

Freie Universität Berlin

Masterarbeit am Institut für Informatik der Freien Universität Berlin

Arbeitsgruppe Informationssicherheit

Enhancing Digital Identity Verification: Design, Development, and User Studies of a Prototype Wallet App Investigating the Role of Photos in On-Site Authentication

Robin Julian Wenzel

Matrikelnummer: 5389510

robin.wenzel@fu-berlin.de

Betreuer/in: Sandra Kostic

Eingereicht bei: Prof. Dr. Marian Margraf

Zweitgutachter/in: Prof. Dr.-Ing. Maija Poikela

Berlin, 13. Mai 2024

Selbstständigkeitserklärung

Name: Wenzel

Vorname(n): Robin Julian

Studiengang: M. Sc. Informatik

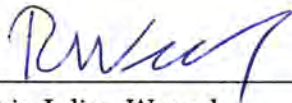
Matr. Nr.: 5389510

Ich erkläre gegenüber der Freien Universität Berlin, dass ich die vorliegende Masterarbeit selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe.

Die vorliegende Arbeit ist frei von Plagiaten. Alle Ausführungen, die wörtlich oder inhaltlich aus anderen Schriften entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch bei keiner anderen Universität als Prüfungsleistung eingereicht.

Berlin, 13. Mai 2024



Robin Julian Wenzel

Abstract

The topic of digital identities is becoming more and more relevant in today's society. These identities are managed through digital identity wallet applications on the users smartphones. With digital identities like a digital ID card being present in the users smartphone through such wallet solutions, it seems feasible to also use them as a replacement for physical ID cards in on-site authentication. The acceptance of such a feature is heavily based on the users trust in the solution.

During this thesis, it is investigated whether the presence or absence of a photo has a significant influence on the perceived trust of users in the solution when using a digital ID card in on-site authentication. A demonstrator wallet Android application has been developed based on a low-fidelity prototype of a wallet concept. This demonstrator is used during user studies to gather information about the usability of such a wallet concept. An A/B test was conducted during these studies to gather information about the perceived trust of users in the solution if they are shown a photo during on-site authentication or not.

The results of the study show that the presence or absence of a photo has a significant influence on the perceived trust and if such an on-site usage is planned for digital ID cards, the presence of a photo is important for users to trust the solution.

Contents

1	Introduction	7
1.1	Motivation	7
1.2	Context of the Thesis and Problem Description	8
1.3	Goals and Scope of the Thesis	8
1.4	Research Questions	10
1.5	Structure of the Thesis	11
2	Theoretical Background and Related Work	12
2.1	Digital Identities and Self-Sovereign Identity	12
2.1.1	Digital Identity	12
2.1.2	Self-Sovereign Identity	14
2.2	Digital Identity Wallets	15
2.3	Smart-eID	17
2.4	eIDAS 2.0 & EUDI-Wallet	17
2.5	Existing Digital Identity Wallet Applications	19
2.5.1	Lissi Wallet	19
2.5.2	esatus Wallet	21
2.6	Related Studies in this Field	23
3	Implementation	27
3.1	Scope of the Demonstrator	27
3.2	Presentation of the Demonstrator Application	28
3.2.1	Introduction Tour & App Authentication Setup	28
3.2.2	Main Wallet Screen & Digital Identity Setup	29
3.2.3	ID Card Detail View	31
3.2.4	App Authentication & Login	32
3.3	Technical Implementation	33
3.3.1	Setup of a Digital ID Card	33
3.3.2	Storage of Identity Data	37
3.3.3	Transfer of Identity Data	38
3.3.4	Inclusion of Photos in Digital ID Cards	44
4	Methodology	46
4.1	A/B Testing	46
4.2	Human Computer Trust Scale	47
4.3	System Usability Scale	47
5	Study Design	49
5.1	Introduction & Concept	49
5.2	Participant Selection & Demographics	49
5.3	Structure of the Study	50
5.4	Modified HCTS	53

6	Study Results	55
6.1	Demographic	55
6.2	SUS Results	57
6.3	HCTS Results	60
6.4	After-Scenario Questions	63
6.4.1	Scenario 1: ID-Wallet Setup	63
6.4.2	Scenario 2: On-Site Authentication Using the Created Digital ID Card	64
6.4.3	Scenario 3: Validating a Digital ID Card Using the ID-Wallet Scanner	65
6.4.3.1	Participants in the Group Without Photo	65
6.4.3.2	Participants in the Group With Photo	65
6.4.3.3	Group-Independent Responses	65
6.5	Participant Comments During the Study	66
7	Discussion	67
7.1	Demographic	67
7.2	SUS Questionnaire	68
7.3	HCTS Questionnaire	69
7.4	After-Scenario Questions and Comments during the Study	70
7.5	Limitations of the Demonstrator Application	73
7.6	Limitations of the Study	74
8	Conclusion	75
8.1	Future Work	76
A	Appendix	86
A.1	Study Script	86
A.2	System Usability Scale Questionnaire from Study	89
A.3	Human Computer Trust Scale Questionnaire from Study	91
A.4	Demographic Questionnaire from Study	93
A.5	SUS Questions	94
A.6	HCTS Questions	94
A.7	ID-Wallet Android Demonstrator Source Code	95

1 Introduction

This introductory chapter will outline the motivation of the thesis, describe the context in which this thesis is written, and what problem is investigated during this thesis. It continues with an overview of the goals and scope of the thesis before outlining the research questions of the thesis. The chapter finishes with a description of the structure of this thesis.

1.1 Motivation

Since the European union successfully voted on the eIDAS regulation in 2014, which aims to establish a framework for digital identities and authentication across the countries of the EU, the relevance of digital identities and also self-sovereign identities has been on the rise [20]. Looking into the current situation in Germany, starting with the *AusweisApp*¹, using the national ID card in the context of digital services to verify a persons identity has become increasingly common even for non tech-savvy people [10]. The next desired step would be to not need to have the physical ID card on hand every time this identification is necessary, but having the identity available in the form of a digital identity. This concept can not only be used for a national ID card, but also for a drivers license, a health insurance card, identities like a library card or employee cards, digital keys for hotel rooms and cars, entrance tickets, and many more examples.

As such, the concept of digital wallets emerged, of which the intention is to hold all these digital identities in a centralised but secure location. Many wallets follow the paradigm of self-sovereign identities, which means that the user of the wallet application is the sole holder and authority of these identities [53]. Parties trying to verify the users identity or use any of these identities stored in the wallet need to request the data from the wallet application, stating which data is needed to proceed and giving the user the possibility to check which of their data will be transferred to the third-party [60]. The user will also explicitly need to confirm the transfer of the requested data to the third-party [60].

To have a high acceptance of such wallet application solutions, it is of utmost importance to give the user the feeling that their data is really secure in those apps and that they are in full control of their data and which data will be transferred when and to which party. It is also of interest to the users of such apps to be able to verify that the requested party is indeed a legitimate service or institution. On the other hand, to avoid discouraging a non tech-savvy person from using the wallet, the application needs to remain easily usable. This means the application should not be tedious to use or the user should not be presented with security-relevant information which they cannot comprehend, as this will possibly frighten them off.

With the revision of the eIDAS regulation in the form of eIDAS 2.0 and the EUDI regulation in 2023, the relevance of digital identities and digital wallets became even more apparent, as now under the EUDI regulation every country in the EU is required to develop a digital identity wallet in the following 2 years after the enactment of the regulation, which is currently set to be in 2026 or early 2027 [21].

¹<https://www.ausweisapp.bund.de/home> (accessed: 07.04.2024)

1.2 Context of the Thesis and Problem Description

This thesis is written in the context of a cooperation with the researchers from the Secure Systems Engineering department of Fraunhofer AISEC². This department has a subdivision called "Usable Security & Privacy" (USP), working on the topic of usability and user-centered design in context of security. The goal here is to research how applications and tools with relevant security implications can be made secure but also remain usable for an user who may not have a larger background in IT as well as limited knowledge and experience in these topics.

The researchers of Fraunhofer AISEC were working as partners in the research project ONCE³, with the aim of developing applications which enable the usage of digital identities in the interaction of citizens with public authorities and other services. In the context of this project, the researchers looked into the usability of wallet apps and their current concepts.

For this goal, they developed a low-fidelity interactive prototype and conducted user-studies using this prototype to gather information about the concepts and design used in this prototype [37]. Even though a lot of informational and useful feedback could be gathered from these user-studies, there are still areas not covered by such a low-fidelity prototype. Especially in regards to the interactions happening between the users ID card and the device or scanning QR-Codes with the devices camera while using such a wallet application, a low-fidelity prototype has severe limitations. As the user-studies have been done during the COVID-19 pandemic, in-person studies have not been possible [37]. This means that there has not been a lot of research possible into this area of usability. Another area that was hard to investigate during the pandemic, and also with a low-fidelity prototype, was the use-case of scanning a digital identity on-site. Since during the pandemic only remote user-studies were possible, this use-case was omitted from the study. The simulation of the required interactions between the users and the devices is also difficult to implement with a low-fidelity prototype.

As these areas are also of interest for the researchers of the mentioned group, a need for a high-fidelity demonstrator in form of an implemented mobile application arises. This mobile application should be able to cover the mentioned use-case of scanning an ID on-site. As such, an additional feature to scan such an ID and validate the data is also needed. The demonstrator should then be tested in more user-studies, focusing on the mentioned use-case.

1.3 Goals and Scope of the Thesis

In the process of this thesis, a high-fidelity demonstrator of a digital identity wallet application based on the low-fidelity prototype that was created previously by researchers from the USP Group of Fraunhofer AISEC was developed.

²Fraunhofer-Institut für Angewandte und Integrierte Sicherheit: <https://www.aisec.fraunhofer.de/> (accessed: 04.04.2024)

³https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/Once/Once.html (accessed: 07.04.2024)

This high-fidelity demonstrator is implemented as an Android application. The design of this demonstrator application is based on the low-fidelity prototype while also taking into account information and feedback gathered during the first user-studies. Since a larger focus should be set on the use-case of scanning an ID on-site, an additional feature to scan such an ID in the form of a QR-Code and display the data in a usable way to a checking party was implemented, so that the data and as such the identity of the person presenting the digital ID can be verified.

As a basis for the digital ID used in this demonstrator, the German national ID card is used. Since it is not feasible to gather the real data from the German national ID card onto the application due to various limitations and the cost of the authorization certificate to transmit real data of the ID card using Near Field Communication (NFC)⁴, the process of reading the data from the ID card using NFC is simulated [28]. This means that NFC is used to recognize the presence of an ID card, but dummy data is used from this point onward. It is important to notice that using the national ID card is only chosen as an example for arbitrary identities. The use of the German national ID card in this use-case and study aims to heighten the awareness for security and feeling of importance in the testing candidates, as the data on the German national ID card⁵ corresponds to the characterization of Personal identifiable information (PII) as outlined by McCallister et al. [46]. The developed demonstrator is then used in an user-study to gather feedback about the concept and design of the ID wallet application and the ease of use, especially focusing on the interactions while transmitting the physical ID card to the wallet and creating a digital identity, and also while presenting and verifying this digital identity on-site. For this purpose, a study concept containing use-cases the candidates will have to go through and also interview questions to be asked after working with the demonstrator is created. The results and feedback gathered during this study is analyzed and suggestions for future improvements of the ID wallet concept are derived.

The German government already began developing a concept to fulfill the requirements of the EUDI regulations [25]. Previously, there already were plans to develop a concept of a digital identity wallet for the national ID card, called *Smart-eID*⁶, so during this thesis it is not intended to develop an alternative system and procedure for handling national ID cards as digital identities. As mentioned, the usage of the national ID card as the digital identity of choice is based on hoping that this example will sensitize the testing candidates about the importance of the data.

The usage of digital solutions in on-site situations is a common occurrence in current times, like paying with the smartphone using Google Pay or Apple Pay, or proving a vaccination status like during the COVID-19 pandemic [13], [49]. With this in mind, it seems of interest to also use the digital ID card in a physical and on-site context to verify ones identity. The ideas regarding the Smart-eID do not include transmitting a picture of the person holding the digital identity to the party trying

⁴<https://developer.android.com/develop/connectivity/nfc>

⁵Overview of the data on the German ID card: <https://www.personalausweisportal.de/Webs/PA/EN/citizens/german-id-card/data-on-the-id-card/data-on-the-id-card-node.html> (accessed:11.04.2024)

⁶Press release regarding smart-eID: <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/09/smart-eID-gesetz-in-kraft.html> (accessed: 08.04.2024)

1. Introduction

to verify the identity on-site. Currently, the picture on the physical ID card is an important factor when trying to verify the identity of a person showing this ID card [12]. As such, the difference of trust in the verification results when a picture of the person in contrast to having no picture shown as the party trying to verify the digital identity is seen as a very interesting factor in this thesis. The assumption is that having a picture shown after scanning the digital identity will lead to a heightened trust in the verification results by the verifying party.

To test this hypothesis, an A/B test is performed during the user-study, where half of the candidates fulfill the task of scanning a digital identity without being shown a photo of the ID holder, while the other half have a photo of the ID holder shown after scanning the digital identity. The participants are then asked for their trust in the results of the verification and the data shown to them. Since there is currently no feasible way to transmit these pictures from the physical identity card into the corresponding digital ID card in a wallet when scanning the card using NFC for non-federal institutions, it is assumed that in the future there will be an agreement with the German federal institutions or another way, as for example to gather these pictures from the residents registration office while creating a digital identity from the national ID card [23]. For the implementation of the demonstrator, and to investigate the hypothesis, this is taken as a given and details regarding an implementation of such a process in the context of the demonstrator are omitted.

1.4 Research Questions

After describing the scope and the context of this thesis, a description of the research questions and the hypothesis regarding these questions will follow in this section. The following three research questions are the leading topics during this thesis and will be investigated with the developed demonstrator application and the user-study. Below each research question, a hypothesis of the authors is given.

- **RQ1:** How well does a digital wallet application that follows the concept described in this paper fulfil the usability requirements of users?
 - **H1:** The developed digital wallet application reaches a mean System Usability Score of at least 80.
- **RQ2:** How much does the presence or absence of a photo in the on-site verification of a digital identity from this wallet application affect the usability?
 - **H2:** The presence or absence of a photo does not have a significant influence on the System Usability Score and perceived usability for the users.
- **RQ3:** How much does the presence or absence of a photo during the on-site verification of a digital identity from this wallet application affect the users perceived trust in the solution?
 - **H3:** The presence or absence of a photo does have a significant influence on the perceived trust of the users in the solution while verifying digital identities.

1.5 Structure of the Thesis

The thesis begins with a general introduction of the topic of digital identities, self-sovereign identities and the usage of wallet apps in the context of these topics, exploring the general concepts of these technologies, how they are used already today, and what will be possible in the future using these concepts in chapter 2. Further, the eIDAS and EUDI regulations are described and the Smart-eID will be looked at in this context. A presentation of two existing digital wallet applications follows, and at the end of this chapter an insight into related studies regarding the usability of digital wallet applications is given.

The following chapter 3 describes the implementation process and the resulting demonstrator application in detail. Starting with an outline of the scope of the implementation, the chapter continues with a presentation of the developed demonstrator application while comparing it to the low-fidelity prototype. This presentation is then followed by a deeper insight into technical implementation steps, starting with simulating the transfer of a physical ID card to the demonstrator application, describing the storage of the data, how the digital ID card data is then transferred to other devices, and how photos are integrated into the verification process in the demonstrator application.

This chapter is then followed by an introduction and description of the techniques and methods used during the study of this thesis in chapter 4. After the techniques used during the study have been introduced, the study design is described in detail in chapter 5, giving information about the demographic and the participant selection, the structure of the study, and how one of the presented questionnaires was modified to better suit the study needs.

Afterwards, the data gathered during the user-study is presented and statistically evaluated in chapter 6. The first section contains a statistical overview of the demographic. This is then followed by a presentation and analysis of the response data of the two questionnaires that were answered by the participants during the study. The chapter closes with a look into the transcripts of the study to analyze the responses given to the after-scenario questions and to explore the comments of the participants gathered during the study.

With the gathered data and statistical analysis results, a discussion of these findings follows in chapter 7. After answering the research questions formulated in section 1.4 and looking into whether the hypothesis are accepted or rejected by the findings, a discussion of limitations regarding the demonstrator implementation and the study design follows.

The thesis finishes with a conclusion derived from the findings and the discussion and an outlook into possibilities for future studies or research regarding the demonstrator and the topic of digital identity wallet applications in chapter 8.

2 Theoretical Background and Related Work

This chapter introduces theoretical background information regarding digital identities and the concept of self-sovereign identities, followed by background information about the concept of digital identity wallets. The concept and ideas of the German Smart-eID are looked at, followed by an overview of the eIDAS 2.0 and EUDI regulations. The chapter closes with an overview of existing wallet applications and related studies regarding digital identity wallets.

2.1 Digital Identities and Self-Sovereign Identity

This section gives an overview of what a digital identity is, how it correlates to the term identity and physical identities, and how digital identities and the concept of self-sovereign identities relate to each other.

2.1.1 Digital Identity

A digital identity is usually understood as a digital reference to a person or entity [55]. It is something that a subject has and uses in response to requests for digital identification, authentication, or proofs of authorization and consists of attributes that can be revoked, deleted, transferred, or exchanged [55]. While often being a human, the subject of a digital identity can also be a legal entity, an animal, or a device, among other things [55].

The term identity can be defined as “the representation of an entity through features that make the entity unique and/or persist through time, in a given context” [60]. The American Heritage Dictionary defines identity as “The set of characteristics by which a person or thing is definitively recognizable or known” [31]. Thus it can be deduced that a digital identity has similarities to a physical identity in representing the characteristics of an entity, but in a digital context [60].

Another definition of digital identities was given by Cameron as “a set of claims made by one digital subject about itself or another digital subject” [11]. Cameron also presents seven so called laws of identity, which they see as essential to explain the success or failure of a digital identity system and which are well summarized by Soltani et al. as the following [11], [60]:

1. Users should be in control of how their identity information is shared.
2. The amount of information disclosed should only be the minimum necessary amount required, and data should not be kept longer than needed by the other entities.
3. The user should be well informed about which entities manage their identity information.
4. The user’s information should not be created or exposed in such a way to allow data correlation, pattern recognition, or entity identification by unauthorized entities.

5. Interoperability and seamless integration among various entities supported by different architecture should be possible.
6. Reliable and secure integration between human users and machines should be empowered.
7. Consistent user experience across multiple contexts and technologies.

According to Soltani et al. [60], digital identity wallets exist in the context of digital identity systems, so these laws also relate to them. Digital identity systems have to balance three different factors: Usability, cost, and risk, as shown in figure 1 [56].

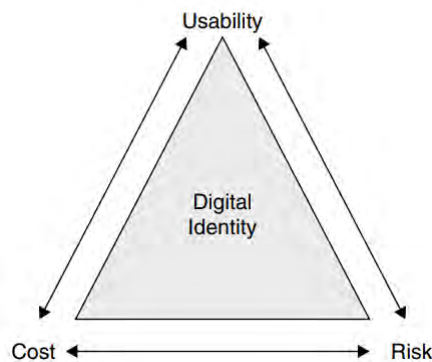


Figure 1: Factors in a digital identity system according to Seigneur et al. [56]

When using a digital identity system, the user has to be aware of risks that may occur if their device or the security of the system is compromised [56]. This has to be balanced with usability, as a system that is difficult to use may produce security risks on its own, for example users may write down passwords as they are not able to memorize all the passwords they have to set and use [56]. The third factor is the cost associated with such digital identity system, as the users should not be burdened with additional cost to achieve risk reduction and usability by for example needing to buy one-time password tokens or similar [56].

Digital identities are managed in accordance with certain identity management models, with three main actors identified by Soltani et al. [60], shown in figure 2.

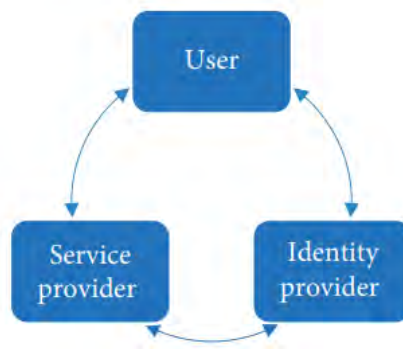


Figure 2: Actors in identity management according to Soltani et al. [60]

2. Theoretical Background and Related Work

The evolution of these models started with the *isolated identity model*, in which the service provider (SP) also took over the role of the identity provider (IdP) and is the sole responsible party for all identity management operations of its users [60]. Drawbacks of this approach are that the users must maintain a large number of credentials, as they need one for each SP, and also the risk of many different service providers storing large amount of user data [60].

This approach was followed by the *centralized identity model*, where SP and IdP were decoupled entities but still belonged to the same organization [60]. Each access to a SP must be authenticated by a central identity provider system in the organization [60]. This concept is susceptible to security risks due to the centralized aspect, allowing a disclosure of users credentials to result in access to all services associated with that user in this organization [60].

The next step is the *federated identity model*, where a group of SP and IdP form a federation and allow the user to authenticate through one of the IdPs of the federation to access all of the federations SPs [60]. Solutions for digital ID cards like the German *eID* also belong to this model [16]. A problem with the federated model is that the user data is remaining at the centralized IdP and thus, the user is dependant on the continued existence of this IdP [16]. Another risk is is that it is easier to combine the identity attributes of the user to create a profile of them without their knowledge [16].

The newest emerging concept is *self-sovereign identity*, which will be discussed in detail in the following section [60].

2.1.2 Self-Sovereign Identity

Self sovereign identity (SSI), also called *self-managed identity* or *user-controlled identity*, is another identity management model and the next step in the evolution of identity management models after the federal identity model [60]. SSI gives the identity holder more control over their data by allowing them to decide how and under what conditions their data is shared with others [60]. It is based on a decentralized approach and promotes the premise that an individual completely owns, controls, and manages their identity [65]. The individual is seen as its own identity provider, as the individuals digital identity is independent of any single organisation [65].

Allen proposed ten principles of SSI, which attempt to ensure the users control over their identity and define an SSI system [1]:

1. **Existence.** Users must have an independent existence.
2. **Control.** Users must control their identities.
3. **Access.** Users must have access to their own data.
4. **Transparency.** Systems and algorithms must be transparent.
5. **Persistence.** Identities must be long-lived.
6. **Portability.** Information and services about identity must be transportable.
7. **Interoperability.** Identities should be as widely usable as possible.

8. **Consent.** Users must agree to the use of their identity.
9. **Minimalization.** Disclosure of claims must be minimized.
10. **Protection.** The rights of users must be protected.

The concept of SSI describes three principal roles: the *Issuer*, the *Holder*, and the *Verifier* [48]. The issuer is responsible for the creation of credentials and the distribution of those credentials to the holder [48]. The credentials used in SSI are called *Verifiable Credentials* (VC) and are cryptographically secured sets of claims that can be verified without contacting the issuing party [16]. The holder receives those VC from an issuer, retains them, and shares the VC with a verifier if required [48]. A verifier requests, receives, and verifies VC presented by a holder by verifying the digital signature of the issuer of the VC and trusting this issuing party [48], [51]. These roles exist in a trust triangle in the concept of SSI, as VCs only convey trust when the verifier trusts the issuer of the VC [51]. A graphical representation of this triangle is shown in figure 3. This figure also contains an element called *digital wallet* at the holder, which is a concept used in SSI to hold the VCs of an user and will be presented in detail in the following section [16].

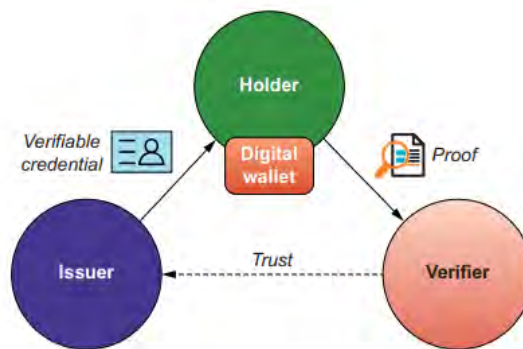


Figure 3: Trust triangle in SSI according to Preuschkat et al. [51]

2.2 Digital Identity Wallets

The term digital identity wallet was introduced in the previous section and presented as an important construct in the concept of SSI [51]. Preuschkat et al. state that “Digital wallets and agents are to SSI what browsers and servers are to the web: the basic tools we need to make the whole infrastructure work.” [51], which emphasizes this strong relation between the concept of SSI and digital identity wallets. This section will describe the idea of digital identity wallets and present current work regarding a unified definition of the term digital identity wallet.

Defining digital identity wallets appears to be a difficult task, as it is only vaguely defined and often used and misused for different technical concepts [50]. Podgorelec et al. [50] conducted a systematic literature review regarding the topic of digital identity wallets to find a definition for the term digital identity wallets based on existing definition attempts. The result of this review is the following definition [50]:

2. Theoretical Background and Related Work

“The digital identity wallet is software that operates in the remote or local environment and enables the storing, managing, and sharing of digital identity-related data. The digital identity wallet also provides secure storage for cryptographic material associated with digital identity-related data. With a digital identity wallet, the user controls and manages identity related data. That includes removing and reviewing identity related data stored in the wallet and explicitly selecting what identity-related data to store/share into/outside the wallet. Moreover, when selecting identity related data to be shared outside the digital identity wallet, a user should be able to combine different identity-related data. Additionally, with the support of the underlying environment, a digital identity wallet can recover and back up identity-related data.” [50]

This describes the basic idea of digital identity wallets in a short but precise way. Ehrlich et al. give a shorter summary of the functionality: a digital identity wallet is used to store and manage the users credentials in an SSI-based system [16]. Podgorelec et al. [50] also define what functionality a digital identity wallet should be able to provide. The mentioned capability of securely storing cryptographic material associated with digital identities also shows similarities to the concept of verifiable credentials, as mentioned in the previous section about SSI [50].

Podgorelec et al. [50] also investigated motivations to use digital identity wallets during the literature review and came to the following answer:

“The primary motivations for applying digital wallets to the digital identity domain are to avoid digital identity related data centralization, enhance the security and privacy of identity-related data, provide control over identity-related data under user responsibility, and ease the use of digital identities.” [50]

They mention the aspect of decentralization of digital identity data which relates to the ideas of SSI, which also revolve around a decentralized identity management, as mentioned in the previous section [50]. They further emphasize the importance of the control of this digital identity data to be the users responsibility, which also can be seen in the ideas of SSI [50]. In the final sentence they also mention the relevance of digital identity wallets to ease the use of digital identities, which emphasizes the relevance of usability in regard to digital identity wallet solutions [50]. This is further supported by Preuschkat et al. [51], who highlight that digital identity wallets are a critical component regarding the user experience with the concept of SSI, as they are the representing component of SSI to the users.

Soltani et al. [60] outline that a digital identity wallet may not only exist as software but may also be a hardware solution. They point out that a wallet may be deployed in various forms, from a mobile application on the users smartphones to a browser application, or even a software as a service cloud-based solution and that users may own multiple wallets at the same time [60].

2.3 Smart-eID

On the first of September 2021, the so-called Smart-eID-law⁷ came into effect in Germany [59]. This law was the cornerstone of the *Smart-eID* project by the German government, which aimed to enhance the functionality of the current eID [59]. Instead of tapping the physical ID card on the smartphone for each usage of the eID, the Smart-eID has the goal to store the ID card data on the smartphone, so that only the phone and the PIN of the ID card are necessary on further authentication attempts [59], [9]. The digital ID card is stored in a hardware-based solution called secure element on the smartphone to allow for high security standards in the storage of identity data [9]. As of 2022, only a few devices from Samsung are supported by the Smart-eID and gave access to the secure element for the purpose of storing a digital ID card [59], [9].

Skierka [59] highlights that the support of all devices from the leading smartphone manufacturers is crucial for the success of the Smart-eID. The plan of the German government was that the Smart-eID would be available to the public by December 2021, and by the first half of 2022 they intended to support most of the smartphones available in the market [9]. Skierka [59] mentions in their article from late 2022 that the Smart-eID is not available to the public and only supported by certain Samsung devices, which shows that these goals could not be met by the German government. A press release from the German government in 2023 also confirms a delay with the Smart-eID, as it is stated that currently no release date can be announced [33]. According to media reports based on a published letter of the German government, the technical development of the Smart-eID has concluded but the continuation of the Smart-eID project is currently on hold because of missing funds [63].

2.4 eIDAS 2.0 & EUDI-Wallet

As a revision of the eIDAS regulation, mentioned in section 1.1, the eIDAS 2.0 regulation was decided upon in 2023 and adopted on the 29th of February 2024 in a final vote of the European parliament [21]. The goal of the eIDAS 2.0 regulations is to enhance the interoperability between digital identity solutions of all EU countries by mandating the development of a national electronic identification [21]. The eIDAS 2.0 regulations are an advancement of the eIDAS regulation with a focus on decentralization and SSI concepts, and the main changes concern the topic of electronic identification [54].

The eIDAS 2.0 regulation is also called EUDI regulation, where EUDI stands for European Digital Identity [6]. The main point of the EUDI regulation is the introduction of European digital identity wallets, which are called EUDI-Wallets and are mandatory to be offered by each EU country to citizens and businesses [21]. The offered wallet can also be developed by cooperation of the state with private companies or organisations, where each party provides various components of the wallet, or even private sector developed wallets when they are certified by the state to operate

⁷Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät: <https://dip.bundestag.de/vorgang/gesetz-zur-einf%C3%BChrung-eines-elektronischen-identit%C3%A4tsnachweises-mit-einem-mobilen-endger%C3%A4t/273933> (accessed: 26.04.2024)

2. Theoretical Background and Related Work

as a wallet issuer and provider [7]. The EUDI-Wallets are supposed to store digital ID cards, but also other identities like a drivers license, diploma, or bank account [21].

To achieve interoperability and a standardized set of guidelines and rules for these EUDI-Wallets, the European commission agreed on the EUDI-Wallet Toolbox, a collection of documents describing the guidelines of the EUDI-Wallet concept and including the so-called Architecture and Reference Framework (ARF)⁸, which describes the objectives of an EUDI-Wallet, roles and actors of the ecosystem, requirements of the EUDI-Wallet, and potential building blocks for such a wallet [19].

The European commission defines the main benefits of EUDI-Wallets for citizens and businesses as the following [21]:

1. **User control:** Citizens will have the power to choose which aspects of their identity and data they share with third parties, ensuring privacy and control over personal information.
2. **Widespread usability:** The EU Digital Identity Wallets will be available across the EU for accessing public and private digital services, making online interactions more seamless and efficient.
3. **Transparency and security:** the EU digital wallets will be open-source licensed, ensuring transparency and security. Users will be reassured that their data is handled securely, with measures in place to prevent misuse or illegal tracking.
4. **Ease of use:** The wallets will offer a user-friendly interface, allowing individuals to easily manage their digital identities and access services. Creating qualified eSignatures for non-professional use will be free, enhancing accessibility.
5. **Smooth onboarding:** Citizens will be able to use national eID schemes to register for the wallets, ensuring a smooth transition to digital identity management.

The first of these points draws parallels to the concept of SSI, highlighting the users control over the identities in an EUDI-Wallet. From the fourth point, the necessity of usability considerations is implied for a successful acceptance of an EUDI-Wallet.

The German government started a project to assess a basis for German EUDI-Wallets under the leadership of the Federal Ministry of the Interior and Community [8]. The project is designed to be an open, participatory, and transparent process with the involvement of the public, academia, and the private sector [8]. An objective of this project is to assess how such a wallet can be provided in a sustainable way, either by the German government itself or a mandated wallet provider [8]. After 60 position papers have been submitted at the beginning of the project by various parties from the mentioned areas, the project now consists of more than 100 people and organisations who participate in workshops to define conditions and use-cases of a German EUDI-Wallet, elaborate potential business models for wallet providers and elaborate on a wallet architecture for a German EUDI-Wallet solution [8].

⁸<https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework> (accessed: 22.04.2024)

2.5 Existing Digital Identity Wallet Applications

This section will present a selection of digital identity wallet applications that are currently in development or already released as a beta to be used by the public. The selected wallet applications are the Lissi wallet⁹ and the esatus wallet¹⁰. Both of these wallet applications offer a demo of their functionality, which will be presented during this section.

2.5.1 Lissi Wallet

The Lissi digital identity wallet is developed and published by Lissi GmbH, a startup that originated from the company neosfer¹¹ who develop digital wallet software following the eIDAS 2.0 regulations [42]. Lissi GmbH is initiator of the IDunion project¹², a project with the aim to create an open ecosystem for decentralised identity management based on European regulations but usable worldwide [34]. The IDunion project contains a digital identity network based on the SSI concept by employing the Hyperledger Indy¹³ framework [38].

The Lissi wallet supports the core standards required by the eIDAS 2.0 and EUDI regulations defined in the Architecture Reference Framework (ARF) already, which are crucial to be recognized as an EUDI-compatible wallet application [41]. This allows Lissi to aim for a recognition as an EUDI-Wallet in the future, but according to Lissi the precise requirements for the recognition are not defined completely for now, so it is uncertain whether this recognition will happen in the future [43].

The Lissi wallet is currently published in a beta state and is offered as a demo to interested users. The demo consists of five use-cases which include a digital ID card, a digital credit card, a digital hotel check-in, a digital university certificate and course enrollment, and a digital purchase proof [44].

To gather information about the appearance and usage of the Lissi wallet, the first two use-cases of the demo will be presented in further detail. The Lissi wallet demo starts with the setup of a login PIN and the decision of using biometric authentication of the device instead of the PIN for future uses. After this setup, an empty wallet screen is shown with the hint that there are currently no identities and the hint to connect with a new contact using the QR-Code scanner. The process of acquiring a digital ID card begins with a QR-Code on the Lissi demo website that needs to be scanned. After scanning the QR-Code, a contact request appears in the Lissi wallet. This contact request shows metadata and a verification status of the organisation which a contact is about to be created. After accepting the contact request, the wallet application redirects to the empty wallet screen, but switching to the contact screen shows the new contact, which offers a new digital ID card. This process is shown in figure 4.

⁹<https://www.lissi.id/> (accessed: 22.04.2024)

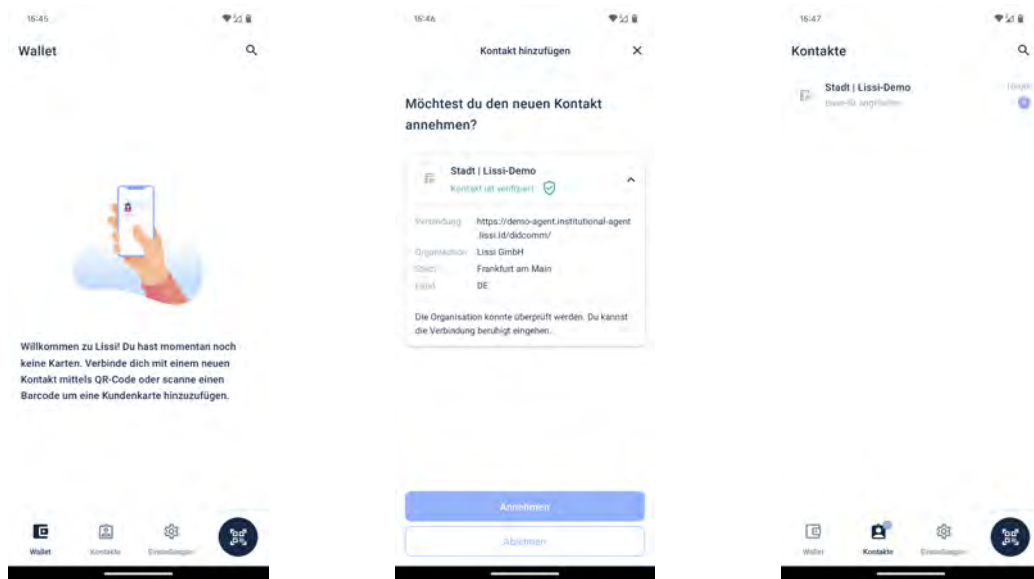
¹⁰<https://esatus.com/en/digital-identity/> (accessed: 22.04.2024)

¹¹<https://neosfer.de/> (accessed: 22.04.2024)

¹²<https://idunion.org/?lang=en> (accessed: 22.04.2024)

¹³Framework for providing digital identities on distributed ledgers: <https://www.hyperledger.org/projects/hyperledger-indy> (accessed: 22.04.2024)

2. Theoretical Background and Related Work



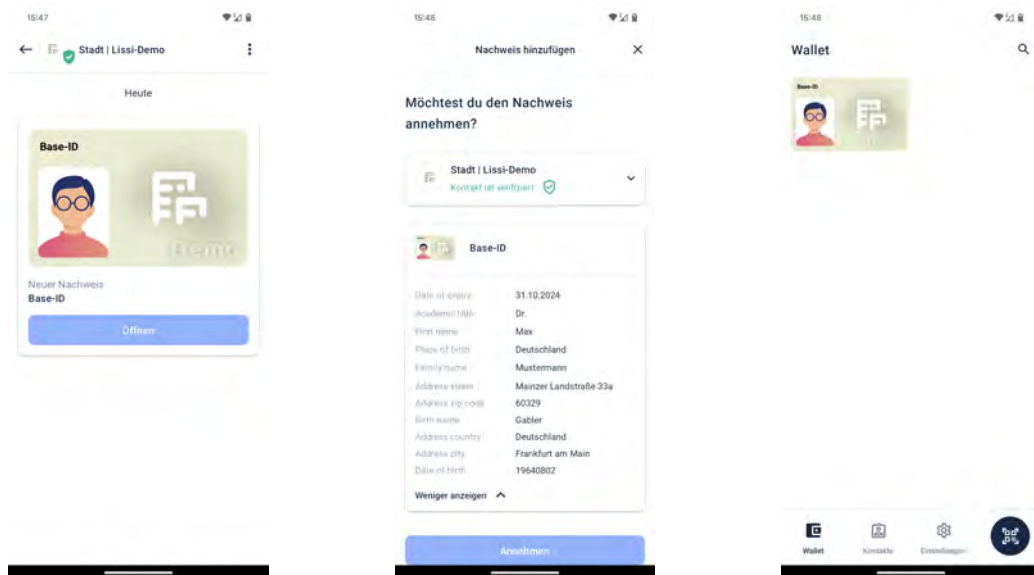
(a) Wallet screen with no identities added.

(b) Contact request after scanning QR-Code.

(c) Contact screen after new contact was added.

Figure 4: Lissi wallet steps to add a new contact.

Clicking on the entry of the new contact leads to a screen that resembles a messaging view, in which a new identity in the form of a digital ID card is offered to the user. Clicking on the open button shows details regarding the issuer of the identity and the new identity itself and the data associated with it. After accepting the identity, the new digital ID card is shown in the wallet screen. These steps are shown in figure 5.



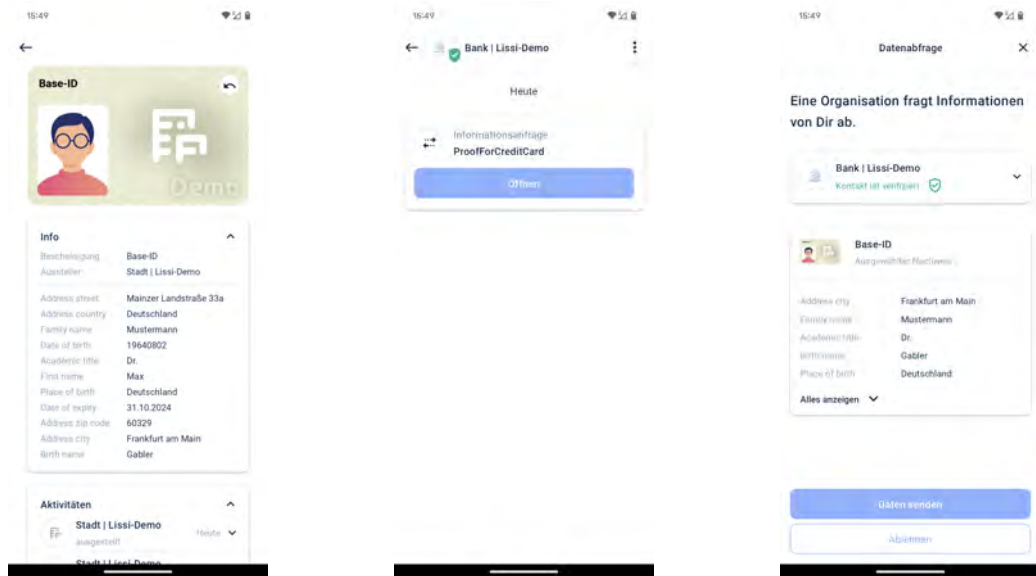
(a) Contact Message screen with new identity offered.

(b) Details of offered identity and issuer.

(c) Wallet screen after digital ID card was added.

Figure 5: Lissi wallet steps to add a new digital ID card.

The information stored in the digital ID card can be reviewed by clicking on the digital ID card entry. The second use-case in the Lissi demo contains the usage of the created digital ID card for identity verification. After approving another contact request, this time from a bank, the new bank contact asks for an identity proof to create a digital credit card. Opening this request shows information about the requesting party and the data that will be shared. It does not appear to be possible to select which data should be shared. This process is shown in figure 6.



(a) Detail view of the digital ID card data.

(b) Identity proof request by contact.

(c) Details of the identity verification request.

Figure 6: Lissi wallet steps to verify identity with a digital ID card.

2.5.2 esatus Wallet

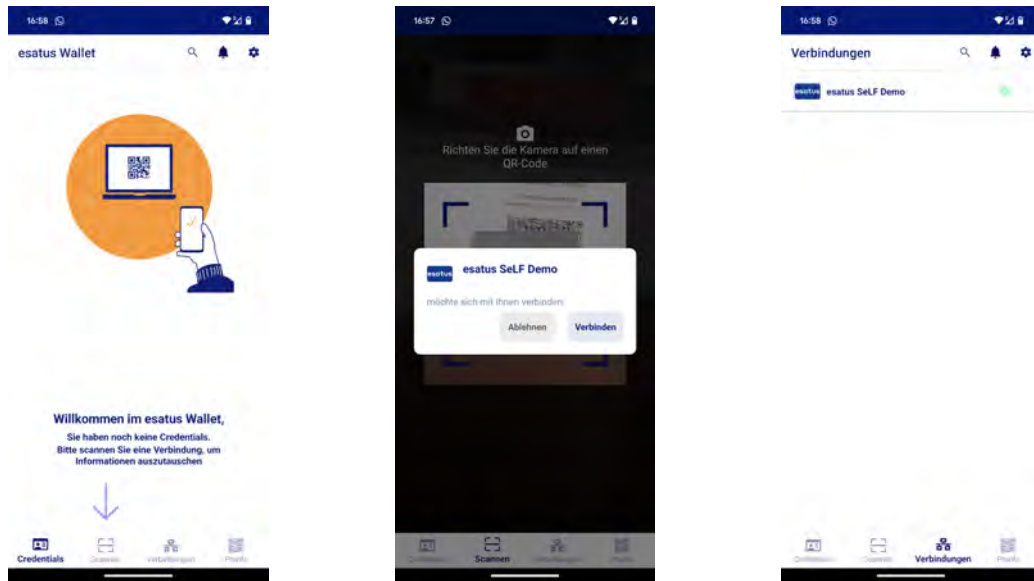
The esatus wallet is a digital identity wallet developed by esatus AG¹⁴, an IT service provider specialized in digital and decentralized identities [17]. The esatus wallet is also part of the IDunion project network, and esatus is a member of this project [35].

The esatus wallet also offers a demo of the application, which includes the creation and usage of a demo credential [18]. In comparison to the Lissi demo, less use-cases are offered and no real physical identity is referenced by this demo credential. The demo will be presented in the following paragraphs.

The esatus wallet demo begins with the setup of an application PIN. No biometric options are offered in this step, but can be activated in the settings of the application. After scanning a QR-Code from the esatus demo website, a request for a new connection is shown in the wallet application. In comparison to the Lissi wallet, only the name of the new connection is shown, no further data or verification status is present. After accepting this request, the new connection appears in the corresponding view of the wallet. These steps are shown in figure 7.

¹⁴<https://esatus.com/en/about-us/> (accessed: 22.04.2024)

2. Theoretical Background and Related Work



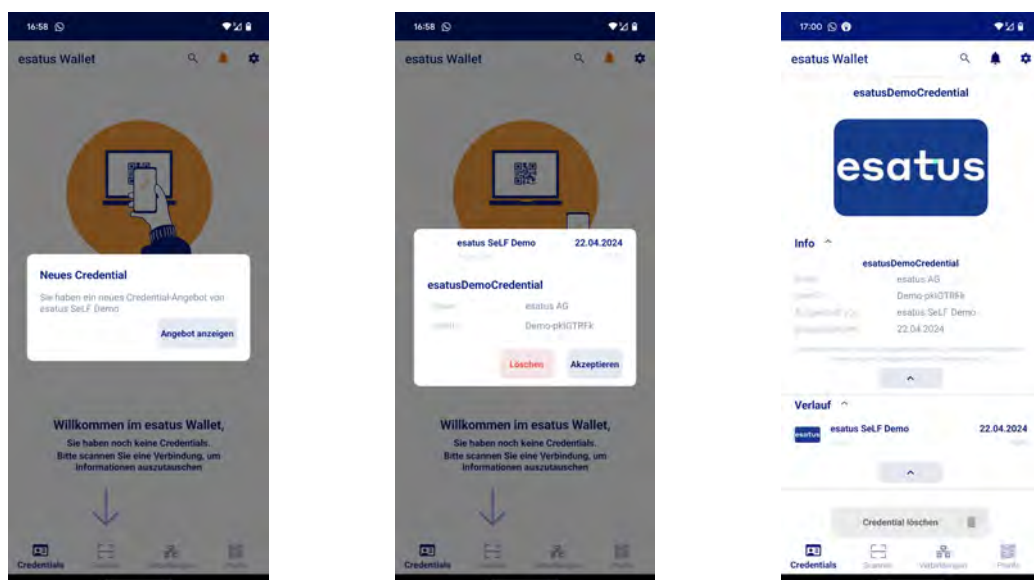
(a) Wallet screen with no identities added.

(b) Connection request after scanning QR-Code.

(c) Accepted connection in the connection screen.

Figure 7: esatus wallet steps to accept a new connection.

Initializing the creation of a demo credential on the esatus demo website leads to a credential offer being shown in the wallet application. Continuing then shows details about the credential. Only an issuer and an user-id are shown, which is the only content of the offered demo credential. The wallet screen then shows the new credential with detail information and usage history in one screen, no separate detail screen is offered. The described process is shown in figure 8.



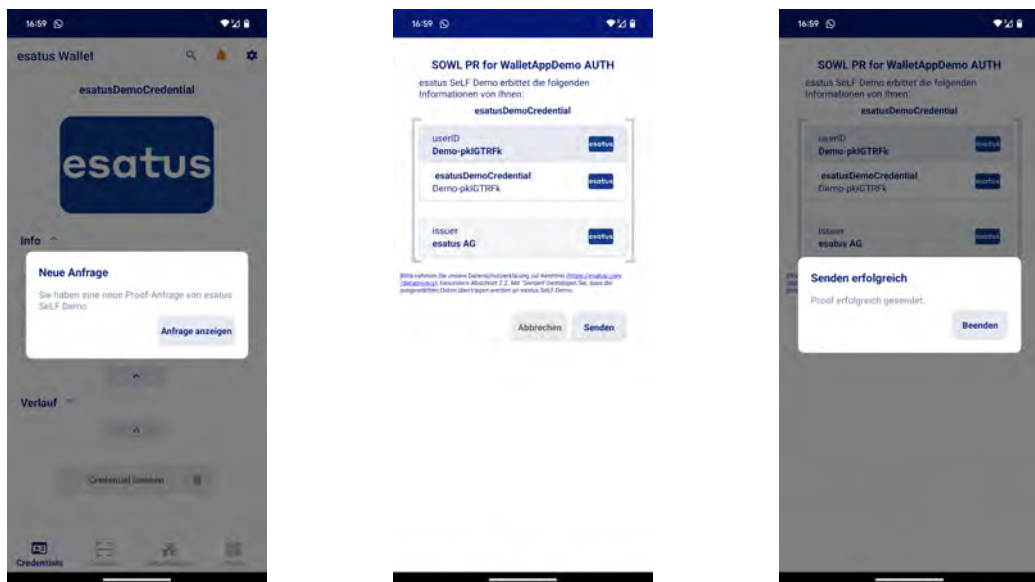
(a) Offer of a new credential.

(b) Details of the new credential offered.

(c) Wallet screen with the new credential.

Figure 8: Steps to add a new credential to the esatus wallet.

An identity verification request is initiated automatically by the esatus demo website and appears in the wallet application. Continuing shows a detail screen of the verification request. This detail screen contains information regarding the issuer and which data is shared, but not much information is given regarding the requesting party except for a name. Accepting the request only shows a confirmation dialog and the confirmed request becomes visible in the history of the credential. These steps are shown in figure 9



(a) Identity verification request.

(b) Details of the verification request.

(c) Confirmation of successful verification.

Figure 9: Identity verification steps in the esatus wallet.

2.6 Related Studies in this Field

A very important related study is the paper "Do Users Want To Use Digital Identities? A Study Of A Concept Of An Identity Wallet" by Kostic et al. [37]. This paper, together with the low-fidelity prototype of a wallet concept that was developed during the process, and the user study they conducted during the research process is the basis and also the trigger for this thesis. During this thesis there are many referrals to the low-fidelity prototype, and the developed Android demonstrator is based on this low-fidelity prototype while expanding the possibilities of testing the interactions of the users with the wallet application and especially with the device and the physical ID card in the process.

During their study, Kostic et al. [37] investigated the following research questions:

- 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?

2. Theoretical Background and Related Work

To develop the prototype and the wallet concept, they collected requirements for the wallet and the handling of data with a focus group of six people, and after developing the concept and prototype they conducted two user studies with eight participants for each study, leading to a total of 16 participants [37]. Due to the study being conducted in September and October 2022 and as such during the COVID-19 pandemic, they conducted the study in a digital format using a video conferencing tool and distributing the digital interactive prototype online to the participants, while the participants shared their screen during the study [37]. The participants were encouraged to think aloud¹⁵ during the study [37]. This remote setup was seen as a limitation to the study, as the interaction between the physical ID card and the smartphone during the process of digitizing an ID card can not be simulated sufficiently in this digital study approach [37].

All participants successfully completed the tasks given to them, and 15 of the participants noted that they were convinced by this wallet concept [37]. As an answer to RQ2, for a majority of the participants it was made clear that the data in the wallet comes from a physical national ID card [37]. Kostic et al. [37] also saw that the identification process was well understood and all participants always knew which data was sent to which service at all time, while participants also highlighted the ease of use of the wallet concept, giving an answer to RQ1.

Kostic et al. [37] noticed great willingness of the participants to use an app based on this concept, as they noticed the added value of such a solution. As an influencing factor on trust and control over the data, Kostic et al. [37] identified the wallet operator to be relevant. The participants appeared divided into two camps, one camp preferring the state as an operator while the other camp preferred a private company as an operator [37]. As these camps were both large, no conclusion regarding a recommended operator can be found from the results [37].

Building upon the study of Kostic et al. [37] is the master thesis of Murtezaj [47] and the study concluded during this thesis. During the thesis, a three-phased study approach was developed and then used in user studies [47]. This approach saw the wallet concept developed by Kostic et al. [37] being evaluated regarding usability and user trust in the first phase of the user study with 15 participants [47]. In the second and third phase, variations of the concept based on the feedback of the first phase were used [47]. Based on these variations, user studies were again conducted with 15 participants in each phase, using the same study tools as in the first phase to allow for comparability [47]. These tools consist of a SUS questionnaire and a HCTS questionnaire combined with open-ended questions during the study [47].

The variations in phase two include an expired identity history and a side drawer menu with information regarding the app like a frequently asked questions section, a setting menu with security settings, information about the app developer, a help and contact option, and an option to rate the app [47]. Variations in the third phase concerned the importance of the wallet operator, as already identified by Kostic et al. [37] during their study [47]. Results from the first phase of Murtezaj's [47] study indicated that the participants preferred the state as the wallet operator, so in the third phase the logo of a state institution was placed in the start screen of the app.

¹⁵The think aloud protocol is a tool in usability testing: <https://www.nngroup.com/articles/thinking-aloud-the-1-usability-tool/>, (accessed: 28.04.2024)

Murtezaj [47] encountered high usability scores from the SUS questionnaire during all three phases of the study, with a mean score of 90.00 in phase 1, 88.00 in phase 2, and 90.33 in phase 3. They also saw participants describing the wallet concepts as intuitive, user-friendly, and easy to navigate [47]. These results further support the results from the study of Kostic et al. [37]. Furthermore, Murtezaj [47] encountered a high level of trust by the participants throughout all three phases, with a score of 76.3% in phase 1, a score of 79.6% in phase 2, and a score of 82.3% in phase 3. The highest scores for both usability and trust have been reached in the third phase of the study, from which Murtezaj concludes that the wallet operator has higher influence on conceived trust than security relevant settings and additional information for the user [47]. They further concluded that the addition of a lot of features in phase two lead to a slight decrease in usability [47]. The focus on digitally literate participants during the studies is identified as a possible limitation by Murtezaj [47], and they suggest further research to also include participants less comfortable with technology.

A study concerning a wallet prototype based on the concepts of SSI was conducted by Korir et al. [36]. They developed a wallet prototype based on the SSI principles, with an Android application and two websites for fictional banks serving as identity provider and service provider [36]. The prototype uses a Hyperledger Indy network (also mentioned in section 2.5.1) [36].

With the prototype, Korir et al. [36] conducted an user study with 30 participants from the USA and the UK to answer the following main research question:

“What are the user-centered privacy and security challenges facing decentralized identity wallets?” [36]

They included a SUS questionnaire in their study and encouraged the participants to think aloud during the study [36]. As the study was also conducted during the COVID-19 pandemic, they used Zoom¹⁶ to do the study in remote with the participants, recording the study procedure for each participant for further evaluation [36].

The results of their study show that the participants did not completely understand the concept of user control about the credentials in the concept of SSI, as many users were unsure whether the identity provider has control over the provided credential [36]. They also identified the usage of the SSI terms like *decentralized identifiers*, *verifiable credentials*, and *identity proofs* as problematic, as these terms may at first spark interest in the application but ultimately hinder the learnability of the wallet application as they are not clearly understood [36]. QR-Codes were also identified as a hindrance in the user journey during their study, and they recommend to minimize the usage of QR-Codes in a SSI-based wallet based on their results [36].

Another study about the usability of SSI-based wallets is the paper of Sartor et al. [53]. In contrast to the previous studies, Sartor et al. [53] did not develop a new concept or prototype, but investigated already existing SSI-based wallets, which are the *Connect.me Wallet*¹⁷, the *Gatata Wallet*¹⁸, the *ID Wallet*¹⁹, and the *Lissi Wallet*²⁰.

¹⁶Video conferencing platform: <https://zoom.us/> (accessed: 27.04.2024)

¹⁷<https://www.evernym.com/blog/connect-me-sovrin-digital-wallet/> (accessed: 27.04.2024)

¹⁸<https://gatata.io/products/wallet/> (accessed: 27.04.2024)

¹⁹Discontinued and no longer accessible: <https://digital-enabling.eu/> (accessed: 27.04.2024)

²⁰<https://www.lissi.id/> (accessed: 27.04.2024)

2. Theoretical Background and Related Work

Sartor et al. [53] conducted interviews during the study and also included an UEQ²¹ questionnaire extended with seven questions specific to characteristics of SSI-wallets to gather quantitative usability data. As the study also took place during the COVID-19 pandemic, 85% of the interviews were conducted using video conferencing software [53]. They conducted 60 interviews in total, with 15 participants for each wallet [53].

A key finding during their study was, that all four wallets ranked bad or below average in the UEQ category of novelty, which surprised them, as SSI-wallets include innovative technologies and allow for workflows previously not available to end users [53]. They see the reason for this in the users not understanding the idea of SSI and the differences to a physical identification process and recommend detailed tutorials and introductions that explain what a SSI-wallet is able to do [53]. Another finding was that all four wallets ranked below average in the category of stimulation, which might go hand in hand with the previous finding and in the opinion of Sartor et al. [53] may be a result of the wallets focus on functionally and administratively oriented purposes. Their data also indicates that a representation of the credentials in graphical form is better accepted by users than a text-based representation, with two participants highlighting that they especially liked a representation close to a physical credential design in the Connect.me wallet [53]. The usage of technical terms of the SSI-concept was also identified as problematic and hindering during the study [53].

²¹User Experience Questionnaire: <https://www.ueq-online.org/> (accessed: 27.04.2024)

3 Implementation

This chapter describes the demonstrator that was developed in the process of the thesis. It starts with a definition of the planned scope of the demonstrator, followed by a general presentation of the demonstrator in relation to the previous low-fidelity prototype created by Kostic et al. [37]. Afterwards, a general overview of the architecture of the demonstrator will be given, followed by detailed descriptions of the implementation of important functionality steps for the usage of the demonstrator. This includes how the physical ID card is transformed into a digital ID card, and how the identity data is stored in the demonstrator wallet. A larger focus will be set on how the identity data is transferred between devices in the demonstrator implementation of this wallet. The last subsection describes how the inclusion, presentation, and transfer of photos is handled in the demonstrator. The source code of the application can be found at [A.7](#).

3.1 Scope of the Demonstrator

The demonstrator developed in the process of the thesis is implemented as an Android application to enable realistic user experiences when using it for user studies. It is written in Kotlin²², the currently preferred programming language for Android app development [57]. The design and functionality is based on the low-fidelity prototype developed by Kostic et al. [37]. As the focus of this thesis is the on-site authentication using a digital ID card and the relevance of photos in this process, the feature set in the demonstrator has been reduced and focused on handling a national ID card. Further identities like a drivers license or a health card are not in the scope of the demonstrator, but preparations for those type of IDs have been done. Furthermore, the functionality of handling other cards like library cards, and the handling of digital keys for cars and hotels has been omitted from this implementation for reasons of focusing on the investigated use-case. The demonstrator has been developed in German due to the usage in user studies with German participants during this thesis, as this allows for easier learnability by these participants.

The demonstrator includes various simplifications in the process of setting up and creating a digital ID card. The demonstrator does not read the real data from a physical ID card. The process is simulated using NFC, but dummy data is used from this point onward. A detailed description of the reasons for this and the implementation of the simulation is found in section 3.3.1. The demonstrator also omits security and safety concerns, as it is focused on serving as a tool for user and usability studies instead of offering a technical complete solution for a wallet app. As such, identity data is stored persistently, but not encrypted or otherwise secured from third-party access in the current implementation. Further details regarding the storage of data are given in section 3.3.2.

As the focus of the thesis is the on-site authentication using a digital ID card, a large focus was the transfer of the identity data between devices, in this case between the person authenticating themselves and the person validating the identity data. For this purpose, a QR-Code based solution was implemented, allowing the transfer of

²²<https://kotlinlang.org/> (accessed: 22.01.2024)

3. Implementation

identity data and also the creation of so-called *authentication requests*, which encode requested identity data as an easy way for the validating party to define which data is necessary for a successful validation. Furthermore, a second app for reading those QR-Codes, containing identity data, was developed to be used in user studies as a mean to allow the verifying part of an on-site authentication to be simulated and studied. This is especially important for the question of this thesis if photos are necessary and increase trust in such wallet solutions. While the implemented solution is transferring the real data stored on the device, there was no focus on technical safety and security as the aim is to provide a tool for user tests. The data is transferred unencrypted and without any tampering checks in place. Details on the implementation of the transfer using QR-Codes and the validation app are given in section 3.3.3.

Regarding the inclusion of photos in the digital ID card data, the demonstrator uses hard-coded photos of the study supervisor and the persona of the sample German ID card, as at the point of writing the thesis and implementation of the demonstrator, no solution for obtaining the photo of the German ID card is offered. The thesis assumes that means to get the photo from the registration office in a digital way will eventually be implemented and as such in the implementation of the demonstrator it is assumed that such a technology will exist in the future. With this assumption in mind, the usage of hard coded photo data for the demonstrator with focus of using it in user and usability tests is seen as sufficient to observe the relevant information in such studies. Further information regarding the limitations and implementation of photos in the process will be given in section 3.3.4.

3.2 Presentation of the Demonstrator Application

This section will give a short overview of the developed demonstrator. The demonstrator is based on the low-fidelity prototype of Kostic et al. [37], deviating slightly in parts where the low-fidelity approach had ideas that were technically not feasible or too time consuming to implement for a demonstrator implementation. It also has slight deviations because of usability concerns found in previous studies regarding the low-fidelity prototype. The most important deviations will be highlighted by side-to-side screenshots of the low-fidelity prototype and the corresponding demonstrator implementation.

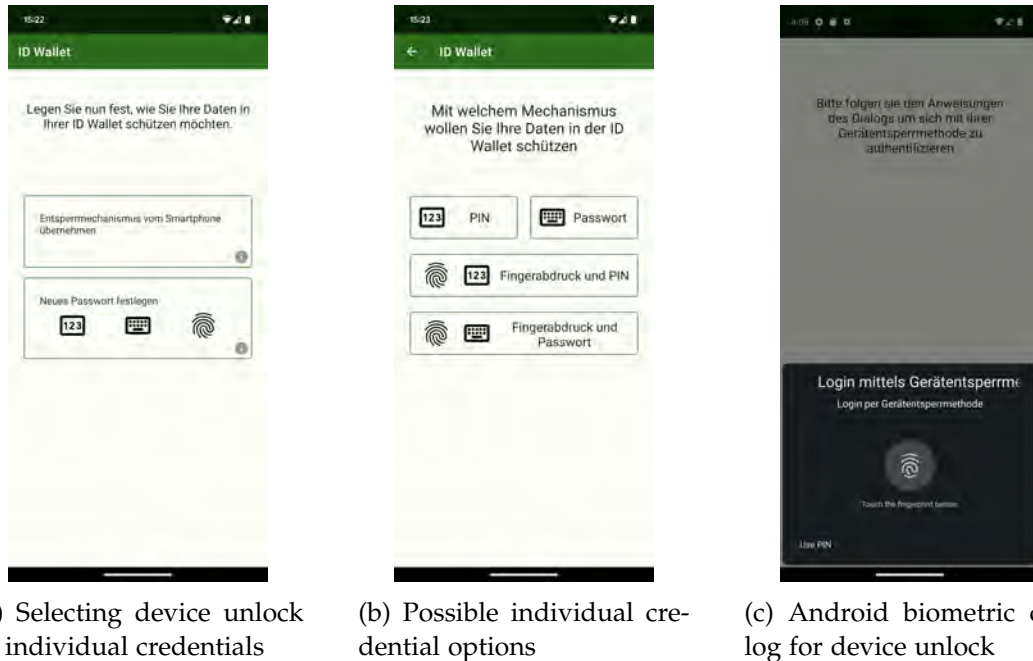
3.2.1 Introduction Tour & App Authentication Setup

The demonstrator Android app also starts with an introduction tour feature, explaining the user the most important features of the ID-Wallet at a short glance. This step is nearly identical with the low-fidelity prototype with minor adjustments to adhere to Android design standards.

This is followed by the first-time setup of the app, which currently only includes setting up an authentication method to login into the app. The user can choose between using the current device unlock mechanism from the smartphone, implemented using the Android biometric API²³, or setting up individual credentials for the wallet. The device unlock mechanism allows to continue with the current fingerprint and

²³<https://source.android.com/docs/security/features/biometric> (accessed: 10.05.2024)

backup pin, pattern, or password setup. If no device unlock mechanism is currently set up, the app will redirect the user to the system dialog to set up a device unlock method, including setting up fingerprint authentication. The selection steps and the device unlock mechanism are shown in figure 10.



(a) Selecting device unlock or individual credentials

(b) Possible individual credential options

(c) Android biometric dialog for device unlock

Figure 10: First setup-step, setting up an unlock mechanism for the ID-Wallet.

3.2.2 Main Wallet Screen & Digital Identity Setup

Following the set up process of the chosen authentication method, the user will be directed to the main screen. The implementation of these views in the Android application demonstrator implemented during this thesis differ from the implementation in the low-fidelity prototype, seen in figure 11.

The low-fidelity prototype presents card items for all kinds of digital identities, which are always visible, even if the digital identity was not already added. Instead of having a separate screen to add new identities, the identity can be added by clicking on an empty card. This view was seen as confusing to the user, as it was not inherently clear that these identities were not already added and also the focus on the national ID card which is important for the thesis gets diminished by this view. A design decision that was taken over from the low-fidelity prototype was the tabbed view for the different kinds of identities, as this is a well accepted grouping concept in the Android design language and an already known interaction pattern to the user as it is used in many mobile applications [64], [2].

In the corresponding view of the Android application, all digital identities are also shown in a tabbed view with tabs for official documents, other identities, and digital keys. When first using the app, no identities are present, instead a placeholder with a button to add a new digital identity is shown. After selecting the button to add a new identity or clicking the plus button at the top-right corner, a selection of

3. Implementation



Figure 11: Main View of the low-fidelity prototype, also showing all identities in a tabbed view. The option to add a new identity is integrated into the main view.

possible identities to be added is shown to the user. As this thesis focuses on the national ID card, this is the only option currently implemented and selectable to the user. All other options are greyed out and marked with *coming soon* in order to keep the demonstrator as realistic as possible for user testing. The main view screens (with and without digital identities) and the selection screen when adding a new digital identity are shown in figure 12.

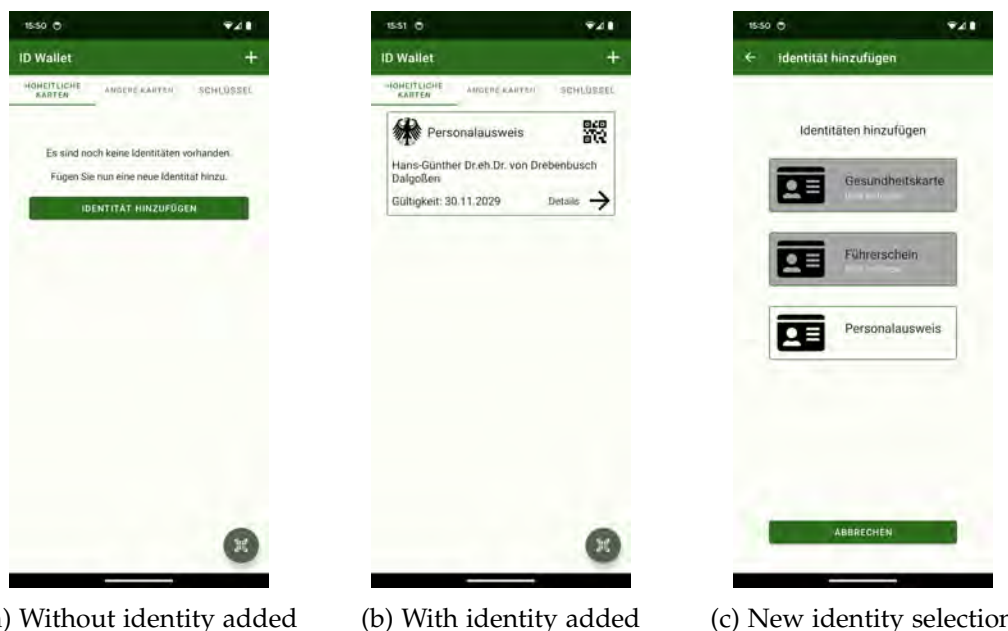


Figure 12: Main View of the ID-Wallet demonstrator and add identity screen.

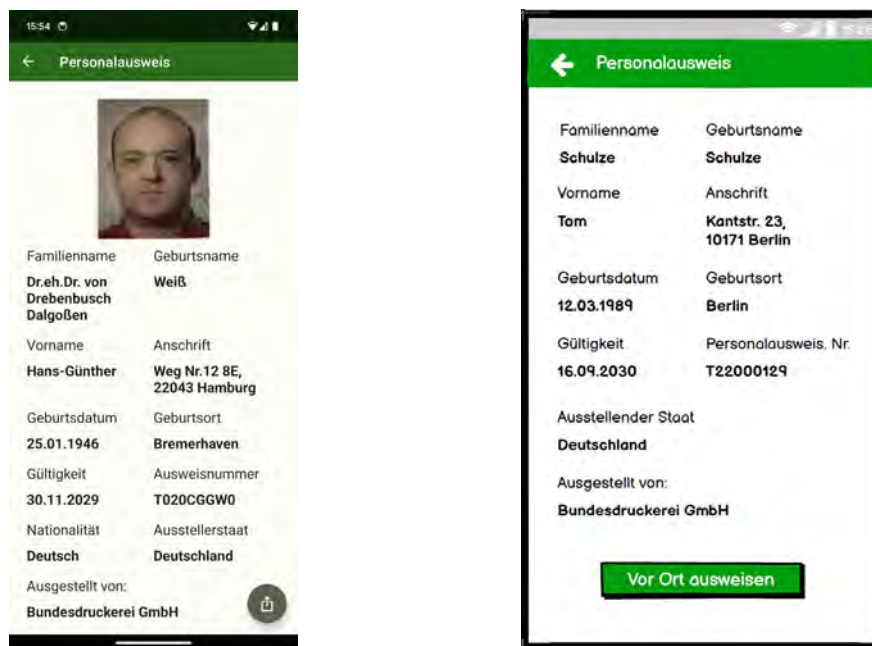
The process of setting up a new digital identity, in this case a national ID card, will be described in detail in section 3.3.1, including technical details how the interaction with the physical ID card is implemented for the demonstrator.

After setting up a new digital identity, this identity will be shown as a card in the main wallet view, as seen in the middle screen of figure 12. It is replacing the placeholder shown when no identity has been set up. Clicking on this card redirects the user to a detail view of the identity, showing all data belonging to this identity. Clicking on the QR-Code icon will directly open a QR-Code to share the data of this identity with a verifying party. Using this shortcut will include all data of the identity.

The floating action button (FAB)²⁴ in the bottom right corner directs to the request scanning functionality, allowing the user to scan request QR-Codes from the verifying party. In these QR-Codes the verifying party can define which information from the identity they need to verify the user. This process is described in more detail in section 3.3.3.

3.2.3 ID Card Detail View

After clicking on the ID card entry in the main screen, the user is directed to a detail view of the data belonging to the identity. The demonstrator currently only offers a national ID card as digital identity, so the detail view is tailored towards this kind of digital identity. The implementation of the detail view in the Android application is shown in the left image of figure 13.



(a) New Android Demonstrator

(b) Original low-fidelity prototype

Figure 13: Detail view of all data belonging to a digital identity. In this case, the detail view for a national ID card is displayed.

The right image of the figure shows the implementation of the low-fidelity prototype for comparison. The basic data display of the Android application is similar to the low-fidelity prototype while a photo of the ID owner was added at the top and the

²⁴<https://m2.material.io/components/buttons-floating-action-button> (accessed: 12.02.2024)

3. Implementation

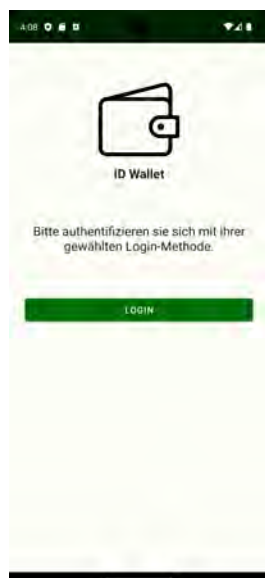
functionality of using the ID in an on-site validation was moved to a floating action button to adhere to modern Android design principles.

Furthermore, the share functionality was extended from the low-fidelity prototype. Detailed information regarding the sharing functionality will be given in section 3.3.3.

3.2.4 App Authentication & Login

The wallet Android demonstrator also features a working implementation of authentication and login state. When suspending the app for longer than ten minutes, the user will be logged out of the wallet. After switching to the app or restarting it, the user will be asked to log in using the method set up when first using the app. This was implemented to keep a realistic wallet impression for study participants. Should they encounter this case, they may wonder why they set-up the login in the first place if it was not enforced.

The implementation in the Android demonstrator differs slightly from the low-fidelity prototype, where the prompt to log in and the functionality (e.g a field for reading the fingerprint or entering the password) were both included in one screen. In the Android demonstrator, the prompt to log in will be shown with a button, leading to a second screen with the control corresponding to the selected authentication method. This is implemented in such a way because of limitations of the Android biometric library, which does not allow to implement fingerprint reader functionality outside of the system dialog. Since opening the system dialog directly on reopening the app would be very confusing and disrupting for the user, a two-screen login process was chosen. Screenshots of these login steps for the selection of the device unlock method as authentication for the wallet are shown in figure 14.



(a) Login start screen



(b) Login with device unlock

Figure 14: Login process after the wallet app has been suspended for more than ten minutes.

The demonstrator checks for the correct previously set up authentication method and corresponding PIN or password, if this option was chosen. The fingerprint and the device unlock method will use Android biometric libraries to verify the correct fingerprint and device PIN or password. The login state is always refreshed to the initial ten minutes when the user switches to a new screen in the wallet, as to not interrupt a study participant during the scenarios and to also only logout the user during inactivity.

3.3 Technical Implementation

This section describes the implementation of important features in detail. These include how the setup procedure of a digital national ID card is simulated, how the identity data is stored persistently on the device, how the data is transferred to a verifying party, and how photos are included into the identity data for study purposes.

3.3.1 Setup of a Digital ID Card

The setup process of a digital national ID card in the demonstrator resembles the procedure currently implemented for the German national ID card in the AusweisApp²⁵, as the targeted user group for the user studies consists entirely of German citizens. Furthermore, a sample German national ID card is used during the study.

Implementing the technical correct process of gathering the data from the physical ID card as used in the AusweisApp is complicated and time consuming. It would also require an application for an authorization certificate which allows the usage of the online ID card function. This application takes time to be checked and also has strict requirements for what the online ID card function can be used. Further, the application has significant cost associated with it²⁶.

Since including the technical correct implementation of gathering the data from the physical ID card is not necessary to accurately simulate the interaction process when setting up a digital ID card in the ID-Wallet, the decision was made to omit a technical correct implementation of this process but still opting for a realistic simulation. This simulation also uses the NFC-capability of the device, but uses sample ID cards and matching sample data in the wallet after the setup process is completed.

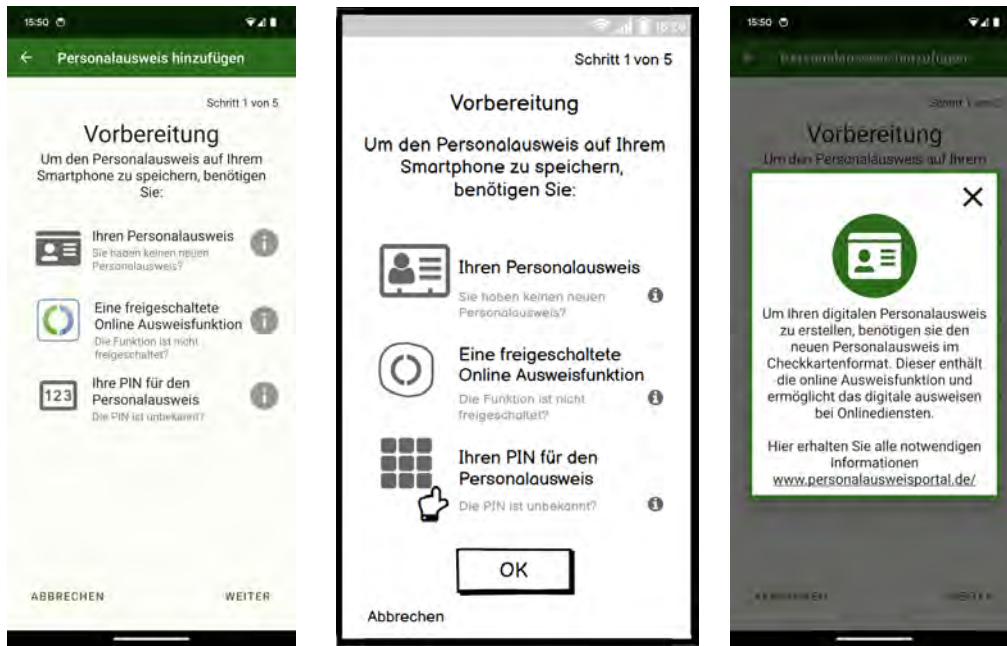
The steps of a setup process resembling the AusweisApp were already implemented in the low-fidelity prototype by Kostic et al [37]. As such, the design was mostly carried over to the Android application with minor alterations to adhere to Android design guidelines.

The first step consists of an informational list of requirements for using the national ID card with the wallet and setting up a digital ID card from it. This step can be seen in figure 15, which on the left shows the screen in the Android app and in the middle the screen in the low-fidelity prototype. Clicking on the information icons on the right will open a dialog with detailed information on how to achieve the requirements for using the ID card, as seen on the right screenshot in figure 15.

²⁵<https://www.ausweisapp.bund.de/> (accessed: 22.01.2024)

²⁶Requirements for the application and associated costs can be found here: <https://verwaltung.bund.de/leistungsverzeichnis/EN/leistung/99008003001000/herausgeber/LeiKa-584864/region/00> (accessed: 22.01.2024)

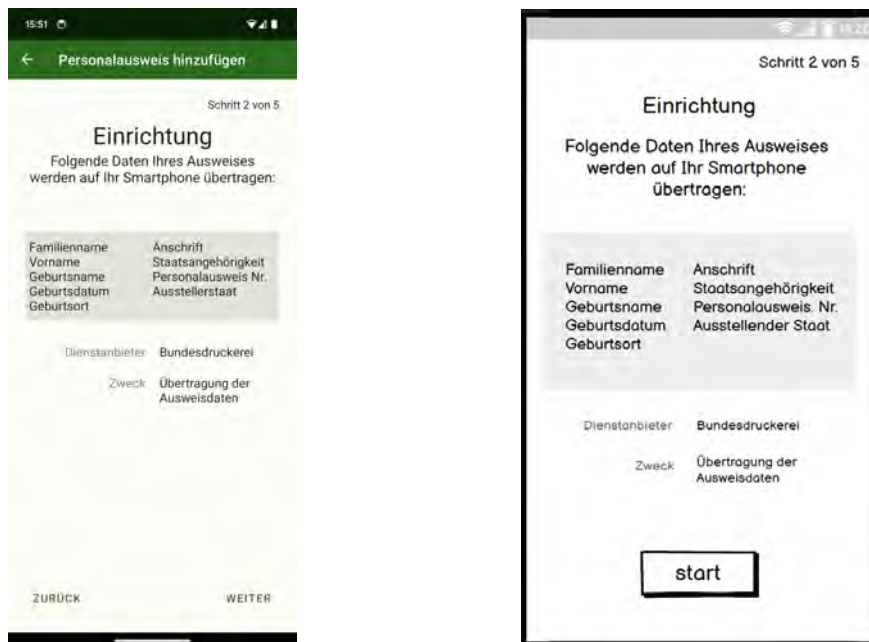
3. Implementation



(a) Android Demonstrator (b) Low-fidelity Prototype (c) Informational Dialog in Android Demonstrator

Figure 15: First step of the digital ID setup process.

The second step, which can be seen in figure 16 gives a short overview of the information that are going to be transferred from the physical ID card and are saved as the digital ID on the device.



(a) New Android Demonstrator (b) Original low-fidelity Prototype

Figure 16: Second step of the digital ID setup process.

It also gives information about the service provider and the usage of the transmitted data. The implemented view in the Android application is nearly identical to the view proposed in the low-fidelity prototype. It serves to enhance the users feeling of security, informing them which data is going to be transferred and stored, which party is responsible for the transfer and storage, and why they need the data.

The following step is the first one where an interaction with the physical ID card is happening. The user is asked to tap the back of the Android device with the physical ID card, as for most Android devices, this is the location of the NFC-reader. As mentioned earlier, the technically correct procedure of reading the ID data using NFC is not implemented in the Android demonstrator because of the application procedures for the necessary certificate and also time constraints. Instead, the Android application will wait for a contact using the NFC-reader and when any NFC-enabled object can be found, the next step will be initiated. This can for example be a real ID card with a NFC-chip, but also other cards with NFC-chips, or even just simple NFC-tags. In this step, no actual data is transferred from the NFC-enabled object, only the presence of such an object is verified by the NFC-reader. As this app is only a demonstrator and targeted at being used in user studies, in which a sample national ID card with NFC-functionality will be provided, this solution is seen as sufficient and also as close to the real interaction as possible for keeping up the impression for the study participant that they really are transmitting data from an ID card during the study. The corresponding view with the prompt can be seen in figure 17. It is identical to the view in the low-fidelity prototype, only the NFC-functionality was added in the Android application.



(a) New Android Demonstrator



(b) Original low-fidelity Prototype

Figure 17: Third step of the digital ID setup process, prompting the user to tap the physical ID card on the back of the device.

3. Implementation

In the fourth step, initiated by tapping an NFC-object on the devices NFC-reader, the user is asked for the online functionality PIN of the ID card. This is similar to the process of the AusweisApp, which also asks for the PIN after the first NFC-contact was made. Since no data is read from the ID card in the demonstrator, there is also no verification of any real PIN implemented in the simulated set up steps. Any 6 character PIN can be entered to reach the next step of the setup process. For study purposes, the participant will be provided with the PIN of the sample ID card beforehand to keep up a realistic impression of the procedure. The PIN prompt can be seen in figure 18. The view of this step in the Android application is also nearly identical to the view in the low-fidelity prototype, only replacing the integrated keyboard with the usage of the Android system keyboard and rephrasing the prompt text to clarify which PIN is meant.



(a) New Android Demonstrator

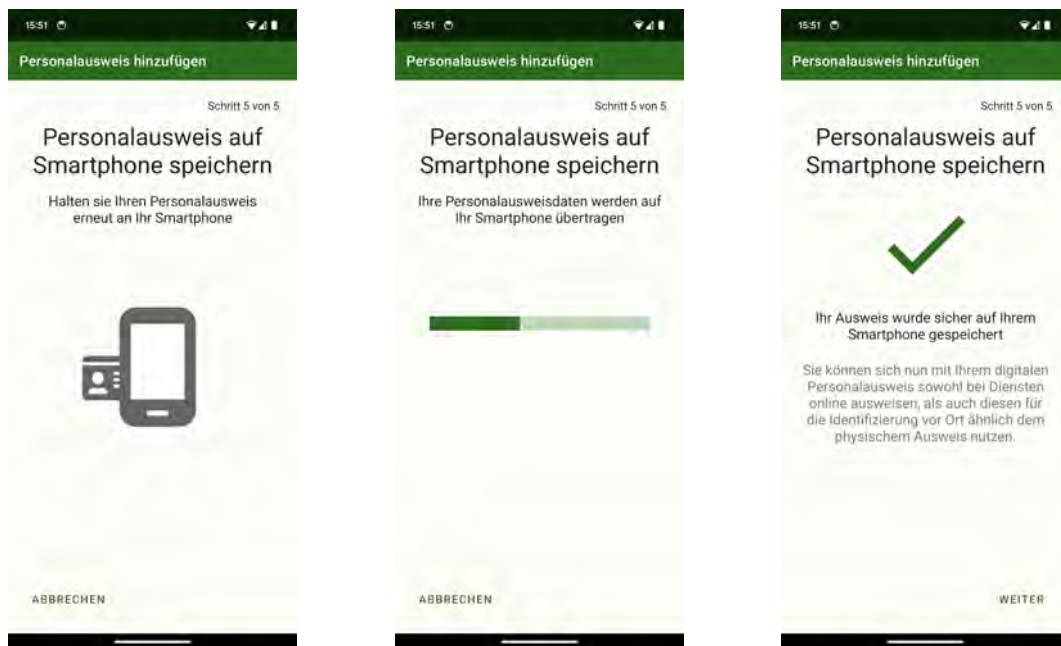
(b) Original low-fidelity Prototype

Figure 18: Fourth step of the digital ID setup process, prompting for the PIN of the ID card.

The fifth and final step prompts the user again to tap the physical ID card on the back of the device. This is also according to the process of the AusweisApp, as in this step the data of the now unlocked ID card (using the PIN provided in the previous step) would be transferred. In the Android demonstrator, no real data is transferred during this step. Instead, the app again checks for any NFC-enabled object being read by the devices NFC-reader. When an object is identified, a progress bar will be shown by the app, indicating a transfer of data to be in progress. This is just a timed progress bar for simulation purposes to give the impression to the user that the ID card data is transferred. After the progress bar finishes, a hard-coded data entry of dummy ID data will be saved in the app. This data entry is tailored to the currently used sample ID card used in the studies carried out during this thesis and needs to be updated if a different sample ID card shall be used in further studies. For the purpose of retaining

a realistic impression of the process during user studies, this simulated transmission of data is seen as sufficient to impersonate the interaction between the physical ID card and the device as it is currently implemented in the AusweisApp.

The three sub-steps of this final step are shown in figure 19. On the left, the initial prompt for tapping the ID card on the back of the device is shown. The screenshot in the middle shows the timed progress bar that simulates data being transferred from the ID card to the device. The right screenshot is a confirmation of the successful data transmission, setup, and storage of the digital ID card in the wallet. After clicking on the *continue* button, the user will be redirected to the main menu, now showing the digital ID that was just set up.



(a) Prompt to tap ID card on the back again.

(b) Timed progress bar to simulate data transmission.

(c) Confirmation of digital ID card setup.

Figure 19: Fifth and last step of the digital ID setup process.

3.3.2 Storage of Identity Data

The identity data that was transmitted in the previous steps and also other identities potentially added in the future are stored persistently in the Android demonstrator using a Room database²⁷. Room is a library provided by Android Jetpack, which in itself is a collection of libraries curated and provided by Google to enable developers to easier adhere to best practices in Android development across different Android versions or devices [27]. The Room library builds upon SQLite databases while providing abstractions for the SQLite APIs by providing data entity and data access object (DAO) support. While data entities represent table entries and handle conversion of objects to database entries and back, DAOs provide methods to interact with these ta-

²⁷<https://developer.Android.com/jetpack/Androidx/releases/room> (accessed: 02.02.2024)

3. Implementation

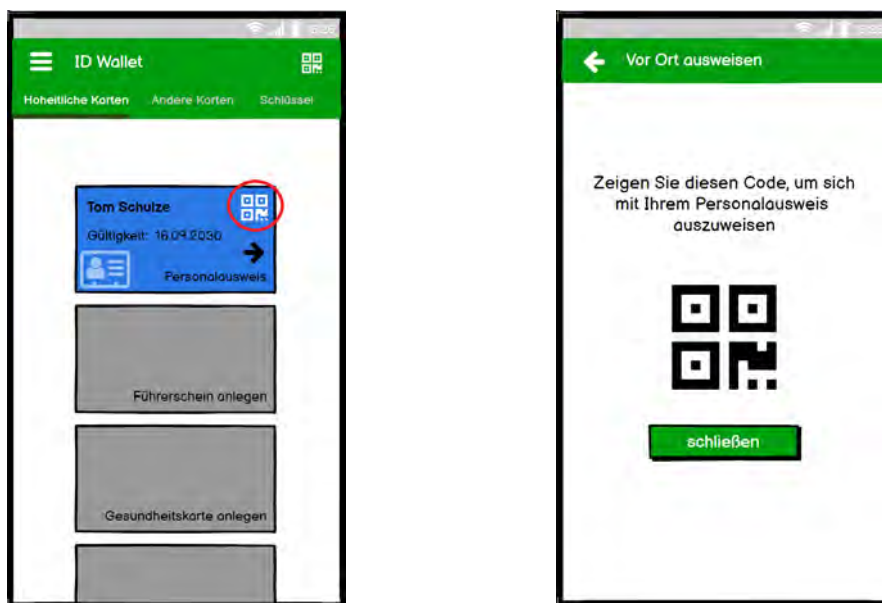
bles like insert, update, or get operations by providing abstractions of the SQL queries as generated functions.

Persisting the identity data, especially the digital ID card allows the identity data to be presented and used again even if the user closes the app or restarts the device. While this use-case is not investigated during the study in the proceedings of this thesis, the aim of this feature is to support further studies using this demonstrator by giving a more realistic impression of how a real world wallet app would behave.

Currently no functionality to delete an identity from the app itself is implemented, as this was also not an use-case investigated in the thesis study and as such has been omitted for now. To delete the persisted identity data, the usage of the devices system settings and the *clear application data* functionality is necessary. If the functionality of deleting identities from the app itself is needed in the future, implementation of this functionality will not be very complicated due to the nature of the abstraction layer provided by the Room Library.

3.3.3 Transfer of Identity Data

The focus of this thesis is the on-site usage of digital identities. Because of this, a functionality to transfer the identity data between devices is necessary, allowing the wallet owner to present their digital ID card to a validating third party. The low-fidelity prototype by Kostic et al. [37] already includes a view regarding on-site authentication with a digital identity by using QR-Codes, as seen in figure 20.



(a) Button to reach QR-Code view.

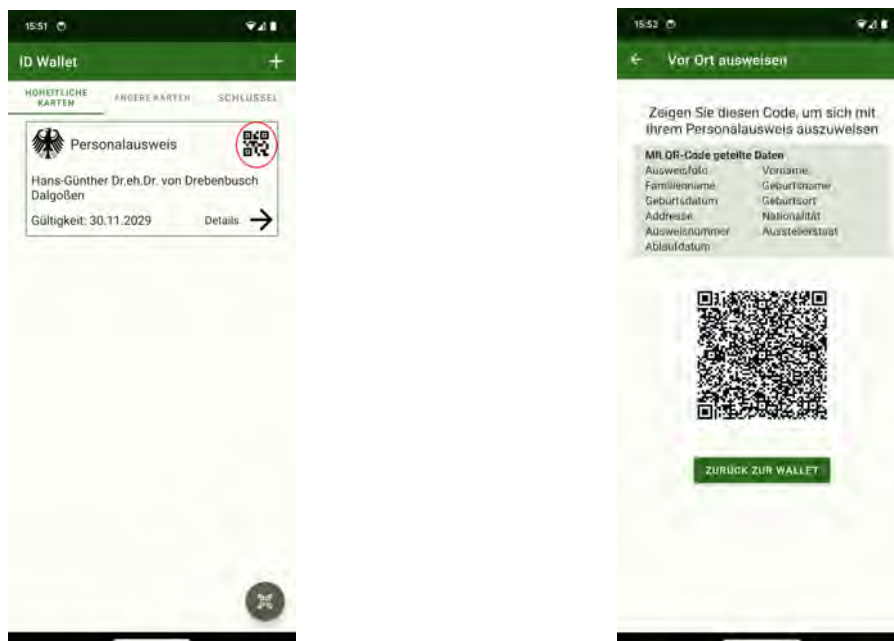
(b) QR-Code with digital ID card data.

Figure 20: On-Site authentication steps in the low-fidelity prototype.

The views in the low-fidelity prototype do not contain any functionality, nor are real QR-Codes used, only symbolic icons. This is a result of the low-fidelity prototype being used in studies during the COVID-19 pandemic. As these studies have been carried out as remote studies, on-site authentication was hard to implement during the study, so the focus was on app-to-app and app-to-web interactions.

The usage of QR-Codes for sharing data between devices in the current day is a known concept for many smartphone users and is widely used, as seen in a statistics report for smartphone users in the US, which indicates that in 2021 75,8% of those users have scanned a QR-Code at least once during the year and forecasts an increase in the usage to 99,5% in 2025 [66]. Especially during the COVID-19 pandemic, the usage and interest regarding QR-Codes in the general public increased considerably, as shown in a report from QR TIGER, which discusses the rise in google searches for QR-Code topics during the COVID-19 pandemic [49]. QR-Codes were employed to allow contactless interactions and also to verify the vaccination status of a person during the pandemic [26]. Because of this rising acceptance of the technology, the decision was reached to expand on the usage of QR-Codes as means to use digital identities for on-site authentication as indicated in the low-fidelity prototype.

For sharing a digital ID card using a QR-Code, the user has multiple options in the Android app demonstrator. The first and quickest way is by clicking the QR-Code icon on the identity card entry in the main view, just like it was designed in the low-fidelity prototype. This button redirects directly to a generated QR-Code, which contains all data from the digital ID card. These steps can be seen in figure 21.



(a) Shortcut button to reach QR-Code view.

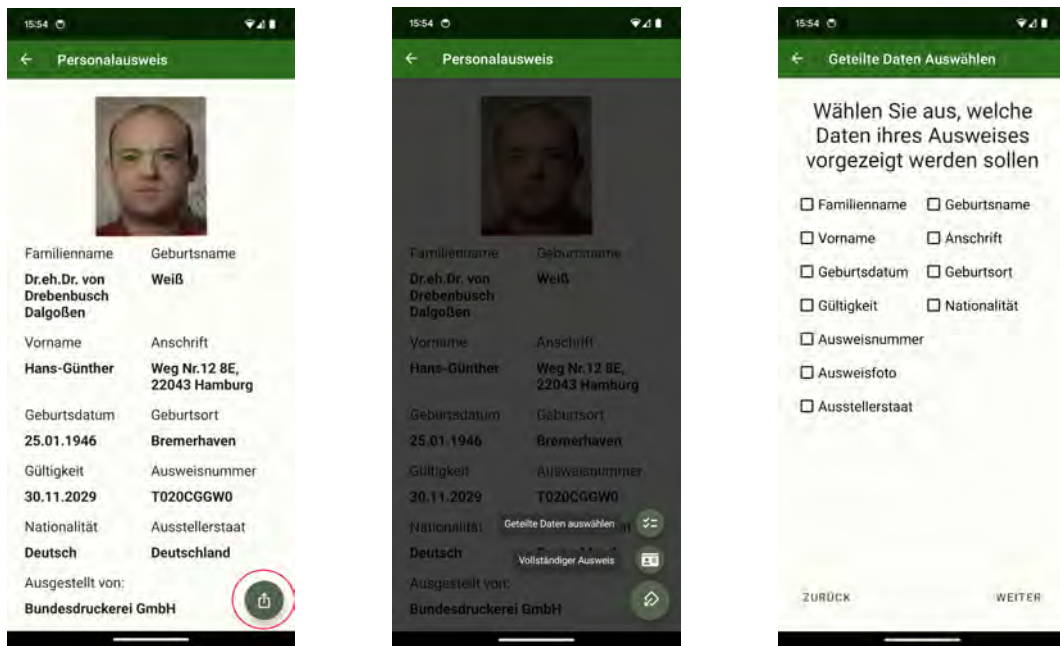
(b) Generated QR-Code containing all digital ID card data.

Figure 21: Quick QR-Code sharing option in the Android Demonstrator.

The second way to share the digital ID card by using a QR-Code can be reached from the detail view of the digital ID card. At the bottom right corner, a floating action

3. Implementation

button with a share icon is present, opening a menu which allows to share either all data from the digital ID card or to select which data should be shared. Clicking on the option to share all data will redirect to the same QR-Code as using the first quick share option from the main screen. The option to select the shared data will redirect to a screen that allows the user to select the shared entries by selecting them and will generate a QR-Code just containing the selected entries from the digital ID card. The described process is shown in figure 22.



(a) Sharing Floating Action Button.

(b) Share menu opening when button is clicked.

(c) View to select shared digital ID card entries.

Figure 22: Sharing a QR-Code from the digital ID card detail view.

The QR-Code is generated by converting the data that was selected to be shared to a JSON²⁸-object and then encoding it into a bitmap graphic QR-Code. For the QR-Code bitmap encoding, an Android adaption of the zxing ("zebra crossing") barcode image processing library²⁹ developed by *journeyapps* was used³⁰. The content of a QR-Code sharing all data of the digital ID wallet is shown in listing 1. Currently, the JSON content in the QR-Code is not encrypted or otherwise secured in any way. As mentioned earlier, the scope of the demonstrator does not include a complete technical implementation of all the features, especially in regard to safety and security, as it is focused on being used in usability studies. Because of this, steps like encryption were omitted in the implementation. When releasing an application like the ID-Wallet for real-world usage, such mechanisms will become necessary and solutions have to be thought about and have to be implemented.

²⁸JavaScript Object Notation: <https://www.json.org/json-en.html> (accessed: 12.02.2024)

²⁹<https://github.com/zxing/zxing> (accessed: 12.02.2024)

³⁰<https://github.com/journeyapps/zxing-Android-embedded> (accessed: 12.02.2024)

```

{
  "address": "Weg Nr.12 8E, 22043 Hamburg",
  "birthDate": "25.01.1946",
  "birthName": "Weiß",
  "birthPlace": "Bremerhaven",
  "expirationDate": "30.11.2029",
  "firstName": "Hans-Günther",
  "idCardNr": "T020CGGW0",
  "issuingState": "Deutschland",
  "lastname": "Dr.eh.Dr. von Drebenbusch Dalgoßen",
  "nationality": "Deutsch",
  "withPhoto": true
}

```

Listing 1: JSON content of a QR-Code containing all digital ID card data.

Another way to generate a QR-Code is to at first scan a verification request QR-Code. This QR-Code is generated by the verifying party and can then be presented to the ID-Wallet owner to prepare a QR-Code of the digital ID card, containing only data that is needed by the verifying party. This verification request QR-Code also contains information about the verifying party and for what the data from the digital ID card will be used. This information is encoded in an URL representing an Android deep link³¹. Scanning this QR-Code with a QR-Code reader application from outside of the ID-Wallet will open the ID-Wallet application and will redirect the user directly to the verification request view. A verification request URL encoded in the QR-Code always has the format *walletprototype://verify_request/<request information data>*. The part *walletprototype://verify_request* is the deep link mentioned and handles the redirect to the correct application and view. The information regarding necessary data entries of the digital ID card and the information about the verifying party are transferred as a JSON object in the path of the URL, as denoted by the *<request information data>* part. Sample request information data is shown in listing 2.

```

{
  "provider": {
    "name": "Freie Universität Berlin",
    "serviceName": "Freie Universität Berlin  
Jahresabschlussparty",
    "certificate": "DFN Germany GmbH",
    "information": "Freie Universität Berlin\nKaiserswerther  
Str. 16-18\n14195 Berlin\ninfo-service@fu-berlin.de",
    "usage": "Erfassen der Daten für die Identifizierung"
  },
  "requestedFields": [
    "first_name",
    "last_name",
    "birth_date"
  ]
}

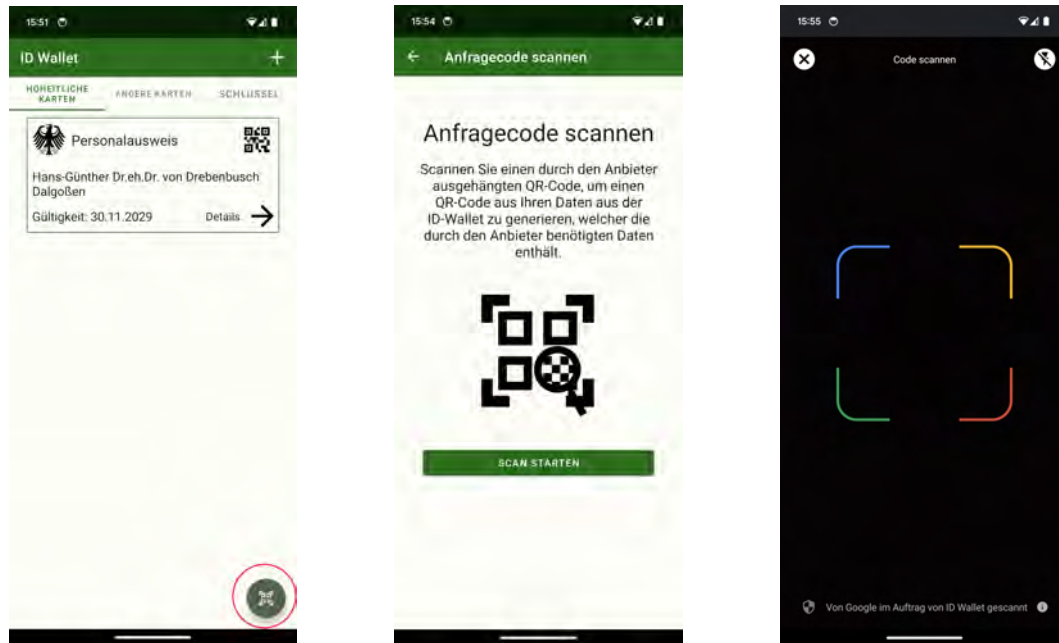
```

Listing 2: Verification request data included in the request QR-Code as JSON.

³¹<https://developer.android.com/training/app-links#deep-links> (accessed: 12.02.2024)

3. Implementation

The ID-Wallet application also includes functionality to scan such a verification request QR-Code from inside of the application by clicking on the FAB with the QR-Code icon in the bottom right of the main view. The Process of scanning a request QR-Code from the application can be seen in figure 23.



(a) Request scan Floating Action Button.

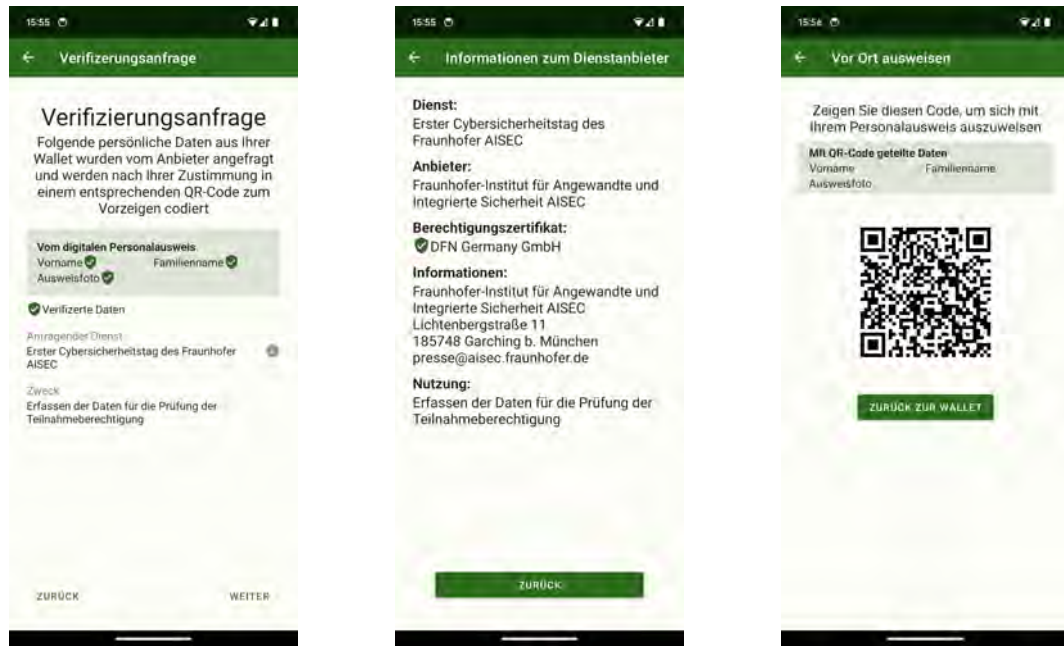
(b) Request scanning start screen.

(c) QR-Code scanner view.

Figure 23: Scanning a request QR-Code from the main view in the Android Demonstrator.

After scanning a verification request QR-Code, the user will be redirected to a view which summarizes the data that the verifying party requests for a successful validation. It is also indicated, from which digital identity the data is being taken. As the demonstrator focuses on the ID card, currently only data from the digital ID card is included. The user is also shown who is requesting the identity data and for which purpose. Clicking on the information icon next to the requesting service opens a new view with detailed information about the requesting service and party. This includes information about the service, the provider of the service, contact information, and also a certificate with which the providers identity is signed as being authentic. When the user confirms the request, a QR-Code with the requested data entries from the digital ID card is generated and can be shown to the requesting party. The views regarding this procedure are shown in figure 24.

This feature was included as idea of an use-case where the ID-Wallet can make the process of verifying the identity of a person easier in day-to-day usage by using the example of an admission process for an event. The verification request QR-Codes can be shown on screens or printed out and presented before people reach the actual admission control, for example while they are queuing. The ID-Wallet users can then scan this code while waiting in the queue and prepare the QR-Code with the requested data while also getting informed about which data will be needed, for



(a) Summary of the requested data and the requesting party.

(b) Detailed information screen about the requesting party.

(c) Generated QR-Code containing only the requested data.

Figure 24: Steps after scanning a request QR-Code in the Android Demonstrator.

which purpose, and who is the responsible party. When the ID-Wallet user reaches the entry control, the verifying party only needs to scan the prepared QR-Code to check if the user is allowed to enter the event or not.

During the implementation of the transfer mechanism for the demonstrator, the decision was made to split the on-site verification functionality by scanning a QR-Code of a digital identity from the ID-Wallet app and to outsource this functionality into another Android application, called the *ID-Wallet Scanner*. This was done to reduce a functionality overload in one app, as the ID-Wallet and ID-Wallet Scanner are used by two different parties with different interests, so having both functionalities unified in one application does not seem to be useful and in the worst case might confuse users during the study, as it is not clear which QR-Code functionality they are currently using.

The ID-Wallet Scanner application consists of only three views: a view which explains what the application is used for and contains a button to start the QR-Code scan process, the QR-Code scan view, and a view showing the data of the QR-Code that was just scanned. These views are shown in figure 25.

The large check-mark image in the top right with the text message suggesting that the data was verified by an official third-party is included to test if a verifying user feels a higher sense of security when being presented by such data of a digital ID card after scanning a QR-Code. Currently there is no technical verification process by an official third-party implemented, but if this feedback is seen as positive or necessary by study participants, an inclusion of such a feature may be feasible or even necessary for gaining enough trust in the digital ID verification process.

3. Implementation

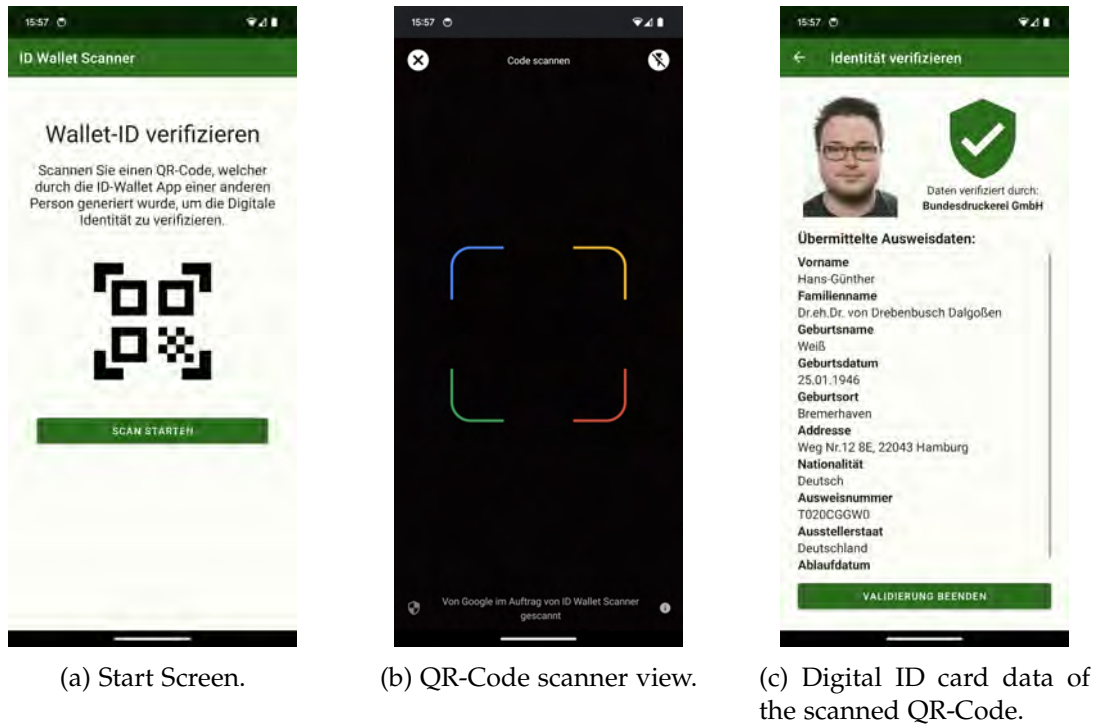


Figure 25: Overview of the ID-Wallet Scanner application.

The QR-Code scanning process uses the Google Code Scanner library, which is part of Google's Machine Learning Kit³². This library delegates the actual scan process to the Google Play Services³³, the ID-Wallet applications only receive the result of the scan in form of the data encoded in the QR-Codes. The scan is done offline, only the ML-Kit model has to be downloaded on the first application start if not already done by other applications used on the device that require the Google Play Services.

3.3.4 Inclusion of Photos in Digital ID Cards

The demonstrator also includes the handling of ID card photos, since one research question of this thesis is, if photos are important or even necessary to enable digital IDs to be used in on-site verification. The photo is part of the data saved on the physical ID card and can be read using the NFC-capabilities of the physical ID card. Currently, only official public authorities are allowed to read the saved photo using NFC [23]. Taking this into account, a production version of the ID-Wallet app will need to either be developed and published by such a public authority or special arrangements will need to be instantiated with the public authorities to enable the usage of photos in digital ID cards and for on-site authentication. For the sake of the demonstrator application and the scope of this demonstrator, it is assumed that such arrangements will be met in the future and a simulated transfer of photos is implemented, disregarding technical details of how the photo will be taken from

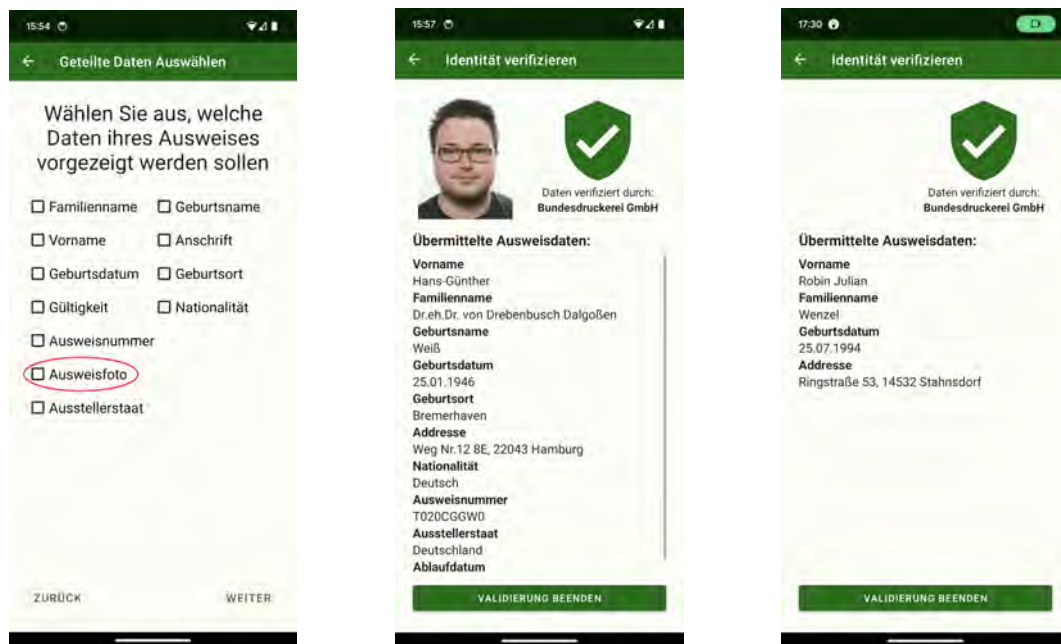
³²<https://developers.google.com/ml-kit/vision/barcode-scanning/code-scanner> (accessed: 12.02.2024)

³³<https://developer.android.com/distribute/play-services> (accessed: 10.05.2024)

the physical ID card or if it is fetched by other means like requesting them from the residents' registration office.

Transferring the photos with a QR-Code also proves to be difficult, as QR-Codes are in the current version 40 limited to a maximum size of 4296 alphanumeric characters [14]. This equals about 3 kilobyte, which is too small for German national ID card photos. These have a size of 17 kilobyte after compression according to the technical guidelines in section 5.6.2.1. [24]. For the sake of the demonstrator, it is also assumed that a way of transferring or loading the photo data during the on-site verification will be possible in the future.

The implemented solution in the demonstrator consists of hard-coded photo data in the ID-Wallet and the ID-Wallet Scanner applications. To enable A/B testing using either a photo or no photo in on-site verification, an option to either show the photo or hide it is transferred using the QR-Code. Depending on this option, the ID-Wallet Scanner application will either show the photo which is stored in the application data or will hide it when a QR-Code is scanned. During a study, the study supervisor can select this option by either selecting or deselecting the photo option in the selection screen of which data of the ID card shall be shared from the ID card detail screen. If the option to share the photo is deselected, the data screen of the ID-Wallet Scanner application will only show a large white space in the place where the photo is usually shown. The different views together with the highlighted photo share option are shown in figure 26.



(a) Photo option in shared data selection.

(b) Data screen after scanning with photo option selected.

(c) Data screen after scanning without photo option selected.

Figure 26: Implementation of photos in the Demonstrator applications.

4 Methodology

This chapter introduces and describes the techniques and questionnaires used during the study in detail.

4.1 A/B Testing

To explain the idea of A/B tests, an excursion into controlled experiments is necessary. Experiments in a scientific context consist of manipulating independent variables to analyze their effect on dependant variables [3]. A controlled experiment is a form of experimentation, where only the desired independent variable is changed between experiment groups while all other possible variables and influences are controlled and kept the same between experiment executions [3]. Controlled experiments require a control group, which acts as a baseline for comparing the results of the experiment by showing the dependant variable in the current state without changing the independent variable [3]. Controlled experiments also often use random assignment, where participants are assigned to either the control group or the variation groups at random to evenly distribute any extraneous participant variables across the groups and with this minimize the influence of these variables on the experiment result [3]. Another technique often found in controlled experiments is masking or blinding, where participants or researchers are not informed about which group the participant belongs to [3]. This aims to minimize research bias where either the participant gets influenced in their decision making by knowing the goal of the experiment in advance due to knowing the difference between groups or the researcher encouraging participants in ways that support their hypothesis due to them knowing which group the participant belongs to [3].

An A/B test is at its base one of the simplest forms of a controlled experiment, consisting of only two groups, the control group (A) and the variation group (B) with only a single independent variable being manipulated between those two groups [67]. A/B testing is being used by user interface researchers since 1960 and is regarded as a productive technique in the selection of UX research methodologies to answer UX-design related questions [67]. The technique is similar to other UX research methodologies like usability testing in its aim to provide insights into user behaviours, but differs in its precise goal from conventional usability testing [67]. While conventional usability testing mostly aims to uncover previously not known or noticed UX problems, A/B testing focuses on known UX problems and tries to determine an optimal solution from a set of possible solutions [67].

As A/B testing is a form of controlled experiment, it also follows the concept of the scientific method [67]. The scientific method is a logical method used by scientists to answer questions arising during their research [15]. The scientific method includes several steps to reach a conclusion, which are also followed during A/B testing [67]. The steps in the scientific method are [32]:

1. Formulate a research question
2. Gather information and do background research regarding the question

3. Formulate a hypothesis based on the gathered information as an educated guess of what to expect
4. Conduct an experiment to test the hypothesis
5. Analyze the data gathered during the experiment and look for evidence that either supports or rejects the hypothesis
6. Conclude whether to accept or reject the hypothesis based on the analyzed data. Report the results and conclusion.

4.2 Human Computer Trust Scale

The Human Computer Trust Scale, abbreviated as HCTS is a questionnaire based on the concept of the Human Computer Trust Model (HCTM) to provide a quick tool to assess the users trust in a software solution, developed by Gulati et al. [30]. The HCTM was proposed by Sousa et al. [61] in 2014 and defined seven attributes (motivation, willingness, competence, benevolence, predictability, honesty, and reciprocity) which according to them are able to predict the users trust in technology interactions [30]. Gulati et al. [30] point out that there were two attempts to empirically assess the feasibility of the HCTM during which the initial attribute collection of the HCTM was refined, but the authors concluded that more empirical research is necessary before a scale can be developed from the HCTM.

Gulati et al. [30] built upon this previous empiric research and refined HCTM and conducted empiric research on two user technology interaction scenarios to further refine the HCTM and emphasize the statistically relevant attributes of the HCTM to assess the perceived trust of users. They found these attributes to be benevolence, competence and perceived risk, the latter not being one of the initial attributes defined by Sousa et al. [61], but a newly defined attribute based on a combination of the attributes honesty and willingness, which was proposed by Gulati et al. [29] in their empirical assessment of the HCTM from 2018 and then formally defined in 2019 [30]. Based on these three attributes, Gulati et al. [30] developed a questionnaire with questions concerning these attributes, which allows an empirical analysis of users trust in technology interactions. The answers of these questions can then be used to calculate a trust value using the means described and employed by TrustedUX³⁴, a survey web platform developed by Sousa et al. [62] based on the HCTS questionnaire to provide an easy way for researchers to use the HCTS during their studies.

4.3 System Usability Scale

The System Usability Scale (SUS) is a widely used standardized questionnaire to assess the usability of a system in an empiric and structured way [39]. It was originally developed by John Brooke in 1984 during a wave of multiple questionnaires being published to evaluate usability and first presented in 1996 [5], [39]. To highlight the widespread usage and popularity of the SUS, Lewis et al. [39] state that the original

³⁴<https://www.trustux.org/resources/> (accessed: 23.03.2024)

4. Methodology

article has been cited 5664 times according to google scholar. At the time this thesis was written, this citation number has grown to over 17000 citations³⁵.

The SUS is a Likert scale and consists of 10 questions with alternating positive and negative tone in its standard form, each question being a five point Likert item where the participant indicates his level of agreement from *strongly disagree* (being the value 1) to *strongly agree* (representing the value 5) [39], [5]. The answers of the SUS can then be scored and result in a single number, representing an overall rating of usability for the system being studied [5]. The scoring begins with determining the *score contribution* of each question in the SUS, ranging from zero to four [5]. To calculate this score contribution, the scores (defined as the position on the scale) of the questions 1, 3, 5, 7, and 9 are subtracted by one, while the scores of the questions 2, 4, 6, 8 and 10 are subtracted from five [5]. The sum of all score contributions is then multiplied by 2.5 to achieve the overall system usability value, which can range from 0 to 100 [5].

Lewis et al. [40] comment that a single system usability score has no real meaning whether it is poor or good, so some form of comparison to other scores has to be established. Based on a large data set of SUS scores, they present a relative grading scale for SUS score results, examining that a SUS score of 68 is equivalent to the center of the range of a grade C, which is also being defined as the median in a typical curved grading scale [40]. The highest and lowest 15 percentiles are respectively considered the A and F range of grades [40]. The grade ranges of A, B, and C have been further divided in 5 percentile ranges to A+, A, and A- (and equivalent groups for B and C grade range), while no such division was done for grades D and F as the authors did not see this as useful [40]. The full scale can be found in table 1. With this grading scale, comparability between SUS scores can be established and the authors notice that it has become a common industry goal to reach a SUS score of at least 80, as this is seen as an above average user experience [40].

Grade	Score	Percentile
A+	84.1 - 100	96 - 100
A	80.8 - 84.0	90 - 95
A-	78.9 - 80.7	85 - 89
B+	77.2 - 78.8	80 - 84
B	74.1 - 77.1	70 - 79
B-	72.6 - 74.0	65 - 69
C+	71.1 - 72.5	60 - 64
C	65.0 - 71.0	41 - 59
C-	62.7 - 64.9	35 - 40
D	51.7 - 62.6	15 - 34
F	0 - 51.6	0 - 14

Table 1: SUS grading scale developed by Lewis et al. [40].

³⁵Examined on 23.03.2024 using https://scholar.google.com/scholar?cites=7479264939553283798&as_sdt=2005&scioldt=0,5&hl=de&scioq=brooke+sus

5 Study Design

This section starts with a short introduction of the study, its purposes, and what is investigated during the study. Following is a subsection describing the general concept and idea of the study. The next subsection gives details about how the participants have been selected for the study. Afterwards, the structure of the study is described in detail, explaining the scenarios the participants are presented with and what questions are being asked during the study cases. This section ends with a description of the modified and translated Human Computer Trust Scale that is used for the study.

5.1 Introduction & Concept

As the developed demonstrator application is planned to be used in user studies regarding the topic of wallets, this study serves as a kind of proof-of-concept or pilot study to show that the developed demonstrator is a feasible solution to be used in further user studies.

As described in section 3.3.4, currently only official public authorities are allowed to read photo data from the ID card. As such, the photo would not be usable in the case of a digital ID card from the wallet if the digital ID card should also be usable in general on-site verification of the identity of a person. A photograph is one of the prominent data entries used from a physical ID card to identify a person as the one the ID card belongs to, so an investigation into whether the presence or absence of a photo in a digital ID card from a wallet has a relevant influence in the perceived trust of the verifying party in such a wallet solution appeared to be an interesting and worthwhile question for the study. The hypothesis in this case is that the absence of a photo of the ID owner will result in a significantly lower perceived trust by the participants of the study. To investigate the influence of the presence or absence of a photo on the perceived user trust, the study contains an A/B test. Participants will proceed through a scenario where they impersonate a party verifying the identity of a person trying to access an event. One group of participants will be presented with a photo of the ID owner when scanning the digital ID of the person, while the other group of participants is not shown a photo of the ID owner.

The study should also show that the demonstrator can be used in usability studies, so not only will the aspect of photos be included in the study scenarios, but also general usage of the ID-Wallet application is a part of the study conducted during this thesis. A standardized usability scale is implemented in the study and information regarding the usability and possible improvements of the current demonstrator application is gathered. Further information will be gathered through remarks and comments by the participants while proceeding through the scenarios and also after-scenario questions.

5.2 Participant Selection & Demographics

The decision was reached that at least 20 participants will be necessary to reach a distinct result in the planned A/B test, resulting in 10 participants for each group.

The participants are selected at random from personal acquaintances of the authors, which aims to result in a varying age demographic and also includes partici-

5. Study Design

pants from various occupations, some of them closely IT-related, while some of them are just vaguely or not at all IT-related. This selection also aims to cover various degrees of technical affinity and day-to-day smartphone usage and usage of digital solutions. No expectations have been set regarding age, gender, or knowledge regarding identity topics of the participants to gather a broad insight into the topic.

5.3 Structure of the Study

The study is structured like an one-to-one interview between the study supervisor and a participant with several cases of interactive usage of the application by the participants during the interview. Each study execution begins with an introduction of the study supervisor and the thesis topic, the environment in which the thesis and study are conducted, and the idea of the demonstrator app.

These points are followed by handing out an example physical ID card (as shown in figure 27), a smartphone with installed ID-Wallet and ID-Wallet Scanner applications and a sheet of paper with the smartphone PIN and the PIN of the ID card to the participant. After handing out the required materials for the study, the supervisor follows with an outline of the following study steps and a request to think aloud³⁶ during the study while ensuring the participant that there are no wrong answers or questions to motivate them to actually comment during the study.



Figure 27: Front and Back of the Example German ID card used during the study.

The following part consists of information regarding the usage of the data acquired during the study execution. The participant is informed that the study execution will be recorded and the results, answers, and comments are going to be anonymized, so no conclusion to the participant will be possible. The participant is informed further that only the authors will have access to and work with the raw data. The finished and potentially publicly published thesis will only contain the anonymized data and the results concluded from this data. This part of the study finishes with information regarding an audio recording of the study execution and the information that the participant can request to access, correct or delete the data gathered during their study execution.

After confirming that the participant does not have any more questions regarding the usage of their data, the audio recording is started and the first study step begins.

³⁶The think aloud protocol is a tool in usability testing: <https://www.nngroup.com/articles/thinking-aloud-the-1-usability-tool/>, (accessed: 28.04.2024)

The participant is asked to complete the set-up steps of the ID-Wallet application to familiarize themselves with it. After successfully completing this first step, the participant is asked to create a new digital ID card in the ID-Wallet application by using the example physical ID card that was provided. When the participant successfully completes this task and confirms that a digital ID card has been created and the data is matching the data on the physical ID card, they are asked three questions:

1. What is your first impression of the application?
2. Were the set-up steps clear to you or did you wish there was more assistance offered? If yes, what kind of assistance?
3. What feeling does digitizing the physical ID card using the application leave you with?

It is important to notice that due to the study being held in German, the questions presented here and all following questions are translated from German to English. During the study, the questions are asked in German as found in [A.1](#).

After discussing these questions, the participant is then presented with the next scenario, in which he is visiting an event. In this case, the event is presented as the *AISEC Insider Day*, an event at AISEC for IT-security experts and people interested in IT-security. It is important to highlight that this is not a real event but just an imaginary event as context for the study. The participant is informed that their identity has to be verified at the entrance to check if they are on the list of invited participants. They are asked to use the newly created digital ID card for this purpose. They are further informed that shortly before they reach the entry and entry control, the print-out shown in figure 28 is present on the walls. This print-out contains a QR-Code and the prompt to scan this code to prepare the digital ID card for presentation at the entry.

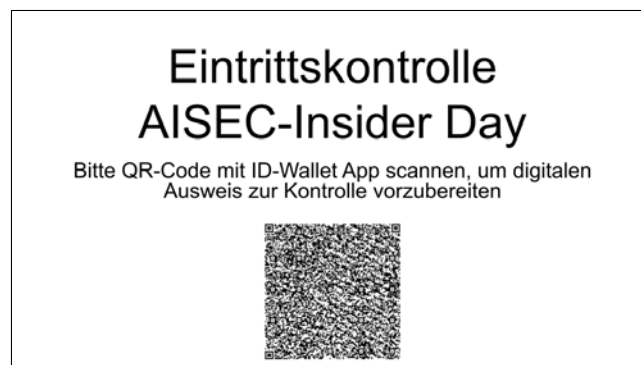


Figure 28: Print-out with prompt to scan QR-Code to prepare the digital ID card for entry control as presented to study participants.

After the participant scans the code and prepares their digital ID card by progressing through the steps mentioned in section 3.3.3, the study supervisor acts as the entry control and uses the ID-Wallet Scanner application on another smartphone to scan the QR-Code of the digital ID card presented by the participant. It is important that the supervisor does not show his smartphone screen to the participant at this step, as the

5. Study Design

supervisor will see a photo from the digital ID card. If the participant would also see the photo at this step, the following scenario with the A/B test regarding photos would be compromised. When the scenario is completed, the participant is asked the following two questions:

1. Was the process of on-site identification clear, or would you have preferred more assistance? If so, what kind of assistance?
2. How do you perceive the digital ID card compared to the physical ID card? Which option would you personally prefer?

When these questions are answered and discussed, the participant is presented with the third and last scenario. In this scenario, the participant takes over the role of validating party while the supervisor is presenting their digital ID card. The participant is instructed that for the event he is asked to do entry control for, only people over the age of 27 and living in Brandenburg or Berlin are allowed. Further, the participant is handed a list of invited guests and asked to verify that the person who wants to enter is on this list. The participant is further instructed to use the ID-Wallet Scanner application for this purpose and additional hints to switch applications are given if the implication is unclear to the participant.

The supervisor then prepares a QR-Code of their digital ID card. At this point, the A/B testing component of the study begins. In both cases, the supervisor shares the first and last name, the date of birth and their address. Depending on which group of the test the participant is in, the supervisor either also shares his photo or omits the photo in the shared code. Group membership of the participant is decided beforehand by the supervisor to achieve a 50-50 split of the groups. The group membership and the existence of such groups is at this point not mentioned to the participant.

The supervisor then presents the QR-Code of their digital ID card to the participant, who uses the ID-Wallet Scanner application to receive the supervisors digital ID card data. After the participant checks all required data for validity and admits or denies entry to the supervisor, the following question is asked:

1. What is your impression of the digital ID card from the validating party's perspective? Do you see the solution as comparable to a physical ID? Please briefly justify your answer.

As the final step after discussing the question, the participant is informed that the questionnaire mentioned in the beginning will now be given out. The participant is further told that the first part of the questionnaire relates to the most recently conducted scenario where the participant was acting as the validating party and was using the ID-Wallet Scanner application. It is further explained that this part of the questionnaire deals with the perceived trust of the participant in the digital ID card solution and the validation process using the ID-Wallet Scanner application. This part of the questionnaire is a modified and translated variant of the *Human Computer Trust Scale*. The modifications and translation process are described in detail in section 5.4.

The participant is then informed that the next part of the questionnaire concerns the usability and user-friendliness of the ID-Wallet application, so the first two scenarios. This part of the questionnaire is a German translation of the System Usability

Scale translated by Bernard Rummel et al. [52]. The used System Usability Scale questionnaire is listed under A.2 and the list of untranslated questions under A.5.

At last, the participant is told that the questionnaire finishes with demographic questions regarding their age group, their occupation, their technical affinity, and day-to-day smartphone usage. The corresponding questionnaire form is listed under A.4. The participant is then handed a tablet with the questionnaire as a Google Forms³⁷ document. This implementation of the questionnaire allows for easier transmission of the results to an usable format for evaluation as Google Forms allows for direct csv³⁸ exports of the answers.

As the first question of the questionnaire, the participant is asked which group he belongs to. The possible answers are *Group 1* and *Group 2*. This is the first time where the participant gets a hint that there may be differences between the study executions of different participants. With just naming the groups after numbers, the authors of the study try to mask the actual difference between the executions and in the ideal case that there even were differences present. The study supervisor will tell the participant to which group they belong. This will be *Group 1* if the participant was not shown a photo in the last scenario during the validation, *Group 2* if they were shown a photo during validation.

5.4 Modified HCTS

As mentioned in section 5.3, a modified version of the HCTS was used during the study. This section aims to describe the modifications in detail and gives the reasoning for those modifications in the context of the study.

The HCTS variant used during the study is based on the refined HCTS developed by Gulati et al. [30], which consists of 12 questions in the original version proposed by the authors. The variant used in the study of this thesis only consists of nine questions taken from the refined HCTS of Gulati et al. [30]. Three questions that were not deemed as fitting for the demonstrator and the scenario of the study were omitted from the employed HCTS. The questions that were omitted are the following:

1. It is risky to interact with (—).
2. I believe that (—) will do its best to help me if I need help.
3. I believe that (—) is interested in understanding my needs and preferences.

The first question of this list was omitted because it is seen as too broad for the purpose of the study, not relaying meaningful information about the actual question of whether a photo is increasing the trust in the digital ID card, as the suspicion is that most participants will answer this question as mostly agreeing regardless of a photo being present or not due to the usage of digital ID cards and ID-Wallets being a new and unknown concepts for most participants.

The second question was omitted because it was not seen as relevant for the scenario of the study because in the scenario the HCTS is used to evaluate the trust,

³⁷<https://www.google.com/forms/about/> (accessed: 04.03.2024)

³⁸Comma separated value: A data format to exchange data to, from, and between spreadsheet applications [58]

5. Study Design

the participant only interacts with the ID-Wallet Scanner application, which is not an application developed with usability standards in mind but only to investigate the necessity of photos when using digital ID cards and as such does not include any help functionality. The application also has just one clearly marked functionality of scanning digital ID card QR-Codes so the authors deemed the question as potentially confusing for the participants and not adding any meaningful information regarding the perceived trust in digital ID cards when a photo is present or absent.

The third question was also omitted because the authors deemed the question to be confusing for the participants as there are no personalization or input components present in the ID-Wallet Scanner application that is used in the scenario which the HCTS asks about. As a consequence of this, there is not really any way in which the application would be able to understand the users needs and preferences in a clear to see way. Further, no meaningful information regarding trust in a digital ID card solution regarding the presence of photos can be extracted from this question.

The questions of the modified HCTS were then translated into German by the authors of this thesis. Gulati et al. [30] also mention in their article that they translated the HCTS question items into German during their study. The translated HCTS questionnaire was not published by them, but they mention that their translation was verified by native speakers to be accurate and relay all meaningful information from the English original and are deemed to be usable for the HCTS evaluation in this case [30]. Keeping this information in mind, the HCTS for this study was also translated into German by a native speaker and verified by different native speakers to convey the same meaning and information as the English equivalent. The modified and translated HCTS for this study can be found under [A.3](#) and a list of the untranslated questions is found under [A.6](#).

6 Study Results

The following chapter will present the results of the study that was carried out during this thesis. The chapter starts with an overview of the demographic of the participants. Afterwards, the results of the SUS and HCTS questionnaires are presented and statistically analyzed. The chapter finishes with a closer look into the answers regarding the after-scenario questions of the study and an insight into relevant and interesting comments from the participants during the study.

6.1 Demographic

The study consists of a sample of 20 participants, which was evenly distributed between group 1, having no photo shown during the digital ID card validation, and group 2, which had a photo shown. The overall age distribution for the participant sample is shown in figure 29.

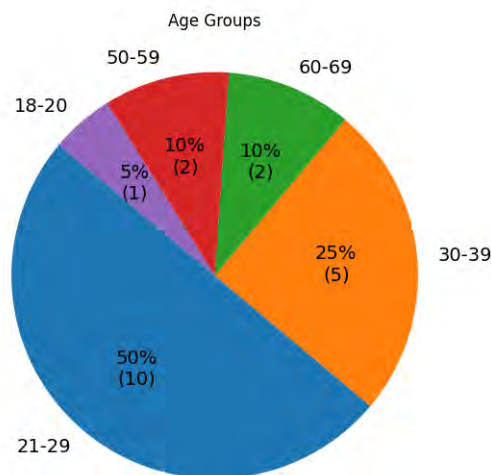


Figure 29: Age distribution of the participants of the study.

The participant group shows a diverse but skewed age distribution. While half of the participants, presenting the majority, belong to the age group of 21-29, there is also a significant participation from the age group of 30-39 with 25% of the participants belonging to this group. 20% of the participants are in the age groups between 50 to 69 while there is also one participant in the age group of 18-20. Absent age groups in the study are participants below age 18, between 40 and 49, and above age 69.

The participants' occupations, shown in figure 30, also show a diverse selection. While 30% of the participants work in an IT-related occupation, the majority of the participants come from a non IT-related background. The answers regarding the occupation were given by the participants as the exact occupation, but were categorized into IT-related and non IT-related occupations by the authors for anonymization purposes. As many occupations appeared only once, presenting the exact occupation would possibly allow to single out participants.

6. Study Results

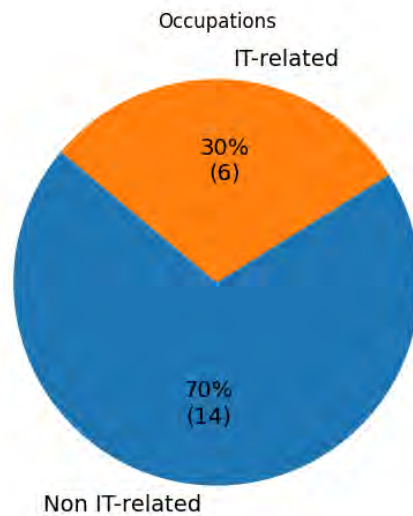


Figure 30: Occupations of the participants of the study.

The self-evaluation of the technical affinity of the participants as shown in figure 31 presents an overall skewed distribution towards high levels of technical affinity. The scores in this chart range from one, corresponding to the answer "very little", up to five, which corresponds with the answer "very strong". Half of the participants see themselves as very technical-savvy with a score of five out of five, and another 20% of the participants evaluate themselves as highly tech-savvy. There are also participants from scores two to three, the only score not present in the answers was a technical affinity score of one. These answers indicate that the technical affinity of the participant group is quite high, and as such the answers and information gathered during the study are more relevant for tech-savvy user groups.

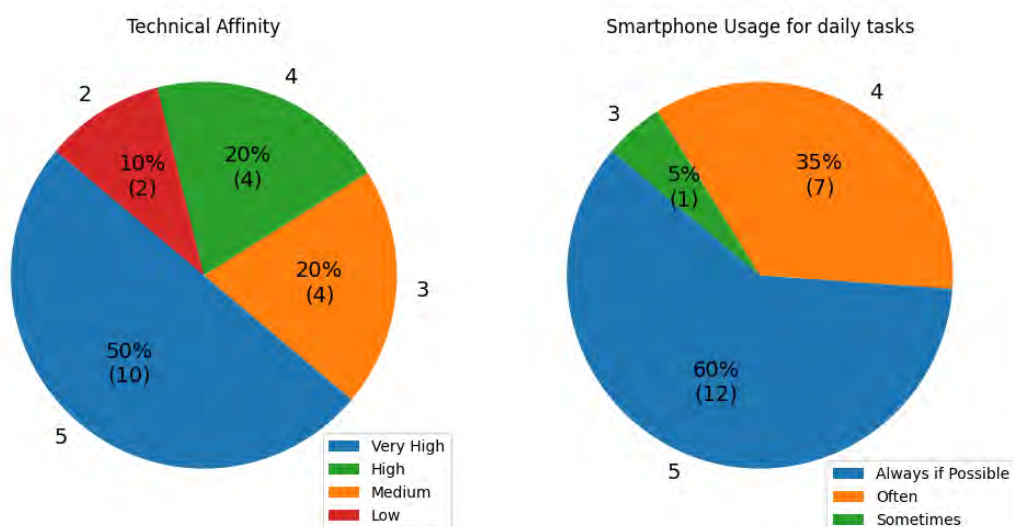


Figure 31: Technical affinity and daily smartphone usage of the participants.

Also shown in figure 31 is the self-evaluated smartphone usage for daily tasks of the participants with possible answers in the questionnaire ranging from one ("never") to five ("always if possible"). Sixty percent of the participants answered that they use their smartphone as much as possible for daily tasks, while 35% answered with a score of four, also indicating a very high smartphone usage for daily tasks. Only one participant answered with a score of three, while no answers with score one or two were given. This indicates that even though the participants come from a diverse technical and occupational background and even from different age groups, they all use or prefer to use their smartphone often for daily tasks, which makes them good candidates for studies regarding this digital ID card and the ID-Wallet.

6.2 SUS Results

To analyze the answers given during the SUS questionnaire, a pandas³⁹ data frame of the answers was generated. The frame structure information generated by the data frame class function *info()* shows a data frame with twelve data columns, one for each of the ten questions, one column for the group the participant belongs to and one column for the self-evaluated technical affinity of the participant. The data frame contains 20 data entries (rows) and all of the 20 participants answered all questions in the SUS questionnaire, indicated by all columns having 20 non-null values.

The calculated SUS scores for each participant divided by group membership are shown in figure 32, and the mean value of all SUS scores is calculated as 93.5. This mean score indicates a rating of **A+** for the ID-Wallet demonstrator application on the SUS grading scale of Lewis et. al. as shown in table 1.

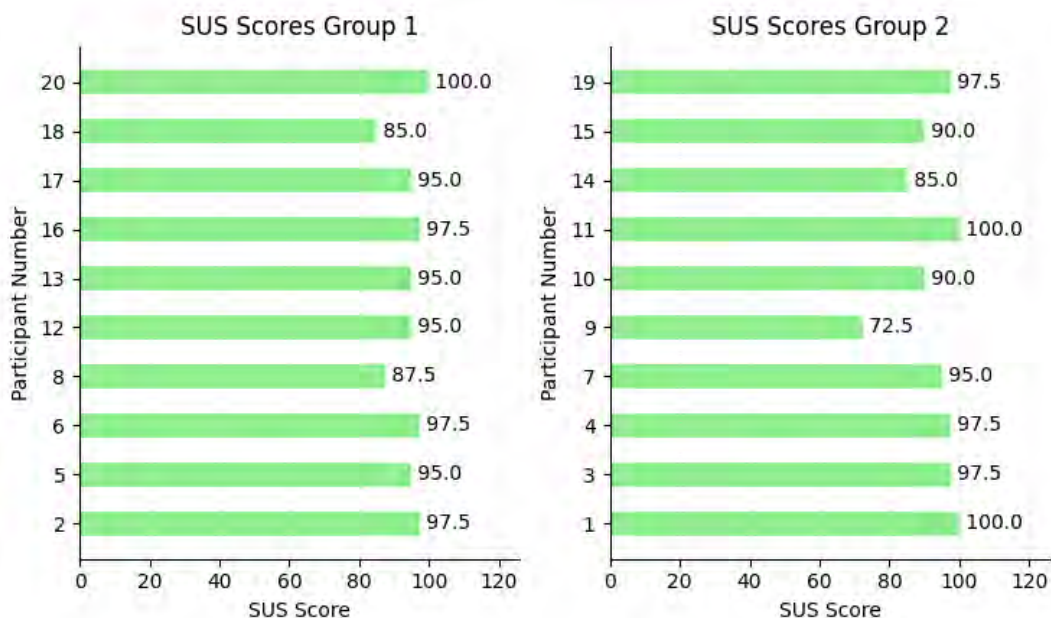


Figure 32: SUS scores for each participant divided by group membership.

³⁹Data structure and analysis tool for python: <https://pandas.pydata.org/> (accessed: 04.04.2024)

6. Study Results

The scores in the groups are not normally distributed, as the Shapiro-Wilk-Test⁴⁰ for both groups gives a p-value of **0.0265** for group 1 and a p-value of **0.0270** for group 2, which in both cases indicates that the sample has not been generated from a normal distribution [45]. Resulting from this, non-parametric statistics like the Spearman correlation coefficient⁴¹ and the Mann-Whitney-U test⁴² are used to analyze the data, as these tests do not require the data samples to be equally distributed and are more fitting for smaller sample sizes [4].

There are three participants (numbers 1, 11, and 20) with a perfect SUS score of 100 and one participant (number 9) with a relatively low score of 72.5 when compared to the mean score. Their score in relation to the self-evaluated technical affinity of these participants is shown in table 2.

Participant Number	Score	Technical Affinity
9	72.5	5
1	100	3
11	100	4
20	100	5

Table 2: SUS scores of interest in relation to the technical affinity of the participant.

These samples do not hint to a relation between the two values, and calculating the Spearman correlation coefficient between technical affinity and SUS score for all participants gives a correlation coefficient of **-0.131**, which can be interpreted as the values having a weak negative linear relationship. A scatter plot of the values, shown in figure 33, does not hint at a relation, as the data points are not closely located to the linear regression plot of the correlation coefficient and no clear pattern is recognizable.

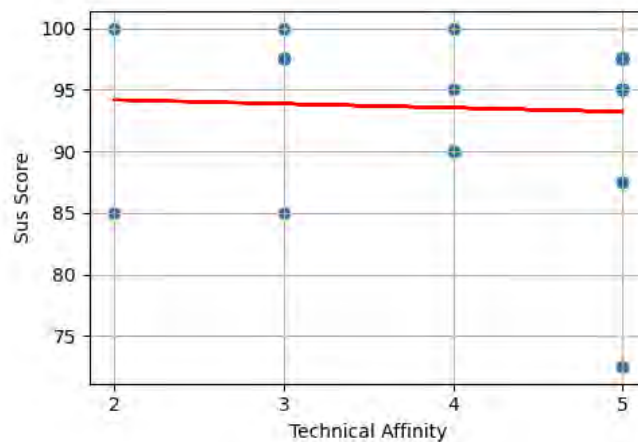


Figure 33: Scatter plot of SUS scores and self-evaluated technical affinity for each participant with linear regression plot of the correlation coefficient.

⁴⁰Statistical test to check for a normal distribution in a group of data: <https://builtin.com/data-science/shapiro-wilk-test> (accessed: 29.04.2024)

⁴¹<https://datatab.net/tutorial/spearman-correlation> (accessed: 29.04.2024)

⁴²Statistical method to determine if statistical significant differences between groups exist: <https://datatab.net/tutorial/mann-whitney-u-test> (accessed: 28.04.2024)

The mean SUS scores of each group and the total mean score are shown in table 3. A small difference between the means of the different groups is shown, with the mean of group 1 being slightly higher than the overall mean, the mean of group 2 being slightly lower than the overall mean.

Group	Mean SUS Score
Group 1	94.5
Group 2	92.5
Overall	93.5

Table 3: Mean SUS score for each group and overall mean SUS score.

The mean scores for each group are also presented as a bar chart with error lines in figure 34 to allow for an easier visual comparison of the means and an insight into the standard deviation of the means.

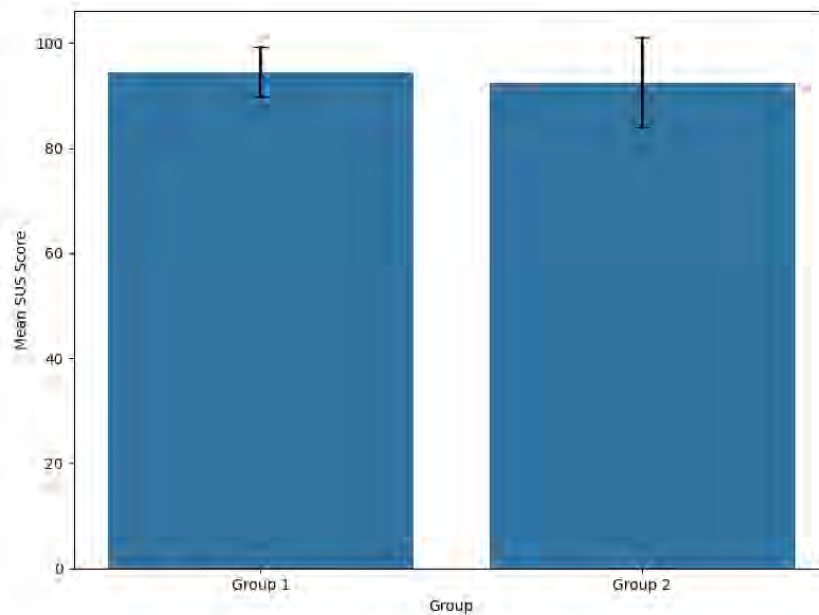


Figure 34: Mean SUS score for each group with standard deviation error lines.

A Mann-Whitney-U Test for the SUS scores between the two groups gave the results shown in table 4. The p-value is 1.0 and as such larger than the significance value of 0.05. This indicates that there is no statistically significant difference between the SUS scores of group 1 and group 2.

Mann-Whitney U	p-value
50	1.0

Table 4: Results of the Mann-Whitney-U Test for SUS scores between the two groups.

6.3 HCTS Results

Analyzing the results of the HCTS questionnaire consists of similar steps to the SUS analysis. A pandas data frame is also generated from the response data of the participants. This data frame also consists of one column for each question (9 columns in this case), one column for the group the participant belongs to, and one column for the technical affinity of the participant, summing up to 11 columns in total. This data frame also holds 20 data entries (rows) and just like with the SUS questionnaire, every column has 20 non-null data values, implying that every participant answered every question of the HCTS questionnaire.

The answers in the data frame were then used to calculate the trust score for each participant as described on TrustedUX documentation, mentioned in 4.2. The described steps were fitted to the modified HCTS used during this study, meaning that only question 1 and 2 had to be reversed because question 3 was omitted from the questionnaire as described in section 5.4. Further, the maximum overall score of the HCTS in this study was 45 instead of the score of 70 mentioned in the documentation of TrustedUX.

Figure 35 shows the calculated trust scores for each participant divided by group membership. Noticeably, the scores from participants belonging to group 1, the group without a photo shown when verifying the digital ID card, are on average lower than the scores from participants of group 2, which were shown a photo of the digital ID card holder when verifying the digital ID card. While the trust scores of participants in group 2 reach a maximum score of 100% two times, no perfect score can be found in group 1, where the highest score achieved is 93.33%.

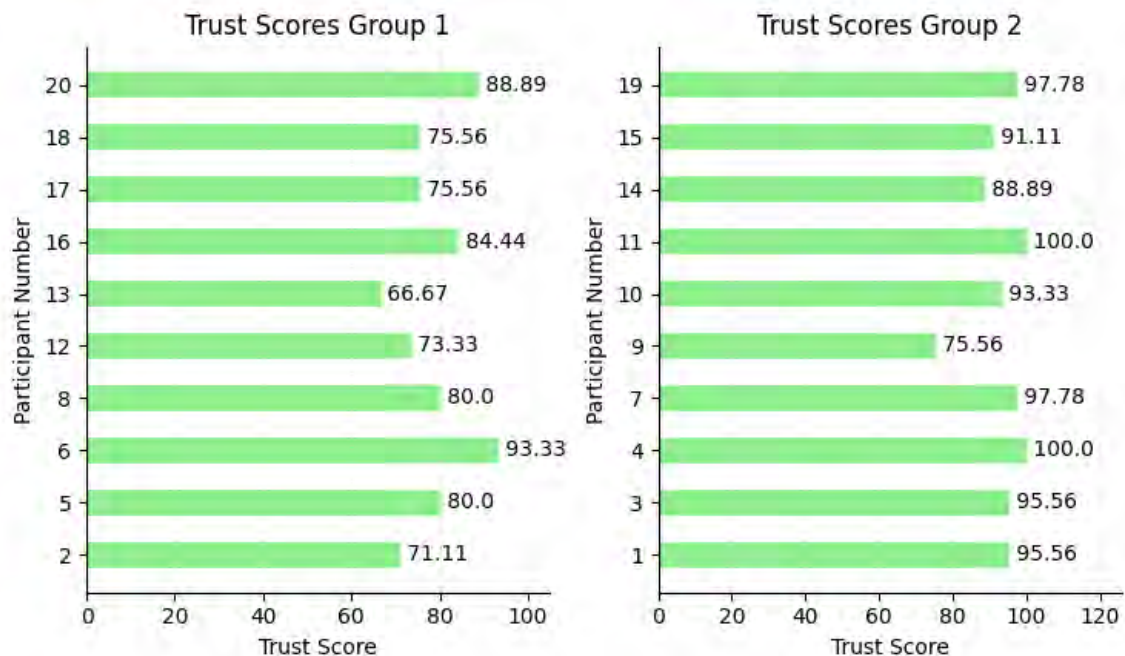


Figure 35: HCTS scores for each participant divided by group membership.

The trust scores in the groups are not both normally distributed. While the Shapiro-Wilk-Test for group 1 gives a p-value of **0.912**, implying that this sample has been generated from a normal distribution, the p-value of the Shapiro-Wilk-Test for group 2 is **0.0178**, which indicates that the sample has not been generated from a normal distribution [45]. As a result, non-parametric tests like the Spearman correlation coefficient and the Mann-Whitney-U test are also used to analyze the trust scores.

The mean values for the trust scores of each group and the overall mean trust score are shown in table 5. It is noticeable that the mean trust score of group 1 is lower than the overall mean trust score, while the mean trust score of group 2 is higher than the overall mean score.

Group	Mean Trust Score
Group 1	78.889
Group 2	93.557
Overall	86.223

Table 5: Mean trust score for each group and overall mean trust score.

The visualization of the mean scores of both groups as a bar chart in figure 36 shows this difference between the means clearly in a more visual way. The error lines of this chart represent the standard deviation of the means for each group.

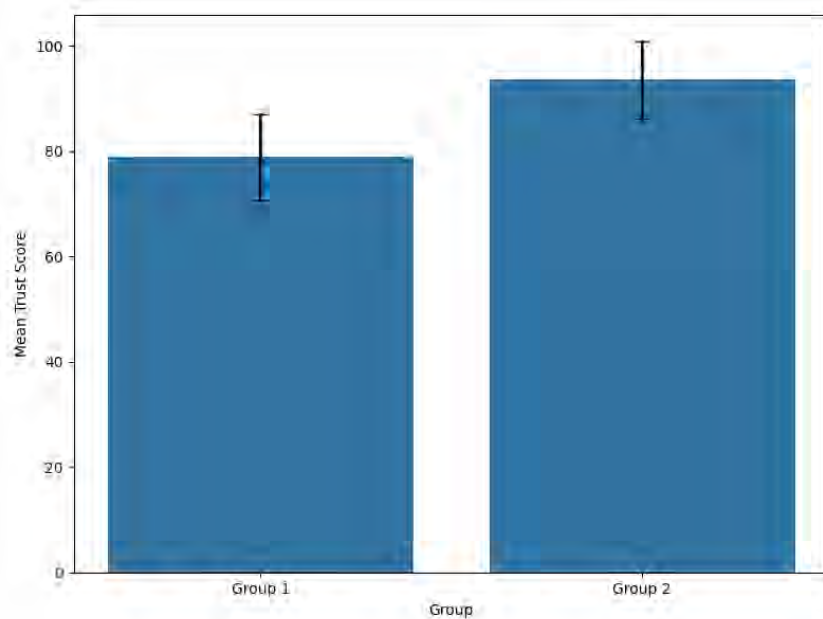


Figure 36: Mean trust score score for each group with standard deviation error lines.

When looking at the trust scores for each participant shown in figure 35 again, there is an interesting score in group 2. Participant number 9 with a score of 75.56 has a much lower score than the mean trust score of group 2, and an even lower score than the mean trust score of group 1. Looking into the responses for this participant shows that even though they were shown a photo, they answered that they think it may have

6. Study Results

negative consequences using the ID-Wallet to verify a persons identity instead of a physical ID card, and they also answered that they think they must be cautious when using the ID-Wallet. They also gave a neutral response of 3 for the statement that they think the ID-Wallet works in their best interest. Their response for the self-evaluated technical affinity is five, so this participant sees themselves as very technically skilled.

This score opened up the question if there is a correlation between technical affinity and the trust score. Calculating the Spearman correlation coefficient results in a correlation coefficient of **-0.144** between the trust score and technical affinity, hinting on a slightly negative linear relation between technical affinity and trust score. Looking at the scatter plot for technical affinity and trust score, shown in figure 37, the data points are not close to the linear regression plot, no pattern is showing, and no significant correlation can be assumed from the plot.

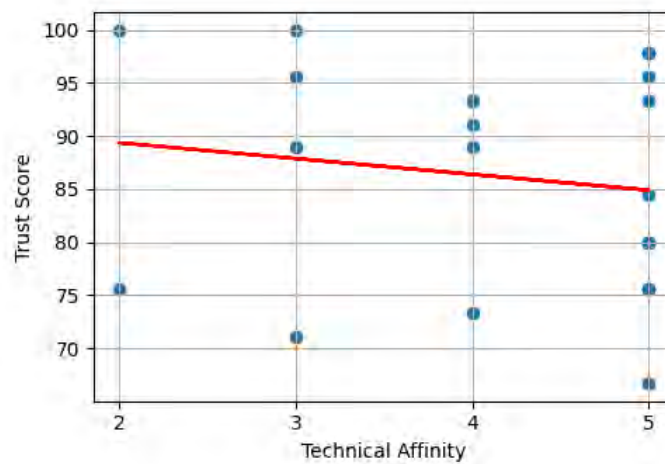


Figure 37: Scatter plot of trust scores and self-evaluated technical affinity for each participant with linear regression plot of the correlation coefficient.

It is further analyzed whether there are significant differences in the mean technical affinity and smartphone usage for daily tasks between the randomly assigned groups. The mean values for each group are shown in table 6.

Group	Mean technical affinity	Mean smartphone usage
Group 1	4.3	4.5
Group 2	3.9	4.6
Overall	4.1	4.55

Table 6: Mean technical affinity and smartphone usage for daily tasks per group and overall.

There is a small difference of 0.1 between the smartphone usage for daily tasks and a slightly larger difference of 0.4 between the means of technical affinity between the groups. Mann-Whitney-U tests for each of these values give a p-value of **0.3921** for technical affinity and **0.5392** for smartphone usage in daily tasks, so no statistical significant difference between those means exist, as both p-values are higher than the significance level of 0.05.

With no significant differences between those two values for the groups, the next analysis step investigates if there is a statistically significant difference between the trust score means for the groups. Table 5 shows the relevant means, and there is already a difference between the groups visible. To see if this difference is significant, another Mann-Whitney-U test is conducted. The results of the Mann-Whitney-U test are shown in table 7. The resulting p-value is **0.002119** and as such lower than the significance level of 0.05. This implies that there is a statistically significant difference between the trust values of both groups, so the null hypothesis is rejected.

Mann-Whitney U	p-value
9	0.002119

Table 7: Results of the Mann-Whitney-U test for HCTS scores between the two groups.

6.4 After-Scenario Questions

The responses to the after-scenario questions and also the remarks from the participants gathered during the study are analyzed by first creating a transcript of the recorded sessions and then going through them, categorizing and coding the responses and interesting remarks to find patterns in the participants impressions and responses.

6.4.1 Scenario 1: ID-Wallet Setup

The first question after the participants are done going through the introduction and setting up the login method for the ID-Wallet is:

SQ1: "What is your first impression of the application?"

All of the twenty participants indicated that they have a good and positive first impression of the application, with many participants remarking that the introduction is well explained and summarizes the functionality in a short and precise way. They also mention that the procedure of digitizing the ID card is well explained and easy to understand.

The second question after this scenario is:

SQ2: "Were the set-up steps clear to you or did you wish there was more assistance offered? If yes, what kind of assistance?"

The transcripts of the sessions indicate that 19 of the participants felt that no further assistance was needed for the application setup and digital ID card setup, with one participant not clearly stating if the setup steps were clear enough, but also not stating otherwise.

The third and last question for this scenario is:

SQ3: "What feeling does digitizing the physical ID card using the application leave you with?"

6. Study Results

Thirteen participants stated that they have good feeling digitizing their ID card and keeping a digital ID card in their phone. Two participants highlighted the easy digitizing process for the ID card, with one stating that it is not a big deal but being extremely simple and quick.

In contrast to these responses, seven participants explained that they are somewhat sceptical of digitizing their ID card. Five participants mention the risk of losing their phone or their phone getting stolen and thus losing the access to their digital ID card and other parties using their digital ID card. Participant 11 remarked that they would feel a lot safer if they could block the digital ID card remotely in case of loss or theft. Participant 7 highlighted that they do not really trust the German government to develop such a wallet application in a secure way and keep it updated, as they explain that they were disappointed with other applications developed by federal German institutions. Participant 16 mentioned that they are sceptical because it was not clear enough for them where the ID card data is stored, if it is stored in any kind of cloud or only locally. They felt the digitizing process went to quick and wished for more information where the data is going to be stored. In contrast to the previously mentioned participant, this participant would prefer if the wallet application was developed and published by an official German federal institution.

6.4.2 Scenario 2: On-Site Authentication Using the Created Digital ID Card

The first question after the participants successfully authenticated themselves using their digital ID card is:

SQ4: "Was the process of on-site identification clear, or would you have preferred more assistance? If so, what kind of assistance?"

Fifteen participants stated clearly through their answers that they felt no need of further assistance, while many of them pointed out that they like the idea of being presented a QR-Code to scan and prepare the digital ID card for on-site authentication.

Five participants highlighted that they themselves did not have much problems finding the button to scan a QR-Code in the application but feel that lesser experienced smartphone users may be troubled to find this button. After being told that they could also use any QR-Code scanner application or the built-in scan functionality of their phone, most of these participants did not see that as a big problem anymore. Participant 3 failed to spot the scan functionality at all but later explained that he only used iOS devices until now and as such did not identify the icon used for the QR-Code, as iOS uses another icon language throughout the system.

The second question is:

SQ5: "How do you perceive the digital ID card compared to the physical ID card? Which option would you personally prefer?"

Sixteen participants replied that they would prefer the digital ID card. The reasons given were that they see it as equal to a physical ID card, that they always have their smartphone with them anyways and also that they felt that the digital solution presented with the demonstrator application is easier to use than a physical ID card.

Two participants indicated that they have no clear preference and are open to use both variants, while two other participants replied that they would strongly prefer to keep using a physical ID card. One of these is participant 11, of which the reason is that they do not use any digital services like paying with their phone, so they would maybe keep a digital ID card as backup but prefer physical ID cards. The other participant is participant 7, who explained that they would prefer a physical card integrating all different kind of currently used cards like health insurance card, drivers license, and also the ID card into one card instead of having a digital solution.

6.4.3 Scenario 3: Validating a Digital ID Card Using the ID-Wallet Scanner

This scenario has only one after-scenario question, which is:

SQ6: "What is your impression of the digital ID card from the validating party's perspective? Do you see the solution as comparable to a physical ID? Please briefly justify your answer."

As this is the part of the study where half of the participants were shown a photo and the other half had no photo shown, the group to which the participant belongs to is important when looking at the responses.

6.4.3.1 Participants in the Group Without Photo

From the 10 participants that were in the group without a photo, seven immediately remarked that they had no photo shown and see this as a problem. Six participants of this group highlighted that a photo is very important for this step, as without a photo they would not be able to verify that the person in front of them is really the owner of the phone and the digital ID card.

6.4.3.2 Participants in the Group With Photo

All of the participants in the group that had a photo shown replied that they feel they get the same information as with a physical ID card and they feel that with the given information they are in a good position to verify the identity of the person in front of them.

6.4.3.3 Group-Independent Responses

Outside of the presence or absence of a photo, eight participants mentioned that they have a better overview of the ID card data, as it is better summarized as on the physical ID card and also all the data is present on one page, so they do not have to switch between two sides like on the physical ID card. Four participants remark that this enhanced overview makes the data quicker to verify.

Two participants mentioned that they like that no physical contact with any card or phone from the person is necessary to verify the identity as this is more hygienic, especially with the COVID-19 pandemic in mind.

6.5 Participant Comments During the Study

The participants were asked to think aloud during the scenarios and highlight things they notice during the usage of the ID-Wallet. Looking at what login method the participants selected during the setup, 10 participants commented that they prefer the current device unlock mechanism, five participants opted for a fingerprint and a newly set PIN, and one participant commented that they want to set up a separate PIN for the application, but no fingerprint.

Six participants mentioned immediately when reaching the main view of the ID-Wallet that they do not know what "Hoheitliche Karten" are. After being explained that this is the official name of cards like the ID card, the drivers license, and the health insurance card in Germany, they understood why this name was used there but still remarked that the term is not really used in daily language and as such not many people will know what is meant with this name. They propose that either an explanation is given for this name or a more generally known name is used for the application.

Many participants suggested improvements for future versions of the ID-Wallet and especially the ID-Wallet Scanner application. Eight participants proposed that the Scanner application could make better use of the possibilities of being digital by not just showing the data of the digital ID card to the verifying party, but also verify the data by itself. They would like to set some parameters for the Scanner application beforehand, like an age restriction or a list of first and last names of allowed visitors. The Scanner app should then immediately indicate with a symbol if the scanned digital ID card fulfills all previously given criteria, or should highlight data that does contradict the given criteria in an easy to see way.

Participant 10 suggested that there should be a history of generated QR-Codes in the ID-Wallet application, as they were to quick to dismiss their generated QR-Code during the second scenario and as such had to do all the steps again. They explained that with a history of generated QR-Codes, they could just pick the generated QR-Code again and present it. They also remarked that those generated QR-Codes should have an expiration in this case, as they think that the list of QR-Codes could become too long really quick otherwise.

Participant 15 explained that they are not really reading texts in mobile applications and as such often skipped through the instructions given in the app and then had to go back and re-read the instructions. They suggested that more animations or images are used as instructions instead of text, as they believe that this would help to understand the instruction steps quicker.

7 Discussion

In this chapter, the results of the data analysis in the previous chapter are discussed and interpretations of the findings are derived. Answers regarding the research questions are investigated and the hypotheses put forward in section 1.4 are reviewed. The discussion is structured closely to the previous chapter, first discussing the demographics. Afterwards, a discussion of the data gathered from the questionnaires is following, giving answers to the research questions. The responses to the after-scenario questions and the comments gathered during the study by the participants are discussed in the following section, following an exploratory approach. The chapter closes with a discussion of the limitations, regarding both the implemented demonstrator application and the study.

7.1 Demographic

As already mentioned in section 6.1 and shown in figure 29, the participant group is of a diverse age distribution, spanning from the age groups 18-20 up to 60-69 while being skewed towards the younger age groups. Even though half of the participants are in the age group of 21-29, the participants in the other age groups allows an overview over many age groups and generations, and their opinion regarding the usability and trust of the presented demonstrator application.

In combination with the categorized occupations of the participants shown in figure 30, this impression of a somewhat diverse participant group is enforced. To gain insight into the interaction of the general population with digital identity wallets like the demonstrator application, it is important to have participants from different backgrounds, ideally not only being IT-related but also from occupations that are not IT-related at all. While the participant group of the study still has 30% of the participants working in an IT-related background, the majority of the participants are coming from non IT-related occupational backgrounds, and even between those occupations a diverse distribution throughout all of society is present, which helps the generalizability of the results of this study.

The distribution of self-evaluated technical affinity and smartphone usage in daily tasks, found in figure 31, shows a less diverse picture. The majority of the participant group rate themselves as highly or very highly tech-savvy, presenting a strongly tech-savvy participant sample and as such the results of the study are more relevant for this user group. Together with the distribution of smartphone usage in daily tasks, where the majority of participants indicate that they use their smartphone always if possible, this impression of a more tech-savvy user group with a high usage of technology is enforced.

This self-evaluation of high technical affinity for the majority is surprising when compared to the occupation areas of the participants, showing many participants working in non IT-related backgrounds. A reason may be that the presented scale for self-evaluation did not allow for a fine enough gradation in technical affinity, as many people also indicate that they use their smartphone a lot for daily tasks and such do see themselves at above an average or medium technical level, while there is still a lot of difference between using a smartphone often and coming from an occupational

IT-related background, so the participants assumed different baseline levels for the technical affinity rating.

7.2 SUS Questionnaire

The responses of the SUS questionnaire and the derived SUS scores show a relatively high perceived usability by the participants. An average SUS score of 93.5 and thus a rating of A+ on the SUS grading scale are good results for the demonstrator application and well above the industry goal of 80, which denotes an above average user experience as mentioned in section 4.3 [40]. In regard to the research questions, this mean SUS score gives an answer to RQ1, as it directly confirms the hypothesis that the demonstrator application reaches a mean score of at least 80. With the mean score of 93.5, the demonstrator application places itself in the 96th-percentile in regards to the SUS grading scale of Lewis et al. [40] which implies a well above average user experience. This allows RQ1 to be answered with a positive response, the findings during the study clearly show that a digital identity wallet application following the concept presented during this thesis satisfy the usability need of the users. This coincides with the findings of Murtezaj [47], who performed usability studies on the low-fidelity prototype developed by the USP group, and also used a SUS questionnaire with a mean SUS score of 90.33 and a rating of A+. In comparison to the result of Murtezaj [47], the mean SUS score for the demonstrator application is a few points higher, which may be a result of the more detailed interactions between device, physical ID card and QR-Codes possible in the Android-based demonstrator. This also confirms the findings of Kostic et al. [37] where users highlighted the ease of use of the wallet concept, as the demonstrator based on this concept reached even higher SUS scores than the low-fidelity prototype.

The gathered data and the interesting scores presented through participant 9 with a relatively low score and participants 1, 11 and 20 with a perfect score opened up the question whether the perceived usability of the participant is related to the self-evaluated technical affinity. The investigation regarding a correlation interestingly did not show a clear relation between these factors, instead no linear relationship could be derived from the correlation coefficient. This is a little unexpected, as an assumption would be that participants who are not that tech-savvy would maybe have more trouble when using the demonstrator application. With the findings not showing an indication of such relation, it can be assumed that a digital wallet application following the presented concept shares a high perceived usability throughout different tech-savvy user groups. This also coincides with the findings of Kostic et al. [37] where all participants were able to clearly understand the identification process while using a low-fidelity prototype of this wallet concept.

The deviation of participant 9 with a relatively low score of 72.5 while having a self-evaluated technical affinity of 5, which means *very strong*, may hint that users from a deep technical background see the demonstrator application as less usable. This may be the case because they think features they would require are missing. The gathered data did not give any hints how this deviation came to be, and since all other participants with such high self-evaluated technical affinity are not following such a trend, this deviation can be seen as a one-off result.

The Mann-Whitney-U test for the SUS questionnaire shows no statistically significant difference between the SUS scores of the groups. This implies that differences between the groups may be a result of random chance alone. This answers **RQ2** by supporting the hypothesis that the presence or absence of a photo during the verification process has no influence on the perceived usability of the demonstrator application. This result was expected because the presence or absence of a photo is only relevant in the ID-Wallet Scanner application, which was not directly a part of the areas the participants should review during the SUS questionnaire. The analysis was done to explore if the participants are subconsciously influenced in their perceived usability of the ID-Wallet by the presence or absence of a photo in the ID-Wallet Scanner application, which was not to be rated during the SUS questionnaire. This notion can be dismissed by the findings, and as such the answer for **RQ2** is, that the presence or absence of a photo does not influence the usability experience of users.

7.3 HCTS Questionnaire

The differences of maximum achieved trust scores visible in figure 35 and described in section 6.3 imply that there may be a difference of trust between the two participant groups. Looking into the mean scores for the groups in table 5 highlights this difference even more, as group 2 (the group with a photo shown) has a mean trust score well above the overall mean trust score for both groups combined, while the mean trust score of group 1 (the group without a photo) is well below the overall mean trust score.

To validate that these differences are not a product of random chance alone, a Mann-Whitney-U test was conducted and confirms that there is a statistically significant difference between the trust score values of each group. This rejects the null hypothesis belonging to **RQ3**, stating that there would be no statistically significant differences, and by doing so supports the hypothesis **H3**. With the hypothesis **H3** accepted through the results of the Mann-Whitney-U test, the research question **RQ3** can be answered with a positive answer: the gathered data during the study suggests that the presence or absence of a photo during the on-site verification process of a digital identity from this wallet application does influence the users perceived trust in the solution by a statistically significant amount. With this finding, it becomes clear that if any digital identity wallet solution intends to also offer on-site usage of a digital ID card, the inclusion of a photo becomes important to achieve the users trust in this solution.

Just like in the SUS questionnaire results, participant number 9 shows up as an interesting deviation in the trust scores. While being in group 2, and such being shown a photo, their responses in the HCTS questionnaire result in a relatively low trust score of 75.56. This score is not just significantly lower than the mean trust score of group 2 but also lower than the mean trust score of group 1, which participants had no photo shown. This consecutive deviating position for participant 9, who self-evaluated as having a very strong technical affinity, further strengthens the impression that participants with a very strong technical background may feel that features or implementation details are missing that they feel are necessary for such a wallet application. This may also include security relevant implementation details

7. Discussion

which due to their strong technical background are more easily identifiable by them.

An investigation regarding a relation between the trust score and the technical affinity did lead to similar results like with the SUS score. The Spearman correlation coefficient implies a weak negative linear relation, but the scatter plot shown in figure 37 does not give any evidence for a significant relation between the two values, as described in section 6.3. This implies that the trust scores collected during the studies are independent from the technical affinity of the participants, helping the generalizability of the findings of the study.

To ensure that a difference in mean trust scores is not a result of unbalanced groups regarding smartphone usage in daily tasks and also in technical affinity, the means for these values for each group and for all participants overall have been calculated, as shown in table 6. As differences between the means for technical affinity and for the smartphone usage in daily tasks became visible, Mann-Whitney-U tests have been performed for each value. The results of these Mann-Whitney-U tests indicate no statistically significant difference between the technical affinity and smartphone usage in daily tasks for the groups, so it can be assumed that the groups are sufficiently balanced for the study and the difference in the trust score means does not result in unequal distribution of participants with different technical affinity and smartphone usage in daily tasks to the groups.

7.4 After-Scenario Questions and Comments during the Study

At the first steps of the study, the participants had to select a login method to secure the ID-Wallet. Based on the comments of the participants gathered during the study, it becomes clear that most participants prefer the convenient way of just using the authentication mechanism already in place for the device. This is especially interesting as the device used during the studies was only protected by a simple numeric code, and no fingerprint or face unlock was set-up. This implies that users tend to choose the most convenient way for them, opting even for lower security standards. A trade off between security and usability needs to be found here, as forcing too rigid mechanisms might deter people from using the application.

The answers given to the after-scenario questions indicate an overall positive experience with the ID-Wallet. Especially the answers regarding SQ1 support this impression, as all 20 participants indicated that they have a positive first impression of the app. This confirms the findings of Kostic et al. [37] where a majority of the participants noted that they were convinced by such a wallet concept. The introductory tour and the explanation of the digitizing process of a physical ID card were highlighted as very helpful in the responses, which indicates that such components are important in a digital wallet application for the first impression of the user. The large number of participants stating that they needed no further assistance also highlights this importance. These comments also enforce the recommendation of Sartor et al. [53] that tutorials and introductions are helpful to showcase to users what such a wallet is able to do.

The immediate negative reaction to the term *Hoheitliche Karten* of many participants hints in a similar direction like the findings of Korir et al. [36] and Sartor et al. [53], who identified the usage of SSI-concept terms to be problematic for the learn-

ability of the wallet application. While the term *Hoheitliche Karten* is not a term from the SSI-context, it still presents an official term from the concept of identities and is not used often in daily conversations, as remarked by the participants.

Regarding the feeling the participants have with digitizing their ID card, a mixed impression can be derived from the responses. While the majority of the participants state that they have a good feeling digitizing their ID card, there were also participants sceptical regarding this process. Reasons were fear of losing their smartphone or the phone getting stolen, which means they lose access to their digital ID card and in the worst case allows other parties the usage of their digital ID card. This is a valid concern, but can be countered by securing the ID-Wallet in ways that do not allow other parties to access the digital identities in case of loss or theft. Participant 11 highlighted that they would feel safer when they had the ability to remotely deactivate the digital ID card like when losing a credit card. This is an interesting idea and should be further investigated, as it would probably help many users with similar concerns and uses a known concept of how to behave in case of the loss of an ID card.

When looking at the process of the on-site authentication, the majority of the participants remarked that they do not need more assistance. This implies that a sharing procedure based on QR-Codes is well accepted by users. It also appears to be a known pattern for users with a strong technical background, but also for users with a less technical background, implied by the fact that users of different self-evaluated technical affinity both came to the conclusion that this process was easy enough to understand and doable without further assistance. With many of them highlighting that they felt positive about the QR-Code to scan and prepare the digital ID card, it is reasonable to assume this is a desirable feature for a wallet application if on-site usage of the digital identities is also planned. This is contrasting the findings and recommendations of Korir et al. [36] that QR-Codes appear to be a hindrance for the user and should be avoided in SSI-based wallets. Looking at the remarks regarding the button for this scan functionality, even though every kind of QR-Code scanner may be used, it seems that the functionality has to be presented better, either with a label in addition to the icon in the button or with a different, more highlighted placement.

The idea of having a history of generated QR-Codes, as participant 10 proposed, is interesting. Currently, if the user clicks on the back or finish button, the generated QR-Code is gone and can not be accessed again, so the user has to go through all steps starting from scanning the request QR-Code again. This may also happen when the user suspends the wallet application or switches off their phones screen, as the Android operation system may suspend the application in these cases. Having this history would allow the users to prepare their digital ID card well in advance and allows them to not worry about having to do all steps again when closing the app or shutting off the screen. The proposed expiration of QR-Codes in this history appears reasonable in this case, as for the most part these QR-Codes have been generated for one specific occasion, which in the envisioned use-cases will happen in a short time span after the code has been generated. As such it would not be useful to keep them in the history forever.

Sixteen of the 20 participants indicated that they would prefer to use the digital ID card instead of a physical ID card. Next to the given reasons that they see the digital

7. Discussion

ID card as equal to the physical ID card and that they always have their smartphone with them anyways, the answers also hint that the proposed and implemented solution in the demonstrator application may also have an influence on the participants preference, as it is stated multiple times that they think the digital ID card feels easier to use in this on-site scenario. These answers also indicate that people are open to use digital ID cards if they offer a more convenient experience than their physical counterparts. Nevertheless, there are two participants who are sceptical of a digital ID card. One of these participants, participant 11, states to be sceptical towards all kinds of digitalized services, as they remark that they do not use services like Apple Pay or mobile payment, so this stems more from their general attitude towards such digital services than the demonstrator application. The other participant, participant 7, proposes an interesting alternative of combining all different kinds of cards into one physical card instead of having those in a digital identity wallet. It is unlikely that such a solution would be possible without storing all the related data of these cards on a chip inside the physical card, as printing all data on the card would be difficult. This then comes close to digital identities, just stored on a physical card with a chip instead of a smartphone, so the chip acts as a kind of a digital identity wallet.

The answers to the after-scenario question **SQ6** in the third scenario support the concluded answer to **RQ3** from section 7.3, as they highlight that photos are important for the on-site verification of another persons identity. Of the group of participants who were not shown a photo in the third scenario, where they were asked to verify another person with the digital ID card of this person presented, seven participants noticed the missing photo immediately and also spoke up that they see this as a problem. Together with the remarks that such a photo would be important, as without a photo they can not verify that the person in front of them is the owner of the phone and the digital ID card, these answers imply a high perceived importance of a photo for this use-case. This notion is underlined by all of the ten participants belonging to the group with a photo shown confirming that they see the digital ID card as similar to a physical ID card and that they feel they are provided with all data they need to do an informed decision regarding the identify verification.

Outside of the presence or absence of a photo, an interesting insight to be taken from this question is that multiple participants highlighted that the digital ID card gives a better overview over the ID card data, as everything is shown on one page instead of needing to flip the card, which also allows for quicker verification in their opinion. This was not a specific focus when developing the demonstrator application, but it shows that a digital ID card solution can enhance the handling even with such seemingly simple improvements.

Another very interesting insight was, that two participants thought of the topic of hygiene with pandemics like COVID-19 in mind. They highlighted the fact that the presented solution in the demonstrator application does not require any physical contact with either the physical ID card or the phone of another person when verifying their identity, and as such may even protect the health of the controlling party in a way. This was not thought of when developing the demonstrator application but is a welcome positive side of using digital identities on-site when following the concept presented in the demonstrator application.

Half of the participants felt that the demonstrator application does not fully use the potential of digitalization, and they proposed an improvement of the ID-Wallet Scanner application to take better advantage of being digital by not just showing the data of the digital ID card, but also already verifying this data based on previously defined criteria like age or an invitation list. This idea was not in mind while conceptualizing and developing the demonstrator application, as the ID-Wallet Scanner was envisioned as just a tool to support the study and the use-case of scanning the digital ID card on-site, but appears to be a useful enhancement of the implemented solution. By making the verification process much easier and quicker for the verifying user, this change may help with the acceptance and as such the widespread offering of identity verification using a digital ID card. This in turn will help the acceptance of a digital ID card and digital identity wallets in everyday usage for all people, as they are more inclined to use such a solution when it is offered to them during a lot of tasks in their day-to-day life.

7.5 Limitations of the Demonstrator Application

Regarding the developed demonstrator application, some limitations have already been mentioned in section 3.1. One limitation of the demonstrator is that not the actual data from the physical ID card is transmitted during the digital ID card setup, but dummy data is used for the digital ID card in the demonstrator application. The reasoning for this decision is described in detail in section 3.3.1, but is for the most part due to the cost associated with the necessary authorization certificate to read the actual data from the physical ID card chip. During the study, a sample ID card is given to the participants and the data in the demonstrator application is then matching the data from the sample ID card to give as much of a realistic impression as possible. While this may help to lessen the effect of the dummy data on participants, they still are not using their own ID card and seeing their own data. This may result in a lowered sense of urgency in the participants regarding trust in the solution and the safety of their data, as they are not using their own data but just the data from a sample ID card. This in turn may lead to a bias when answering the HCTS questionnaire, and may thus hurt the internal validity.

Another limitation of the current implementation of the demonstrator application is, that not much attention has been given to the security and safety of the implementation for now. To be able to serve as a demonstrator for the user studies during this thesis, these implementation details were not relevant and have been omitted. As mentioned in section 3.1, the application stores data persistently but not encrypted or otherwise secured. The same holds true for the transmission of the digital ID card data, which happens unencrypted and unsecured without any checks for tampering attempts. The photo data used in the ID-Wallet and ID-Wallet Scanner is hard-coded, no actual photo data is transmitted from the physical ID card and also not during a verification with the ID-Wallet Scanner using the QR-Codes. While this does not have a large influence on the participants of the user studies as they do not see these technical implementation details, the need of changes to secure the ID-Wallet and adhere to safety standards may introduce changes in the implementation that alter the current concepts of the ID-Wallet and thus may hurt generalizability, as a wallet application

in the real world may differ strongly from the concept presented in this thesis as it needs to adhere to security and safety standards.

7.6 Limitations of the Study

The study also shows some limitations, beginning with the demographic. While the age groups of the participants were quite diverse, there is a noticeable underrepresentation of participants younger than 20 and participants older than 69 years of age, with a majority of participants in the age group of 20-29, which may hurt generalizability. Especially the group below the age of 20 may be an interesting age group to investigate further, as they possess high digital skills [22].

When looking at the occupations of the participants, while having a majority in non IT-related occupations, there is a notable amount of IT-related occupations present. This may be a threat to generalizability and thus external validity. For future research it may be interesting to gather a larger selection of participants with IT-unrelated occupations.

The low sample size of the participant selection is also a heavy limitation of the study. While the selected sample size is large enough to gather first insights, a larger sample size allows for much better generalization of the results and thus helps the external validity of the study.

Another threat to external validity is the focus on one specific implementation of the concept of a digital identity wallet in the form of the ID-Wallet demonstrator application presented during this thesis. This allows insights into usability and trust regarding the specific demonstrator application, but makes it harder to generalize these insights for more digital identity wallet applications, especially if they follow a different concept than the one presented during this thesis.

A further limitation is the focus of this study on the German national ID card and German participants, influenced by the authors living and working in Germany. This limits the generalizability regarding users and identity cards from other countries. As mentioned in 1.1, due to the EUDI regulations every country in the EU has to offer a digital identity wallet solution until late 2026 to early 2027, so insights regarding other identity cards of EU countries may be of interest.

A threat to internal validity stems from the fact that some participants know each other and may have talked about the study, thus influencing their opinion and responses to the questionnaires. As the study executions were not all done on the same day but individually over the extent of multiple months, a participant that already participated in the study may have talked about the study with another candidate that had not done the study already, even though the study supervisor asked them to not talk about the study with other participants until they were also done with the study, and asking participants before each study execution if they already talked with others about it. All participants denied that they talked about the study with others beforehand.

8 Conclusion

During this thesis, the usability and user trust of a digital identity wallet concept was investigated. The focus of this concept and investigation was the usage of digital identities in on-site authentication. To reach a better understanding regarding the user trust, the example of the German national ID card was used, and the influence of presence or absence of a photo during the identity verification process using a digital ID card on the users trust in the solution was investigated.

For the purpose of this investigation, a digital identity wallet demonstrator Android application was developed and presented. This demonstrator application was then used during a user study with 20 participants, who went through three different scenarios and use cases during the study, covering the setup of the wallet application, the creation of a digital ID card using a physical ID card, and the usage of the digital ID card in on-site authentication from the side of the person presenting their digital ID card, but also from the side of the person verifying a digital ID card. For the purpose of testing the impact of the presence or absence of a photo, the participant group was divided into two subgroups of equal size, where one group was shown a photo during the last scenario where they were asked to verify another persons identity using a digital ID card from the demonstrator application, the other group was not shown a photo during this scenario. The participants answered standardized questionnaires regarding usability and trust, and during the study questions were asked after each scenario. The participants were also asked to think aloud during the study and comment on what they are doing.

The results of the study show that the presented concept, which was implemented in the demonstrator application, is well received by the participants, achieving a mean system usability score of 93.5 and a usability rating of A+ on the usability grading scale of Lewis et al. [40]. This score and rating indicates a higher than average usability for the demonstrator application, which by industry standard is defined as a score of or above 80 [40]. This impression is strengthened by the responses of the participants to the after-scenario questions and the comments gathered during the study, indicating an overall positive first impression for all participants.

The results also show, that the presence or absence of a photo when verifying another persons identity using their digital ID card has no influence on the perceived usability of the application. This was expected, as the usability was mainly focused on the other parts and use cases of the wallet application.

Where this presence or absence of a photo did have a strong influence was the perceived trust of the users in the solution. The group with no photo shown did achieve a significant lower mean trust score of 78.889 in comparison to the group which had photo shown when verifying another persons identity, which achieved a mean trust score of 93.557. Statistical evaluation shows that this difference in the means of trust scores between the groups is not a result of chance alone, but is in fact statistically significant. Investigation whether this difference may be a result of imbalanced groups regarding technical affinity or smartphone usage of daily tasks show no statistically significant difference between the groups regarding these both factors.

8. Conclusion

From these results, it can be concluded that the presence of a photo is important for gaining a high perceived trust of the users for a digital ID card and a digital identity wallet solution if it is intended to be used in on-site verification.

8.1 Future Work

From the comments of the participants, interesting topics for future research can be derived. Many participants proposed that the ID-Wallet Scanner application could make better use of the digital possibilities by not just showing the data of the scanned digital ID card to the user, but also verifying the data based on previously set up parameters like for example an age rating or a participant list. This proposal is discussed in more detail in section 7.4. The proposal seems interesting and a good way to achieve a better acceptance of the solution for verifying parties, which in turn may help with the widespread usage of digital ID cards. As such, it appears interesting to investigate the impact of such a feature on the usability of the application but also if it influences the users trust in the solution.

Another interesting proposal to enhance the usability is the addition of a history for generated QR-Codes from the digital ID card, as discussed in section 7.4. The impact on the usability of such a feature in day-to-day usage of the presented wallet concept may be an interesting future research topic.

As mentioned in section 7.6, the study was centered on German participants and the German national ID card. With the importance of digital identity wallet solutions for all countries in the EU due to the EUDI regulations, research regarding ID cards of other nations in the EU may be promising.

A further recommendation is to repeat the study with a much larger sample size. Due to the context of this thesis, the sample size was not very large, so results found during this study are lacking in generalizability, and a repeat of the study with a larger participant sample, ideally with also a less skewed distribution of technical affinity would help confirm the findings of this thesis and help to generalize these findings.

References

- [1] C. Allen. "The path to self-sovereign identity," *Life With Alacrity*. (Apr. 26, 2016), [Online]. Available: <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/> (visited on 04/19/2024).
- [2] N. Babich, *Tabs for Mobile UX Design*, 2016. [Online]. Available: <https://uxplanet.org/tabs-for-mobile-ux-design-d4cc4d9410d1> (visited on 05/10/2024).
- [3] P. Bhandari. "What Is a Controlled Experiment? | Definitions & Examples." (Apr. 2021), [Online]. Available: <https://www.scribbr.com/methodology/controlled-experiment/> (visited on 03/23/2024).
- [4] P. D. Bridge and S. S. Sawilowsky, "Increasing Physicians' Awareness of the Impact of Statistics on Research Outcomes: Comparative Power of the t-test and Wilcoxon Rank-Sum Test in Small Samples Applied Research," *Journal of Clinical Epidemiology*, vol. 52, no. 3, pp. 229–235, Mar. 1999, ISSN: 0895-4356. DOI: [10.1016/S0895-4356\(98\)00168-1](https://doi.org/10.1016/S0895-4356(98)00168-1). (visited on 04/29/2024).
- [5] J. Brooke, "SUS: A 'Quick and Dirty' Usability Scale," in *Usability Evaluation In Industry*, CRC Press, 1996, ch. 21, pp. 189–194, ISBN: 978-0-429-15701-1.
- [6] Bundesministerium des Innern und für Heimat, *Die eIDAS-Verordnung*. [Online]. Available: <https://www.digitale-verwaltung.de/Webs/DV/DE/digitale-identitaeten/eidas-2-0/eidas-2-0-node.html> (visited on 04/26/2024).
- [7] Bundesministerium des Innern und für Heimat, *FAQ - EUDI-Wallet / eIDAS 2*. [Online]. Available: <https://bmi.usercontent.opencode.de/eidas2/en/faq/> (visited on 04/26/2024).
- [8] Bundesministerium des Innern und für Heimat, *Homepage - EUDI-Wallet / eIDAS 2*. [Online]. Available: <https://bmi.usercontent.opencode.de/eidas2/en/start/> (visited on 04/26/2024).
- [9] Bundesministerium des Innern und für Heimat and Bundesdruckerei GmbH. "Online-Ausweis kann bald im Smartphone gespeichert werden: Smart-eID-Gesetz in Kraft." (2021), [Online]. Available: https://www.personalausweisportal.de/SharedDocs/kurzmeldungen/Webs/PA/DE/2021/09%5C_Smart-eID-GE%5C_in%5C_Kraft.html?nn=14626780 (visited on 04/26/2024).
- [10] Bundesministerium des Innern und für Heimat and Bundesdruckerei GmbH, *Infografik_nutzungszahlen eid*. [Online]. Available: https://www.personalausweisportal.de/SharedDocs/bilder/Webs/PA/DE/Infografiken/Infografik_Nutzungszahlen.jpg?__blob=panorama&v=3 (visited on 05/10/2024).
- [11] K. Cameron, "The laws of identity," 2005. [Online]. Available: <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>.
- [12] A. Chinapas, P. Polpinit, N. Intiruk, and K. R. Saikaew, "Personal Verification System Using ID Card and Face Photo," *International Journal of Machine Learning and Computing*, vol. 9, no. 4, pp. 407–412, Aug. 2019, ISSN: 20103700. DOI: [10.18178/ijmlc.2019.9.4.818](https://doi.org/10.18178/ijmlc.2019.9.4.818). (visited on 05/03/2024).

References

- [13] D. Curry. "Mobile Payments App Revenue and Usage Statistics (2024)." (2024), [Online]. Available: <https://www.businessofapps.com/data/mobile-payments-app-market/> (visited on 05/03/2024).
- [14] DENSO WAVE INCORPORATED, *Qr code standardization | qrcode.com | denso wave*. [Online]. Available: <https://www.qrcode.com/en/about/standards.html> (visited on 02/15/2024).
- [15] G. Dodig-Crnkovic, "Scientific methods in computer science," in *Proceedings of the Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden, Skövde, Suecia*, sn, 2002, pp. 126–130.
- [16] T. Ehrlich, D. Richter, M. Meisel, and J. Anke, "Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten," *HMD Praxis der Wirtschaftsinformatik*, vol. 58, no. 2, pp. 247–270, Apr. 1, 2021, ISSN: 2198-2775. DOI: [10.1365/s40702-021-00711-5](https://doi.org/10.1365/s40702-021-00711-5).
- [17] esatus AG, *Esatus about*. [Online]. Available: <https://esatus.com/en/about-us> (visited on 04/22/2024).
- [18] esatus AG, *Esatus wallet demo*. [Online]. Available: <https://wallet-demo.esatus.com/> (visited on 04/26/2024).
- [19] European Commission. "EU Digital Identity Wallet Toolbox Process | Shaping Europe's digital future." (Mar. 2024), [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox> (visited on 04/26/2024).
- [20] European Parliament and Council of the European Union, *eIDAS Regulation | Shaping Europe's digital future*. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation> (visited on 04/07/2024).
- [21] European Parliament and Council of the European Union, *European Digital Identity (EUDI) Regulation | Shaping Europe's digital future*. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation> (visited on 04/07/2024).
- [22] Eurostat. "Digital skills in 2023: Impact of education and age." (Feb. 22, 2024), [Online]. Available: <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240222-1> (visited on 04/15/2024).
- [23] Federal Ministry of the Interior and Community, *Personalausweisportal - data stored in the Chip*. [Online]. Available: <https://www.personalausweisportal.de/Webs/PA/EN/citizens/german-id-card/data-stored-in-the-chip/data-stored-in-the-chip-node.html> (visited on 04/07/2024).
- [24] Federal Office for Information Security, *Bsi technical guideline tr-03121-3 - biometrics for public sector applications - part 3: Application profiles, function modules and processes - volume 2: German identity documents (gid) - version 6.0*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03121/TR-03121-3_2_Biometrics_GID_6_0.pdf?__blob=publicationFile&v=2, 2023. (visited on 02/15/2024).

- [25] German Federal Ministry of the Interior and Community. "EUDI-Wallet / eIDAS 2." (Mar. 2024), [Online]. Available: <https://bmi.usercontent.opencode.de/eidas2/en/start/> (visited on 04/08/2024).
- [26] G. Goggin and R. Wilken, "QR codes and automated decision-making in the COVID-19 pandemic," *New Media & Society*, vol. 26, no. 3, pp. 1268–1289, Mar. 2024, ISSN: 1461-4448. DOI: [10.1177/14614448231201649](https://doi.org/10.1177/14614448231201649).
- [27] Google for Developers, *Android jetpack dev resources - android developers*. [Online]. Available: <https://developer.android.com/jetpack> (visited on 02/02/2024).
- [28] Governikus GmbH & Co. KG, *How to use the eid function*. [Online]. Available: <https://www.ausweisapp.bund.de/en/how-to-use-the-eid-function> (visited on 05/03/2024).
- [29] S. Gulati, S. Sousa, and D. Lamas, "Modelling trust in human-like technologies," in *Proceedings of the 9th Indian Conference on Human-Computer Interaction*, ser. IndiaHCI '18, Bangalore, India: Association for Computing Machinery, 2018, pp. 1–10, ISBN: 9781450362146. DOI: [10.1145/3297121.3297124](https://doi.org/10.1145/3297121.3297124).
- [30] S. Gulati, S. Sousa, and D. Lamas, "Design, development and evaluation of a human-computer trust scale," *Behaviour & Information Technology*, vol. 38, no. 10, pp. 1004–1015, 2019.
- [31] HarperCollins Publishers. "The american heritage dictionary entry: Identity." (2022), [Online]. Available: <https://www.ahdictionary.com/word/search.html?q=identity> (visited on 04/19/2024).
- [32] A. M. Helmenstine. "Six steps of the scientific method." (2020), [Online]. Available: <https://www.thoughtco.com/steps-of-the-scientific-method-p2-606045> (visited on 03/23/2024).
- [33] Heute im Bundestag. "Noch kein Datum für öffentlichen Start der Smart-eID." (2023), [Online]. Available: <https://www.bundestag.de/presse/hib/kurzmeldungen-979152> (visited on 04/26/2024).
- [34] IDunion, *IDunion – ermöglicht selbstbestimmte identitäten*. [Online]. Available: <https://idunion.org/?lang=en> (visited on 04/22/2024).
- [35] IDunion, *Projekt – IDunion*. [Online]. Available: <https://idunion.org/projekt/> (visited on 04/22/2024).
- [36] M. Korir, S. Parkin, and P. Dunphy, "An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022, pp. 195–211.
- [37] S. Kostic and M. Poikela, "Do users want to use digital identities? a study of a concept of an identity wallet," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 2022, pp. 195–211.
- [38] A. Kudra, "Self-Sovereign Identity (SSI) in Deutschland," *Datenschutz und Datensicherheit - DuD*, vol. 46, no. 1, pp. 22–26, Jan. 1, 2022, ISSN: 1862-2607. DOI: [10.1007/s11623-022-1555-1](https://doi.org/10.1007/s11623-022-1555-1).

References

- [39] J. R. Lewis, "The system usability scale: Past, present, and future," *International Journal of Human-Computer Interaction*, vol. 34, no. 7, pp. 577–590, 2018. doi: [10.1080/10447318.2018.1455307](https://doi.org/10.1080/10447318.2018.1455307). eprint: <https://doi.org/10.1080/10447318.2018.1455307>.
- [40] J. R. Lewis and J. Sauro, "Item benchmarks for the system usability scale," *Journal of Usability Studies*, vol. 13, no. 3, pp. 158–167, 2018.
- [41] Lissi. "Lissi ID-wallet: Towards eIDAS2 and EUDI-wallet compatibility," Medium. (Dec. 7, 2023), [Online]. Available: <https://lissi-id.medium.com/lissi-id-wallet-towards-eidas2-and-eudi-wallet-compatibility-0eec47d0b468> (visited on 04/22/2024).
- [42] Lissi GmbH, *Digital wallet EU experts*, Lissi. [Online]. Available: <https://www.lissi.id/about> (visited on 04/22/2024).
- [43] Lissi GmbH, *Lissi - news & resources*. [Online]. Available: <https://www.lissi.id/news-resources> (visited on 04/22/2024).
- [44] Lissi GmbH, *Lissi demo*, lissi. [Online]. Available: <https://try.lissi.id/lissi.id> (visited on 04/22/2024).
- [45] G. Malato. "An Introduction to the Shapiro-Wilk Test for Normality." (2023), [Online]. Available: <https://builtin.com/data-science/shapiro-wilk-test> (visited on 04/29/2024).
- [46] E. McCallister, T. Grance, and K. Scarfone, "Guide to protecting the confidentiality of Personally Identifiable Information (PII)," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-122, 2010, NIST SP 800–122. doi: [10.6028/NIST.SP.800-122](https://doi.org/10.6028/NIST.SP.800-122).
- [47] D. Murtezaj, "Unlocking Digital Trust: A Study of User Trust and Usability in a Digital Identity Wallet Concept," M.S. thesis, Freie Universität Berlin, 2023.
- [48] N. Naik and P. Jenkins, "Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity," in *2020 7th International Conference on Behavioural and Social Computing (BESC)*, Bournemouth, United Kingdom: IEEE, Nov. 5, 2020, pp. 1–6, ISBN: 978-1-72818-605-4. doi: [10.1109/BESC51023.2020.9348298](https://doi.org/10.1109/BESC51023.2020.9348298).
- [49] N. P. "Detailed statistics report: Qr code usage worldwide before and after covid-19." (2023), [Online]. Available: <https://www.qrcode-tiger.com/qr-code-statistics-before-and-after-covid-19> (visited on 02/02/2024).
- [50] B. Podgorelec, L. Alber, and T. Zefferer, "What is a (digital) identity wallet? a systematic literature review," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, ISSN: 0730-3157, Jun. 2022, pp. 809–818. doi: [10.1109/COMPSAC54236.2022.00131](https://doi.org/10.1109/COMPSAC54236.2022.00131).
- [51] A. Preukschat and D. Reed, *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*, 1st ed. Manning Publications, 2021, ISBN: 9781617296598.
- [52] B. Rummel and E. Ruegenhagen. "System usability scale – jetzt auch auf deutsch." (Feb. 2016), [Online]. Available: <https://community.sap.com/t5/additional-blogs-by-sap/system-usability-scale-jetzt-auch-auf-deutsch/bap/13487686> (visited on 03/04/2024).

- [53] S. Sartor, J. Sedlmeir, A. Rieger, and T. Roth, "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets," *ECIS 2022 Research Papers*, Jun. 2022.
- [54] S. Schwalm, D. Albrecht, and I. Alamillo, "Eidas 2.0: Challenges, perspectives and proposals to avoid contradictions between eidas 2.0 and ssi," in *Open Identity Summit 2022*, Bonn: Gesellschaft für Informatik e.V., 2022, pp. 63–74, ISBN: 978-3-88579-719-7. DOI: [10.18420/OID2022_05](https://doi.org/10.18420/OID2022_05).
- [55] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021.
- [56] J.-M. Seigneur and T. E. Maliki, "Identity management," in *Computer and Information Security Handbook*, Elsevier, 2009, pp. 269–292, ISBN: 978-0-12-374354-1. DOI: [10.1016/B978-0-12-374354-1.00017-0](https://doi.org/10.1016/B978-0-12-374354-1.00017-0).
- [57] M. Shafirov. "Kotlin on android. now official | the kotlin blog." (May 2017), [Online]. Available: <https://blog.jetbrains.com/kotlin/2017/05/kotlin-on-android-now-official/> (visited on 01/22/2024).
- [58] Y. Shafranovich, *Common Format and MIME Type for Comma-Separated Values (CSV) Files*, RFC 4180, Oct. 2005. DOI: [10.17487/RFC4180](https://doi.org/10.17487/RFC4180). [Online]. Available: <https://www.rfc-editor.org/info/rfc4180>.
- [59] I. Skierka, "Digitale Identitäten," in *Handbuch Digitalisierung in Staat und Verwaltung*, T. Klenk, F. Nullmeier, and G. Wewer, Eds., Wiesbaden: Springer Fachmedien Wiesbaden, 2022, pp. 1–12, ISBN: 978-3-658-23669-4. DOI: [10.1007/978-3-658-23669-4_66-1](https://doi.org/10.1007/978-3-658-23669-4_66-1). (visited on 04/26/2024).
- [60] R. Soltani, U. T. Nguyen, and A. An, "A survey of self-sovereign identity ecosystem," *Security and Communication Networks*, vol. 2021, C. Galdi, Ed., pp. 1–26, Jul. 17, 2021, ISSN: 1939-0122, 1939-0114. DOI: [10.1155/2021/8873429](https://doi.org/10.1155/2021/8873429).
- [61] S. Sousa, D. Lamas, and P. Dias, "A model for human-computer trust," in *Learning and Collaboration Technologies. Designing and Developing Novel Learning Experiences*, P. Zaphiris and A. Ioannou, Eds., Cham: Springer International Publishing, 2014, pp. 128–137, ISBN: 978-3-319-07482-5.
- [62] S. Sousa, P. Martins, and J. Cravino, "Measuring Trust in Technology: A Survey Tool to Assess Users' Trust Experiences," in *Proceedings of the International Conference on Information Systems Development (ISD)*, Aug. 2021.
- [63] F. Steiner. "Smarte eID: Online-Ausweis wegen Haushaltslage vorerst gestoppt." (Dec. 2023), [Online]. Available: <https://www.heise.de/news/Smarte-eID-Online-Ausweis-wegen-Haushaltslage-vorerst-gestoppt-9576180.html> (visited on 04/26/2024).
- [64] *Tabs - material design*. [Online]. Available: <https://m2.material.io/components/tabs> (visited on 05/10/2024).
- [65] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," 2017. [Online]. Available: <https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>.

References

- [66] "US QR code usage statistics (2019-2025)." (2022), [Online]. Available: <https://www.businessinsider.com/us-qr-code-user-statistics> (visited on 02/02/2024).
- [67] S. W. H. Young, "Improving Library User Experience with A/B Testing: Principles and Process," *Weave: Journal of Library User Experience*, vol. 1, no. 1, 2014, ISSN: 2333-3316. DOI: [10.3998/weave.12535642.0001.101](https://doi.org/10.3998/weave.12535642.0001.101).

List of Figures

1	Factors in a digital identity system according to Seigneur et al. [56] . . .	13
2	Actors in identity management according to Soltani et al. [60]	13
3	Trust triangle in SSI according to Preuschkat et al. [51]	15
4	Lissi wallet steps to add a new contact.	20
5	Lissi wallet steps to add a new digital ID card.	20
6	Lissi wallet steps to verify identity with a digital ID card.	21
7	esatus wallet steps to accept a new connection.	22
8	Steps to add a new credential to the esatus wallet.	22
9	Identity verification steps in the esatus wallet.	23
10	First setup-step, setting up an unlock mechanism for the ID-Wallet. . .	29
11	Main View of the low-fidelity prototype, also showing all identities in a tabbed view. The option to add a new identity is integrated into the main view.	30
12	Main View of the ID-Wallet demonstrator and add identity screen. . . .	30
13	Detail view of all data belonging to a digital identity. In this case, the detail view for a national ID card is displayed.	31
14	Login process after the wallet app has been suspended for more than ten minutes.	32
15	First step of the digital ID setup process.	34
16	Second step of the digital ID setup process.	34
17	Third step of the digital ID setup process, prompting the user to tap the physical ID card on the back of the device.	35
18	Fourth step of the digital ID setup process, prompting for the PIN of the ID card.	36
19	Fifth and last step of the digital ID setup process.	37
20	On-Site authentication steps in the low-fidelity prototype.	38
21	Quick QR-Code sharing option in the Android Demonstrator.	39
22	Sharing a QR-Code from the digital ID card detail view.	40
23	Scanning a request QR-Code from the main view in the Android Demonstrator.	42
24	Steps after scanning a request QR-Code in the Android Demonstrator. .	43
25	Overview of the ID-Wallet Scanner application.	44
26	Implementation of photos in the Demonstrator applications.	45
27	Front and Back of the Example German ID card used during the study.	50
28	Print-out with prompt to scan QR-Code to prepare the digital ID card for entry control as presented to study participants.	51
29	Age distribution of the participants of the study.	55
30	Occupations of the participants of the study.	56
31	Technical affinity and daily smartphone usage of the participants. . . .	56
32	SUS scores for each participant divided by group membership.	57
33	Scatter plot of SUS scores and self-evaluated technical affinity for each participant with linear regression plot of the correlation coefficient. . . .	58
34	Mean SUS score for each group with standard deviation error lines. . .	59
35	HCTS scores for each participant divided by group membership.	60

List of Figures

- 36 Mean trust score score for each group with standard deviation error lines. 61
- 37 Scatter plot of trust scores and self-evaluated technical affinity for each participant with linear regression plot of the correlation coefficient. . . . 62

List of Tables

1	SUS grading scale developed by Lewis et al. [40].	48
2	SUS scores of interest in relation to the technical affinity of the participant.	58
3	Mean SUS score for each group and overall mean SUS score.	59
4	Results of the Mann-Whitney-U Test for SUS scores between the two groups.	59
5	Mean trust score for each group and overall mean trust score.	61
6	Mean technical affinity and smartphone usage for daily tasks per group and overall.	62
7	Results of the Mann-Whitney-U test for HCTS scores between the two groups.	63

A Appendix

A.1 Study Script

Skript Studiendurchführung:

Hallo, vielen Dank, dass Sie sich die Zeit genommen haben, mich bei dieser Studie zu unterstützen. Sie helfen mir damit sehr.

Ich bin Informatikstudent an der FU Berlin. Im Rahmen meiner Masterarbeit habe ich in Zusammenarbeit mit der Arbeitsgruppe "Usable Security & Privacy" der Secure Systems Engineering Forschungsabteilung des Fraunhofer AISEC eine prototypische Anwendung namens "ID-Wallet" entwickelt, welche die digitale Verwaltung und Nutzung von Identitätskarten wie dem Personalausweis, dem Führerschein, Kundenkarten aber auch digitalen Schlüssel und Ähnlichem möglich machen soll. Diese Identitätsnachweise werden dabei zur selben Zeit auf dem Gerät gespeichert. Die prototypische Implementierung fokussiert sich auf die Nutzung der ID-Wallet mit dem Personalausweis. Die Fähigkeit, sich mit diesem Vor-Ort auszuweisen, ist dabei im Rahmen meiner Masterarbeit das hauptsächlich untersuchte Thema.

Zu Beginn werde ich Ihnen ein Smartphone mit installierter Anwendung sowie einen Musterpersonalausweis zur Verfügung stellen. Ich habe eine Liste von Aufgaben bzw. Anwendungsfällen vorbereitet, insgesamt umfasst diese Liste 3 Anwendungsfälle, die Sie durchlaufen sollen und dabei die Anwendung kennen lernen. Nach jedem Anwendungsfall stelle ich Ihnen einige Fragen, um Ihr Feedback zu der Anwendung in strukturierter Form aufzunehmen. Abschließend werde ich Ihnen einige demographische Fragen stellen. Ich würde mich freuen, wenn Sie Ihre Erlebnisse und Tätigkeiten sowie Dinge, die Ihnen auffallen, während der Durchführung laut aussprechen bzw. kommentieren. Dies wäre für meine Arbeit sehr relevant und würde mir stark helfen, die Ergebnisse besser zu verstehen und auswerten zu können. Wichtig ist hierbei, dass es darum geht, die Anwendung und nicht sie selbst zu testen. Es gibt keine falschen Aussagen oder Antworten, ganz im Gegenteil: Alles, was sie sagen oder feststellen, hilft mir, das Produkt zu verbessern.

Die Durchführung wird protokolliert und die Ergebnisse werden anonym weiterverarbeitet und innerhalb der Masterarbeit diskutiert. Sind sie damit einverstanden?

Mit Ihrem Einverständnis protokollieren wir Ihre Antworten. Diese werden anonymisiert, sodass kein Rückschluss auf Sie als Person möglich ist. Die anonymisierten Daten werden im Verlauf der Masterarbeit diskutiert und im Auswertungsprozess verwendet. Die Rohdaten werden nur von mir bearbeitet, die anonymisierten und ausgewerteten Daten werden im Rahmen der Veröffentlichung der Arbeit öffentlich zugänglich sein.

Während der Studiendurchführung werden wir eine Tonaufnahme Ihrer Kommentare, Anmerkungen und Antworten auf Fragen anfertigen.

Sie haben selbstverständlich das Recht, die aufgenommenen Daten einzusehen, zu korrigieren oder auch löschen zu lassen. Zu diesem Zwecke werde ich Ihnen abschließend meine Kontaktdaten aushändigen.

<Schriftliche Einwilligung unterschreiben lassen>

Haben Sie zum Vorgehen oder zur Verwendung Ihrer Angaben noch Fragen?

<eventuelle Fragen beantworten>

Gut, dann beginnen wir jetzt mit der Studie [starte jetzt Tonaufzeichnung].

<Studie>

Beginnen wir nun mit den Nutzungsszenarien der Anwendung. Ziel des ersten Szenarios ist es, die Anwendung kennenzulernen und sich einen ersten Eindruck zu verschaffen. Dazu bitte ich Sie, die ID-Wallet Anwendung zu starten und einzurichten. Bitte kommentieren sie dabei Ihre Schritte und Dinge die Ihnen auffallen

<Bearbeitung Szenario 1.1>

Anschließend bitte ich Sie darum, einen digitalen Personalausweis in der Anwendung anzulegen. Zu diesem Zweck verwenden Sie bitte den bereitgestellten Musterausweis **(Falls Proband zu still, erneut auffordern: Auch hierbei hilft es mir, wenn Sie dabei laut mitdenken und Ihre Eindrücke kommentieren.)**

<Bearbeitung Szenario 1.2>

- Welchen ersten Eindruck haben Sie von der App?
- Waren Ihnen die Einrichtungsschritte klar oder hätten Sie sich mehr Hilfestellung gewünscht? Wenn ja, welche Art von Hilfestellung?
- Welches Gefühl hinterlässt das Digitalisieren des Ausweises mittels der App bei Ihnen?

Sie sind zum AISEC Insider-Day eingeladen worden! Eine Veranstaltung am AISEC Institut für den wissenschaftlichen Austausch für IT-Security Interessierte und Experten. Am Eingang muss sichergestellt werden, dass Sie auch wirklich die Person auf der Einladungsliste sind. Im nun folgenden Szenario werden Sie Ihren gerade erstellten digitalen Ausweis nutzen, um sich vor Ort auszuweisen. Wie würden Sie vorgehen? **(Falls Proband zu still, erneut auffordern: Auch hierbei hilft es mir, wenn sie dabei laut mitdenken und ihre Eindrücke kommentieren.) <evtl Hinweis auf Anfrage QR-Code?>**

<Bearbeitung Szenario 2>

- War der Ablauf des Vor-Ort-Ausweisens klar oder hätten Sie sich mehr Hilfestellung gewünscht? Wenn ja, welche Art von Hilfestellung?
- Wie ist Ihr Eindruck des digitalen Ausweises im Vergleich zum physischen Ausweis? Welche Variante würden Sie persönlich bevorzugen?

Nun werden die Rollen getauscht. Sie sind jetzt mit der Einlasskontrolle zum Event beauftragt. Im folgenden werde ich mich mit meinem digitalen Ausweis aus der ID Wallet App ausweisen. Zu diesem speziellen Event sind nur Teilnehmer ab 27 Jahren zugelassen, die in Berlin oder Brandenburg wohnen. Ebenfalls liegt eine Teilnehmerliste vor, auf der die Namen der angemeldeten Personen vermerkt sind. Prüfen Sie bitte, ob ich berechtigt bin,

das Event zu besuchen. Nutzen Sie zu diesem Zweck die ID-Wallet Scanner App. (**Falls Proband zu still, erneut auffordern: Auch hierbei hilft es mir, wenn sie dabei laut mitdenken und ihre Eindrücke kommentieren.**)

<Bearbeitung Szenario 3>

- Wie ist Ihr Eindruck des digitalen Ausweises von der Seite des Prüfenden? Sehen Sie die Lösung als vergleichbar zu einem physischen Ausweis an? Bitte begründen sie Ihre Antwort kurz

Zum Abschluss habe ich einen Fragebogen vorbereitet. Der erste Teil dieses Fragebogens bezieht sich auf das zuletzt durchgeführte Szenario und beschäftigt sich mit Ihrem gefühlten Vertrauen in die Lösung des digitalen Personalausweises und das Auswerten mittels der App. Anschließend folgen Fragen zur Nutzbarkeit und Benutzerfreundlichkeit der App im gesamten. Abschließend noch einige demographische Fragen zu Ihrem Alter, Ihrem Beruf, Ihrer technischen Affinität und Ihrer Smartphonennutzung im Alltag. **<Formular aushändigen und ausfüllen lassen>**

Vielen Dank für Ihre Zeit und die wertvollen Erkenntnisse und Antworten. Würden sie für eventuelle Folgeinterviews zur Verfügung stehen?

<Verabschiedung>

A.2 System Usability Scale Questionnaire from Study

Fragebogen zur Benutzerfreundlichkeit der ID Wallet

Die folgenden Fragen beschäftigen sich mit Ihrem Vertrauen in die ID-Wallet App im Rahmen des Ausweisens Vor-Ort mittels des digitalen Ausweises in der Rolle der prüfenden Person. Bitte wählen Sie die Option, die Ihre sofortige Antwort auf jede Aussage widerspiegelt. Bitte denken Sie nicht zu lange über jede Aussage nach und stellen Sie sicher, dass Sie zu allen Aussagen eine Antwort geben. Die Fragen werden mittels einer Skala von 1 - 5 beantwortet, wobei 1 für "Stimme überhaupt nicht zu", 5 für "Stimme völlig zu" steht.

Ich denke, dass ich das System gerne häufig benutzen würde. *

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

Ich fand das System unnötig komplex. *

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

Ich fand das System einfach zu benutzen. *

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

Ich glaube, ich würde die Hilfe einer technisch versierten Person benötigen, um das System benutzen zu können. *

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

Ich fand, die verschiedenen Funktionen in diesem System waren gut integriert. *

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

A. Appendix

Ich denke, das System enthielt zu viele Inkonsistenzen. *						
	1	2	3	4	5	
Stimme überhaupt nicht zu	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Stimme voll zu
Ich kann mir vorstellen, dass die meisten Menschen den Umgang mit diesem System sehr schnell lernen. *						
	1	2	3	4	5	
Stimme überhaupt nicht zu	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Stimme voll zu
Ich fand das System sehr umständlich zu nutzen. *						
	1	2	3	4	5	
Stimme überhaupt nicht zu	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Stimme voll zu
Ich fühlte mich bei der Benutzung des Systems sehr sicher. *						
	1	2	3	4	5	
Stimme überhaupt nicht zu	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Stimme voll zu
Ich musste eine Menge lernen, bevor ich anfangen konnte das System zu verwenden. *						
	1	2	3	4	5	
Stimme überhaupt nicht zu	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Stimme voll zu

A.3 Human Computer Trust Scale Questionnaire from Study

Fragen zum Vertrauen in die ID-Wallet App

Die folgenden Fragen beschäftigen sich mit Ihrem Vertrauen in die ID-Wallet App im Rahmen des Ausweisens Vor-Ort mittels des digitalen Ausweises in der Rolle der prüfenden Person.

Bitte wählen Sie die Option, die Ihre sofortige Antwort auf jede Aussage widerspiegelt. Bitte denken Sie nicht zu lange über jede Aussage nach und stellen Sie sicher, dass Sie zu allen Aussagen eine Antwort geben. Die Fragen werden mittels einer Skala von 1 - 5 beantwortet, wobei 1 für "Stimme überhaupt nicht zu", 5 für "Stimme völlig zu" steht.

Ich glaube, dass es negative Konsequenzen haben könnte, wenn die ID Wallet zur *
Überprüfung der Identität einer Person verwendet wird, anstatt den physischen
Ausweis zu kontrollieren

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

Ich denke, dass ich vorsichtig sein muss, wenn ich die ID Wallet zur Überprüfung *
der Identität einer Person verwende, anstatt den physischen Ausweis zu
überprüfen.

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

Ich glaube, dass die ID Wallet in meinem besten Interesse handelt, wenn ich die *
Identität einer anderen Person überprüfen muss.

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

Ich bin der Meinung, dass die ID Wallet eine physische ID-Karte im Falle einer *
persönlichen Identitätsüberprüfung einer anderen Person kompetent und effektiv
ersetzen kann.

1 2 3 4 5

Stimme überhaupt nicht zu Stimme voll zu

<p>Ich glaube, dass die ID Wallet seine Rolle als Ersatz für einen physischen Personalausweis bei der persönlichen Identitätsüberprüfung einer anderen Person gut erfüllt. *</p>
<p>1 2 3 4 5</p>
<p>Stimme überhaupt nicht zu <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> Stimme voll zu</p>
<p>Ich denke, dass die ID Wallet über alle Funktionen verfügt, die ich zur Überprüfung der Identität einer Person erwarten würde *</p>
<p>1 2 3 4 5</p>
<p>Stimme überhaupt nicht zu <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> Stimme voll zu</p>
<p>Wenn ich die ID Wallet zur Überprüfung der Identität einer Person anstelle eines physischen Personalausweises verwenden würde, könnte ich mich voll und ganz auf sie verlassen *</p>
<p>1 2 3 4 5</p>
<p>Stimme überhaupt nicht zu <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> Stimme voll zu</p>
<p>Ich kann mich immer darauf verlassen, dass die ID Wallet mir genügend Informationen liefert, um die Identität einer Person zu überprüfen *</p>
<p>1 2 3 4 5</p>
<p>Stimme überhaupt nicht zu <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> Stimme voll zu</p>
<p>Ich kann darauf vertrauen, dass die Informationen, die mir die ID Wallet liefert, gültig sind und mit dem physischen Ausweis der Person übereinstimmen, deren Identität ich zu überprüfen versuche. *</p>
<p>1 2 3 4 5</p>
<p>Stimme überhaupt nicht zu <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> Stimme voll zu</p>

A.4 Demographic Questionnaire from Study

Demografische Fragen

In diesem Abschnitt werde ich Ihnen einige persönliche Demografische Fragen stellen. Die Beantwortung dieser Fragen ist freiwillig, hilft mir allerdings stark bei der Einordnung meiner Studienergebnisse.

Zu welcher der nachfolgenden Alterskategorien gehören Sie?

17 oder jünger

18-20

21-29

30-39

40-49

50-59

60-69

70 oder älter

In welchem Beruf arbeiten Sie?

Meine Antwort _____

Wie technikaffin würden Sie sich selbst einschätzen?

1 2 3 4 5

Sehr wenig Sehr stark

Wie häufig nutzen Sie ein Smartphone in Ihrem Alltag?

1 2 3 4 5

Nie Wann immer möglich

A.5 SUS Questions

- Q1: I think that I would like to use the ID-Wallet frequently.
- Q2: I found the ID-Wallet unnecessarily complex.
- Q3: I thought the ID-Wallet was easy to use.
- Q4: I think that I would need the support of a technical person to be able to use the ID-Wallet
- Q5: I found the various functions in the ID-Wallet were well integrated.
- Q6: I thought there was too much inconsistency in the ID-Wallet.
- Q7: I would imagine that most people would learn to use the ID-Wallet very quickly.
- Q8: I found the ID-Wallet very cumbersome to use.
- Q9: I felt very confident using the ID-Wallet.
- Q10: I needed to learn a lot of things before I could get going with the ID-Wallet.

A.6 HCTS Questions

- Q1: I believe that there could be negative consequences from using the ID-Wallet to verify the identity of a person instead of using the physical ID card.
- Q2: I feel I must be cautious when using the ID-Wallet to verify the identity of a person instead of using the physical ID card.
- Q3: I believe that the ID-Wallet will act in my best interest when I need to verify the identity of another person.
- Q4: I think that the ID-Wallet is competent and effective in replacing a physical ID card in the case of an on-site verification of another persons identity.
- Q5: I think that the ID-Wallet performs its role as a replacement for a physical ID card in the case of an on-site verification of another persons identity very well.
- Q6: I believe that the ID-Wallet has all the functionalities I would expect to verify the identity of another person.
- Q7: If I use the ID-Wallet to verify the identity of a person instead of using the physical ID card, I think i would be able to depend on it completely.
- Q8: I can always rely on the ID-Wallet for giving me enough information to verify the identity of another person.
- Q9: I can trust the information presented to me by the ID-Wallet are valid and match the information on the physical ID card of the person whose identity I try to verify.

A.7 ID-Wallet Android Demonstrator Source Code

The source code for the ID-Wallet demonstrator applications can be found in the FU-Gitlab under the following repository: <https://git.imp.fu-berlin.de/robiw94/wallet-prototype>. The last commit was 471f68c7 from 12.01.2024 with the hash 471f68c72107990ace8d91b551cf6c451eb463e5.