google were dominant identity providers, and that 75% of relying parties request more than authentication state from identity providers [18]. One reason for a relying party to prefer one identity provider relates to the *attributes* that an identity provider can provide to a relying party. These attributes could be trustworthy to different degrees. For example, a first name and surname may not be reliable from Google. However, Facebook performs some basic validation of names, which might make Facebook more desirable if an application requires the user's "real" name [31].

## 2.3 User Centricity and Decentralized Identity

User centricity is a crucial framework in Federated Identity Management (FIM) because it forces reflection on *how* to implement FIM to respect the privacy of the end-user. There are three dimensions to user-centricity: user control, architecture, and usability [7]. For example, technologies such as those compliant with FIDO standards [35] are user-centric.

Decentralized identity – also known as *self-sovereign identity* (SSI) [59]) – is borne out of dissatisfaction with the privacy properties and power dynamics inherent to some user-centric identity technologies. Decentralized identity manifests as principles to reinforce the goal that the user is central to the administration of their identity [3]. Furthermore, several specific elements are commonly associated with decentralized identity: (i) an eco-system of multiple identity providers, (ii) a decentralized *trust registry* [56] - a root of trust that contains tamper-resistant shared records and has no single point of failure, and (iii) an identity wallet for end-users that stores personal information and provides cryptographic techniques for privacy-friendly information disclosure. For the latter, Decentralized Identifiers (DIDs) [65] are user-generated identifiers that decouple identifiers from identity providers and are verifiable through public-key cryptography. A *verifiable credential* (VC) [72] can digitally represent attributes found in physical identity documents such as name or date of birth and new things that have no physical equivalent, such as ownership of a bank account. In addition, VCs contain digital signatures, which makes their authorship verifiable and their contents tamper-resistant. Zero knowledge proofs [34] are also considered to be relevant techniques. Candidate schemes that embody these techniques have already been proposed [48] and the user experience of constituent technologies will be critical for future uptake [25, 26].

# 3 Identity Wallets

The design of user-centric identity infrastructures requires the existence of a means to provide the user with control of personal data and disclosures. In most cases, this necessitates the existence of a conceptual or visual control panel where the user can inspect the status of their entitlements and data and provide consent to, and initiate, information disclosure. There are numerous examples of approaches to design this control panel. This could, for instance, be a simple user interface displayed by a website requesting consent to disclose information to another party. For example, in the Microsoft InfoCard project, the *identity selector* [15] was built into the Windows operating system and provided a point of control where the user can select which cards (credentials) to disclose.

In the context of decentralized identity [59], this control panel takes the form of an identity wallet which stands to inherit additional complexity than seen in previous user-centric systems such as InfoCard for multiple reasons. For example, the integrity and authenticity of identity information depends upon public-key cryptography secured primarily by the wallet, the design of an identity wallet is geared to portable devices which might be lost, the user journeys cut across multiple devices and workflows are asynchronous, and the wallet must also interact with a decentralized trust registry. Furthermore, the wallet software may not be controllable by an identity provider or a relying party.

We wanted to understand the dominant design approaches inherent to decentralized identity wallets. Therefore we firstly gathered publicly available decentralized identity wallets that we could find, namely: uPort [46], Connect.Me [30], Lissi [45], ShoCard [58], and SelfKey [64]. None of these apps appeared authoritative. Therefore, we abstracted the user journeys to create an identity wallet app template (which can be seen in Figure 1). We learned that there are three key journeys envisioned in identity wallet apps:

1. **Connect Identity Wallet** - The wallet scans a QR code created by the online service and looks up the public key of the online service from a decentralized registry using its W3C Decentralized Identifier (DID) [65]. The wallet generates a new DID and shares this with the online service, and negotiates a shared key with the online service using its public key. This process results in a secure connection between the identity wallet and the online service.

2. **Obtain Credential** - The wallet requests a W3C Verifiable Credential [72] from the identity provider for attributes that were verified apriori. The identity provider sends a *credential request* to the identity wallet. The user must read and accept this credential request, and then the credential – digitally signed by the identity provider – is sent to the wallet for secure storage.

3. **Enrol Using Proof** - The end-user navigates to a new online service and selects to enrol using an identity proof. The online service sends a *proof request* JSON structure to the identity wallet that lists the attributes that the user

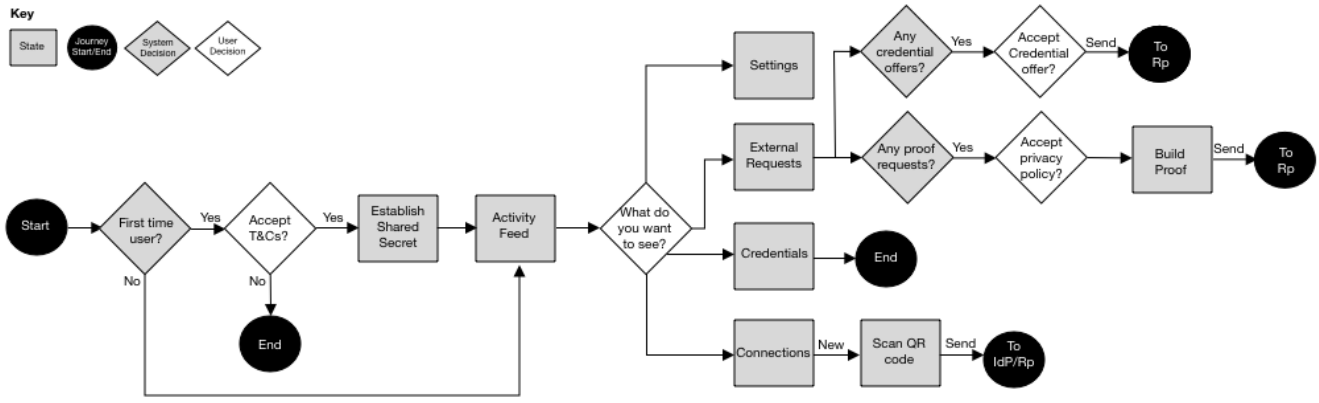


Figure 1: In order to understand the characteristics of existing decentralized identity wallets, we evaluated the user journeys of several publicly available wallets. We found that there were three journeys that apps had in common: (i) Connect Identity Wallet, (ii) Obtain Credential, and (iii) Enrol Using Proof. We also found that user journeys within the identity wallet are brief and usually involve a task switch to interact with the system of an identity provider (IdP) or relying party (Rp) using a different app or device.

must evidence before enrolment. The user then responds by matching a credential with each attribute and sending the proof, along with cryptographic proof that the wallet owns the credential(s).

We also learned that each user journey in the app is brief and requires the switch to another app or device to interact with the online system of the identity provider or relying party.

## 3.1 Open Challenges

An identity wallet combines processes that are individually challenging according to user-centered security and privacy research, such as understanding privacy policies, obtaining informed user consent, personal information storage, and cryptographic key management. Prior work has also highlighted the specific challenges facing user uptake of identity management technologies such as an unclear user proposition [20], lack of perceived urgency to adopt identity management technology [68], and a focus from the technology designers on owning data of the user [42]. However, it remains unclear if identity wallets will solve, or suffer from, the same issues.

Moving data-sharing processes online generally brings challenges, for instance, in how users can be supported not to over-disclose personal information when interacting with services [41]. Identity wallets act then as a consolidated tool to manage how data is shared with requesters, removing web interfaces as a potential source of confusion or friction. Identity wallets are, in essence, an attempt to provide a user-centric solution for individuals' data-sharing practices. Encompassed in this challenge is how to encourage adoption of complex yet well-intentioned technologies while providing the necessary assurances, as with encrypted communications (e.g. [32, 67]).

Secondly, the design promise of an identity wallet is that it should deliver enhanced end-user control [7] over the storage and disclosure of identity attributes when compared to incumbent, paper-based methods. However, it is unclear whether the dominant technical framing of user control will constitute a driver of uptake for end-users. Finally, while the need for identity wallets is widely assumed, their current state as a concept means we cannot yet enumerate the challenges they will present to the security and privacy of end-users. Therefore there is a pressing need to research these challenges before large-scale deployments occur. For example, one aspiration is that 80% of Europeans will be using identity wallets by 2030 [29].

# 4 User Study

We conducted a user study to explore our overarching research question: *What are the user-centered privacy and security challenges facing decentralized identity wallets?* We scoped our interest in this broad research question through three sub-questions: i) Which problems do users have today to prove identity online? ii) How are the privacy properties of the technology valued by end-users? iii) What are the usability properties of identity wallets?

## 4.1 Methodology

To explore our research questions, we performed a *contextual inquiry* [61] which is a well-established method in human-computer interaction for uncovering requirements and problems relating to a context of use. Our contextual inquiry was composed of three tasks for participants to complete,

where data included insights from "thinking aloud" and a *semi-structured interview*. The most challenging aspect of addressing the research questions was to gather experiences of a technology that is nascent and where end-to-end implementations are not openly available. Therefore, we needed to develop our own prototype that was broadly representative of identity wallets that can be found today to simulate the experiences that users might have in practice, and draw conclusions for that entire class of technology. Future-oriented prototypes can be of great value in usable security and privacy research as they can facilitate *problem-scoping* and *problem-solving* [49].

Conducting a contextual inquiry (including think-aloud techniques) to gauge potential user acceptance of future-facing prototypes is a well-established practice in user-centered security and privacy research. For example, Lyastani et al. [37] at IEEE S&P 2020 instrumented a dummy online service with FIDO2 authentication libraries in order to collect usability insights on FIDO2 passwordless authentication, which was not widely deployed at that point in time. Sun et al. [68] at SOUPS 2011 instrumented a prototype to simulate a browser-enabled version of OpenID, though behind the scenes their prototype contained a man-in-the-middle proxy to relay login details (since websites were not compatible with the technology). Brostoff et al. [12] explored the use of federated government ID to access healthcare information using low fidelity prototypes before such a service had seen deployment.

In order to explore our interest in perceptions of privacy features, particularly user control, we created a concise *mental model* scale designed to try to hone in on security and privacy perceptions of a specific identity wallet component and also to reveal participants' intuition about their control over personal data. This mental model scale sought to check the *functional* mental model participants had of some properties of an identity wallet and how they relate to tasks; this is as opposed to a *structural* mental model of the underlying details of how the system works [23]. Such approaches are helpful to probe users' understanding of the properties of, for example, end-to-end encryption (E2EE) [19]. Similar approaches to relate beliefs to the functional workings of security-related technologies can probe, for example, beliefs about the safety of online browsing and the use of dedicated security software [74]. Here we probe a mix of functional and sentiment-driven perceptions.

Finally, we chose to situate the context of the study in the banking and financial services sector since the industry faces multiple problems in verifying customer identity in the face of anti-money laundering regulation [36]. In addition, novel proposals aim to provide a digital identity infrastructure specifically for banking [28, 76]. Furthermore, banking is a use case of importance to members of the public that we hoped would provoke curiosity and insight.

## 4.2 Prototype

Our prototype worked end-to-end and had three components: the identity wallet mobile app, the backend distributed ledger network, and the end-user facing websites to depict the identity provider (IdP) and the relying party (Rp). Screenshots of the Android prototype are in Figure 2. We created the identity wallet app for the Google Android platform and used the Hyperledger Indy SDK (herein Indy SDK) [39]. The Indy SDK provides functionality for several fundamental components of a decentralized identity wallet: W3C Decentralized Identifiers (DIDs), W3C Verifiable Credentials,and data retrieval from a Hyperledger Indy ledger.

We created websites that resembled fictional banks: Alpaca Bank (IdP) and Bank of Carpathia (Rp). These sites had plausible domain names for financial institutions and LetsEncrypt [44] TLS certificates. We hosted the service providers on Amazon Web Services, and both entities could read and write to the Indy ledger. A snapshot of the user interface of these services is in Figure 2.

We also created a five-node Hyperledger Indy network [39]. Indy records references to verifiable credentials and provides functions for revocation. The IdP can write to the Indy ledger to add a credential reference to a cryptographic accumulator, and the Rp can read the same cryptographic accumulator to verify the validity of credentials bundled in a proof.

## 4.3 Method

Before the study, we sent the participant a URL to the study information sheet and captured their consent to participate using an eSignature tool. Then, after agreeing on a convenient time for the study, we asked the participant to install the identity wallet app on their mobile device via a private URL in the Google Android Play Store.

We conducted the study as follows: The participant connected to the video call; the experimenter then checked that the participant joined the meeting on both a laptop and a mobile device. The experimenter firstly gave a brief verbal description of the study and allowed the participant to ask any questions. Next, the experimenter led the participant through a semi-structured interview that generally covered their online identity experiences. We then asked the participant to screen share on their mobile device while connected to Zoom, and to carry out individual steps for the following tasks while *thinking aloud* [61]: making a connection, obtaining a credential from the IdP, and building a proof. The experimenter noted the critical incidents encountered using Nielsen's usability incident taxonomy [54] as the participant thought aloud. The experimenter then led the participant through a second part of the semi-structured interview, using a mental model scale to identify their perceptions of privacy and the identity wallet concept, and the System Usability Scale [11] to assess the subjective usability of the identity wallet app.

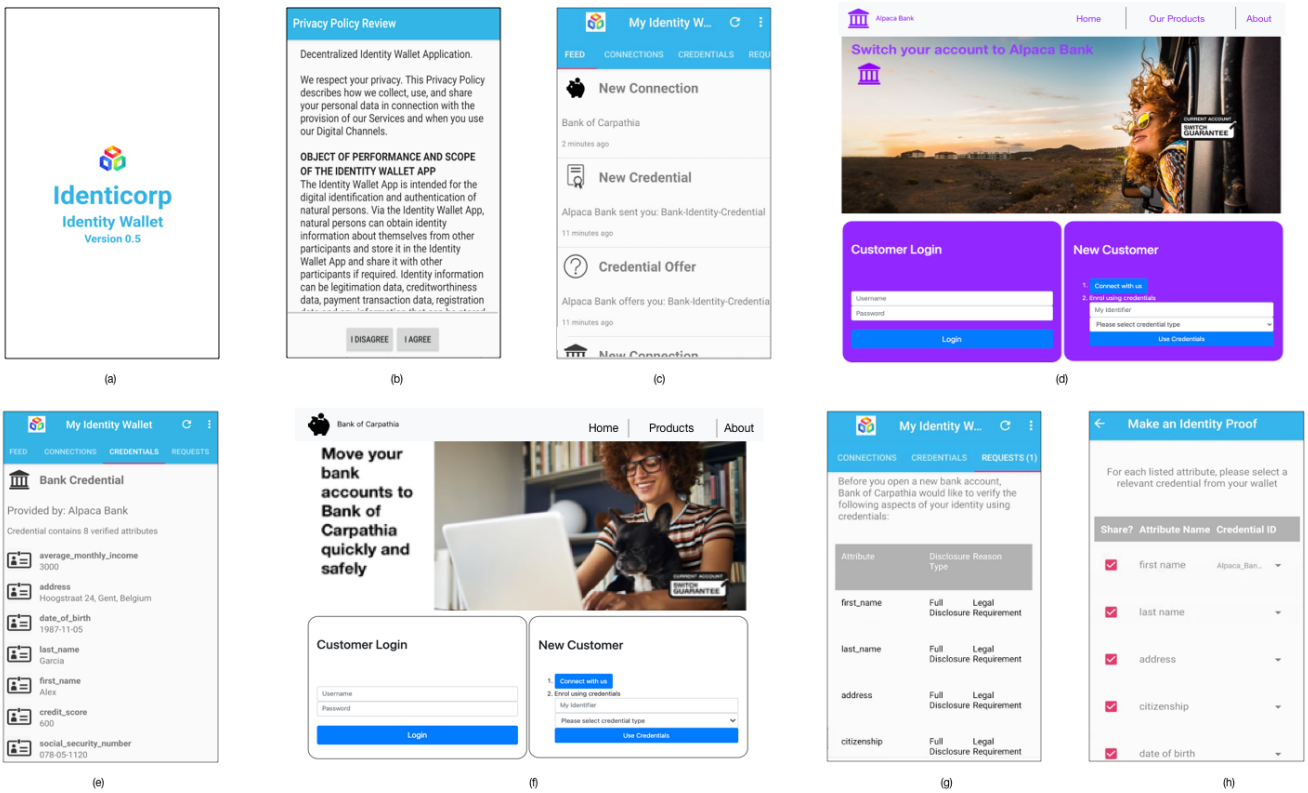


Figure 2: Screenshots from different aspects of our identity wallet prototype: (a) introductory screen, (b) privacy policy, (c) a news feed that illustrates recent and relevant events, (d) the identity provider web page, (e) an example of a verifiable credential (VC), (f) the relying party's web page, (g) a proof request from the relying party that details the attributes that the bank needs from the end-user, and (h) the process of building an identity proof, by selecting which attributes to share and which VC to use to evidence that attribute.

The full study questionnaire accompanies this paper in the Appendix and has the following sections:

**Current forms of identity and identification.** Questions focused on how participants currently identify themselves, the techniques they use, how they perceive the process, and if they encounter any challenges (usability, security, and privacy).

**Interactions with the identity wallet.** Questions following participants' interaction with the identity wallet app focusing on their perception of the identifier, credentials, and identity proof.

**Reflection on identifiers and proofs.** Questions focused on how participants perceived the opportunity to generate an identifier for themselves using the identity wallet app, to control the information they share with the Rp, the fact that their transactions are invisible to the IdP, and the security and privacy offered by the identifier, credentials, and proofs.

**Usability and user expectations.** Questions focused on the usability of the identity wallet app, participants' trust in the app, and, in general, how they saw the identity wallet app fitting into their existing practices to identify themselves.

### 4.3.1 Qualitative Analysis

We extracted audio from the video recording of each participant and performed a complete transcription of all sessions. The process yielded approximately 30 hours of transcribed audio data. Transcripts were then anonymized and subjected to a deductive thematic analysis using the method proposed by Braun and Clarke [9]. Our deductive analysis focused on identifying text that pertained to the sub-research questions that we describe in Section 4. Since we designed our user research sessions to address the research questions, our analysis procedure resembled an inductive analysis. First, we summarized each text extract with an open-ended code. After creating a preliminary codebook, regular meetings were held amongst the research team to understand better and refine the code book and to group codes into themes.

## 4.4 Participants

We recruited 30 participants for the study with an even split between male and female participants. Seventeen were from the United States and thirteen from the United Kingdom. Participant ages tended to the younger end of the spectrum: two in the range 18-24; 12 in the range 25-34; 10 in the range 35-44; 4 in the range 45-54; and finally, two aged 55+. Participants were generally highly-educated, with 73% educated to at least a bachelor's degree level and 17% with a background in computer science.

Due to restrictions on in-person research as a result of Covid-19, we conducted the study remotely and recruited participants using the research participant recruitment service *user interviews*[1]. We paid each participant $50 for a one-hour session. Given the nature of this online platform, we can assume this platform enabled us to recruit adults who were savvy users of the World Wide Web. The *user interviews* platform has been used in other user-centered research studies [10, 38]. We required that participants have a Google Android phone (minimum version 10) and one additional computing device, e.g. a laptop, to access the websites of our prototype online service providers.

## 4.5 Ethics

We received research ethics approval from the authors' respective organizations. The study adhered to the principles of the Menlo Report [24]. Participants received an information sheet with details about the study. They were free to participate and could withdraw at any time. There were no disadvantages for those who took part. The study complied with GDPR requirements; for example, we only collected data that was relevant to the study.

# 5 Results

## 5.1 Quantitative Results

### 5.1.1 Task Timings

Using the recordings of the video calls with participants, we measured the time to complete each of the three tasks. Figure 3 illustrates the distribution of task lengths broken down by task. Such data gives a sense of the learnability and efficiency of usage of the identity wallet.

For task one, the median completion time was 225 seconds (Inter-Quartile Range = 160), for task two: 121 seconds (IQR=49.5), and task three: 177 seconds (IQR=84).

### 5.1.2 User Journey Issues

Four classes of issue contributed to lowering the task completion efficiency: QR codes, security and privacy misunderstandings, device switching, and authentication.

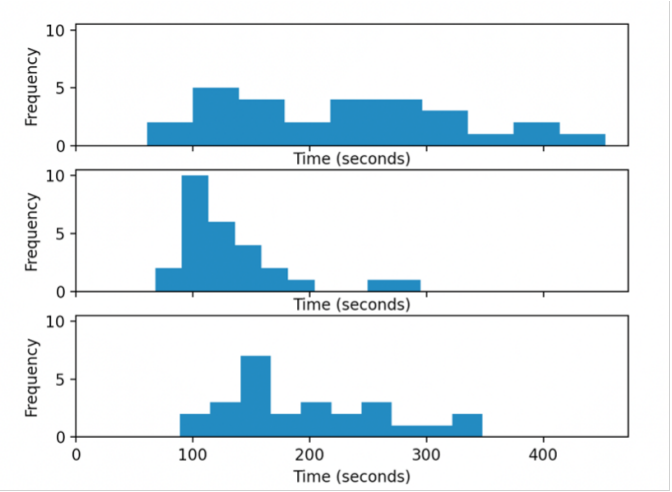


Figure 3: Distribution of task completion times recorded for (top) Task one; (middle) Task two; (bottom) Task three. Task one shows the greatest spread, partially due to the fact that this task requires interaction with QR codes and also user authentication to the IdP.

QR codes contributed to the most significant proportion of user journey disruptions, some minor and some severe [53]. An example of low severity issues includes difficulty focussing the phone camera on the QR code; an example of a higher severity issue is when the user tries to scan the QR code in the native camera application on the mobile device rather than in the identity wallet app.

Misunderstanding relates to instances where the correct understanding of the identity wallet was not in place, which created a barrier to progress in the task. For example, confusion why the identifier of a newly received credential was different to the recently generated decentralized identifier (DID); the user perceives the credential ID and DID as alphanumeric passwords, and the user was concerned about the memorability of both; concern that a mistake had taken place since the user sent a credential issued by the IdP to the Rp; expectation that the IdP and Rp shared a database, so the authentication material for the IdP should be the same on the Rp website.

Other significant sources of hesitation and confusion included *device switching*, where participants were unsure whether to interact with the IdP, the Rp, or the identity wallet. The *authentication* category relates to issues that emerged from the entry of an alphanumeric password that was required to access the services of the IdP. The password was not a mnemonic and was seemingly randomly composed, which introduced some issues. Example issues relate to matching case sensitivity, copying and pasting, and locating symbols on keyboards with different language layouts.

[1] http://www.userinterviews.com

| Question | X=Decentralized Identifier | | | X=Verifiable Credential | | | X=Identity Proof | | |
|---|---|---|---|---|---|---|---|---|---|
| | **Yes** | **No** | **Unsure** | **Yes** | **No** | **Unsure** | **Yes** | **No** | **Unsure** |
| X is secure and cannot be forged. | 50% | 11% | 39% | 59% | 4% | 37% | 69% | 8% | 23% |
| X minimises the personal data that I need to share* | 75% | 4% | 21% | 70% | 11% | 19% | 88% | 8% | 4% |
| X will be trusted by Alpaca Bank (IdP) | 75% | 0% | 25% | - | - | - | - | - | - |
| X will be trusted by Bank of Carpathia (Rp) | - | - | - | 81% | 11% | 15% | 100% | 0% | 0% |
| I trust the X | 64% | 0% | 36% | 81% | 0% | 19% | 85% | 4% | 12% |
| I need to keep X secret | 79% | 4% | 18% | 85% | 7% | 7% | 73% | 12% | 15% |
| Alpaca Bank (IdP) can control X | - | - | - | 33% | 37% | 30% | 31% | 54% | 15% |
| Bank of Carpathia (Rp) can control X | 11% | 61% | 29% | - | - | - | - | - | - |
| X has the features I require for my task | 68% | 0% | 32% | 85% | 0% | 15% | 92% | 0% | 8% |
| I would be worried if I lost X | 43% | 50% | 7% | 48% | 52% | 0% | 38% | 54% | 8% |

Table 1: The table displays the results of administering the mental model scale to participants. We administered the set of questions associated with each component after the relevant task in the user study. We did not ask specific questions (denoted by a dash above) if a different formulation of the same question was more pertinent to discussing a particular decentralized identity component. (*) indicates the question is paraphrased for brevity. The full text of the question can be found in the appendices.

#### 5.1.3 System Usability Scale (SUS)

We calculated the SUS for each participant using a widely accepted method [11]. The SUS data were normally distributed (Shapiro-Wilks test $p = 0.2$), and the identity wallet received an SUS score of $\mu = 71, \sigma = 16$. The overall SUS score is not a percentage and is graded on a curve. A score of around 71 implies that an identity wallet is ranked slightly above the 50th percentile. However, there is a relatively large standard deviation. A system where users are likely to be net promoters would receive an SUS score of at least 80 [11].

#### 5.1.4 Mental Models

Table 1 illustrates results from our mental model scale. Regarding security perceptions, we learned that 50% had positive intuition about the security of the decentralized identifier (DID); the corresponding result was 59% for verifiable credentials and 69% for identity proofs. These numbers are not particularly high and reflect concerns that participants generally had about how this process could be more secure than processes involving existing paper-based methods.

One question we designed to test participants' understanding of the DID related to whether the relying party (Rp) could control it. The correct answer is no – since the user had not encountered the Rp at that point of the study – yet 11% responded yes, and 29% were not sure. Further questions about whether the IdP could control the verifiable credential or the identity proof were more challenging to answer and resulted in a split of yes, no, and unsure. In reality, Alpaca Bank (the IdP) could revoke the verifiable credential without the user's oversight. Therefore, the IdP has considerable power to control the verifiable credential's utility and the identity proof's verifiability.

At least 50% of participants expressed no concerns about losing access to their decentralized identifier, verifiable credential, or identity proof. The result reflects an expectation that one of the parties in the scenario would correct the problem and re-establish user access to their data.

In terms of utility, of all three components, participants perceived the decentralized identifier (DID) to be the least helpful wallet component for the completion of their task (68% agreed with its utility). Participants were generally slow to appreciate the merits of DIDs compared to other aspects of the wallet technology.

### 5.2 Qualitative Results

The 30 participants generated 506 codes which led to four main themes: i) current challenges with identity (20.9% of codes, $n$ = 106), e.g. participants highlighting oversharing of data and acknowledging improvements to identity processes; ii) assurances about the identity wallet service (35.6% of codes, $n$ = 180), e.g. assuming the presence of trustworthy organizations and expressing concern over bad actors; iii) expectations of the identifier (12.1% of codes, $n$ = 61), e.g. contributing to user confidence about the security; and iv) examining stakeholders and their roles (28.4% of codes, $n$ = 144). Finally, some participants' responses did not adequately address the research questions and were consequently difficult to code. These were coded as 'other' (2.9% of codes, $n$ = 15). We first summarize our findings concerning the current challenges users might face with identity. We then discuss participants' expectations of the identity wallet service and the identifier, followed by their perceptions of the stakeholders and roles. The results discussed in the first section will provide context to support the remaining results.

#### 5.2.1 Challenges Users Have with Current Forms of Identity

We identified one theme from participants' statements relating to current forms of identity, that is, *Status quo is limited,*

*convenient, and improving*. This theme captured the challenges participants encountered with identity and possible improvements. Passports and driver's licenses were the dominant forms of identity referenced by participants, with driver's licenses dominant for participants from the USA, and a mix of both used by UK-based participants.

The majority of participants' concerns related to *oversharing* of data (20 participants), and we typically observed responses in one of two ways. First, a resignation to oversharing data and users thinking that there was little they could do to share less data or control what happened to their data, e.g. (P22): *"You know I work in information technology already and part of me says the idea that you keep your information secure and people not knowing it is a ship that has probably already sailed"*. Second, some participants drew comfort despite an apparent oversharing of their data for several reasons (where they provided information that was not necessary for a given process). For example, the feeling of comfort due to their having control over access to the identity document, legal structures which protect the use of their data, and their ability to define how the identity document should be used. Four of these participants expressed sentiments related to *both* comfort and resignation.

Other challenges experienced by participants related to the amount of *time* identity and related processes took. This was both online and in-person. Participants' statements referred to the inconvenience of *delays* which did not meet their expectations for more immediate service, e.g. (P18) referred to delays when they needed to replace a lost identity document in person: *"I mean down here in [LOCATION], the process is annoying because there's always a long line outside especially early in the morning to go back to get another license you'll be sitting out there for hours."* However, participants also experienced *convenience* and *ease of use*, as well as improvements to the identity process. In the latter case, the information they needed to provide to identify themselves was reduced, e.g. when opening (bank) accounts (P14): *"It's no longer, oh yeah, like I need a copy of your driver's license, proof of address and utility bill. Here's your account details and that's it. Oh my god that used to take like a week."*

When we asked participants to reflect on the security and privacy of their current forms of ID, they shared *perceptions of forgery*, whereby they were worried about losing their identity document, thought that their identity documents could easily be forged, but were also skeptical whether there was any value for a criminal to forge their ID documents. While current forms of ID received criticism for insecurity, this matter did not seem to be something participants had considered before in detail. Participants focused on *who* they were identifying themselves to so as to address concerns about misuse of the identification document e.g. (P13): *"... I'm only showing it to people who are like from an organization that is like nationally recognized"*, and the length of time the ID document was out of their possession, e.g. (P16): *"it's got my information on, the address and everything but it's only a quick look anyway. It's not like it's going to be in their possession quite some time, because then obviously I would question that as you've seen it why do you need to hold on to it."*

Participants also made positive statements as they commented on *onboarding improvements* that they had experienced, for example, services using existing information, which the user perceives as minimising their effort (P21): *"There's a thing called government gateway and when you need to renew your passport or your driver's license they're almost interconnected. So I know when I first got my driver's license I didn't really have to do anything they had my information from my passport, so if they could maybe get their checks done through like a government site or a you know post office they also do like an identity service as well."* However, *life changing problems* occurred for participants where identity processes did not work well e.g. (P10): *"And so, when I bought my first house you know 10-12 years ago, they were not able to give me the keys after the closing. [I]had to wait a few days, I think... three or four days, because my name comes up in some kind of watch list or something."*

### 5.2.2 Assurances about the Identity Wallet Service

The majority of participants (22) questioned *who controls what* as they sought to understand the use of the identity wallet app and the three tasks involving the identifiers, credentials, and proofs. They emphasised their *personal agency* in these three tasks, rather than having the IdP or Rp in control, e.g. (P22): *"I would say no it's not Alpaca bank controlling, it's me controlling it. I mean they can offer to give me the credential but I am the person who is controlling it and allowing them to do so."* On the other hand, participants also thought that the *identity provider controlled the information shared with the Rp*. From their statements, it was clear that they did not perceive that the service was designed to empower them first in decisions on data sharing, e.g. (P23): *"I think Alpaca Bank are deciding what this Bank of Carpathia can know about me, so I would say they are in control because they're the ones that are divulging information to the second party involved. So I would think that they could potentially withdraw your social security number if that is what they chose to do."* Participants were in favour of a *separation of concerns* and did not expect the IdP and Rp to share information with each other, e.g. (P3): *"... I don't think that the Bank needs to have any idea that I'm doing something with a different bank. That's my private business, so I like that it kind of mentions that and I think that's important."* As such, we see this design feature meeting some, but not all of participants' expectations. Concerns about the empowerment of users to truly control their own data-sharing in the face of service demands has parallels to social media platforms, for instance Facebook [50], where Nadon et al. also noticed the potential for users to feel personal failure if they over-shared once given control. This also

contrasts with Farke et al.'s study of online activity data [33], wherein negative consequences of services holding data may not promote action, whereas here in the context of sharing identity information, comparable levels of transparency are evident but it raised questions about where the data was going and to who. Similar concerns have been surfaced when users are confronted with access of data on Google accounts by approved third-party services [4].

*Foundations of trust* were also highlighted in most of the participants' (23) statements. *Trustworthy entities* were highlighted with a focus on some organizations being better at such service provision than others, therefore they or their products being perceived as trustworthy, e.g. (P10): *"I don't know if I trust my device as being as secure as like potentially you know, the bank's devices or network or their security is probably more enhanced than just my phone."* This statement highlights the expectation that the user trusts their device and is willing to use it for identity, thereby flagging a critical issue for adoption if this assumption does not hold in practice.

*Privacy and security evaluations* were carried out with primarily *positive feelings* expressed about using the app for identity and how secure participants thought the process was, e.g. (P10): *"Because it seems like, you know, it might be that if, even if I lost a proof, there might be some other part of it, that is needed to you know to complete any kind of functions with the banks."*

The user interaction did not seem to match participants' mental models as they flagged what they perceived as *sharing violations* where the focus was on perceptions of either sharing too much information, sharing with unexpected recipients, or, notably, being asked to share what they perceived as too little information, e.g. (P7): *"Where they're not asking for driver's license or social security number seems too convenient, because those are two usually two critical pieces of identity..."* It would seem, in this case, that participants' expectations have shifted to match practice, and requests to share less information than they expect might be met with suspicion or mistrust. Other issues which did not match participants' mental models include the *language* used, and the novelty of the process since use of the identity wallet app was *unrelated to existing practices*.

Participants were *fearful of bad actors* (11 participants), thinking that use of identity wallet apps would open new avenues for attack (P11): *"Oh man, I can see just a whole new breed of hackers. Oh God, as we speak they're breeding."*

#### 5.2.3 Expectations of the Identifier

This theme captured participants' (23) *expectations tied to the identifier*. Here, participants were confident about the security of the identity wallet app as a result of the randomness and uniqueness of the identifier, as well as its apparent entropy. This highlights ways in which users can perceive design features to convey assurances about security.

The identifier represented something participants thought only they should know and as a result should be kept *confidential*. From participants' statements, we understood that this expectation of confidentiality was linked to their use of the identifier to open a bank account. While this was a misconception akin to a folk model of security [73], participants notably suggested a behavior which was more rather than less secure. The perceived need to keep the identifier confidential was also linked to its similarity to a password, e.g. (P16): *"You don't give out your password, so why would you go on sharing your unique code for your identifier... ."*

Participants were *confused* about the need to *generate their own identifier* and expressed concern that other users might not understand the procedure, e.g. (P6): *"So I will say that I am used to things like these really long string of numbers and letters. But I think that would probably throw off the average user."*

#### 5.2.4 Examining Stakeholders and Their Roles

Participants (19) *weighed up the interaction*, assessing it based on the *efficiency, usefulness,* and *intuitiveness* of the identity wallet app. Issues emphasised included the time and effort participants expected use of the identity wallet app to take especially when considering they would interact with several relying parties (P21): *"For me, it feels too time consuming. And the criteria is not the same for every bank or you know every place that you're looking to identify yourself so I'd rather do it on a case by case basis, rather than having something you know, an app on my phone."* This then may create a kind of fatigue similar to the 'authentication fatigue', the perceived high effort required to access services to reach personal goals [62]. A knock-on effect here could be, as found with the Passfaces authentication technology [13], that the relative cost of a security technology compared to the primary task may be so high that users would delay important tasks and need more time to access services.

Fifteen participants stated that they found the identity wallet app easy to use, however, they also questioned the value of the app, e.g. (P21) *"I mean I'm able to use it. Whether I want to use it is a different thing."* Additionally, they did not find the processes intuitive or familiar, (P24): *"I think it's still a bit... It's definitely different than a lot of other apps that are used, so there is a learning curve, especially for someone that, I think I'm pretty technologically competent and I think I would still have a bit of a difficulty with this here and there."*

When queried about how they expected to recover from failure or loss, nineteen participants expressed *confidence in fallbacks*. They expected that *recovery was a basic feature* and *automated*. Notably, participants were concerned about the *location* of the backups e.g. (P25) *"I wouldn't expect it to be on your phone. I don't think it's very safe to have everything just on your phone. I would expect it to be somewhere and just be able to get it back from a backup place"* and

had different perspectives about *who* was responsible for the backup, e.g. the app provider (P13): *"So, because, like, I mean at the end of the day, all these I'm assuming that all these data points are feeding into IdentiCorp's like their, whatever their database for something like that. So I think it's the first. I think they are respon... like they are going to be the, the one that I should reach out to instead of other organizations."* Note that IdentiCorp was the name used in the study to refer to the wallet provider. Participants expected that *backups were kept* but they did not think that they were responsible for this. Additionally, they expected that recovery would be a *hassle*. Similar concerns to these have been raised about FIDO2 authentication technologies (e.g. [47]), wherein users also need to place a great deal of reliance on the service to make meaningful use of it.

While minimisation is a key feature of decentralized identity, eighteen participants had varying *interpretations of minimisation*. *Exercising control* over the information that was shared was a notable feature as they could choose not to share information if they deemed it unnecessary, e.g. (P20): *"I really did like the fact that I could choose like the optional ones and choose not to disclose [those] that weren't necessarily needed by the other bank."* At the same time, participants perceived that there was limited control as they would not be able to refuse to give information which was requested, e.g. (P5): *"If [Bank of] Carpathia wanted to know exactly how much I make a month, they would ask for it. And I wouldn't be able ... to say no."* As such, the environment supporting minimisation also needs to ensure users are not penalised for withholding information. Participants perceived minimisation to be *futile*, questioned *what was being minimised*, and perceived that it was their *effort rather than the data* that was being minimised.

## 6 Study Limitations

As with any research, our findings are subject to limitations. The pre-screen of participants may introduce bias into the results. For example, we specified that participants must be active users of Google Android. While Google Android is the dominant mobile operating system according to market share [66], we additionally specified that the personal device of the participant supported at least Android 10. Therefore, along with the fact that we recruited participants from *user-interviews.com* we can characterize our participant pool as Internet-savvy 'early adopters' of technology rather than representative of a perfectly random sample.

Identity wallets are a nascent technology, and we cannot be certain that today's design trends will be the same design trends years from now. However, we are confident that the user journeys we replicated capture the core functions of how identity wallets must behave, even if minor details of the user journey change over time.

We did not take steps to evaluate the generalizability of our results. The quantitative results we report are descriptive statistics, and the qualitative results are innately not generalizable. However, our research method did surface challenges and problems captured using a trustworthy method, and resulting insights are transferable to other contexts with caution.

## 7 Discussion

### 7.1 Security Perceptions Enhanced by Trust

We learned that participants had mixed perceptions of the security of the decentralized identity system. We found that 50% felt that decentralized identifiers were secure (concerning forgery), 59% felt verifiable credentials were secure, and 69% felt this way with identity proofs. However, we captured mixed rationales underpinning this argument, highlighting the subjectivity inherent in answering the question. Specific security concerns voiced by participants include the risk of leaking personal information from the user interface of the mobile device and the risk of providing data to the wrong online service during enrolment.

Several threads fed into a positive perception of security – including the identity wallet collating accurate personal information and the acquisition of credentials from financial institutions, but also through misunderstandings of the technology. On the latter, we noted multiple assertions that the randomized alphanumeric composition of the Decentralized Identifier (DID) represents the secure encoding or encryption of personal information. Of course, this was not true, yet the perceived presence of cryptography provided a sense of confidence and comfort. This observation brings to mind ongoing debates around how to create security cues for users of encrypted communications apps (e.g. [67]). Due to the lack of widely used security cues in decentralized identity prototypes, our intuition is that participants derive most security comfort from the trust of the key actors in the study scenario rather than confidence in technical mechanisms.

### 7.2 User Control and Necessity of Fallbacks

The shared vision of decentralized identity intimates that the user can operate with autonomy from third parties and exercise control (in the purest sense) over the disclosure of verifiable personal attributes. Probing the understanding of user control in our research was particularly interesting concerning the verifiable credential. We observed an almost even 33% split between yes-no-don't know regarding whether the identity provider could control the verifiable credential. In simple cases, the identity proof is a signed wrapper containing verifiable credentials; however, more participants indicated they were in control of the proof than the verifiable credentials. These results show that ascribing control to actors and techniques in a decentralized identity scenario is challenging,

primarily due to the interrelationships between key technologies and the opacity and complexity of the infrastructure.

Participants reporting a positive sense of control over the identity wallet were generally not concerned about losing access to their identity wallet application or stored data. The lack of fear was primarily due to the view that one of the trusted parties in the scenario would be ready to restore access to lost data. Combined with our observation that it is challenging for users to articulate where control lies in the identity network, it presents a challenge in enabling users to pinpoint their locus of control and thus correctly identify risks to the continuity of access to services. There are parallels with the sense of 'distributed responsibility as noted by Abdelaziz et al. [2] where users may not even know how to recover their identities without the help of a service provider.

## 7.3 Privacy Appraised More in the Value Exchange, and Less in the Identity Wallet

At the point of the study where the user sent an identity proof to the relying party, we captured the most lively discussion about data minimization. For example, despite leveraging advanced disclosure functions of the identity wallet (e.g. zero knowledge, or optional disclosures), participants predominantly evaluated privacy based on the value provided by the magnitude of the disclosure rather than on the technical tools at their disposal. We also noted that while participants may be surprised if they must disclose a seemingly long list of attributes, once a certain threshold of disclosures is approved, we noticed that participants could become numb to the discomfort of sharing additional attributes. A comparable phenomenon has been noted during e.g. reviewing Google 'My Activity' data collection information [33], where users have been seen to lack a sense of action due to the number of data disclosures they would need to process.

That end-users evaluate privacy in an overall transaction allows what we might expect from the privacy in context framework [55]. However, this suggests that innovation in user control cannot exist only in end-user technology and that suitable innovation in data collection practices must also come from service providers.

## 7.4 Identity Wallet Usability Not in a Vacuum

The identity wallet has inherent complexities that create usability challenges. The identity wallet resides at the intersection of the systems of three principal actors, the identity provider, the relying party, and finally, the wallet provider. Technology that resides at the boundaries between systems can create challenges for adhering to many of the heuristics for good usability [53]. Furthermore, the dominant terminology used in decentralized identity prototypes is esoteric: i.e. "decentralized identifiers", "verifiable credentials", and "identity proofs". While these terms initially create intrigue, they ultimately form a barrier to the system's learnability and limit users' confidence to persevere and resolve problems. Previous endeavors in the identity domain have experimented with optimal names for system components. For example, Microsoft's CardSpace [5] used the term 'card' to refer to a specific credential. Future research can seek to refine this terminology and find consensus between service providers to use terms consistently.

### 7.4.1 Design Considerations for Identity Wallets

Our research suggests practical ways to improve future (decentralized) identity wallets and related technologies.

- **Minimize reliance on QR codes**. QR codes were at the root of many user journey disruptions, and there may be efficiency gains in minimizing their usage. Rethinking the assumption that the user interacts with a laptop and mobile device simultaneously would open new avenues of interaction — e.g. mobile inter-app communication.
- **Provide meaningful errors in blockchain SDKs**. At times, we found it impossible to explain to participants why a cryptographic signature check might sporadically fail when expected to succeed (e.g. in an identity proof). We also had difficulty quickly understanding and explaining blockchain-specific errors.
- **Deploy Decentralized Identifiers (DIDs) only if essential**. DIDs are more complex than traditional email-based usernames. If DIDs replace traditional usernames, there will be undesirable scenarios where users must type a DID string, or where a service cannot authenticate a DID due to system problems elsewhere. Therefore designers must deploy DIDs only if essential to a use case.

# 8 Conclusion

There is a growing expectation that political and technical initiatives towards digital identity will gather pace in the foreseeable future. However, user perspectives have not been a driving force in shaping those ongoing initiatives. The findings of this study point to the dominance of paper/card-based identity methods for online identity verification and a large gap between identity verification today and what it might be in the foreseeable future. Our results suggest that technical narratives might not be a compelling driving force for future uptake and that, as previous work in identity management has highlighted [20], the user proposition should receive further thought. What seems most salient to drive adoption is the existence of supporting (infra)structures, the appeal of the list of available verifiers, and the low complexity of using a new identity wallet tool. Future work might evaluate identity wallet apps in the wild to identify opportunities to close these gaps between technical idealism and everyday reality.

## References


[1] OAuth 2.0. https://oauth.net/2/, Last accessed on 6th Jan 2022.

[2] Yomna Abdelaziz, Daniela Napoli, and Sonia Chiasson. End-users and service providers: trust and distributed responsibility for account security. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–6. IEEE, 2019.

[3] Christopher Allen. The Path to Self-Sovereign Identity, 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html, Last accessed on 6th Jan 2022.

[4] David G Balash, Xiaoyuan Wu, Miles Grant, Irwin Reyes, and Adam J Aviv. Security and Privacy Perceptions of Third-Party Application Access for Google Accounts. *USENIX Security '22*, 2022.

[5] Vittorio Bertocci, Garrett Serack, and Caleb Baker. *Understanding Windows CardSpace: An Introduction to the Concepts and Challenges of Digital Identities*. Addison Wesley, 2007.

[6] Patrick Beuth. Verantwortungslos und gefährlich, 2021.

[7] Abhilasha Bhargav-Spantzely, Jan Camenisch, Thomas Gross, and Dieter Sommer. User centricity: a taxonomy and open issues. In *Proceedings of the Second ACM Workshop on Digital Identity Management - DIM '06*, page 1, New York, New York, USA, 2006. ACM Press.

[8] Luís T. A. N. Brandão, Nicolas Christin, George Danezis, and Anonymous. Toward Mending Two Nation-Scale Brokered Identification Systems , no.2, 2015, pp.135-155. In *Proceedings on Privacy Enhancing Technologies (PETS)*, pages 135–155, 2015.

[9] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[10] Deanna G Brockman, Lia Petronio, Jacqueline S Dron, Bum Chul Kwon, Trish Vosburg, Lisa Nip, Andrew Tang, Mary O'Reilly, Niall Lennon, Bang Wong, et al. Design and user experience testing of a polygenic score report: a qualitative study of prospective users. *BMC Medical Genomics*, 14(1):1–20, 2021.

[11] John Brooke. SUS: A retrospective. *Journal of Usability Studies*, 8(2):29–40, 2013.

[12] Sacha Brostoff, Charlene Jennett, Miguel Malheiros, and M. Angela Sasse. Federated identity to access e-government services - Are citizens ready for this? In *Proceedings of the 2013 ACM Workshop on Digital Identity Management*, pages 97–107, New York, New York, USA, 2013. ACM Press.

[13] Sacha Brostoff and M Angela Sasse. Are passfaces more usable than passwords? A field trial investigation. In *People and computers XIV—usability or else!*, pages 405–424. Springer, 2000.

[14] Kim Cameron. The Laws of Identity. Technical report, Microsoft, 2005.

[15] Kim Cameron and Michael B. Jones. Design Rationale behind the Identity Metasystem Architecture. In *ISSE/SECURE 2007 Securing Electronic Business Processes*, pages 117–129. Vieweg, Wiesbaden, 2007.

[16] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, pages 339–356, USA, 2019. USENIX Association.

[17] Congressman Bill Foster. US Congressmen reintroduce sweeping digital ID bill, 2021. https://foster.house.gov/media/in-the-news/us-congressmen-reintroduce-sweeping-digital-id-bill, Last accessed on 6th Jan 2022.

[18] Kevin Corre, Olivier Barais, Gerson Sunyé, Vincent Frey, and Jean-Michel Crom. Why Can't Users Choose Their Identity Providers On The Web? In *Proceedings on Privacy Enhancing Technologies*, pages 75–89, Minneapolis, Aug 2017.

[19] Albese Demjaha, Jonathan M Spring, Ingolf Becker, Simon Parkin, and M Angela Sasse. Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption. In *Proc. USEC*, volume 2018. Internet Society, 2018.

[20] Rachna Dhamija and Lisa Dusseault. The Seven Flaws of Identity Management: Usability and Security Challenges. *IEEE Security and Privacy*, 6(2):24–29, mar 2008.

[21] DIACC. Pan-Canadian Trust Framework, 2021. https://diacc.ca/trust-framework/, Last accessed on 6th Jan 2022.

[22] Die Deutsche Kreditwirtschaft. DK begrüßt Experimentierklausel zur Kundenidentifizierung, mit der Banken und Sparkassen innovative digitale Initiativen erproben werden, 2021.

[23] Andrea diSessa. Models of computation. *User centered system design*, pages 201–218, 1986.

[24] David Dittrich and Erin Kenneally. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, 2012.

[25] Paul Dunphy, Luke Garratt, and Fabien Petitcolas. Decentralizing Digital Identity: Open Challenges for Distributed Ledgers. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 75–78, 2018.

[26] Paul Dunphy and Fabien A.P. Petitcolas. A First Look at Identity Management Schemes on the Blockchain. *IEEE Security & Privacy*, 16(4):20–29, Jul 2018.

[27] Serge Egelman. My profile is my password, verify me! The privacy/convenience tradeoff of Facebook Connect. In *Conference on Human Factors in Computing Systems - Proceedings*, pages 2369–2378, New York, NY, USA, apr 2013. ACM.

[28] N. Sakimura et al. E. Garber, M. Haine, V. Knobloch, G. Liebbrandt, T. Lodderstedt, D. Lycklama. Gain Digital Trust: How Financial Institutions are taking a leadership role in the Digital Economy by establishing a Global Assured Network. In *European Identity and Cloud Conference,*, Munich, 2021.

[29] European Commission. Commission proposes a trusted and secure Digital Identity, 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663, Last accessed on 6th Jan 2022.

[30] Evernym. Connect.me. https://www.connect.me/, Last accessed on 6th Jan 2022.

[31] Facebook. What names are allowed on Facebook?, 2020. https://www.facebook.com/help/112146705538576, Last accessed on 6th Jan 2022.

[32] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander. Helping Johnny 2.0 to encrypt his Facebook conversations. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pages 1–17, 2012.

[33] Florian M Farke, David G Balash, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. Are privacy dashboards good for end users? Evaluating user perceptions and reactions to Google's My Activity. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 483–500, 2021.

[34] U. Feige, A. Fiat, and A. Shamir. Zero-knowledge proofs of identity. *Journal of cryptology*, 1(2):77–94, 1988.

[35] FIDO Alliance. The FIDO Alliance, 2020. https://fidoalliance.org, Last accessed on 6th Jan 2022.

[36] Financial Conduct Authority. FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings, 2017.

[37] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285. IEEE, May 2020.

[38] Cal Halvorsen and Sylvia Brown. In their own words: Small-and mid-level donors express their views on charitable giving. *SSRN 3916288*, 2021.

[39] Hyperledger Foundation. Hyperledger Indy SDK, 2019. https://github.com/hyperledger/indy-sdk, Last accessed on 6th Jan 2022.

[40] IDUnion. IDUnion, 2021. https://idunion.org/, Last accessed on 6th Jan 2022.

[41] Kat Krol and Sören Preibusch. Control versus effort in privacy warnings for webforms. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, pages 13–23, 2016.

[42] Susan Landau and Tyler Moore. Economic Tussles in Federated Identity Management. *First Monday*, 17(10), oct 2012.

[43] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "It's stored, hopefully, on an encrypted server": Mitigating users' misconceptions about FIDO2 biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 91–108, 2021.

[44] Let's Encrypt. Let's Encrypt. https://letsencrypt.org/, Last accessed on 6th Jan 2022.

[45] LISSI. The new solution for identities: Digital. Decentralized and Self-sovereign., 2020. https://lissi.id/, Last accessed on 6th Jan 2022.

[46] Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton, and Michael Sena. uPort: A Platform for Self-Sovereign Identity. Technical report, 2017.

[47] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy*, pages 268–285, 2020.

[48] Deepak Maram, Harjasleen Malvai, Fan Zhang, Nerla Jean-Louis, Alexander Frolov, Tyler Kell, Tyrone Lobban, Christine Moy, Ari Juels, and Andrew Miller. CanDID: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability. *Proceedings - IEEE Symposium on Security and Privacy*, 2021-May:1348–1366, May 2021.

[49] Florian Mathis, Kami Vaniea, and Mohamed Khamis. Prototyping usable privacy and security systems: Insights from experts. *International Journal of Human–Computer Interaction*, 38(5):468–490, 2022.

[50] Guillaume Nadon, Marcus Feilberg, Mathias Johansen, and Irina Shklovski. In the user we trust: Unrealistic expectations of facebook's privacy mechanisms. In *Proceedings of the 9th International Conference on Social Media and Society*, pages 138–149, 2018.

[51] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical report, 2008.

[52] Lily Hay Newman. Microsoft's Dream of Decentralized IDs Enters the Real World, 2021. https://www.wired.com/story/microsoft-decentralized-id-blockchain/, Last accessed on 6th Jan 2022.

[53] Jakob Nielsen. 10 Usability Heuristics for User Interface Design, 1994.

[54] Jakob Nielsen. Usability inspection methods. In *Conference Companion on Human Factors in Computing Systems*, CHI '94, page 413–414. Association for Computing Machinery, 1994.

[55] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books, 2009.

[56] Darrell O'Donnell. The Current and Future State of Digital Wallets. Technical report, Continuum Loop Inc, 2019.

[57] Onfido. Onfido Identity Fraud Report 2022. Technical report, Onfido, 2022.

[58] Ping Identity. ShoCard | Identity for a Mobile World. https://www.shocard.com/en.html, Last accessed on 6th Jan 2022.

[59] Alex Preukschat and Drummond Reed. *Self-Sovereign Identity*. Manning Publications Co, 2021.

[60] Lee Rainie. Americans' complicated feelings about social media in an era of privacy concerns. Technical report, Pew Research Center, 2018.

[61] Y Rogers, H Sharp, and J Preece. *Interaction design: Beyond human-computer interaction*. John Wiley and Sons, 2 edition, 2011.

[62] M Angela Sasse, Michelle Steves, Kat Krol, and Dana Chisnell. The great authentication fatigue–and how to overcome it. In *International Conference on Cross-Cultural Design*, pages 228–239. Springer, 2014.

[63] M.A. Sasse, Sacha Brostoff, and D Weirich. Transforming the 'Weakest Link' – a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, 19(3):122–131, Jul 2001.

[64] SelfKey. SelfKey. https://selfkey.org/, Last accessed on 6th Jan 2022.

[65] Manu Sporny, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, and Christopher Allen. Decentralized Identifiers (DIDs) v1.0. Technical report, W3C, 2021.

[66] Statcounter. Mobile Operating System Market Share Worldwide: Jan 2021 - Jan 2022, 2022. https://gs.statcounter.com/os-market-share/mobile/worldwide, Last accessed on 6th Jan 2022.

[67] Christian Stransky, Dominik Wermke, Johanna Schrader, Nicolas Huaman, Yasemin Acar, Anna Lena Fehlhaber, Miranda Wei, Blase Ur, and Sascha Fahl. On the limited impact of visualizing encryption: Perceptions of E2E messaging security. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 437–454, 2021.

[68] San Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. What makes users refuse web single sign-on?: An empirical investigation of OpenID. In *SOUPS 2011 - Proceedings of the 7th Symposium on Usable Privacy and Security*, page 1, New York, New York, USA, 2011. ACM Press.

[69] UK Government. UK digital identity & attributes trust framework: Alpha version 2. Technical report, UK Government, 2021.

[70] U.S. Department of Justice - Office of the Inspector General - Audit Division. The Department of Justice's Efforts to Combat Identity Theft. Technical report, 2010.

[71] Jennifer van Grove. Each Month 250 Million People Use Facebook Connect on the Web, 2010.

[72] W3C. Verifiable Credentials Data Model 1.1, 2021.

[73] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, New York, NY, USA, 2010. Association for Computing Machinery.

[74] Rick Wash and Emilee Rader. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 309–325, 2015.

[75] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Technical report, 2014.

[76] World Economic Forum. A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity. aug 2016.

## A Information Sheet

**What is the purpose of the study?**

We are inviting you to take part in a research study to help us investigate and understand users' experience of a digital identity wallet app. The app gives users a way to identify themselves (that is, who they are) in order to access various services over the Internet.

**Why have I been approached?**

We need to recruit several adult participants to take part in the study. You have been approached in an effort to recruit people who have a Google Android phone (running at least Android 10), some experience with Internet banking and banking apps, and who have installed (or can install) the Zoom application on a laptop/computer and a mobile phone.

**Do I have to take part?**

Participation is entirely voluntary. If you change your mind about taking part in the research study, you can withdraw at any point during the study.

**What happens during the study?**

The research study will take place remotely over Zoom. You will be asked to install the digital identity wallet app on your Google Android phone. You will join the Zoom call both from your computer and your mobile phone and will share the screen on the mobile phone so we can see how you use the app. The digital identity wallet app will not collect any information from your phone, and at the end of the study, you can uninstall it. You will be given three tasks to carry out using the digital identity wallet app and you will be asked to share your thoughts of the experience as you carry out the tasks. After you complete the tasks, you will be asked to fill in a questionnaire about the app and your experience and to answer a few questions about the process. The study will last approximately 45 minutes. The research study will be audio- and video-recorded for review and analysis in order to gain insights into users' experience using the digital identity wallet app. No identifying information will be shared outside the research team.

**What are the possible disadvantages and risks of taking part?**

We do not anticipate any disadvantages or risks associated with participation in this study.

**What are the possible benefits of taking part?**

While individual benefits may be limited, your participation will help us to build an understanding of users' experience of digital identity wallet apps. It is hoped that the results of this research study will contribute to the development of such apps in the future.

**Who is organising and funding the research?**

The research is conducted by Maina Korir and Dr. Paul Dunphy from the OneSpan Innovation Centre.

**Will my participation be confidential?**

Yes. We will not share personally identifying information outside of the research team.

**What happens if something goes wrong?**

In the unlikely case of concern or complaint, please contact Dr. Paul Dunphy, Principal Research Scientist at the OneSpan Innovation Center (paul.dunphy@onespan.com).

**Where can I get more information?**

If you would like more information, please contact the researcher: Maina Korir (maina.korir@onespan.com).

**Data protection**

All collected data will be de-identified soon after the research study and before the data is analysed. Participants will be given a pseudonym to refer to their data during the data analysis process meaning it will not be possible to link this data back to any of the participants.

## B Consent Form

Participants could indicate yes or no in response to the following:

- I have read and understood the information sheet and have had the opportunity to ask questions about the study.
- I consent voluntarily to be a participant in this study and understand that I can withdraw from the study at any time if I so choose.
- I understand that taking part in the study involves joining a Zoom call, installing and using a mobile app, and taking part in an audio- and video-recorded interview to discuss my experience of using the app.

- I agree to the interview being audio- and video-recorded and to the interview being transcribed and personal identifiers removed.
- I understand that information I provide, which cannot identify me, may be published in journals, conference proceedings and reports.
- I understand that personal information collected about me that can identify me, such as my name will not be shared beyond the research team.
- I understand that my data will be stripped of personal identifiers during the transcription process. I understand that data that cannot identify me will be encrypted and stored for the duration of the project.
- After the data has been stripped of all personal identifiers and has been anonymized I agree that the information I provide during the interviews can be quoted in research outputs.

## C Interview Script

We asked participants the following questions, touching on the issues identified in the different categories:

**Current Forms of Identity and Identification**

- For the purposes of this interview, what name can I use to refer to you?
- *Name selected*, if I asked you to prove that you are *name*, what would you do?
- Have you been in a situation where you've been asked to prove that you are *name*?
- Could you tell me about the experience?
- How do you feel about using a *item indicated by participant* as a means of ID?
- Are there ways that a *participant's ID document* is a secure form of ID?
- Are there ways that a *participant's ID document* as a form of ID offers you privacy?
- How do you feel about an opportunity to decide what piece or pieces of information to share to identify yourself?
- If you could change one thing about the process of identifying yourself online, which one would you pick?
- Why would you choose to focus on that?

**Interactions with the Identity Wallet**

*Scenario*

Imagine that you are Alex. Alex is a customer at Alpaca Bank. Alex opened a bank account in person at the bank branch closest to where they live. Alex now wants to open another account with a second bank - Bank of Carpathia. You will carry out three tasks to achieve this goal using the digital identity wallet app. The building blocks of a new privacy-respectful identity wallet app are: identifiers which you will interact with in the first task, credentials, which you will interact with in the second task, and proofs, which you will interact with in the third task. You will carry out each task in turn and I will ask you a few questions about the experience between each task.

**Reflection on Identifiers and Proofs**

*Participants were given instructions to carry out the steps for the three tasks: identifiers, credentials, and proofs. They then answered the following questions:*

- MyIdentifier is secure, that is, it cannot be forged
- My Identifier will minimise the information about me that I have to share to identify myself
- My Identifier will be trusted by Alpaca Bank
- I trust My Identifier
- I need to keep My Identifier secret
- Bank of Carpathia can control My Identifier
- My Identifier has the features I require for my tasks
- I would be worried if I lost My Identifier

*We replaced 'MyIdentifier' with 'verifiable credential' and 'proof' for the second and third tasks.*

**Usability and User Expectations**

- Based on your experience using the digital identity wallet app today, what would you say is the best thing about the app?
- What would you say are the limitations of the app?
- Are there any needs or challenges you have faced with identity that the digital identity wallet app addresses?
- Are there any needs or challenges you have faced with identity that the digital identity wallet app does not address?
- In what ways do you see the digital identity wallet app fitting into your regular practice of identifying yourself?