Do Users Want To Use Digital Identities? A Study Of A Concept Of An Identity Wallet

Sandra Kostic
Fraunhofer AISEC

Maija Poikela
Fraunhofer AISEC

Abstract

People can be identified by means of identification documents. To ensure identification in the digital environment, a digital identity is required. This work presents a concept that is under the control of the user and allows the storage of multiple digital identities in one app. This application, the so-called *identity wallet*, enables both the secure storage of a sovereign document such as the national identity card, as well as the storage of identities from the municipality or from private companies, so that users can identify themselves online with different levels of assurance. In addition to identities, keys (for vehicles, hotel rooms, etc.) can also be stored.

This wallet concept was tested with a total of 16 participants. The participants were convinced by the concept and were ready to adopt it. The results of the study indicate that the wallet operator has an influence on the extent to which the application is trusted and whether it will be used. A small majority of the participants favored the state as the wallet operator, while the rest preferred a private company.

1 Introduction

People can be uniquely identified by personal data, such as their name and date of birth. So-called digital identities are needed to identify people online. Examples of digital identities are already offered by services such as Facebook or Google. With these services, users can create an account containing their personal data and use this account (their digital identity issued by Facebook or Google) to identify themselves to other services[1] [2]. Problems with these digital identities are twofold. First, they cannot be used for online services that require identification with a verified sovereign document. Second, the identity is stored with the services. This means that users have no influence on what these services do with their data [5] [12].

In Germany, for example, a solution (*AusweisApp2*[3]) is already available that enables digital identification with the national ID card [8]. However, applications such as the AusweisApp2 have major requirements that have to be met before users can use their national ID card in the digital world. It involves the activation of the national ID card for the online context as well as the purchase of certain hardware to be able to read the ID card. In addition, the processes are not always user-friendly, which makes them more difficult to use [1].

To overcome these challenges, there are currently approaches that provide digital identities with a simple set-up process, and thus a low threshold for creating them.[4] [5] [6] These approaches do not, however, follow the same security requirements as the national ID card, meaning that they do not meet the level of assurance [2], and therefore only few service providers accept them as means of identification. In addition, there is evidence (cf. [6], and [10]) that these application have great challenges in terms of usability.

Considering the three aforementioned problems — the requirement for a high level of assurance of the digital identity, the absent user control over their data, as well as the lack of service providers accepting the digital identity from a source that can provide only a low level of assurance — a potential solution is a so-called *wallet* consisting of multiple identities, for which a concept is presented in this paper.

These identities coexist in a single application operated by

[1] https://developers.facebook.com/docs/facebook-login/?locale=en_US

[2] https://developers.google.com/identity/sign-in/web/sign-in

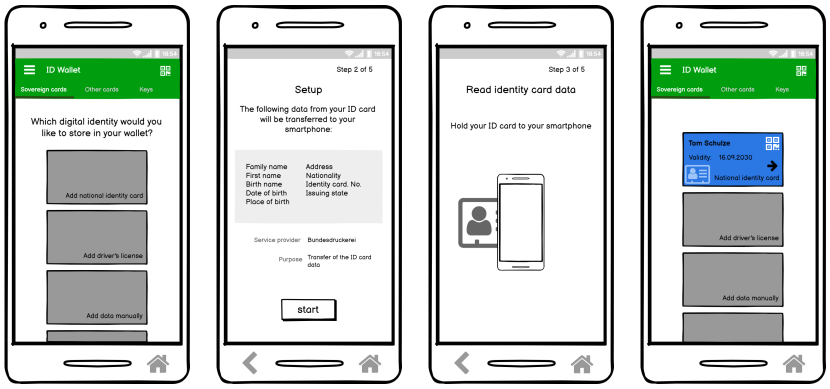
[3] https://www.ausweisapp.bund.de/en/about-us

[4] https://www.evernym.com/connectme/

[5] https://jolocom.io/blog/production-ready-smartwallet/

[6] https://uportlandia.uport.me/

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



(a) Selection of the national identity card

(b) Setup screen with data overview

(c) Storing the data by scanning the identity card

(d) Stored national ID on the smartphone

Figure 1: Creation of the digital national identity
(Note: These screens represent only highlights from the creation of the digital identity.)

the user and may contain identities from different sources. This allows users to simultaneously use identities that have higher requirements in creation but have a wide range in use, as well as identities that have low requirements but can be used in use cases relevant for the user.

In addition to identities, this concept also deals with storing tickets (airline tickets, public transportation tickets, etc.) as well as keys (hotel room, car, etc.). This is to create an application that can be used for various use cases (both government and private sector) in the digital space.

Three main research questions were investigated:
RQ1: How understandable and acceptable is the identity wallet concept?
RQ2: To what extent are the users aware that the ID comes from a sovereign document?
RQ3: Which factors influence the perceptions of control over the data?
In order to answer these research questions, a user study was conducted with 16 participants.

Every participant was able to successfully create an identity and understood the identification process using the national ID card. The participants also showed a great willingness to use the wallet based, among other things, on the impression of always having control over the data. The results suggest that the *wallet operator* plays an important role in whether the participants trust their data to be handled responsibly in the wallet. About half of the participants saw the state as the only acceptable alternative for the wallet operator, whereas the rest preferred a private company.

2 Wallet concept

The concept of this wallet is to allow the simple and secure storage of identities, tickets and keys in one smartphone application. The owner of the wallet should always have control over the stored data and decide for themselves which exact data should be sent to a service for the requested purpose.

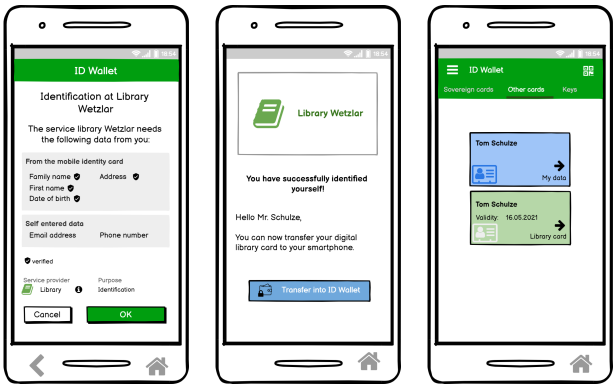
This wallet not only supports the creation of a digital identity from the wallet itself based on the national ID card, but at the same time identities provided by other issuers (such as a library card, student ID, employee ID, etc.) can be transferred to the wallet. The goal here is to let users decide which identity they want to store in the wallet and offer them a wide range of choices.

Since the wallet stores personal data and potential users should trust the wallet, requirements for the wallet and the handling of data were collected with the help of a focus group consisting of 6 people. These requirements, which were implemented as security and privacy features, are presented in the following section 2.1.

2.1 Function of the wallet

The concept of the wallet consists of the functions of an introduction to the wallet features, the setting of a protection mechanism, the digitization of the national identity card (see Figure 1), the identification using the identities stored in the wallet (app to app, app to web) as well as the transfer of identities to the wallet provided by other issuers (see Figure 2), the storage of keys and lastly the digitization of the driver's license with the service of the driver's license authority. Some of the functions are described below in more detail.

Setting a protection mechanism of the wallet
In order to prevent unauthorized access to the wallet, the user may decide either to use the already established unlocking mechanism of the smartphone or to set a new protection



(a) Identification towards the library with the digital identity card

(b) Successful identification and transfer of the digital library card

(c) Stored digital library card

Figure 2: Identification and transferring a library card to the wallet

mechanism (PIN, password, fingerprint).

Digitization of the national ID card
To use the ID card as an identification document, the user can digitize the ID card using the wallet app only. To do this, the ID card must be read via the smartphone's NFC interface (see Figure 1c) and the ID card PIN must be entered. The ID is then securely stored exclusively on the smartphone using the secure element [13] [11].[7] At the end of the process, the ID card is displayed as a card stored in the wallet (see Figure 1d).

Identification by means of stored identities
After ID documents have been stored in the wallet, they can be used both for online identification and with a QR code for on-site identification. The wallet can communicate with other services that require identification.[8] Users receive an overview in advance of which specific data is requested (see Figure 2a), they can view further details about the requesting service (e.g.is there a valid authorization certificate to issue this request), and also only send the data to the service with additional consent (e.g. by entering the specified wallet PIN).

Transfer of an identity provided by an issuer
After successful identification, identities provided by an issuer can be transferred to the wallet via a deep link or by scanning a QR code (see Figure 2b and 2c). These identities can in turn be used as means of identification, both online and on-site.

[7] A secure element is a hardware-based chip on mobile devices that provides protection against unauthorized access.

[8] for app to app communication using a deep link, for app to website communication using a QR code.

3 User study

In order to investigate the extent to which the concept is understood by users and how willing they are to use it, two user studies were conducted with eight people each (a total of 16 participants) in September and October 2020 in Germany[9]. Three main research questions were to be investigated.

Participants, aged between 18 and 56, were acquired for a fee of 25€/hour via the Testing Time platform.[10] We excluded participants who were experts in the fields of security, UX design and usability. In addition, we also made sure that there was an approximately equal distribution of women and men as well as young and older adults participating in the study.

Due to the COVID-19 pandemic, the study was conducted in digital format with a video conferencing tool. The digitally prepared interactive prototype was made available to the participants via a link, and they were asked to share their screen in an online meeting so that they could be observed operating the prototype.

Participants were given tasks to complete using the prototype, each task followed by interview questions to gain further details about their perception and understanding of the prototype. The tasks were the following:
1. Setting up the wallet and establishing a wallet PIN.
2. Creating a digital national identity card.
3. An online identification using the digital ID card stored on the smartphone.
4. Transferring the digital library card from the digital library to the wallet (app to app communication).
5. The creation of digital driver's license (web to app communication).
6. The storing of a vehicle key of a rented vehicle.

During these tasks, the *think aloud* method [14] was used, which allowed us not only to observe the actions of the study participants during the study, but also to note their thoughts, assumptions, and comments. Afterwards, a final interview was conducted to determine the participants' overall impression of the application (see appendix 8 for the study guideline).

4 Results and Discussion

All participants were able to successfully create a digital identity and use it for digital identification. However, due to the pandemic, only a digital user test with a digital prototype could be conducted, and to determine the correct success rate of the use of digital identities, it is necessary to observe the interaction between the smartphone and the ID document (or smartphone and the QR code displayed). This can only be correctly determined within an in-person study.

Nevertheless, the study shows that that a large number of participants (15 out of 16) were convinced by this concept

[9]

[10] https://www.testingtime.com/en/

and want to use the wallet. They saw great added value in it for themselves, because it not only simplifies administrative processes, but also enables access to various use cases. This was particularly welcomed because the smartphone was seen as the device that is always carried, even if the wallet or keys are sometimes forgotten at home. This finding that German citizens want to use a digital ID card was confirmed within a study one year later in 2021 [3]. With regard to RQ2, for a majority of the participant (15 out of 16) it was clear that the digital national ID card is stored on the smartphone.

The study also shows that the identification process was well understood. Not only did all participants succeed in being digitally identified, for all participants it was also always clear which personal data was sent to which service. This not only gave them the feeling of having control over the process, but also of being able to understand the individual steps of the process well. According to the participants, this was also supported by the ease of use of the wallet: 10 out of 16 participants confirmed that they appreciated the simple design of the wallet, which was also easy to understand.

Because this application handles personal data, it was particularly important when developing the concept to give users the impression that they always have control over their own data. The results of the study indicate that the participants perceive that. For example, the participants confirmed that they welcome the fact that the wallet provides a separate protection mechanism to protect data. The study participants thus not only showed that they recognized the need for data protection, they were even willing to make this extra effort to protect their data from unauthorized access (7 out of 16). Here, a large proportion of participants preferred to use the fingerprint to protect the wallet (11 of 16). Not only because a protection mechanism was to be set, but also because the data could only be sent after the user had seen and checked it (see Figure 2a) and additionally confirmed it by entering a password, the participants had the impression that the wallet was secure (7 out of 16). However, there were still concerns about saving a key. Here, 3 out of 16 participants said they were too worried about losing the key and the associated damage.

Finally, the extent to which the wallet is trusted was also examined. As a positive outcome of this evaluation, all participants stated that they trust the concept of the wallet. However, this trust is strongly dependent on the wallet operator. Here strongly distinct opinions could be identified. 9 out of 16 participants preferred the state as wallet operator. This group saw the justification in the fact that the state already provides sovereign documents. Therefore, the participants saw that it would only make sense for the state to play a significant role in this type of solution as well. On the other hand, others stated that companies would only be interested in the data, which is why these would not be suitable wallet operators. The remaining 7 out of 16 participants preferred a private company to operate the wallet. Their reasoning was similar, with the difference that they saw the state as the party interested in only the data. Therefore, they felt more comfortable having a private company in charge of the digital identity.

5 Limitations and Future Works

In the period when the user study was conducted, an app was released in Germany called Corona-Warn-App, which was designed to provide privacy-friendly contact tracing to identify chains of infection anonymously.[11] As it was the first government application released in this form, the Corona-Warn-App was heavily discussed in the German media. Here, questions were often raised about the extent to which the app is actually privacy-friendly and does not serve a national surveillance [9] [7] [4]. Since references to the Corona-Warn-App were frequently voiced by the participants during the study and this app was strongly represented in the media, it can be assumed that the participants were strongly sensitized to the topic of security and data protection. In addition, it is possible that the discussion about the Corona-Warn-App had a significant influence on the decision about the wallet operator, which could have led to the formation of these two groups [15]. Future research is planned to investigate to what extent this discussion has influenced the results. Additionally, this study was only conducted with German citizens. Therefore, the group of participants will be expanded to include other nationalities in future studies.

6 Conclusion

This paper presents an app concept with multiple identities (wallet), and a user study on elaborating the acceptance to use a wallet and understanding the identification process.The results suggest that the concept was well understood, including the process of digitizing a national ID card as well as the identification process. Furthermore, the wallet was considered to be secure and easy to use, and the users stated that they felt they had control over their data. Since various services can be performed with the smartphone alone, the participants immediately recognized the added value in the app and showed great willingness to use it. The concept was also trusted, but for each participant this depended on whether the wallet operator was the state or a private company. However, since the two large camps between the state as wallet operator and the company as wallet operator are not in agreement, the authors give no recommendations on the operator.

7 Acknowledgement

The concept was developed within the ONCE project funded by the German Federal Ministry of Economic Affairs.[12]

[11] https://www.bundesregierung.de/breg-de/themen/corona-warn-app

[12] ONCE project website https://once-identity.de/

References

[1] Susanne Asheuer, Joy Belgassem, Wiete Eichorn, Rio Leipold, Lucas Licht, Christoph Meinel, Anne Schanz, and Maxim Schnjakin. *Akzeptanz und Nutzerfreundlichkeit der AusweisApp : eine qualitative Untersuchung ; eine Studie am Hasso-Plattner-Institut für Softwaresystemtechnik im Auftrag des Bundesministeriums des Innern*. 2013.

[2] Colette Cuijpers and Jessica Schroers. Eidas as guideline for the development of a pan european eid framework in futureid. In Detlef Hühnlein and Heiko Roßnagel, editors, *Open Identity Summit 2014*, pages 23–38, Bonn, 2014. Gesellschaft für Informatik e.V.

[3] PwC Deutschland. Der online ausweis auf dem smartphone und die digitale brieftasche. Brochure PwC-Studie 2021, 2021. https://www.pwc.de/de/finanzdienstleistungen/der-online-ausweis-auf-dem-smartphone-und-die-digitale-brieftasche.html.

[4] The Guardian. Glitches dent german enthusiasm for covid contact-tracing app. https://www.theguardian.com/world/2020/sep/23/glitches-dent-german-enthusiasm-for-covid-contact-tracing-app. Accessed 2022-24-05.

[5] et al. Karegar, Farzaneh. Helping john to make informed decisions on using social login. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 2018.

[6] Alina Khayretdinova, Michael Kubach, Rachelle Sellung, and Heiko Roßnagel. *Conducting a Usability Evaluation of Decentralized Identity Management Solutions*, pages 389–406. Springer Fachmedien Wiesbaden, Wiesbaden, 2022.

[7] Netzpolitik. Contact-tracing-apps: Kritik an datenschutzfolgenabschätzung für die corona-warn-app. https://netzpolitik.org/2020/contact-tracing-apps-kritik-an-datenschutzfolgenabschaetzung-fuer-die-corona-warn-app/. Accessed 2022-24-05.

[8] Torsten Noack and Herbert Kubicek. The introduction of online authentication as part of the new electronic national identity card in germany. *Identity in the Information Society*, 3(1):87–110, 2010.

[9] Zeit Online. Eine app, die niemand nutzt, nutzt niemandem. https://www.zeit.de/digital/datenschutz/2020-12/corona-warn-app-datenschutz-effizienz-kontaktverfolgung. Accessed 2022-24-05.

[10] Sebastian Sartor, Johannes Sedlmeir, Alexander Rieger, and Tamara Roth. Love at first sight? a user experience study of self-sovereign identity wallets. In *30th European Conference on Information Systems (ECIS)*. Timisoara, Romania, 2022.

[11] Matthias Schwan and Tim Ohlendorf. Mobile-id based on secure elements. Fraunhofer SmartCard Workshop, 2019.

[12] Charles Scott, Devin Wynne, and Chutima Boonthum-Denecke. Examining the privacy of login credentials using web-based single sign-on - are we giving up security and privacy for convenience? In *2016 Cybersecurity Symposium (CYBERSEC)*, pages 74–79, 2016.

[13] Syscom Corporation ltd. Morpho Safran Sonal Rohilla, Reaserch Development. Secure element an evolution to existing secure technology. *International Journal of Scientific and Research Publications, Volume 5, Issue 7*, 2015.

[14] Maarten van Someren, Yvonne Barnard, and Jacobijn A. C. Sandberg. The think aloud method: a practical approach to modelling cognitive processes. *Knowledge Based Systems*, 1994.

[15] Yunfei Xing, Yuhai Li, and Feng-Kwei Wang. How privacy concerns and cultural differences affect public opinion during the covid-19 pandemic: a case study. *Aslib Journal of Information Management*, ahead-of-print, 06 2021.

8 Appendix

Guideline for the user study

Task 1 - Set up the app

"Your first task is to set up the app. So start the ID Wallet app now and follow the instructions!"

Questions:

1. You have now set up your app. Has it been made clear to you what the scope of functions of the app you have set up is?
2. Was it clear to you what the PIN / PW or fingerprint should be set for?
3. What is your opinion on the use of the fingerprint, e.g. for authentication?
4. Do you prefer to use the locking mechanism from the smartphone or set a new password?

Task 2 - Creating a digital ID card

"You have set up your ID Wallet. Because you want to identify yourself to another service, you now need a digital identity."

Questions:

1. Can you please briefly recap in your own words what you have just done?
2. You now have a digital ID card: What impression does the app give you of where your identity is stored?
3. What is your impression of what you can now do with this digital ID card?
4. What do you hope to be able to do with the digital ID card?
5. What data has now been collected through the process?

Task 3 - Creating a digital driver's license (web to app communication)

"You have discovered the service that you can save not only the ID card but also the driver's license digitally on the smartphone. To do this, you call up the service via your PC in a web browser. Your task now is to create the digital driver's license."[13].

Questions:

1. Can you please briefly recap in your own words what you have just done?
2. To apply for the digital driver's license, you first had to identify yourself. Was it transparent to you here what data the Bund.de website requires from you for identification?
3. The identification was successful. The Bund.de website apparently received the requested data. Was it clear which data you sent to the Bund.de website?
4. What impression did you have of what you had identified yourself with?
5. What impression were you given of how you obtained the digital driver's license?
6. In the process, you had to scan a QR code twice. What impression were you given of what these two QR codes were used for (What do you see as the difference)?

[13]Note: This and the following task were alternated in each user study to rule out the possibility that the second use case was only understood based on the previous one

Task 4 - Registration to the library app (app to app communication)

"In addition to a digital ID card, you can also enter data manually and save it to your ID Wallet." (Show the participant what is already stored in the Wallet).

"For your work, you need a book as a basis for your research and have discovered a library where you can also create a digital library card and store it in your Wallet. Your tasks now is to create this card."

Questions:

1. Can you please briefly recap in your own words what you have just done?
2. A provider usually wants some data from you for identification purposes. Was it transparent to you here what data the library needs from you for identification?
3. The identification was successful. It appears that the library received the requested data. Was it clear what data you sent to the library?
4. The data you were able to send was divided into two groups. What do you see as the difference [verified and editable]?
5. (If the person looked more closely at the service) What was your motivation to learn more about the service?
6. Was it clear how the library received the data?
7. Did you have any concerns about sending this data / your data to the service?
8. (If the answer was yes) What would help dispel the concerns?
9. What impression were you given about how you got the digital library card?

Task 5 - Saving a vehicle key (app to app communication)

"You are on vacation and have rented a vehicle there, which you have already booked. The service now offers you a service that no longer forces you to have your car key with you. Your task now is to test this new service."

Questions:

1. Can you please briefly recap in your own words what you have just done?
2. Did it become clear to you where the key was stored?
3. How would you use this key now?

Final interview

Questions:

1. What is your overall impression of such an application?
2. Do you use similar applications in real life? (If 'yes': which ones?, if 'no': why not?)
3. Would you use this application in real life? (If 'yes: why? What do you see as the benefits? If 'no': Why not?)
4. Are you ready to trust such an application? What would influence your willingness?
5. Regardless of whether you would use the application: What do you see as the advantage in using such an app?
6. What do you think about the idea of an identity stored on your smartphone?
7. And how about the key and ID being stored together?
8. You have tested the application interacting both via a website and via an app. Which variant do you prefer?
9. Do you prefer web or app applications in general?
10. Which applications in general or in particular would motivate you to use the ID Wallet for this purpose?
11. Finally, I would like to ask you a few questions about your general usage behavior: Do you use the apps that are installed on your device more often, or do you install apps more often via platforms like Google Play or the Apple Playstore?