Freie Universität Berlin

Department of Computer Science

Master's Degree

Unlocking Digital Trust: A Study of User Trust and Usability in a Digital Identity Wallet Concept

Doruntina Murtezaj

5564564

Born on 12.09.1999 in Berlin

First reviewer: Prof. Dr. Marian Margraf

Second reviewer: Jun.-Prof. Dr.-Ing. Maija Poikela

Advisor: Sandra Kostic

Berlin, 11 November 2023

……

Abstract

The digital era has marked a transition in the way individuals manage their identities, with digital identity wallet apps offering a promising solution. These apps have the potential to enhance and secure personal identification and offer a convenient alternative to traditional physical documents. However, the adoption of such apps depends on user trust, a complex construct influenced by individual differences and social norms. Therefore, this thesis investigates the trust dynamics of users of a digital identity wallet, using a multiple-phase approach of user studies. The wallet app under examination is a conceptual app prototype and not a fully developed real-world application. So, the first phase of the user studies served to gather feedback from users about their behaviour and perceptions of the wallet app and formed the basis for the following phases. In the second phase, users were presented with a version of the wallet app that had been improved in terms of security measures, support and information aspects. The third phase focused only on the wallet operator. User studies include interviews and validated surveys. The Human-Computer Trust Measure and System Usability Scale surveys are used to quantify user trust and system usability. The study found that users attached great importance to factors such as security, simple design and reputation of the wallet app operator. Participants expressed higher levels of trust when they knew the wallet app operator was a government entity. Improvements in usability had a positive effect on user trust. Adding more features to the app led to a slight decrease in the usability score. Lastly, practical recommendations to increase user trust include clear instructions, improved security measures, and transparent data handling policies.

Selbstständigkeitserklärung

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, 11.11.2023

Doruntina Murtezaj

Table of Contents

1 Introduction

The introductory chapter lays the foundation for this thesis by outlining the motivations and goals of the study. It sets the stage for the following chapters and provides context for the research on user trust and usability in digital identity wallet apps.

1.1 Motivation

In today's increasingly interconnected and digital world, the use of digital identities has become pervasive across various aspects of our lives. From online banking and e-commerce to social media and government services, our digital identities are fundamental to establishing our online presence [13]. Digitalization of government services is motivated by the need to reduce lead times and improve service quality [31]. Due to its widespread applicability and considerable interest in both academic and industrial sectors, digital identity is currently a highly pertinent subject. The chart in Fig. 1 is generated from Google Trends data for the keyword "Digital Identity" for the period 2004-2023 worldwide. The axis of interest over time represents the search interest relative to the highest point in the chart for the given region and time span. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A value of 0 means that there was not enough data for that term. This trend illustrates the continuous and increasing interest in this field.

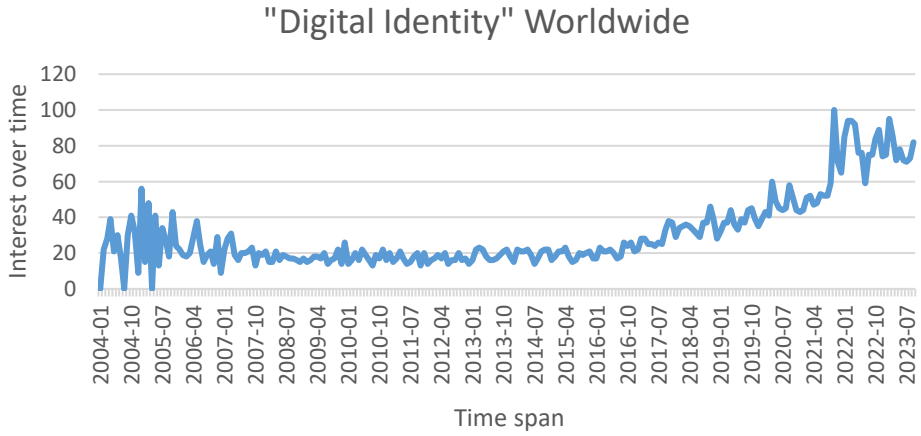


Fig. 1 Google Trends data for the keyword "Digital Identity" [18]

Digital identity fulfils several important tasks in the online landscape [14]. It provides a streamlined approach to registering with new services and eliminates the need for repeated data entry. It also serves as a secure access key to personal accounts and various digital resources. In the area of transactions, digital identity plays a central role in commitments, signing documents, and other forms of digital interaction. In addition, digital identity enables individuals to assert their rights and duties, gain access to a resource, sign up for a new service and make a commitment in a trustworthy manner. Overall, these reasons underscore the importance of digital identity in improving convenience, security, and credibility in the digital world.
However, with this reliance on digital identities comes the critical need for trust. Trust is the foundation upon which our digital interactions are built. It enables individuals and organizations to confidently engage in transactions, share sensitive information, and rely on the authenticity of digital identities [42]. When trust is compromised, the consequences can be severe, ranging from financial fraud and privacy breaches to reputational damage for both individuals and businesses. The unethical behaviour at one business school involving the submission of false data to ranking organizations severely tarnished the university's image and disappointed stakeholders' expectations, causing them to re-evaluate their trust in the institution [40]. When trust is lost, restoring it at the organizational level is a complex task [4]. Yet, despite its importance, trust in digital identities faces numerous challenges and concerns. The evolving technological landscape brings forth issues related to data security, authentication mechanisms, identity theft, and user consent. As the digital ecosystem expands, so does the need for robust and reliable trust models to mitigate these risks.

1.2 Goal

In an era characterized by the integration of digital technologies into various aspects of life, understanding the complex dynamics of user trust has become an important task. This thesis is driven by the recognition that trust constitutes a cornerstone upon which the successful adoption and utilization of digital identities are built. The overarching goal of this research is to uncover the interplay between user trust and usability of a digital identity wallet concept. The following research questions will guide this investigation:

- RQ1: What factors influence user trust in digital identity wallet applications?
- RQ2: How does perceived usability affect user trust in digital identity wallet applications?

By engaging with diverse scenarios, this thesis also seeks to find out how user trust influences decision-making processes, user behaviour, and overall digital interactions. By delving into these dimensions, it strives to make valuable contributions not only to the domain of user trust but also to broader fields such as human-computer interaction, user experience design and usable security. Moreover, recognizing the regulatory and legal implications of digital identities, this exploration aspires to provide insights that can inform the formulation of legal frameworks and regulations concerning trust. By achieving these goals, this thesis will provide stakeholders and decision makers with a solid foundation for making informed decisions in the ever-evolving world of digital interaction.

1.3 Structure of the Work

The structure of this thesis is designed to provide a broad analysis of the relationship between user trust, usability and digital identities. Beginning with Chapter 1, which outlined the motivations and goals of the study, the subsequent literature review in Chapter 2 addresses the three main concepts of user trust, usability and digital identity. The research methodology in Chapter 3 describes the prototype of the digital identity wallet app concept that is used for this thesis, the overall research design, the sample selection process, data collection and analysis techniques. The empirical analysis is part of Chapter 4 and focuses on the development of interview guidelines and surveys, and the implementation of the user studies in three phases. Chapter 5 presents the general results of the overall study and the results for each phase. Chapter 6 discusses the findings derived from the research results and interprets the results obtained in each phase. The conclusion in Chapter 7 summarizes the implications and contributions of the study, highlights the key findings and discusses the limitations. Practical recommendations for future research directions are also provided.

2 Literature Review

This chapter addresses the broader understanding of user trust, usability, and digital identities. In particular, it looks at the definition and different dimensions of user trust, examines theoretical frameworks for trust and usability, and explains important notions used in the field of digital identities. It also provides a thorough overview of existing studies related to this work.

2.1 The Concept of User Trust

The presence of trust can influence the willingness of users to embrace and incorporate technologies, thereby shaping their adoption trajectory [62]. Trust plays a central role in the field of digital identity, as it creates a sense of reliability with regard to the legitimacy of digital identities and the associated transactions. The establishment of trust encompasses diverse elements including security, privacy, accountability, and user experience [3]. Trust is also recognized as a central factor in social interactions between people, where people evaluate the reliability and credibility of the other party. Absence of trust might impede the widespread adoption and efficient utilization of digital identity systems, thereby curbing their potential advantages for individuals, organizations, and the broader society [57]. Trust is typically defined through the lens of a relationship involving a trustor, the person relying on a particular entity, and a trustee, who is the entity being trusted. Thereby, the following definitions are introduced to further elaborate this concept.

Trust as a social psychological concept refers to "the psychological state that reflects an actor's willingness to put himself in a vulnerable situation with respect to the actions or intentions of another actor without being able to directly monitor or control the other party" [36].

In the sharing economy [63], the impact of trust and reputation information on users' judgments was analysed. To accomplish this, Zloteanu et al. (2018) conducted two studies using an artificial accommodation platform that varied the amount and type of information available about hosts' digital identities. The result was that trust and reputation information significantly increased perceptions of hosts' trustworthiness, credibility, and sociability, as well as the likelihood of renting a private room in their home. These findings have important practical implications for businesses operating in the sharing economy, as they suggest that the use of trust and reputation information can improve the user experience and drive growth.

In terms of understanding partnerships between humans and automation, trust is described as "the attitude that an agent will help achieve the individual's goals in a situation characterized by uncertainty and vulnerability" [26].
In the context of digital identity wallets, trust is generally understood as the confidence that users have in the security and privacy of their identity-related data when using digital services [42]. The interpretation of trust varies depending on the target group. Trust can be delineated based on three aspects [57]: Integrity and Confidence, Ability and Competence, and Benevolence. The dimensions of credibility, integrity, ability, and confidence refer to the source of a service, while benevolence refers to consumers' perception of the provider's intentions. For this thesis, trust is defined as:

> "The willingness of the trustor to rely on a trustee to do what is promised in a given context, irrespectively on the ability to monitor or control the trustee, and even though negative consequences may occur." [3]

The definition chosen best fits the framework used for measuring trust in this thesis. When defining trust, it is important to distinguish between "trust" and "trustworthiness". "Trust" embodies the belief held by a trustor and is rooted in the attributes or traits of a trustee. Conversely, "trustworthiness" pertains to the intrinsic qualities of the trustee that evoke this belief [21]. In essence, "trust" is the trustor's perspective, while "trustworthiness" covers the objective characteristics that underpin this perception.

2.1.1 Types of Trust

Trust is a multi-layered concept that can be understood from different points of view [50]. In general, trust can be categorized into offline and online forms [6]. Offline trust pertains exclusively to individuals or organizations, whereas online trust encompasses technologies like hardware, software, the Internet, and the associated devices. Online trust evolves when individuals or organizations encounter favourable experiences during online engagements and willingly embrace the vulnerability inherent in such interactions [17].
The exploration of the types of trust encompasses technological trust, including but not limited to trust in automation, trust within human-robot interactions, and trust in automated systems. Trust is measured on the confidence an individual shows on the usefulness and security of a technology. This implies that trust can be broken down into two other broad categories [48]: usefulness and security. Usefulness refers to the extent to which a technology is perceived to be helpful or beneficial, while security

refers to the extent to which a technology is perceived to be free from errors and frauds.

It is suggested that there are three fundamental elements of trust that contribute to assessing the reliability of an interaction [27]: cognitive, emotional, and behavioural factors. These components provide a comprehensive framework for understanding the various dimensions of trust. These dimensions encompass cognitive versus affective trust, dispositional versus situational trust, and interpersonal versus system trust [21].

Within the sphere of digital identity management, trust can be broadly classified into two types: trust in the Identity Provider (IdP) and trust in the Service Provider (SP). Trust in the IdP pertains to the confidence that users have in the security and privacy of their identity-related data when stored and managed by the IdP. Trust in the SP, on the other hand, refers to the confidence that users have in the security and privacy of their identity-related data when shared with the SP for the purpose of accessing digital services [42]. Before accessing the services, users need to undergo through a successful identity verification and authentication process. Subsequently, a control party, often formed by law enforcement bodies, takes on the task of verifying identity data transactions, mainly for privacy and security reasons. The main goal of these control parties is auditing [64]. The communication process in an identity management system that includes all four entities is shown in Fig. 2.

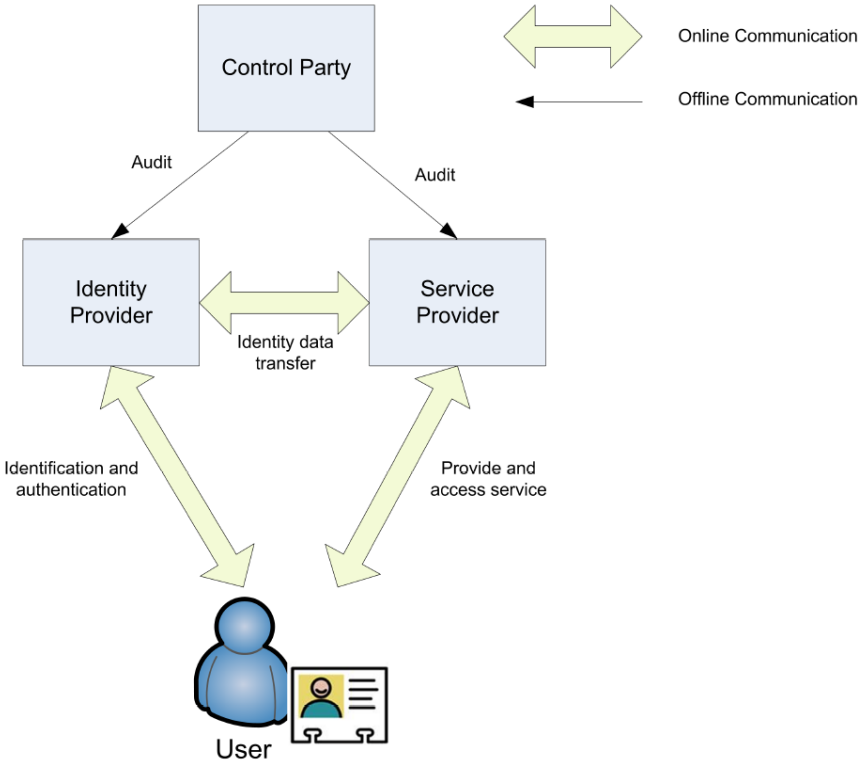


Fig. 2 Entities involved in an identity management system [64]

Based on the stage of interaction, two trust categories are identified and discussed [62]: initial trust and continuous trust. Initial trust refers to the trust that users place in service providers before they interact with them. In contrast, continuous trust refers to the trust that users gradually develop as they engage with services over a longer period of time. While many of the categorizations apply to digital identity wallet apps, this thesis focuses specifically on the trust definition within the sphere of digital identity management systems.

2.1.2 Survey Instruments for Measuring User Trust

Recent developments in artificial intelligence and machine learning applications have led to a growing interest among researchers in studying the impact of trust in technology [16]. This section explores theoretical frameworks that can be used to evaluate user trust in technology.

2.1.2.1 The Technology Acceptance Model (TAM)

A widely used theoretical framework for understanding and predicting user acceptance of technologies is the Technology Acceptance Model (TAM). It was first proposed in the late 1980s and has since been applied in a variety of contexts to explain and predict user behaviour towards different types of technology [12]. The model assumes that perceived usefulness and perceived ease of use are the most important determinants of user acceptance of technologies [11]. Perceived usefulness refers to the extent to which a user believes that a particular technology will improve their work performance or make their life easier. Perceived ease of use refers to the extent to which a user believes that a particular technology is easy to use. The model also assumes that attitudes towards using a technology are influenced by the user's beliefs about the technology, which in turn are influenced by external factors such as social norms and individual differences. The TAM has also been applied in a variety of contexts, including e-commerce [22], mobile computing [32], and healthcare [58]. Key applications of the TAM include predicting user acceptance of new technologies, evaluating the effectiveness of technology training programs, and identifying factors that may influence user acceptance of technologies. Although the TAM is widely praised, it is not without controversy because of its perceived theoretical insufficiency and limited explanatory power in complex technological environments [11].

2.1.2.2 The Human-Computer Trust (HCT)

With the rapid growth of computer and network technology, trust between humans and computers has received attention [61]. It is crucial to properly

assess the user's trust in the guidance of a machine, as an incorrect or inappropriate decision can have serious consequences for the user, especially depending on the type of task they are engaged in [33]. A meticulous approach [35] was taken to construct and validate the psychometric instrument for measuring human-computer trust. This instrument was precisely tailored to assess cognitive and affective aspects of trust in computer systems. Its high internal consistency was confirmed with a reliability score of 0.94, as measured by Cronbach's alpha. The research's findings substantiate the viability of measuring both these facets, underscoring that the affective components emerged as the most robust determinants of trust. Affective aspects in particular proved to be especially strong indicators of trust. In addition, a significant relationship was found between perceived technical competence and affective and cognitive-related trust. Interestingly, Moore and Benbasat (1991) found that perceived system reliability had an influence on affective trust but not on cognitive trust. The expected relationship between perceived system reliability and cognitive trust could not be confirmed by the results of the above mentioned study.

2.1.2.3 The Human-Computer Trust Measure (HCTM)

The Human-Computer Trust Measure (HCTM) is a trust assessment tool focused on the dynamic between humans and artefacts. This tool has been subjected to rigorous empirical research in various human-object contexts. [20] [21] [19]. The HCTM is divided into four subscales: Risk Perception, which includes three items with inverted scoring; Competence, comprising three items; Benevolence, consisting of three items; and Reciprocity, with two items. Participants are asked to assess each item using a five-point Likert scale, where 1 corresponds to "strongly disagree" and 5 corresponds to "strongly agree" [41].

The existing model of trust in technological systems, was refined by identifying the key driver constructs that predict trust, and gradually evolved toward scaling. After testing for statistical significance to determine which attributes of the HCTM predicted trust, it was decided which items should be included in the final instrument. The scale was developed and validated in two independent studies [21] using different future scenarios. The first one involved 200 participants who were asked to rate their trust in two scenarios: "Homes for life" and "New School". The second one involved 300 participants who were asked to rate their trust in four scenarios: "Smart Home", "Autonomous Car", "Online Shopping" and "Health Monitoring". In the first study, competence had the greatest influence on trust, followed by perceived risk, while in the second study, perceived risk had the greatest influence on user trust, followed by competence and benevolence. In summary, the three attributes, namely risk perception, benevolence, and

competence, exhibit statistical significance and are acknowledged as fundamental trust dimensions. The results showed that the scale has high internal consistency and reliability and can be used to assess people's trust in technical systems and to guide the development of trustworthy systems [21].

2.2 The Concept of Usability

There is a wealth of literature on trust, and research enriches our understanding by examining the relationship between trust and usability. Usability is another factor that strongly influences the use of a system and has been extensively studied in human factors research [2]. It was observed that systems with higher usability were also associated with higher levels of trust [2]. Usability is a relative concept, meaning it can be defined within specific contexts. Despite variations in definitions within the field, a notable and widely recognized description of usability comes from the ISO/IEC 25,010 2011 standard [55]. It characterizes usability as:

> "The degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use".

This definition of usability is used for this thesis because it also encompasses the aspect of user experience referred to as "satisfaction", which is an important aspect of this work. A standardized questionnaire for assessing the perceived usability of a system or product is the System Usability Scale (SUS), which is described in more detail in the following subsection.

2.2.1 The System Usability Scale (SUS)

The System Usability Scale (SUS) is a standardized questionnaire utilized for evaluating perceived usability. Originally developed by John Brooke in 1984 as part of a usability engineering program at Digital Equipment Co. Ltd (DEC), the scale has gained widespread adoption and adaptation, extending its application beyond computer systems into various contexts. The SUS has found extensive use in industrial usability studies and boasts over 5,000 citations in academic literature [28]. It comprises ten five-point items alternately framed with positive and negative tones. Respondents rate their level of agreement with each item on a scale of 1, indicating "strongly disagree", to 5, indicating "strongly agree".
To calculate the SUS score [28], the score contributions of the individual elements are first added. The score contribution for each item falls within the range of 0 to 4. For items 1, 3, 5, 7, and 9, the score contribution equals the scale position minus 1. Meanwhile, for items 2, 4, 6, 8, and 10, the

contribution is derived by subtracting the scale position from 5. Then the sum of these values is multiplied by 2.5 to get the total SUS value. To obtain a single score between 0 and 100, the average score is calculated. Higher scores indicate higher perceived usability [30]. A SUS score of 68 falls within the "C" grade range. In a typical grading system, the 50th percentile, or median, aligns with an average grade "C". The highest and lowest 15 percentile points correspond to "A" and "F" grade ranges, respectively. Furthermore, the top 15 percent of the SUS mean scores were categorized into "A+", "A", and "A-", while a similar breakdown was applied to "B" and "C" grades. It was not deemed useful to make a similar distinction for "D" and "F" grades. The Tab. 1 presents the complete curved grade scale, displaying the SUS score range for each grade alongside its corresponding percentile range.

Tab. 1 Interpreting SUS scores [30]

Grade	SUS	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

The SUS has been shown to correlate well with other subjective measures of usability. This means that the SUS can be used to compare the relative usability of different systems within the same context, or to track changes in usability over time within a particular context [7]. As a quick and reliable tool for assessing perceived ease of use, the SUS has moved beyond its original application in computer systems. Researchers have broadened its scope to retrospectively measure perceived usability across products or product categories. Ongoing research efforts on the SUS are advancing, revealing untapped potential for further exploration and filling existing research gaps.

2.3 The Concept of Digital Identity

A digital identity is a representation of an entity in a specific context [46]. While the physical identity and digital identity are distinct, the underlying principles remain consistent. The physical identity encompasses tangible

traits, behaviours, and personal details. Conversely, the digital identity comprises virtual attributes, online behaviours, elements of the physical identity, and personal information. It is imperative to safeguard both the physical and digital identities. Cameron (2005) defines digital identity as:

> "A set of claims made by one digital subject about itself or another digital subject" [9].

He also presents the Seven Laws of Identity. These laws are as follows [49]:

(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) User 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 must be guaranteed.

Remaining vigilant is essential to prevent personal information from being shared with untrusted individuals, systems, or websites [44]. Some concepts and attributes associated with digital identity are [25]:

- Identifier: An identifier comprises attributes that enable an application domain to link a declared identity to a digital entity previously recognized by the system.
- Uniqueness: An identifier is one-of-a-kind within an application domain's naming space, making it possible to directly link to a single entity within the domain.
- Authentication: Digital identity authentication involves the presentation of an identifier and digital proof of identity to confirm that the declared identity is genuine.
- Anonymity: Anonymity refers to information that cannot be used to identify the individual it pertains to, either directly or indirectly.
- Unlinkability: Unlinkability means that it is impossible to connect at least two separate pieces of information to a single individual or a group of individuals.

- Linkability: In contrast to unlinkability, linkability is the ability to trace something back to the identity of a cybercriminal or another entity.
- Pseudonymity: Pseudonymity involves information associated with a pseudonym. A pseudonym can reference a digital identity within an application domain without revealing the true identity. Unlike anonymity, linkability is possible with pseudonyms.
- Trust: Trust is a measure used by an application domain to assess the honest or dishonest behaviour of a digital identity during a transaction. This assessment reflects the domain's perception of the entity rather than the perception of other entities.
- Reputation: Multiple digital identities can interact within the same application space and rate each other after transactions to publicly assess the quality of the relationship and the service provided. These ratings contribute to the overall reputation of an entity. Entities with good reputations are preferred by others when seeking services.

A Digital Identity (DID) or Electronic Identity (e-ID) refers to the digital depiction of information associated with an individual, organization, or object [45]. It mirrors the real identity of a person or entity in the scope of computer networks. It encompasses data about individuals, organizations, or devices, serving as the virtual representation within computer networks. This information holds diverse applications, including but not limited to the verification of one's identity. As shown in Fig. 3, digital identity should manage three interconnected cornerstones [46]: usability, cost, and risk.

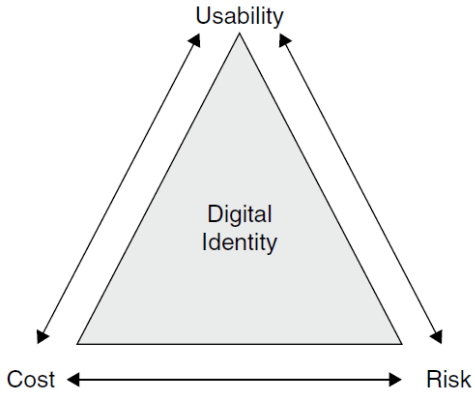


Fig. 3 Management of the digital identity environment [46]

Users need to be informed about possible security risks associated with their devices or software. Ensuring usability is equally important, as complicated systems can lead to security problems, such as users writing down passwords due to their complexity. The cost of implementing a system should be carefully evaluated in relation to risk and ease of use. For example, expensive solutions such as one-time password tokens may not be practical for large-scale deployment. Identity management has traditionally focused

on service providers' needs for cost efficiency and scalability. Thus, an identity model can be described as follows [46]:

- A user seeking access to a service.
- IdP, responsible for issuing user identity.
- SP, acting as an intermediary enforcing identity verification.
- Identity (Id), representing a collection of user attributes.
- Personal Authentication Device (PAD), a device holding multiple identifiers and credentials, often used for mobility.

The emergence of digital identity as a legal concept has evolved alongside the transition of government services and businesses to the Internet [45]. Currently, there are different types of identity management in the digital world. These include centralized identities, user-centric identities, federated identities and self-sovereign identities [52]. Self-Sovereign Identity is a new concept for digital identity management, described further in the next subsection.

2.3.1 Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) is a standard framework used to ensure sovereignty with respect to digital identity and personal data [39]. SSI is the next step in the evolution of digital identity management systems, giving users complete control over their identity and associated confidential information [36]. SSI is based on the principles of privacy, security and user control and enables individuals to use their digital identities seamlessly across different services and platforms. It allows users to independently perform operations, removing the need for authorization or involvement from a central authority or service provider and selectively disclose personal data [39]. Roles refer to the different actors in the SSI ecosystem. As illustrated in Fig. 4, SSI assumes three pivotal roles in its ecosystem: Issuer, Holder, and Verifier [56].

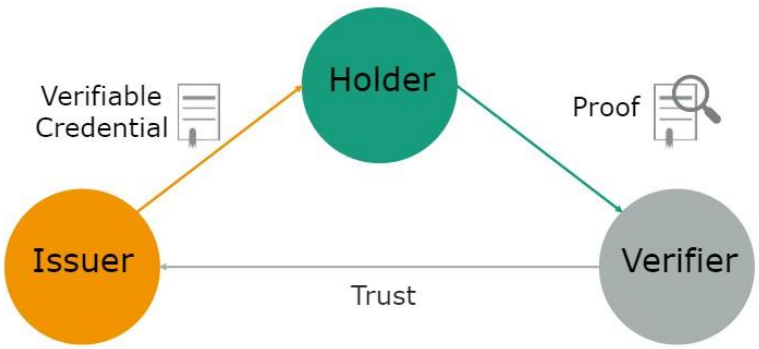


Fig. 4 Roles in an SSI system [52]

An issuer creates a credential and issues it to a holder. The holder receives the credentials from an issuer, keeps them, and passes them on to a verifier as needed. A verifier receives and verifies credentials submitted by a holder [39]. SSI stands apart from previous identity models through the utilization of innovative standards like Verifiable Credentials (VC). Verifiable credentials are digital documents that contain identity information and can be verified by third parties [52]. Such standards facilitate the creation of a cryptographically verifiable digital identity, over which the owner exercises complete control [38]. SSI also includes digital wallets and agents that help the exchange of credentials between different parties [52].

2.4 Related Work

This section reviews previous research on digital identities and analyses their results in terms of user trust and usability, where applicable. In the field of digital identity management, an identity wallet application is used to securely store various digital identities, from national ID cards to private corporate affiliations. Accordingly, a new concept for the wallet was developed and evaluated [24]. Based on the principles of user acceptance and the intricacies of the identification process, the above-mentioned study shows that participants are enthusiastic about this app concept and the sense of data control it offers. It aimed to determine the level of trust participants have in the identity wallet. Hereby, it is made clear that the core of trust lies on the chosen wallet operator. Additionally, it deepens this discourse by revealing participants' perspectives on the comparative trustworthiness of government and private companies as operators. The result is a harmonious chord among participants - an inherent trust in the wallet concept itself, but closely intertwined with the chosen operator. However, no conclusive recommendation was made for the preferred operator. It is noteworthy that this thesis uses the prototype of this concept of the identity wallet application as a basis for further study.
Other research, such as that by Gulati et al. (2019), developed and evaluated a trust scale for human-computer interactions to assess human trust in technical systems [21]. The authors aimed to improve an existing HCTM by identifying the critical driver constructs that anticipate trust and moving progressively to scale formulation. The major outcome of the above mentioned study is the introduction of a human-computer trust scale that includes four main attributes: Risk Perception, Benevolence, Competence, and Reciprocity. This scale was carefully elaborated and validated in two separate studies with different future scenarios. The results show that the attributes are consistent across both studies and have high internal consistency and reliability. The proposed scale is intended to effectively measure human trust in technical systems and provide guidance for designing reliable systems.

The study of cross-cultural measurement of perceived trust in technology is conducted using a validated questionnaire based on the Human-Computer Trust Model [50]. The study by Sousa et al. (2021) had the overarching aim of producing results applicable across various contexts, including those less explored. This design study primarily sought to assess the practical applicability of the Human-Computer Trust Scale (HCTS) in the field of design. One notable outcome of this investigation affirmed the HCTS as a valuable and user-friendly instrument for assessing users' predispositions to trust technology, spanning diverse cultural backgrounds. However, this particular study also emphasized the need for supplementary guidance in analysing and interpreting the scale's outcomes.

In the field of robotics, a framework for assessing trust in industrial Human-Robot Collaboration (HRC) was provided [10]. The research by Charalambous et al. (2016) aimed to fill the gap in trust development studies in this context and provide an assessment tool for trust evaluation. The scale was developed through a two-stage process, with the first stage involving an exploratory study to qualitatively capture participants' perspectives, followed by a confirmatory study in the second stage to validate the scale. The resulting scale includes 24 items and has demonstrated high reliability and validity.

The factors that influence user trust and flow experience are also studied in the use of mobile banking services [62]. The study further explored the interconnections among trust, flow experience, usage intention, and the tangible usage of these services. Furthermore, the study was extended to the potential impact of network externalities on the behaviour of mobile banking users and provided insights into the evolutionary nature of user behaviour through a longitudinal analysis. The findings unveiled a substantial influence of both trust and flow experience on usage intention, subsequently influencing the concrete adoption of mobile banking services. Special attention was paid to the so far little researched aspect of the influence of flow experiences on user behaviour. The article also emphasizes the importance of providing users with an engaging experience, especially given the limitations of mobile devices.

The application of IT governance trust models was addressed in the tourism sector amid the pandemic [47]. It introduces the IT Governance Trust (ITGT) model, employed to evaluate the influence of user trust on IT governance. The aforementioned research concludes that ensuring high-quality service support is imperative to offer comprehensive and up-to-date information to users utilizing tourism applications, especially in the midst of the COVID-19 pandemic. Notably, the article emphasizes the significance of qualitative validation in elucidating and contextualizing the circumstances for implementing research.

Exploring the concept of SSI as an innovative model for Identity Management (IDM) is an important research issue in the field of digital

identities [37]. SSI enables users to have complete control over their identity and securely manage their personal and confidential data [36]. The paper of Mühle et al. (2018) not only presents the essential criteria for evaluating new SSI solutions, but also conducts an in-depth analysis of two such solutions: uPort[1] and Sovrin[2]. The analysis included their architecture, components and operating mechanisms. The two solutions are evaluated against the proposed SSI specifications, highlighting their strengths and limitations. The uPort project has since split into two new projects, Serto[3] and Veramo[4], both of which aim to decentralize the Internet and return control of data to individuals. The results of that study demonstrate the potential of SSI to transform digital identity management. This requires a careful evaluation of the multiple dimensions of SSI to establish its effectiveness as an operational IDM.

In the context of the sharing economy, Zloteanu et al. (2018) conducted two studies using a simulated accommodation platform to investigate how trust and reputation information about hosts influences users' judgments. The studies [63] found that providing such information significantly improved hosts' perceived trustworthiness, credibility, and sociability and increased the likelihood that users would rent out private rooms in their homes.

Addressing the relationship between perceived trust and perceived utility in the adoption of mobile wallet technology is a fundamental research endeavour. In this context, researchers aimed to explore the mediating effect of perceived trust on the relationship between perceived usefulness and intention to use. Regarding the research findings [48], it was observed that perceived trust significantly influences a merchant's adoption of mobile wallet technology and also acts as a mediator in the relationship between perceived usefulness and their intention to use it.

[1] https://www.uport.me/ (Accessed: 26.09.2023)
[2] https://sovrin.org/ (Accessed: 26.09.2023)
[3] https://www.serto.id/ (Accessed: 25.10.2023)
[4] https://veramo.io/ (Accessed: 25.10.2023)

3 Research Methodology

This chapter begins with a detailed examination of the concept of the digital identity wallet app used in this thesis, looking at its main features. Then, it describes in detail the research design and the sample selection process. Further, it provides insight into the data collection process and analysis techniques used to gain meaningful insights from the data collected. It also includes the rationale for selecting the two main survey instruments: the HCTM and the SUS (see subsections 2.1.2.3 and 2.2.1).

3.1 Description of the Concept of the Digital Identity Wallet App

In Germany, an established solution called AusweisApp2[5] permits digital identification using the national ID card [60]. Yet, applications like AusweisApp2 demand substantial prerequisites before users can use their ID cards digitally. These prerequisites include but are not limited to activating the card for online usage and obtaining specific hardware for card reading [24].

Digital Wallets are software applications that allow individuals to store and manage their digital credentials [52]. The digital identity wallet app concept [24] used in this thesis was developed by Fraunhofer AISEC[6] as part of the ONCE[7] project funded by the German Federal Ministry of Economics and serves as the basis for this study. This digital identity wallet app is designed to revolutionize how users manage their digital identities in today's interconnected world. With the growing need for secure and convenient digital identity storage, the wallet app aims to provide users with a comprehensive solution that offers ease of use, advanced security features, and complete control over their personal information. The wallet app allows the simple and secure storage of identities in one smartphone application. The owner of the wallet has control over the stored data and can decide which exact data should be sent to a service for the requested purpose.

The wallet app concept encompasses an introduction to its features and functionalities. Existing wallets, e.g. in Germany, do not offer a combination of ID card and proof of identity. For this reason, a new concept was developed as part of the AISEC project. It supports the creation of a digital

[5] https://www.ausweisapp.bund.de/en/about-us (Accessed: 26.09.2023)
[6] https://www.aisec.fraunhofer.de/ (Accessed: 03.11.2023)
[7] https://once-identity.de/ (Accessed: 26.09.2023)

identity from the wallet itself based on the national ID card, and identities provided by other issuers such as the library card can be transferred to the wallet. The wallet app also allows for the digitization of the driver's license with the service of the driver's license authority. The wallet has several security and privacy features, including the setting of a protection mechanism to prevent unauthorized access. After the identity documents are stored in the wallet, they can be used for online identification as well as with a QR code for on-site identification. The main features of the wallet app are explained in more detail below and it is important to emphasize that all the illustrations of the wallet concept in this thesis are translations of the original German concept:

- Setting up the protection mechanism of the wallet: To avoid unauthorized entry into the wallet app, users have the option to employ their smartphone's existing unlocking method or establish a new security mechanism, which could involve a PIN, password, fingerprint, or a hybrid of fingerprint and PIN/password. The available options for the setup are shown in Fig. 5.

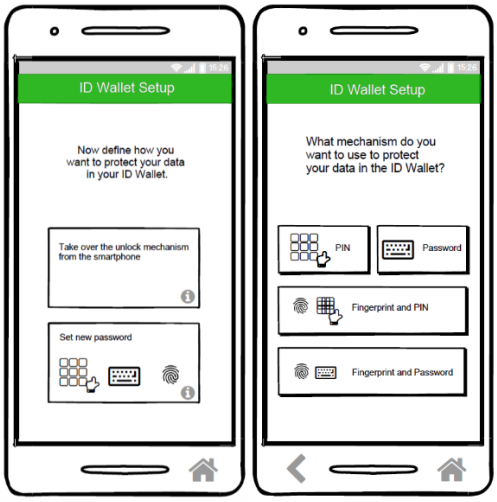


Fig. 5 Setting up the protection mechanism
(Note: The displayed screens offer selected insights into the setting up process.)

- Digitization of the national ID card: To use the ID card for identification purposes, the user has the option of converting the ID card into a digital format via the wallet app alone. To do this, the ID card is scanned via the smartphone's NFC interface and the corresponding PIN is entered. The ID is then securely stored on the smartphone via the secure element, which is a hardware-based chip on mobile devices that provides a protection against unauthorized access. At the end of this process, the ID is displayed as a card in the

wallet. The key steps in the process of creating the digital ID card are shown in Fig. 6.

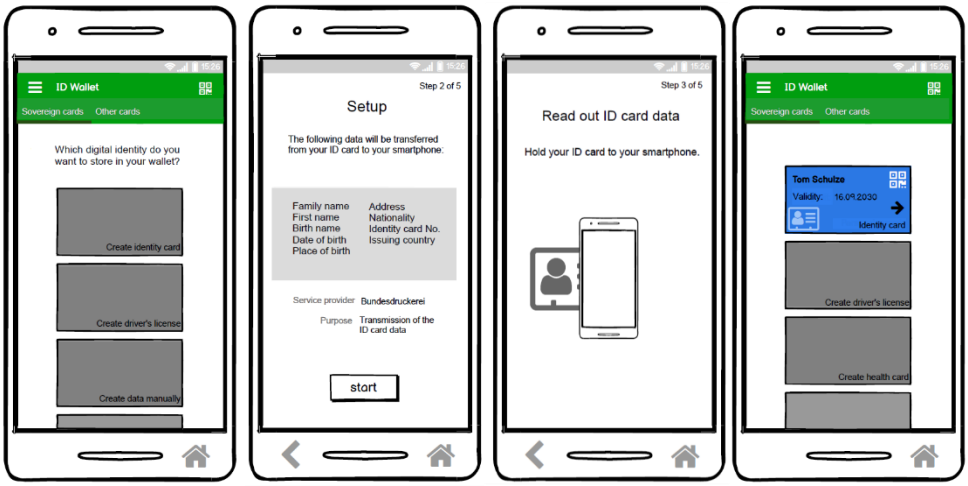


Fig. 6 Digital national identity creation
(Note: The displayed screens offer selected insights into the creation process.)

- Transferring the digital library card from the digital library to the wallet app: The wallet app can also communicate with other services that require identification. This function symbolizes the app-to-app communication feature. Users get an overview in advance of what data is specifically requested. They can add data manually and view further details about the requesting service. The data can only be sent to the service with additional consent. After successful identification, the library card can be stored in the wallet via a deep link. The key steps in the process of transferring the library card to the wallet are shown in Fig. 7.

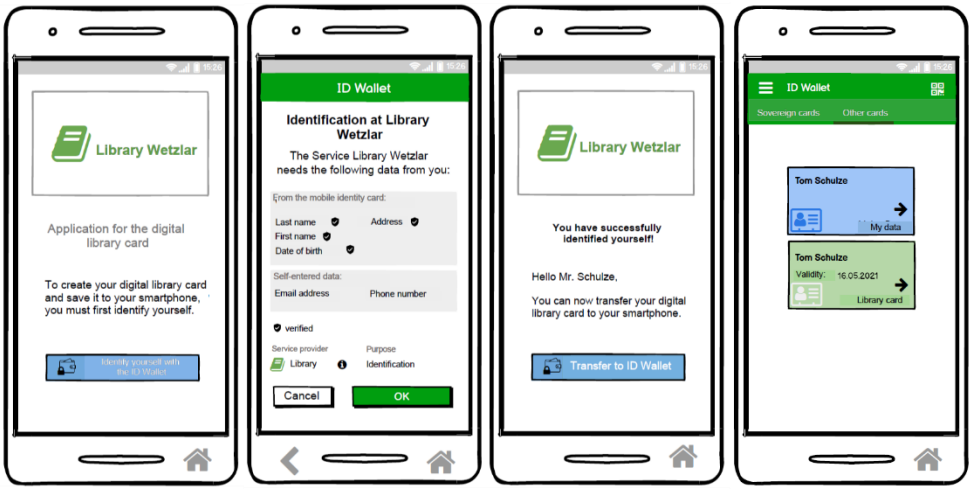


Fig. 7 Identification and transfer of a library card to the wallet
(Note: The displayed screens offer selected insights into the transfer process.)

- The creation of digital driver's license: This function represents the web-to-app communication feature. The wallet app communicates with the service via a QR code. Identification takes place with the help of the already stored national ID card. Similar to the library card, the user is given an overview in advance of what specific data will be requested and also sends the data to the service only with additional consent. After successful identification, the mobile driver's license is transferred to the smartphone. One step in the process of creating the digital driver's license is shown in Fig. 8.

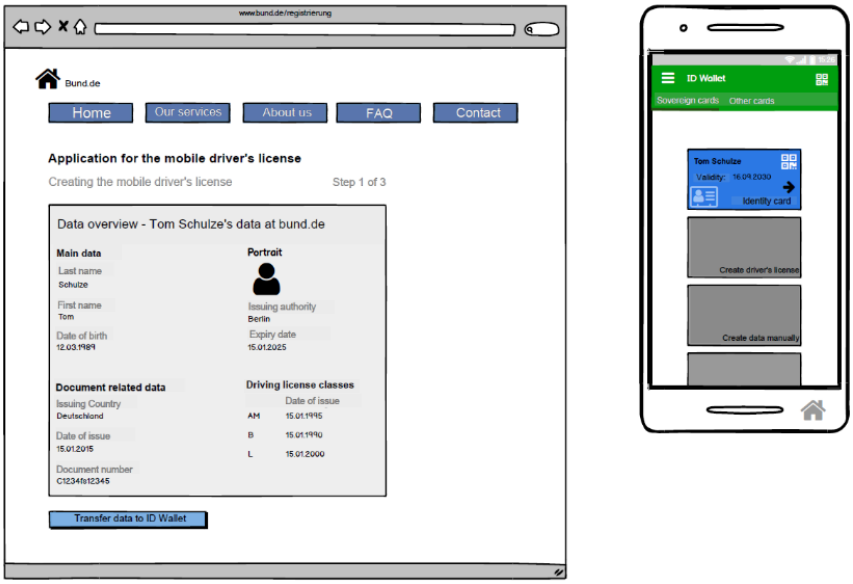


Fig. 8 Creation of the driver's license
(Note: The displayed screens show only one step of the creation process.)

3.2 Research Design

This section presents the research methodology used in this thesis to investigate the dynamics of user trust and usability in the context of a digital identity wallet application. The methodology outlines the systematic approach taken to gather and analyse qualitative and quantitative data over the course of three phases of user studies as presented in Fig. 9.

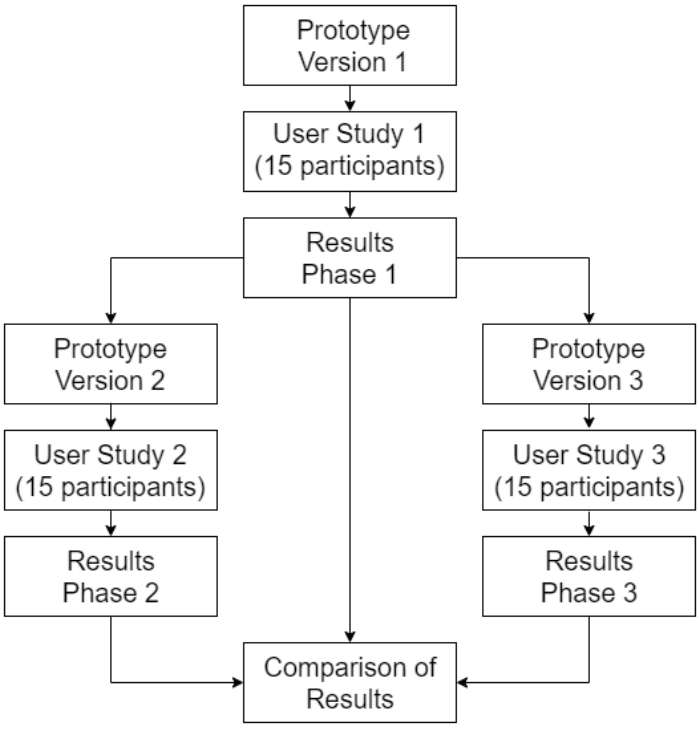


Fig. 9 Research methodology flowchart

Initially, only one phase of user studies was planned with the wallet app concept described in section 3.1. However, following feedback from the participants in the first phase, the idea arose to create a second and third version of the prototype using the first one as a basis. Therefore, this thesis includes three phases of user studies, with a different version of the prototype used for analysis in each phase. The iterative development process of the wallet app including a number of changes at each phase aimed at improving trust and usability in the second and third phase.
Each round comprised 15 participants who were part of the user studies, resulting in a total of 45 participants for the entire study. Every user study was conducted in a face-to-face format to ensure uniformity in situational conditions. The decision of having three different versions of the prototype was motivated by several key factors. First and foremost, it allowed for systematic testing of how specific alterations could impact user perceptions

of trust and usability. These variations were intentional and guided by research objectives.

For instance, several key adjustments were introduced to the second version of the prototype. This included the addition of tabs, improving user access to historical data and expired cards management. Furthermore, a comprehensive menu list was integrated, encompassing sections like History, Security, FAQ, Help, About Us, and a Rate Us feature. These updates were implemented to simplify user interactions, provide easy access to information, and boost user trust by offering robust support and accessible resources. They also provide an opportunity to assess how these elements affected user experiences and, consequently, trust levels.

A decisive change was introduced with the third version of the prototype. Here, the only difference from the first version was the inclusion of a logo that clearly identified the wallet operator as a state institution. It served as an exploratory test to determine if this visual cue had a noticeable influence on users' trust. By introducing these incremental changes, this thesis sought to enlighten the interplay between app features and trust building.

The purpose of the second and third phases is to find out if the additional features or the wallet operator will have a greater impact on trust and usability. It is worth mentioning that an important step before conducting the user studies was the translation of the prototypes. All the prototype versions of the wallet app were made available in both German and English to accommodate international participants.

The user studies consisted of qualitative and quantitative research. The qualitative aspect is represented by semi-structured interviews, wherein participants share their insights. These interviews are conducted with participants' consent and recorded to ensure accurate documentation. Each interview is transcribed and subjected to the think-aloud method. By encouraging participants to vocalize their thoughts as they interact with the digital identity system, the think-aloud method [59] offers an unfiltered view into their cognitive processes. This real-time verbalization allows to capture not only the final decisions or opinions but also the decision-making journey, uncertainties, and considerations that might not be evident solely from the final responses. On the other hand, the quantitative research study employs two surveys for evaluation, one for trust and one for usability, providing a structured approach to gather data and assess participants' responses.

In the initial phase (see subsection 4.2.1), participants evaluated the first version of the prototype described in section 3.1. Their interaction was guided by an interview sheet containing tasks and open-ended questions. The tasks aimed to explore the app's features, while the open-ended questions sought participants' opinions to enhance the prototype's initial version, leading to its evolution into the second and third version.

Additionally, participants were asked to complete two questionnaires, the HCTM (see subsection 2.1.2.3) and the SUS (see subsection 2.2.1), both utilizing Likert scale responses.
Subsequently, the second phase (see subsection 4.2.2) of user studies involved testing the updated prototype's second version. In this iteration, user ideas and suggestions for improvement from the first phase were taken into account to enhance both the level of trust and the usability of the system. Additional features were implemented in the prototype and additional tasks were added to the interview sheet to test the new features accordingly. The assessment in this phase involved a concise interview, focusing solely on interaction tasks within the app and excluding open-ended questions. This change was made in anticipation of the third phase, which was to be based on the results of the first phase and not on those of the second phase. The two questionnaires for the evaluation process remained the same.
In the third and final phase (see subsection 4.2.3), the prototype from the initial phase served as the foundational model, enhanced by the integration of supplementary details concerning the wallet's operator. This augmentation was manifested through the inclusion of a pertinent icon strategically placed on relevant prototype pages. Participants were asked to complete the same tasks as in the first phase, and noteworthy is the omission of open-ended questions due to this phase concluding the research. The administration of the HCTM and SUS questionnaires (see subsections 2.1.2.3 and 2.2.1) marked the end of the user study in this phase, remaining consistent across all study phases.
The outcomes of each phase were initially analysed in isolation. After completing all three phases, a comprehensive comparison was carried out in order to formulate conclusive results for the entire research study. This methodological framework seeks to explore users' perceptions, behaviours, and experiences, and to decipher the complex facets of user trust related to the adoption and use of digital identity wallet apps. Ethical considerations such as informed consent, validation efforts, and potential limitations are also addressed to ensure transparency and rigor in the research process.

3.3 Sample Selection

The participant selection process for this thesis employed a purposive sampling method, chosen for its alignment with the study's specific objectives. This approach facilitated the targeted selection of individuals who are well versed in digital identity management and ensure a comprehensive understanding of the subject matter.
The target population consisted of professionals deeply engaged in sectors heavily reliant on digital identity technologies. This encompassed fields like computer science (12 participants), finance (8 participants), healthcare (6

participants), e-commerce (5 participants), law (4 participants), psychology (4 participants), language and communication (3 participants), and education (3 participants). This eclectic composition aimed to capture a comprehensive spectrum of digital identity perspectives across diverse sectors and disciplines.
Inclusion criteria specified that participants should hold at least a bachelor's degree in their respective fields, ensuring the collection of informed insights and feedback from individuals with the necessary educational background. The participant pool spanned educational levels, including master's and doctorate degrees, offering a comprehensive representation of expertise.
Participants were recruited through different approaches that relied on industry-specific online forums, professional networking events, and direct invitations through friend referrals. This diverse approach contributed to securing a well-rounded and varied participant group.
In an effort to strike a balance between achieving depth of insights and ensuring practicality, a sample size of 45 participants was deemed appropriate. This number aimed to ensure a thorough exploration of perspectives while maintaining manageable levels of data collection and analysis.

3.4 Data Collection Methods

This section provides insight into the rigorous techniques used to collect data for this thesis. It also focuses on the justifications for selecting the two survey instruments, the HCTM and the SUS.

3.4.1 Data Analysis Techniques

The data analysis techniques employed in this study encompass a mixed approach, integrating both qualitative and quantitative methodologies. For the qualitative aspect, thematic analysis is utilized to extract patterns, themes, and underlying meanings from the transcribed interviews. This process involves identifying recurring concepts, organizing data into categories, and interpreting the significance of these themes in relation to the research objectives.
On the quantitative front, statistical analysis is employed to quantify and analyse the survey responses. The TrustedUX[8] survey system was used to measure user trust. The survey system uses the validated HCTM with nine items (see section *The Research Questionnaires*) to measure technology trustworthiness. The HCTM is designed to assess trust across three dimensions: risk, benevolence and competence [21]. The final score is then

[8] www.trustux.org (Accessed: 26.09.2023)

analysed to provide an overall measure of trustworthiness. The system has demonstrated its value as a tool for investigating and mapping trust behaviour towards technology [51]. The survey tool is designed to be simple and user-friendly so that it can be shared with users by designers and stakeholders. In addition, the survey system can be supplemented with other evaluation techniques such as usability testing to gain a comprehensive understanding of users' trusting interactions with the technology. The SUS questionnaire has 10 items (see section *The Research Questionnaires*). The calculation process for the SUS score involves several steps (see subsection 2.2.1) and it results in a score range of 0 to 100, providing a standardized gauge of usability perception [7]. The responses were collected through Google Forms[9] to mitigate the possibility of errors stemming from manual data entry.

Descriptive statistics provide an overview of participants' perceptions, while inferential statistics, such as correlations, enable the exploration of relationships between variables. Descriptive statistics methods are analytical techniques used to summarize and describe the key characteristics of a dataset. These methods provide a clear overview of the characteristics of the data and help to understand the central tendencies, variability, and distribution of the data. Common descriptive statistics include measures such as [34]:

- Mean: The mean, also known as the average, is calculated by adding up all the values in a dataset and then dividing by the number of values. It gives you a sense of the central tendency of the data.
- Median: The median is the middle value of a dataset when it is ordered from lowest to highest. It is not affected by extreme values and provides a robust measure of central tendency.
- Mode: The mode is the value that appears most frequently in a dataset. It can help identify the most common value or category in the data.
- Standard Deviation: The standard deviation measures the amount of variation or spread in a dataset. A higher standard deviation indicates greater variability, while a lower one indicates more consistency.
- Variance: The variance is the average of the squared differences from the mean. It is a measure of how much the values in a dataset differ from the mean.

[9] https://www.google.com/forms/about/ (Accessed: 27.09.2023)

- Range: The range is the difference between the maximum and minimum values in a dataset. It provides a simple measure of the spread of data.
- Percentiles: Percentiles divide a dataset into 100 equal parts. The nth percentile is the value below which n percent of the data falls. For example, the 25th percentile, also known as the first quartile is the value below which 25% of the data falls.

Inferential statistics involve using sample data to make inferences or draw conclusions about a larger population. Correlation is one of the inferential statistics methods [54]. A correlation matrix is a table that displays the correlation coefficients between multiple variables in a dataset. It is a way to summarize the relationships between pairs of variables and thus quickly see how strongly and in which direction the variables are related. In a correlation matrix:

- Each row and column represents a variable.
- The diagonal cells contain the correlation of a variable with itself, which is always one.
- The off-diagonal cells contain the correlation coefficients between pairs of variables.

Correlation coefficients can range from -1 to +1:

- +1 indicates a perfect positive correlation, meaning the variables increase together.
- -1 indicates a perfect negative correlation, meaning one variable increases as the other decreases.
- 0 indicates no linear correlation between the variables.

Researchers and analysts use correlation matrices to identify patterns, determine the strength and direction of relationships, and guide further analysis or decision-making.

3.4.2 Reasons for Choosing HCTM

Choosing the HCTM as a framework for this thesis is a prudent choice for several compelling reasons. First and foremost, the HCTM is purpose-built to gauge users' confidence in information and communication technologies, directly aligning with the research objective of evaluating trust within the

context of a digital identity wallet. Leveraging this scale offers a structured approach to measure users' perceptions of the wallet's trustworthiness, reliability, and other key dimensions pertinent to the investigation.
Importantly, the scale's established framework can expedite the research process. It provides a validated and proven foundation, negating the need to construct a questionnaire from scratch. This is particularly advantageous, as the scale has been employed across diverse research scenarios, ensuring that the findings can be seamlessly compared to existing research results, thus enhancing the credibility and robustness of the thesis [33].
A notable benefit of using this scale lies in its likely validation history. Past research likely subjected the scale to rigorous validation processes, affirming its reliability and validity [61]. This not only fortifies the quality of the study but also strengthens the academic rigor of the work.
Given the multifaceted nature of trust in digital identity systems, the scale's comprehensive coverage of various dimensions, including risk, benevolence, and competence, can yield insights into users' perceptions of the wallet app. This is particularly valuable as the assessment of trust within digital identity systems demands an in-depth understanding of users' cognitive and emotional perspectives [21]. So, by using the HCTM as the basis for the study, a reputable and recognized tool [41] is used to examine the dynamics of user trust in the space of digital identities.

3.4.3 Reasons for Choosing SUS

The SUS emerges as a well-suited choice because it circumvents respondent fatigue and maintains engagement. Another key advantage is its efficiency and broad applicability, adaptable to various systems and products. Furthermore, the SUS's standardized scoring mechanism presents a clear advantage, enabling direct comparison of usability perceptions not only within a single wallet but also across different wallet designs or versions [8]. This becomes particularly relevant when aiming to discern which specific design elements foster heightened usability and subsequently impact user trust.
The robust psychometric properties associated with the SUS confer credibility to research findings. Its well-established reliability and validity enhance the integrity of conclusions drawn from the survey results. It can be used with confidence on both large and small sample sizes [23]. Moreover, the SUS's deliberate focus on user perceptions aligns seamlessly with the exploration of the intertwined relationship between usability and user trust. Since trust often hinges on subjective perceptions and emotional responses to a system, the SUS's emphasis on user experience resonates effectively with the investigation of this interplay.

A significant advantage of the SUS lies in its holistic approach to usability assessment. Rather than fragmenting usability into isolated components, the SUS encapsulates overall usability perception [28].

The SUS's popularity in usability research also offers the benefit of comparability with existing studies. Beyond its quantitative score, the SUS's individual items serve as probes, spotlighting specific usability pain points that warrant attention. This feature fits seamlessly into a user-centric approach and yields practical recommendations to improve the system's usability [5]. However, while the SUS offers a powerful framework, its insights can be enriched when paired with other methods such as qualitative interviews or usability testing scenarios [29].

4 Empirical Analysis

This chapter explores the empirical analysis that forms the core of this thesis. It begins with the detailed process of the interview development and the design of the surveys. The conduction of the user studies, which spans three distinct phases, is closely revealed, offering insights into how user trust and perceptions evolve over time.

4.1 Interview Development and Survey Design

In line with established best practices [53], it was essential to avoid common pitfalls in the interview and survey design. This involved refraining from leading respondents towards specific answers, crafting clear and unambiguous questions devoid of technical jargon, and maintaining simplicity to prevent complexity from hindering comprehension. Duplicate questions referring to multiple questions at the same time were avoided, as were negative or double-negative phrases that might confuse participants and jeopardize the overall user experience. The final version of the interview was a result of several drafts. The interview needed to capture all relevant aspects of the wallet, striking a balance between scope and participant comfort. In each round of the user studies, a set of three pilot interviews was executed to assess the interview process and facilitate any necessary refinements. The interview sheet began with a brief introduction, explaining the objectives of the study and outlining the subsequent interview process. The sheet served as a discussion guide and helped facilitate the semi-structured nature of the interview by allowing follow-up questions based on the interviewees' responses.

The interview comprises three sections. In the first section, participants are tasked with activities associated with specific functions within the wallet app. Successful completion of these tasks involves setting up the wallet's protection mechanism, digitizing a national ID card, conducting the identification process using stored identities, and transferring identities from an issuer. These tasks were designed to familiarize users with the wallet app.

The second section encompassed 18 open-ended questions, organized into six categories, each containing three questions. An example of each category of questions is shown in Tab. 2. The goal of developing these questions was to collect feedback from users after their first interaction with the app. This feedback should then be used for the next phases of the user studies.

Tab. 2 The categories of the interview questions

1. Overall Experiences	Which aspects of this app impressed you the most and which disappointed you?
2. Functionality and Features	What features or functions did you find particularly useful or lacking?
3. Usability	What difficulties or confusion did you encounter while using this app?
4. Visual Design	How would you rate the visual design of this app, e.g. aesthetics, layout, colour scheme? (1 - very dissatisfied; 5 - very satisfied)
5. User Trust	This app can be operated by the state or by a private company. Who would you rather trust with your data and why?
6. User Feedback and Preference	What would you like to add, change, or remove from this app to better meet your needs and improve your experience with the app?

The third and final section guided participants to complete two surveys: the first one gauged their trust in the system, while the second assessed the system's usability. Instructions on how to complete the questionnaire were meticulously formulated to be explicit, clear, and polite, emphasizing the importance of user comfort and understanding. Moreover, careful attention was paid to guaranteeing that all categories within rating scales were mutually exclusive when a single response was required. Participants were encouraged to use the think-aloud method [59] to express their thoughts at different stages of the interaction. With their consent, these sessions were recorded to ensure accurate documentation and then transcribed for further analysis.

4.2 Implementation of the User Studies

The user studies were systematically carried out in three phases. The overarching methodology remained consistent across the phases. However, to enhance the study's effectiveness, the prototype and interview sheet were tailored based on the insights garnered from the initial phase. This iterative approach ensured that the subsequent phases were more finely tuned to the participants' experiences and requirements. Furthermore, the interview and surveys underwent rigorous piloting, involving a select group of individuals closely resembling the target sample. This process served as a valuable quality assurance step, highlighting any potential ambiguities or shortcomings in the user studies design. Throughout the user studies, participants had the freedom to inquire or pause the process at any point. This approach was instrumental in crafting a research instrument that met the standards of clarity, user-friendliness, and data integrity.

4.2.1 Phase One

The initial phase of the user studies focused on laying the foundation for the investigation of user trust and perceptions of usability in the context of digital identity. This phase used the first version of the prototype as described in the section 3.1 and involved establishing baseline data, assessing user attitudes, and identifying key themes. The user studies were conducted in the form of a semi-structured interview that began with an introductory section explaining the purpose of the interview and obtaining respondents' consent to participate. The respondent had the opportunity to choose between the German and the English version of the prototype. The procedural framework for this initial phase closely aligns with the one outlined in the research design (see section 3.2). To familiarize themselves with the app's functionalities, participants were asked to complete the following four tasks:

Task (1): Setting up the app;
Task (2): Creation of a digital identity card;
Task (3): Registration to the library app;
Task (4): Creation of a digital driver's license.

The task descriptions were enriched with explicit explanations to guarantee user clarity regarding the upcoming steps. To enhance comprehension, certain explanations were further elucidated with real-world use cases as illustrations. In order to accomplish the tasks, users alternated between the interview sheet to review the task description and the prototype to engage with the app. The second section introduced open-ended questions, structured into six categories:

(1) Overall Experience;
(2) Functionality and Features;
(3) Usability;
(4) Visual Design;
(5) User Trust;
(6) User Feedback and Preference.

Each category comprised three questions. These inquiries were employed as a means to delve deeper into users' perspectives regarding the wallet app, their grasp of its underlying concept, and their level of trust in the application. The user study ended with the completion of the two questionnaires HCTM and SUS on trust and usability, respectively. In this final part, respondents were granted privacy and autonomy as they engaged with the surveys, without any direct observation. Unlike the interactive tasks

and open-ended questions, this part did not involve active discussion, unless a participant specifically sought clarification or assistance. The entire interview sheet can be found in the appendix (see subsection *The Research Interview Sheet).*

4.2.2 Phase Two

In this phase, the most important feedback from the initial phase, which is discussed in subsection 5.2.1, is incorporated into the prototype and then subjected to further testing. Pertinent feedback in this context encompasses suggestions and ideas frequently emphasized by respondents and deemed technically feasible. Participants in the first phase expressed the need for a more comprehensive view of their digital identity history, which included expired cards. This change aimed to provide users with a more complete and transparent understanding of their digital identity within the wallet app. Similarly, the expanded menu list was introduced based on user recommendations. Participants emphasized the importance of having easy access to information about the application's security measures, frequently asked questions, assistance, and details about the operator of the wallet. Therefore, the main reason for developing the second version of the wallet app was to address these findings by adding the following features:

- The "Expired Cards" tab: The "Expired Cards" tab displays a list of cards, including national ID cards and others, that have reached their expiration date. This section provides an overview of cards that are no longer valid, helping users keep track of outdated identification documents. If there are no expired cards stored in the app, a message, as shown in Fig. 10, will be displayed.

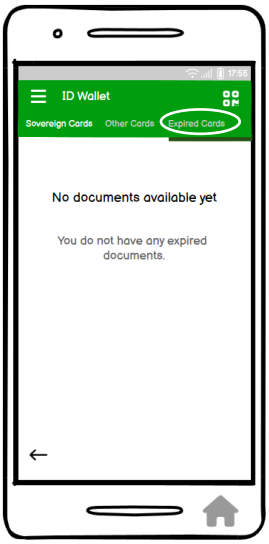


Fig. 10 Screen after clicking on the "Expired Cards" tab

- The Menu List: The menu list is a user interface element that displays a list of options when clicked. It allows users to access a variety of functions and navigate to different sections of the app. The menu list of the wallet app contains seven active menu items.

  (1) The "My ID Wallet" feature (screen a) of Fig. 11) is the first and takes the user back to the home screen.
  (2) The "History" feature (screen b) of Fig. 11) serves as a comprehensive log that records all interactions and transactions with cards stored in the app. This log also includes the app-to-app and web-to-app communication, giving users a detailed overview of their card-related activities and interactions with external platforms. If there are no interactions, a message is displayed that no history is available yet.
  (3) The "Security" feature (screen c) of Fig. 11) includes several important functions to improve data protection and user control. Users have the option to enable or disable screenshot mode to protect their data from unauthorized access. Also, users can change the wallet protection mechanism if they know the previous one. In addition, the feature allows for a complete data wipe, where all stored information within the app is deleted and a restart is initiated.
  (4) The "Frequently Asked Questions (FAQ)" page (screen d) of Fig. 11) is a helpful section within the app that addresses common user questions and concerns. It provides concise answers and explanations to a number of typical questions, helping users navigate the app and better understand its features. This section is designed to provide quick solutions and valuable insights to make the user experience seamless and informative.
  (5) The "Help" feature (screen e) of Fig. 11) is a comprehensive support hub within the app, offering various avenues for users to seek assistance and guidance. It includes options for users to contact the app's support team through voice calls, video calls, or email, allowing for real-time communication and personalized assistance. This screen is designed to cater to users' needs when they require direct help or have specific inquiries that extend beyond the FAQ section.
  (6) The "About us" feature (screen f) of Fig. 11) serves as a section within the app where users can access detailed information about the app's background, mission, and values. Additionally, this page prominently features the app's privacy policy, providing insights into how user data is collected, used, and protected. Among other points, this section explicitly states that no cookies are used when

using the app. It aims to enhance transparency and build trust by clearly articulating the app's commitment to user privacy and data security.

(7) The "Rate us" feature has been integrated to collect user feedback and ratings regarding the application's performance and functionality. Users are provided with the option to assign a star rating, with five stars representing the highest level of satisfaction. Furthermore, a comment section is available, allowing users to provide more detailed feedback or suggestions.

The main screens showing the menu items are summarized in Fig. 11.

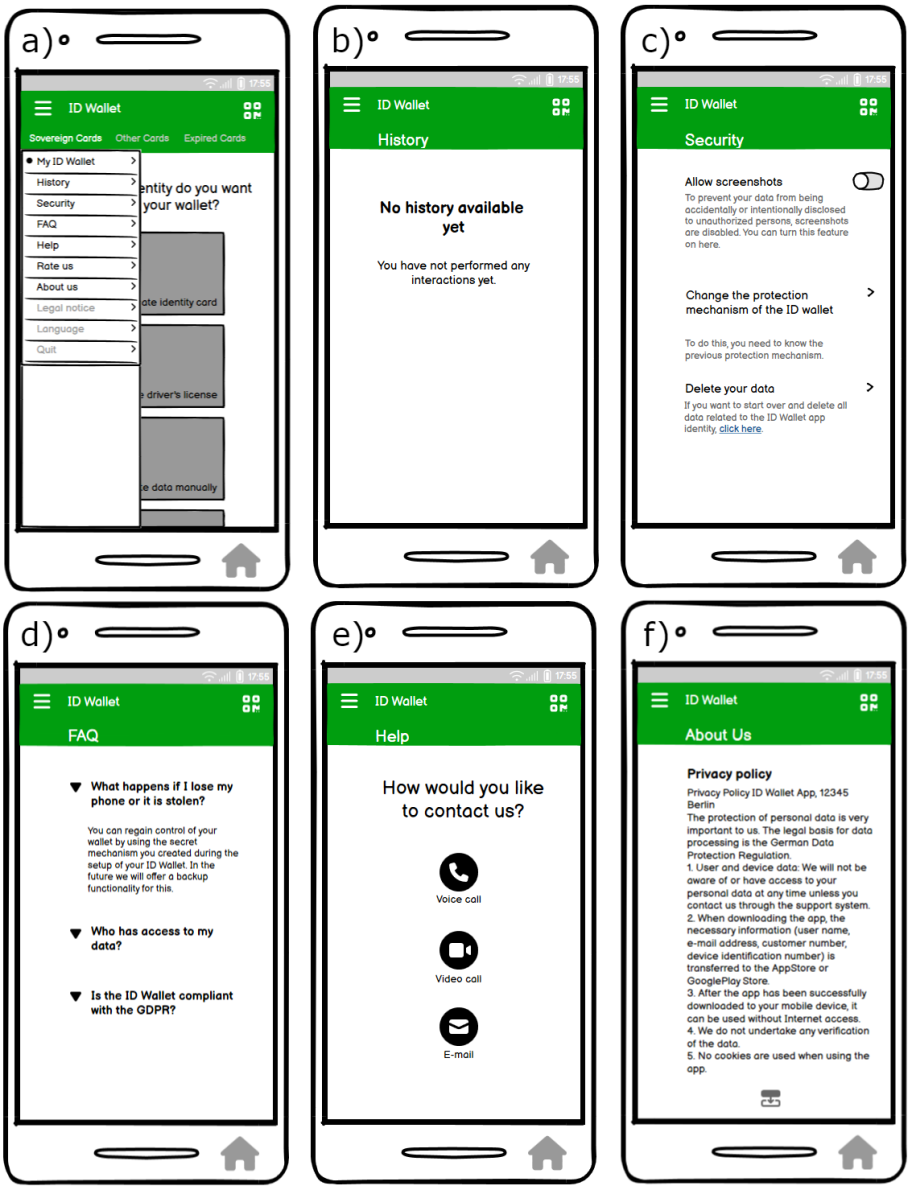


Fig. 11 The menu list functionalities
(Note: The displayed screens show only highlights of the menu list functionalities.)

Combined with the user-friendly menu and feature-rich options, the wallet app should be even more intuitive and trustworthy for digital identity management at this stage. Balsamiq[10] is a widely-used wireframing and prototyping tool [15] that was instrumental in editing the prototype of the wallet app to incorporate the new features. Balsamiq provides a user-friendly and intuitive platform for creating low-fidelity wireframes and interactive prototypes. It is known for its simplicity, allowing to quickly sketch out and visualize the layout, structure, and functionality of the product [43].
The interview sheet in the second phase contained only user tasks and the surveys. The tasks from the first phase were retained and supplemented by an additional task targeting the new functions of the app. This task focuses on guiding a new user of the wallet app to explore and understand its menu items, addressing various scenarios like checking card expiration, accessing recent actions, seeking customer support, changing protection mechanisms, and understanding data policies. The objective of this phase was to assess the impact of the prototype refinements on trust and usability. By excluding the open-ended questions, the focus was on optimizing the duration of the user study and gathering only essential data for further analysis.
This phase also ended with the completion of the SUS and HCTM questionnaires. Since questionnaires do not provide insight into the reasons for participants' responses, the completion of questionnaires was closely monitored. To gain a deeper understanding of the users' assessments, the questionnaires were supplemented with additional "why" questions. These questions were intended to stimulate discussion and elicit the specific reasons for the participants' decisions.

4.2.3 Phase Three

The third phase of this thesis focuses on the significance of the operator of the wallet, in this case the state. This phase also builds on the feedback collected in the first phase, which is summarised in subsection 5.2.1, and uses the prototype developed in the first phase as its basis. The feedback received clearly showed that the majority of participants preferred the state as a potential operator of the wallet. Participants expressed concerns about trust and transparency, particularly regarding the operator's identity. To address this concern and improve user trust, the prototype in this phase includes an essential addition: it prominently displays the wallet operator's identity as the state, indicated by the inclusion of the logo of a state institution. This visual cue was implemented to reinforce user trust, as users demonstrated a preference for government-backed identity management solutions. This modification aims to evaluate how users' perceptions of the

[10] https://balsamiq.com/ (Accessed: 26.09.23)

digital wallet are influenced when they are explicitly informed that the wallet operator is a governmental entity. The logo of the Federal Ministry of the Interior and Community, as depicted in the second screen of Fig. 12, was incorporated into the prototype. The decision to integrate this logo is based on the fact that this authority is responsible for the electronic identification with the German identity card[11].

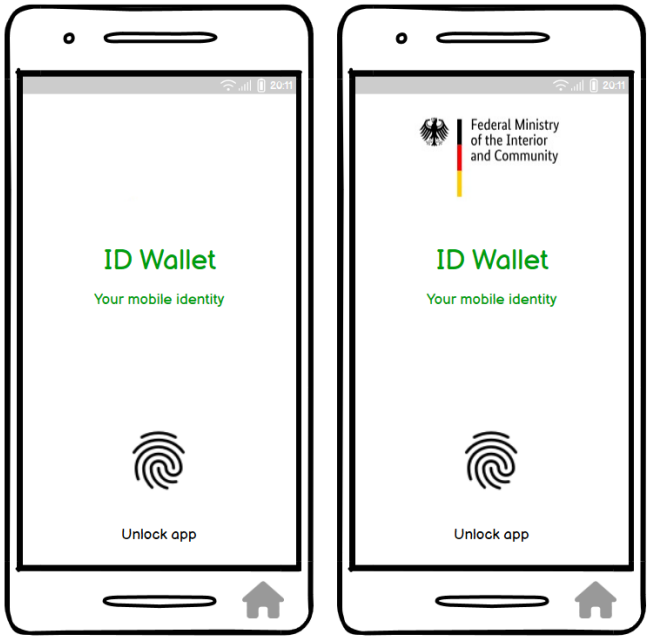


Fig. 12 An example of a screen before and after the state as the wallet operator

The interview sheet retained the identical set of tasks that were initially presented in phase one (see subsection 4.2.1). Notably, the open-ended questions were also omitted in the third phase. Furthermore, the same questionnaires, specifically the SUS and HCTM, were utilized, maintaining consistency with the previous two phases. In line with the methodology introduced in phase two (see subsection 4.2.2), the process of completing these questionnaires was enhanced by supplementing them with "why" questions. This addition was introduced to stimulate discussion and gather deeper insights into the reasons behind participants' assessments.

[11]https://www.personalausweisportal.de/Webs/PA/EN/citizens/electronic-identification/electronic-identification-node.html (Last visited: 10.09.2023)

5 Results

This chapter is dedicated to the presentation of the results of this work. In addition to the overall results, the results from each phase of the study are presented separately in detail. The results of this thesis have significant implications for the development and improvement of digital identity wallet applications.

5.1 Results of the Entire Study

The insights gathered from all phases of the user studies offer a comprehensive understanding of user perceptions and experiences with the wallet app. The participant pool of 45 individuals was evenly distributed across the three phases of the user studies. Each phase therefore comprised 15 participants. The distribution of gender and age in each phase is shown in Fig. 13, Fig. 14, and Fig. 15, respectively.

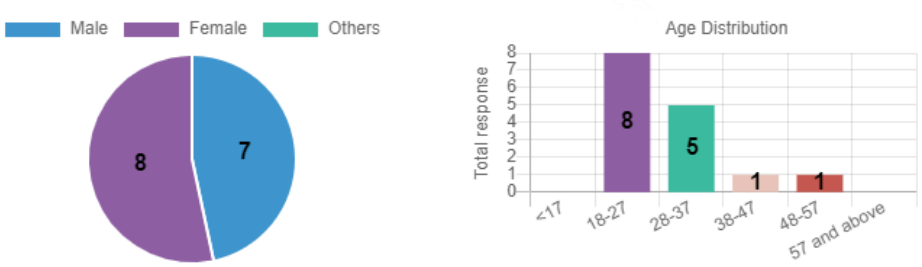


Fig. 13 Gender and age distribution of the first round of the user studies

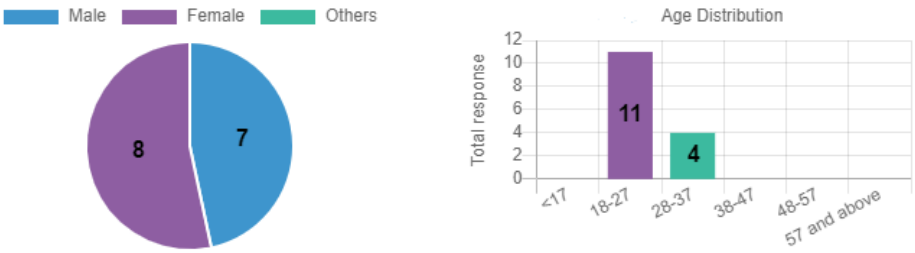


Fig. 14 Gender and age distribution of the second round of the user studies

Fig. 15 Gender and age distribution of the third round of the user studies

Participants were almost equally divided between two genders and spanned an age range of 18 to 57 years. There were 32 people in the 18 to 27 age group in the sample, making them the majority.
All participants had an overall positive experience with the wallet app. They highlighted the importance of including essential cards, such as ID cards and driver's licenses. They also suggested the addition of other type of cards, such as credit cards for greater versatility. Among the 45 participants, 30 believed that their data was well-protected. Disabling screenshots by default was seen as a security-enhancing feature. Despite positive feedback, users also provided constructive suggestions for improvement. These included implementing extra security measures, such as identification via webcam when using the app for the first time. The diagram in Fig. 16 visually summarizes participants' agreements on some discussed topics, displaying the number of participants concurring with each statement.

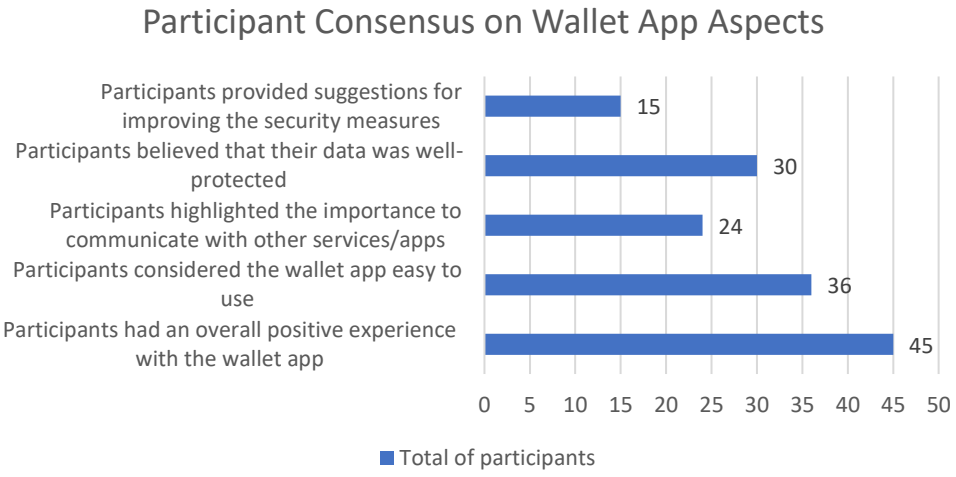


Fig. 16 Highlights of the general research findings

The overall trust scores obtained through the HCTM in three distinct phases of the study, are presented in Tab. 3. The scores are measured on a scale from 0 to 100, with higher scores indicating greater satisfaction. Compared to the first phase, the value increased in the second phase and peaked in the third phase at 82.3%.

Tab. 3 Average trust scores across phases

Phase	Overall Trust
1	76.3%
2	79.6%
3	82.3%

The average SUS scores for each phase are shown in Tab. 4. There was a slight decrease in the second phase compared to the first. The maximum value of 90.33 was reached in the last phase.

Tab. 4 Average usability scores across phases

Phase	Overall Usability
1	90.00
2	88.00
3	90.33

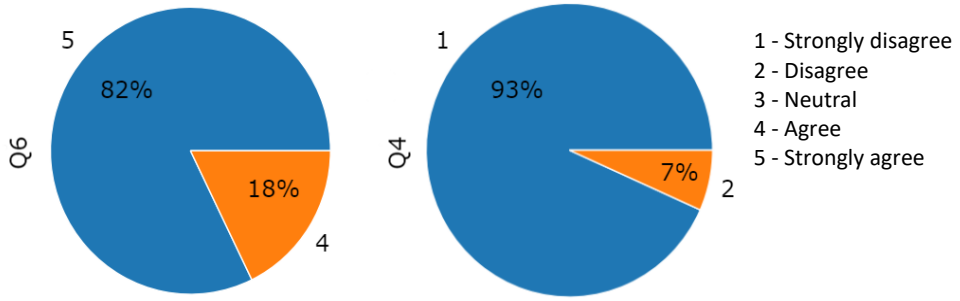
To gain a comprehensive understanding of the collected data, two distinct datasets were created. The first dataset integrates all responses from the HCTM surveys conducted across the three phases. Simultaneously, the second dataset encapsulates responses from the SUS surveys conducted in the three phases. Both datasets share a common structure. They include crucial variables such as a unique participant ID, a categorical designation representing the respective study phase, individual survey questions, and the individual score. Remarkably, as demonstrated in Fig. 17, both datasets exhibit exemplary data integrity, with no instances of missing values.

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 45 entries, 0 to 44
Data columns (total 12 columns):
 #   Column          Non-Null Count  Dtype
---  ------          --------------  -----
 0   Participant_ID  45 non-null     int64
 1   Group           45 non-null     object
 2   Q1              45 non-null     int64
 3   Q2              45 non-null     int64
 4   Q3              45 non-null     int64
 5   Q4              45 non-null     int64
 6   Q5              45 non-null     int64
 7   Q6              45 non-null     int64
 8   Q7              45 non-null     int64
 9   Q8              45 non-null     int64
 10  Q9              45 non-null     int64
 11  TRUST_Score     45 non-null     float64
dtypes: float64(1), int64(10), object(1)
memory usage: 4.3+ KB
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 45 entries, 0 to 44
Data columns (total 13 columns):
 #   Column          Non-Null Count  Dtype
---  ------          --------------  -----
 0   Participant_ID  45 non-null     int64
 1   Group           45 non-null     object
 2   Q1              45 non-null     int64
 3   Q2              45 non-null     int64
 4   Q3              45 non-null     int64
 5   Q4              45 non-null     int64
 6   Q5              45 non-null     int64
 7   Q6              45 non-null     int64
 8   Q7              45 non-null     int64
 9   Q8              45 non-null     int64
 10  Q9              45 non-null     int64
 11  Q10             45 non-null     int64
 12  SUS_Score       45 non-null     float64
dtypes: float64(1), int64(11), object(1)
memory usage: 4.7+ KB
```

Fig. 17 Information about the trust and the usability dataset

The Fig. 18 presents two pie charts, each representing the distribution of responses for specific survey statements in the HCTM and SUS surveys. The first chart refers to statement number six (Q6) in the HCTM and the second chart refers to statement number four (Q4) in the SUS questionnaire. Notably, in the HCTM survey, 82% of respondents strongly agreed with the statement Q6: "I believe that the ID Wallet app is interested in understanding my needs and preferences". This strong agreement was reflected in the rating of a "5". For this dataset, the exact same percentage was also achieved for statement Q9: "I think that the ID Wallet app performs its role very well". In contrast, 93% of participants in the SUS survey disagreed with the statement Q4: "I think that I would need the support of a technical person to be able to use the app". These participants rated this statement a "1", meaning "strongly disagree".



Q6: "I believe that the ID Wallet app is interested in understanding my needs and preferences".
Q4: "I think that I would need the support of a technical person to be able to use the app".

Fig. 18 The distribution of responses for statement (Q6) in the HCTM and (Q4) in the SUS

In Fig. 19, a correlation matrix is generated for the HCTM survey statements in the DataFrame using the Pandas library in Python. The method *corr()* calculates the pairwise correlation between these columns and returns a correlation matrix. The other libraries like NumPy, Seaborn and Matplotlib are responsible for the visualization of the matrix.

```
data = df[['Q1', 'Q2', 'Q3', 'Q4', 'Q5', 'Q6', 'Q7', 'Q8', 'Q9']].corr()
mask = np.zeros_like(data)
mask[np.triu_indices_from(mask)] = True
sns.set_style('whitegrid')
plt.subplots(figsize = (15,10))
sns.heatmap(data,
            annot=True,
            cmap = 'RdBu',
            linewidths=.5,
            linecolor='black',
            fmt='.6g',
            center = 0,
            square=True)
plt.title("Correlation of the items", y = 1, fontsize = 18, pad = 40);
```

Fig. 19 Generating the correlation matrix for the HCTM variables

The resulting heatmap in Fig. 20 illustrates the relationships between the HCTM set of variables. Each cell represents the correlation coefficient between two variables, with colour intensity indicating the strength and direction of the correlation. For example, statement Q1: "I believe that there could be negative consequences from using the ID Wallet app", exhibits a negative correlation of approximately -0.67 with statement Q4: "I believe the ID Wallet app will act in my best interest". This negative correlation means that participants who expressed higher agreement with statement Q1 were less likely to strongly agree with statement Q4 and vice versa. Additionally, the heatmap reveals a robust positive correlation of approximately 0.67 between statements Q8 and Q9. Statement Q8: "I think that the ID Wallet app has all the functionalities I would expect from it", aligns closely with statement Q9: "I think that the ID Wallet app performs its role very well". This positive correlation implies that participants who believed the app had the expected functionalities were more likely to perceive it as performing its role effectively, and vice versa.

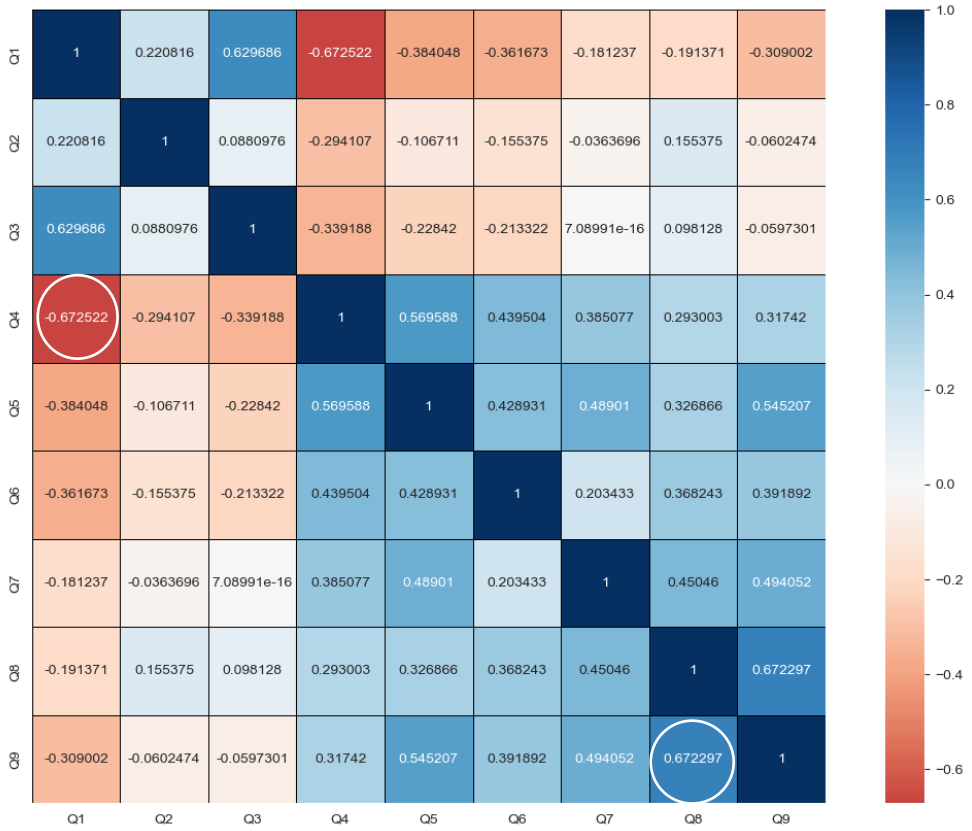


Fig. 20 The correlation matrix for the data of the HCTM survey

In Fig. 21, another correlation matrix is created for the statements in the SUS survey, similar to the HCTM survey, with the only difference being that here there are ten statements.

```
data = df[['Q1', 'Q2', 'Q3', 'Q4', 'Q5', 'Q6', 'Q7', 'Q8', 'Q9', 'Q10']].corr()
mask = np.zeros_like(data)
mask[np.triu_indices_from(mask)] = True
sns.set_style('whitegrid')
plt.subplots(figsize = (15,10))
sns.heatmap(data,
            annot=True,
            cmap = 'RdBu',
            linewidths=.5,
            linecolor='black',
            fmt='.6g',
            center = 0,
            square=True)
plt.title("Correlation of the items", y = 1, fontsize = 18, pad = 40);
```

Fig. 21 Generating the correlation matrix for the SUS variables

The visualization of the correlation matrix is displayed in Fig. 22, providing insights into the relationships among the SUS set of variables. Notably, statement Q3: "I thought the app was easy to use", exhibits a negative correlation of approximately -0.65 with statement Q4: "I think that I would need the support of a technical person to be able to use the app". This negative correlation implies that participants who found the app easy to use were less likely to feel the need for technical support, and vice versa.

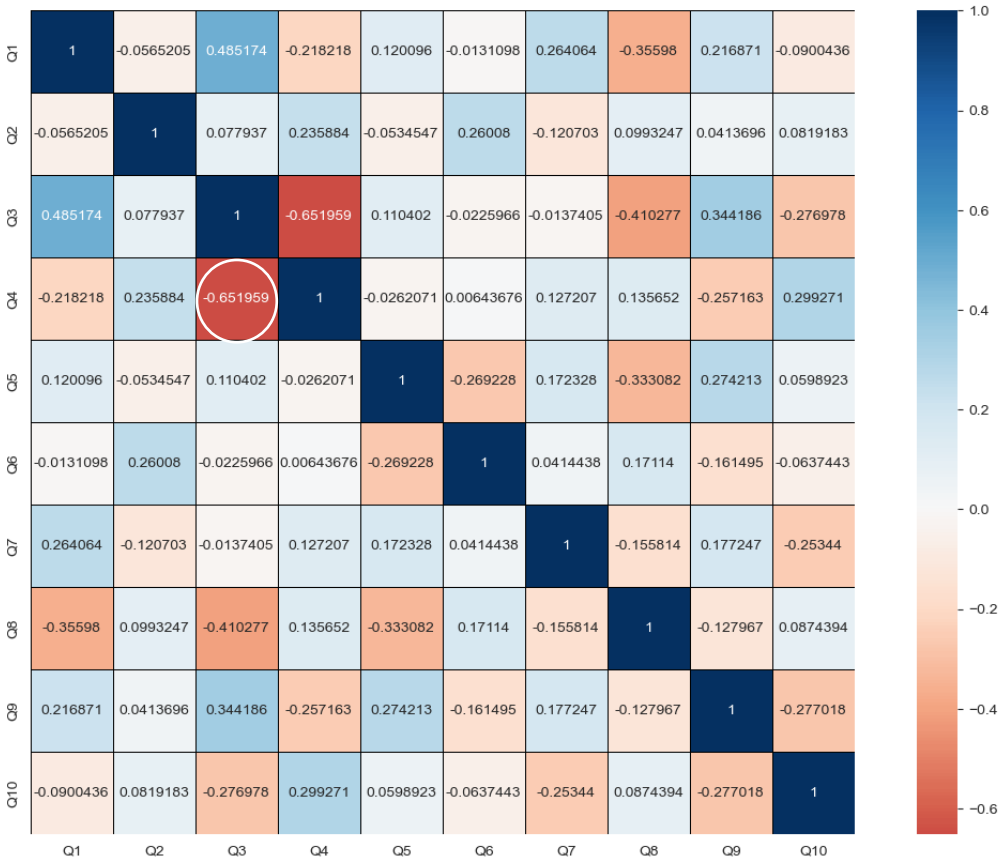


Fig. 22 The correlation matrix for the data of the SUS survey

Based on the results of the One-Way ANOVA for the HCTM survey, displayed in Fig. 23, there is a significant difference between the means of the groups in the *group*_variable. The p-value (PR(>F)) of 0.008872 is less than the significance level of 0.05. So, there are statistically significant differences between at least some of the group means in the group_variable.

One-Way ANOVA Results:

	df	sum_sq	mean_sq	F	PR(>F)
group_variable	2.0	805.463111	402.731556	5.298619	0.008872
Residual	42.0	3192.289333	76.006889	NaN	NaN

Fig. 23 Results of the One-Way ANOVA for the HCTM survey

In the context of the provided One-Way ANOVA results for the SUS survey presented in Fig. 24, the p-value is 0.672055. Since the p-value is greater than the typical significance level of 0.05, there is no sufficient evidence to reject the null hypothesis. The null hypothesis typically states that there are no significant differences between the groups in terms of system usability scores.

One-Way ANOVA Results:

	df	sum_sq	mean_sq	F	PR(>F)
group_variable	2.0	47.777778	23.888889	0.4012	0.672055
Residual	42.0	2500.833333	59.543651	NaN	NaN

Fig. 24 Results of the One-Way ANOVA for the SUS survey

5.2 Results of the Individual Phases

This section presents the results of each of the three user study phases separately, diving deep into the data to uncover significant trends and unique insights.

5.2.1 Results from Phase One

In the first phase of the user studies, participants provided insights into their perceptions and experiences with the digital identity wallet app concept. They understood the concept of digital identity as the storage of identity data in digital form and found it transparent and user-friendly. Users had a positive experience, appreciating the app's convenience and simplicity. Security and data protection were highlighted as important concerns, with users valuing double confirmation for added security. The app exceeded their expectations, but some desired more customization options. Additionally, a few participants expressed concerns about the wallet operator and the increasing digitization of the world. These findings,

presented in more detail in Tab. 5, guided further development and testing of the app.

Tab. 5 Summary of the interview responses from the first phase

Category	Comments from the participants
Overall Experience	The concept of "digital identity" is clear. Users defined it as the "storage of my identity data in digital form". Users found the experience very transparent, not time-consuming, easy to use, easy to follow, well-structured, and intuitive. Some expressed uncertainty about where their data might end up, but overall, they enjoyed using the app. Users were impressed by the entire app, the convenience of not needing their physical wallet, the multiple options for the protection mechanism, and the ability to quickly store and use cards. Some users conveyed their disappointment regarding the growing trend of digitization in the world. They also mentioned that there were too many confirmations required when using fingerprints.
Functionality and Features	Users noted that the digital identity app exceeded their expectations. They found it to be less complicated than anticipated and were surprised by features like the app-to-app and the web-to-app communication. Users appreciated the convenience of having all their cards stored in one place, the ease of adding and using different cards, the added security of double confirmation, and the presence of clear step-by-step instructions. Users were worried about potential data loss if they were to lose their phone. Additionally, they found it challenging to delete cards or correct data in case of errors.
Usability	Some users encountered confusion and difficulty during specific points of their interactions with the app. This included expectations that storing the driver's license would follow the same process as storing the national ID card. Additionally, there were mentions of frequent confirmations requiring fingerprint authentication, as well as some challenges related to the understanding of the action button, which was only for testing purposes. Many users found the navigation in the app to be straightforward and user-friendly. They appreciated the minimal steps required for various tasks, such as storing cards. Users noted that the process of storing cards was completed very fast, and transferring data between different services was completed within few clicks. Furthermore, the ability to navigate back and forth within the app was seen as convenient by users.
Visual Design	Users provided an average rating of 4 (1 - very dissatisfied; 5 - very satisfied) for the design of the app. They found the design

	to be consistent, appreciated its serious and straightforward nature, and noted that the simplicity of the design made it easy to locate different features and functions within the app. In terms of specific feedback, some users expressed a desire for a dark mode option in the app. Additionally, there were some suggestions to allow users to change or customize colours within the app. However, participants believed that adding more colours could potentially distract users from important information. Some mentioned having difficulty recognizing the icon for scanning QR codes. Users also stated that they would like the colour of the digital card to match their physical card for consistency. Overall, they felt that the design was user-friendly and did not hinder their experience.
User Trust	Nine out of fifteen (9 out of 15) respondents chose the first screen from the three options depicted in Fig. 25 as their most trusted screen. They expressed their preference by stating, "I feel more secure every time I have to enter a PIN" or "I appreciate having the opportunity to select my preferred protection mechanism". Fourteen out of fifteen (14 out of 15) respondents expressed preference for the state as their preferred wallet operator. One of the reasons they gave was that the state already owned their sensitive data by providing ID cards and other personal documents. Participants felt better protected by the state in the event of problems with the app. A lack of trust in private companies handling personal data was noted due to concerns about their profit motives. On the other hand, one out of fifteen (1 out of 15) respondents chose a private company as the preferred wallet operator. The reason mentioned was that private companies are more cautious and vigilant out of concern for their reputation. This respondent also pointed out that personal information is often even shared on social media, leading to a sense of trust in the app. Respondents identified several factors that would diminish their trust in this app. These included concerns about the app allowing screenshots and ads, sharing their information with other contacts without their consent, storing unencrypted data in the cloud, and demanding access to their location data.
User Feedback and Preference	In terms of potential additions, participants suggested several features such as digitizing credit cards, including student ID cards, integrating flight tickets, facilitating payments within the app, adding a support chat, implementing face recognition, and incorporating the smart fingerprint functionality. Additionally, users recommended security enhancements like not displaying sensitive data in plain text, introducing an extra identification step through a webcam for initial app use or receiving notifications every time the app is accessed. Importantly,

participants agreed that the screenshot functionality should be prohibited within the app.
Regarding the situation of an in-person identification, the majority, specifically fourteen out of fifteen (14 out of 15) respondents expressed a preference for using the digital card, highlighting its convenience and time savings. Nevertheless, one respondent expressed scepticism regarding the widespread acceptance of the digital ID card and chose to maintain the physical ID card as a backup. Interestingly, only one out of fifteen (1 out of 15) respondents was open to the idea of completely forgoing the physical ID card.

Different users have different preferences and priorities. Offering users the choice of selecting the most trusted screen from three options (see Fig. 25) aligns with the principles of user-centered design [1]. This type of question was designed to investigate which screen design and functionalities promote user trust. The majority of respondents (9 out of 15) preferred the first screen as their most trusted option. Their rationale included feeling more secure when required to enter a PIN and valuing the ability to choose their preferred protection method. The minority of respondents who preferred screens two (3 out of 15) and three (3 out of 15) cited specific reasons. For the second screen, users mentioned that they liked to be provided with a summary before taking an action. As for the third screen, users expressed trust in the homepage because they knew they had already stored their cards successfully.

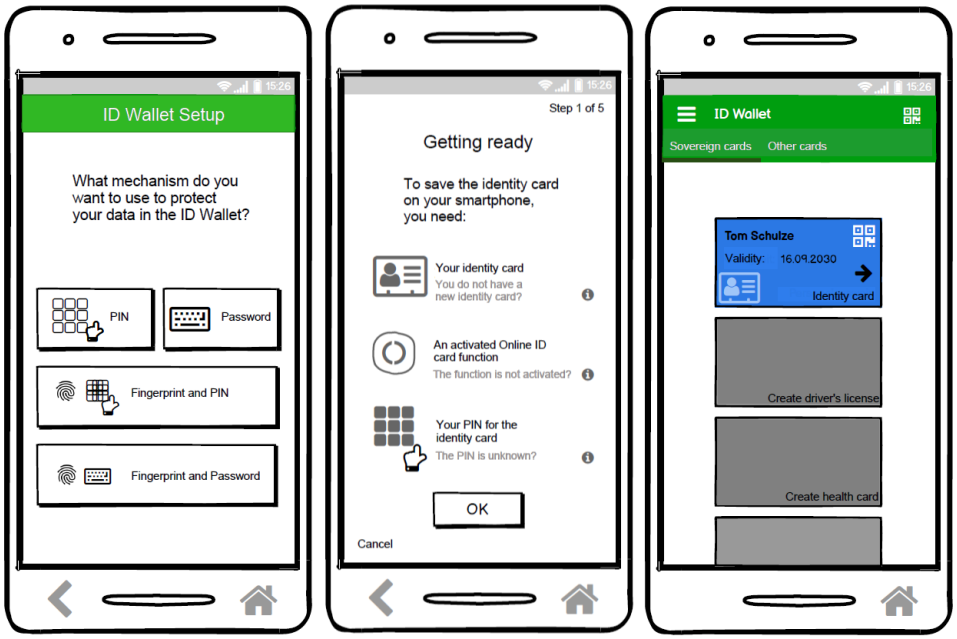


Fig. 25 The options for selecting the most trusted screen

Based on the results of the HCTM questionnaire, users expressed a remarkable level of satisfaction, with a score of 76.3%. Furthermore, users perceive low risk associated with the system, as reflected in the risk perception score of 52.9%. In terms of benevolence, users exhibit a high level of trust, scoring the system at 86.7%. Similarly, users have strong confidence in the system's competence, assigning it a score of 89.3%. Collectively, these findings are presented in Fig. 26 and depict a positive user perception of the digital identity app.

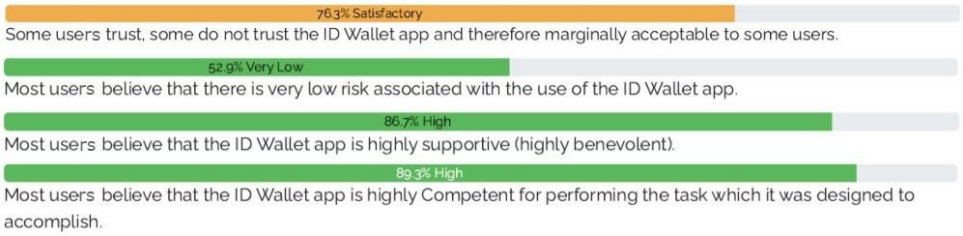


Fig. 26 HCTM results of the first phase

In Fig. 27, individual SUS scores of the user study participants are shown. Each data point represents an individual user's rating of the system's usability, with a range of scores across the spectrum. Notably, the average SUS score stands at 90. This average score reflects the overall perception of the system's usability. The individual ratings range from a top score of 100 to a minimum score of 75. Users consistently rated the system as remarkably user-friendly, efficient, and intuitive. The variability in individual scores provides insights into the range of experiences and preferences among the user base. With the potential for even higher average scores in subsequent evaluations, this score establishes a strong benchmark for usability excellence.

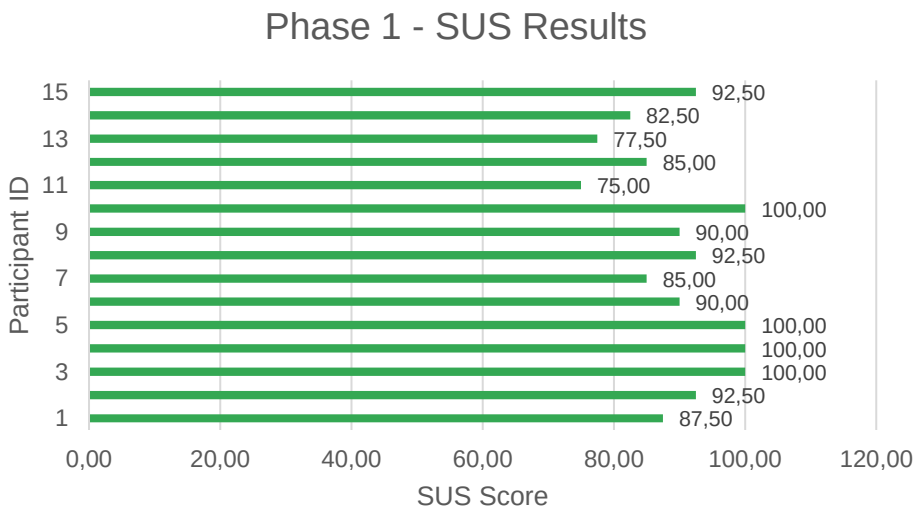


Fig. 27 SUS results of the first phase

5.2.2 Results from Phase Two

The second phase of the user studies provided further insights into the evaluation of user trust and usability after the wallet app prototype had been updated with regard to the additional functions in the menu list. The most frequently mentioned reasons for each response in the HCTM survey are listed in Tab. 6. Participants expressed a heightened sense of trust in the system's security, transparency, and reliability. A notable majority, specifically, 12 out of 15 participants still favoured the state as the preferred wallet operator. Their reasons remained consistent, including the state's established access to personal data, the provision of physical ID cards, and an overall perception of heightened security with a government-operated system. Users found that the digital identity wallet either met or exceeded their expectations. They recognized the need for user responsibility, particularly in avoiding unintentional data disclosure, and appreciated default security features. Only one third of the participants recognized the fact that the screenshot function was disabled by default. Overall, users generally did not perceive the app as risky, citing its data storage practices and encryption. Participants viewed the app as competent and effective, mainly due to its ease of use and protection mechanisms. While there were varying preferences for support, with 9 out of 15 participants seeing voice call support as their first choice, in general they saw the FAQ tab as suitable for simpler questions, reserving customer support for more specific queries.

Tab. 6 Summary of responses to HCTM from the second phase

HCTM Statement	Reasons (Frequency)
I believe that there could be negative consequences from using the ID Wallet app.	I think it depends on the operator of the wallet, I would be less afraid of consequences if the state is behind it. (8 out of 15)
I feel I must be cautious when using the ID Wallet app.	The user should be careful with any app to avoid mistakes. In the case of the ID Wallet app, this can be the unintentional disclosure of data to some service providers. (11 out of 15); I like the fact that screenshots are disabled by default. (5 out of 15)
It is risky to use the ID Wallet app.	I do not think using the app is risky because of the security features mentioned, such as storing data only on the smartphone and encrypting the data. (10 out of 15)
I believe the ID Wallet app will act in my best interest.	If it comes from the state, yes, because it would be easier to manage the identities of citizens and the state already has the data because it provides us with these cards. (12 out of 15)

I believe that the ID Wallet app will do its best to help me if I need help.	I believe that the FAQ tab is appropriate for the simpler questions and the customer support for more specific questions. (13 out of 15); Voice call is the first choice. (9 out of 15)
I believe that the ID Wallet app is interested in understanding my needs and preferences.	This is in the interest of both the app operator and the user, as in this way the operator tries to increase the number of users and retain current users by satisfying their needs. (14 out of 15)
I think that the ID Wallet app is competent and effective.	I have not used other apps with the same features, so I find it competent. (14 out of 15); The ease of use makes it effective. (7 out of 15); The protective mechanisms make it effective. (7 out of 15)
I think that the ID Wallet app has all the functionalities I would expect from it.	The most important card like the ID card, the driver's license and the library card were integrated in the app. (10 out of 15); Additional features would be the storing of other cards. (5 out of 15)
I think that the ID Wallet app performs its role very well.	Overall, I like the purpose of the app and had a good experience with it. (15 out of 15)

In the second phase of the study, user satisfaction with the app reached 79.6%. In this phase, risk perception fell slightly to 52.4% compared to the first phase. On the other trust-related dimensions, the wallet app excels in both benevolence and competence. Both scores improved in the second phase. Users express a high level of trust in the app's benevolence, scoring it at 93.3%. Additionally, the competence of the app is highly regarded with a score of 92.9%. The results of the HCTM discussed in relation to the trust dimensions are shown in Fig. 28.

Fig. 28 HCTM results of the second phase

During this phase, the users' assessment of usability remained positive, even if the scores for usability fell slightly compared to the first phase. The most frequently mentioned reasons for each response in the SUS survey are listed in Tab. 7. The app was largely perceived as intuitive, with 13 out of 15 participants finding it straightforward and easy to follow, pointing to effective design and user guidance. All 15 participants indicated that they felt comfortable navigating the app and they appreciated the availability of

customer support in case they encountered any difficulties. For 7 out of 15 participants, the app's communication capabilities exceeded their expectations, implying that it effectively facilitated interactions with other services or platforms. The app's design received positive feedback from 8 out of 15 participants, who noted its consistency and simplicity. Some repetitive processes, such as fingerprint confirmation, were mentioned, indicating a degree of familiarity. Participants believed that individuals accustomed to using mobile apps would find it relatively easy to navigate the wallet app. The clarity of the instructions provided by the app was appreciated, as they were easy to follow. Lastly, while not all participants felt the immediate need to use them, 13 out of 15 acknowledged the presence of the FAQ and support tabs. These features were seen as valuable resources for addressing potential queries or issues in the future.

Tab. 7 Summary of responses to SUS from the second phase

SUS Statement	Reasons (Frequency)
I think that I would like to use the app frequently.	I want to have everything in my smartphone. (11 out of 15)
I found the app unnecessarily complex.	No, it was easy to use. (8 out of 15)
I thought the app was easy to use.	The app was intuitive and easy to follow. (13 out of 15)
I think that I would need the support of a technical person to be able to use the app.	I just interacted with the app on my own and it ran quite smoothly. There was also customer support in case of a difficulty. (15 out of 15)
I found the various functions in the app were well integrated.	The communication with other services exceeded the expectations. (7 out of 15)
I thought there was too much inconsistency in the app.	The simple design was consistent, and there were some repetitive processes, such as fingerprint confirmation for sending data. (8 out of 15)
I would imagine that most people would learn to use the app very quickly.	People who use smartphones and similar apps will also be able to work with it. There is nothing unusual that cannot be found in other apps. (7 out of 15)
I found the app very cumbersome to use.	The instructions were clear, it was easy to follow the actions to complete the tasks. (8 out of 15)
I felt very confident using the app.	After successfully completing the tasks, I was confident that I would be able to use the app in the future without any difficulties. (7 out of 15)
I needed to learn a lot of things before I could get going with the app.	No, I used the app without being prepared for it, but there was a FAQ and a support tab that could be useful in some cases. (13 of 15)

In Fig. 29, individual SUS scores obtained during the second phase of the user studies are displayed. Each bar in the chart represents a participant's SUS score, reflecting their assessment of the app's usability. Upon analysing these scores, it is evident that there is some variability in user perceptions, as indicated by the range of scores. It is worth noting that the average SUS score for this phase is 88, which is slightly lower than the average achieved in the first phase. The individual scores range from the highest score of 100 to the lowest score of 72.5, showcasing the diversity in user experiences. However, it is important to emphasize that the overall usability still reflects a high level of usability, as the majority of participants rated the app positively.

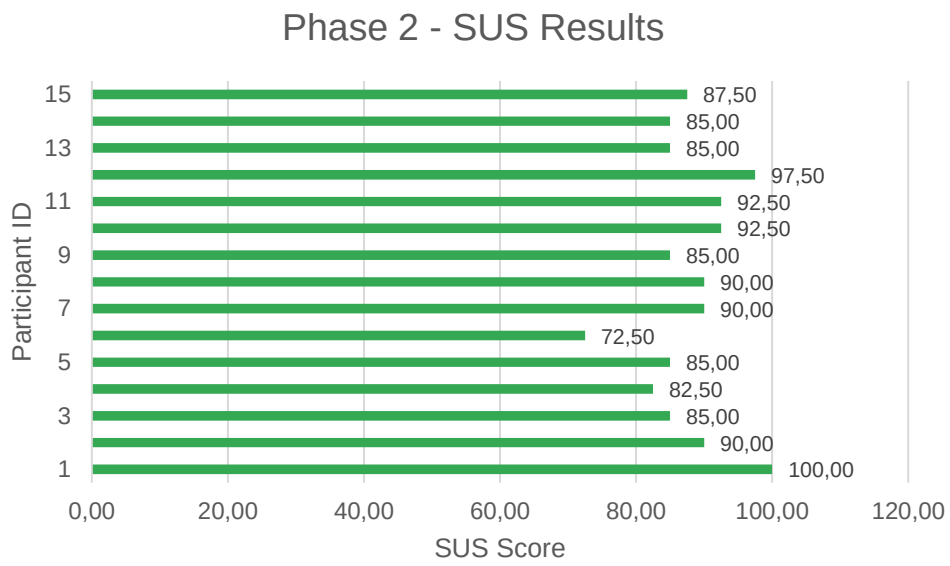


Fig. 29 SUS results of the second phase

5.2.3 Results from Phase Three

The third and final phase of the user studies aimed to test the further refinements of the digital identity wallet app in relation to the wallet operator. The most frequently mentioned reasons for each response in the HCTM survey are listed in Tab. 8. In this phase, several key insights emerged from the participants' responses. The majority of users expressed a high level of trust in the app. When asked whether they believed the wallet app would act in their best interest, 12 out of 15 participants expressed trust in the app's intentions. They cited the app's association with the state and the fact that the state already possesses their data as reasons for their trust, believing that these factors align with their best interests. Participants generally saw the app as a convenient solution for storing personal data, with many emphasizing its competency in this regard. Moreover, respondents appreciated the integration of essential cards and perceived

the app as a tool that simplifies their lives. Overall, the third phase revealed a positive perception of the app's trustworthiness, competence, and utility among users.

Tab. 8 Summary of responses to HCTM from the third phase

HCTM Statement	Reasons (Frequency)
I believe that there could be negative consequences from using the ID Wallet app.	Negative consequences can happen with any app, but it is less likely if it is released by the state. It should be more secure. (8 out of 15)
I feel I must be cautious when using the ID Wallet app.	No, I trust the app with my data. (10 out of 15); Yes, as it is personal data that is processed through the app. (5 out of 15)
It is risky to use the ID Wallet app.	No, because I think that it is first checked by the state and that the state does not misuse sensitive data. (10 out of 15)
I believe the ID Wallet app will act in my best interest.	Since it comes from the state, yes. The state already has our data. (12 out of 15)
I believe that the ID Wallet app will do its best to help me if I need help.	I think this is in the interest of both sides, the wallet operator and the user. (9 out of 15)
I believe that the ID Wallet app is interested in understanding my needs and preferences.	Yes, to encourage me to use the app. (7 out of 15)
I think that the ID Wallet app is competent and effective.	I have not heard about other apps that allow storing the national ID card, so I find it competent. (14 out of 15)
I think that the ID Wallet app has all the functionalities I would expect from it.	The most important cards have been integrated in this app. (10 out of 15)
I think that the ID Wallet app performs its role very well.	Overall, I think the app makes our lives easier. (12 out of 15)

In this phase of the study, the HCTM yielded noteworthy results, as presented in Fig. 30. User satisfaction with the wallet app saw a substantial increase, reaching an impressive 80.3%. Conversely, the perceived risk associated with the app decreased significantly, with a low score of 44.9%. Respondents demonstrated an exceptionally high level of trust in the benevolence of the app, scoring it at 98.7%. Furthermore, they also perceived the app as highly competent, with a competence rating of 97.3%.

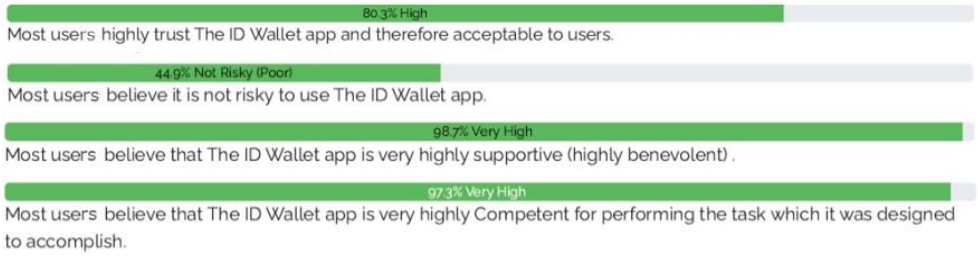


Fig. 30 HCTM results of the third phase

During the SUS survey discussions in this phase, users highlighted several key points. Most preferred to have all the cards on their smartphone because it is so convenient to have only the smartphone with them at all times. Again, they found the app to be user-friendly, intuitive, and easy to navigate, emphasizing its simple design. Users praised the government's implementation of the app and its seamless communication with other services. Additionally, 13 out of 15 participants relied only on the provided instructions and their prior knowledge to effectively use the app. The exact reasons for the SUS responses in the final phase are summarized in Tab. 9.

Tab. 9 Summary of responses to SUS from the third phase

SUS Statement	Reasons (Frequency)
I think that I would like to use the app frequently.	I always want to have all the cards with me in my smartphone. I never forget my smartphone. (9 out of 15)
I found the app unnecessarily complex.	In contrast, the app was simple to use. (10 out of 15)
I thought the app was easy to use.	It was very user-friendly. (11 out of 15)
I think that I would need the support of a technical person to be able to use the app.	I think the government implemented it well, so everyone should be able to use this app. (7 out of 15)
I found the various functions in the app were well integrated.	The communication with other services exceeded the expectations. (7 out of 15)
I thought there was too much inconsistency in the app.	No, the design and the process of storing the cards were consistent in the app. (8 out of 15)
I would imagine that most people would learn to use the app very quickly.	Yes, because the instructions guide the users and there is nothing completely new in this app. (6 out of 15)
I found the app very cumbersome to use.	I easily found the things I was looking for in the app. (8 out of 15)
I felt very confident using the app.	Knowing that the app comes from the state gave me confidence that I was not doing anything wrong with my data. (7 out of 15)
I needed to learn a lot of things before I could get going with the app.	No, I only used the given instructions and some prior knowledge. (13 out of 15)

The Fig. 31 illustrates individual SUS scores from the final phase. Notably, the average SUS score in this phase stands at a noteworthy 90.33, representing a slight increase compared to both previous phases. It is worth noting that users' assessments ranged from an optimal score of 100 to a minimum individual score of 72.5.

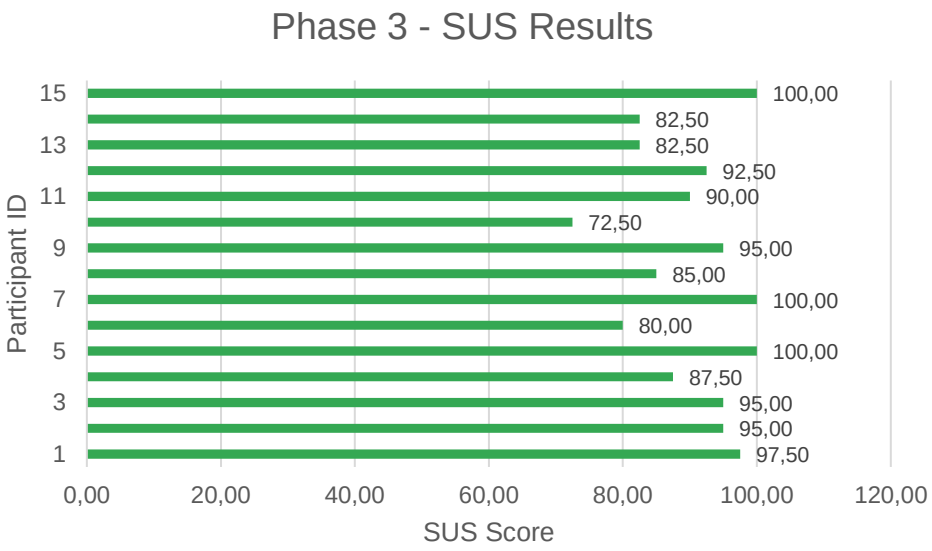


Fig. 31 SUS results of the third phase

6 Discussion of Results

This chapter is intended to discuss the results of this work by providing specific interpretations and possible reasons. It is divided into two subsections, the first refers to the general results of the entire study, the second deals with the individual phases in more detail. Through a comprehensive examination of user experiences, trust dynamics, and usability factors, this thesis contributes valuable insights into fostering user trust in wallet applications.

6.1 Discussion of the Results of the Entire Study

The equal number of participants in each phase ensured a balanced representation of perspectives throughout the study. The different age range aimed to capture a broad spectrum of generational perspectives.
Over the course of the study, the trust scores demonstrated a consistent trend of increasing user satisfaction and the usability scores indicated a favourable user experience. This is due to the fact that users consistently praised the simplicity, user-friendliness and intuitive design of the app. The simple navigation and straightforward completion of tasks led to positive user experiences. These positive perceptions were also a result of the wallet app's clear instructions and familiar user interface. Notably, users' expectations were exceeded by the app's ability to communicate with other services or apps.
Trust in the app's security measures was an important factor for user acceptance. The increase in the usability rating had a positive effect on user trust. The integration of additional features to inform, assist and protect user data led to a slight decrease in the usability rating. As the state was involved in the operation of the wallet app, users felt that their data was well protected, which resulted to a higher level of trust. This indicates that the wallet operator has a greater influence on the trust level than the additional features of the wallet app.
The survey results not only affirmed the strong internal consistency and reliability of the survey dimensions as previously documented [21], but also underscored the uniformity of participants' responses. This consensus among participants highlights a clear collective agreement on the app's performance. Therefore, the app does indeed consistently meet user expectations and usability requirements. Based on the results of the correlation matrix for trust, it came out that functionality and performance are positively related in participants' perceptions. This positive correlation

means that participants who believed that the app had the expected functions were more likely to think that it worked effectively and vice versa. On the other side, the correlation matrix for usability showed that usability and the need for support within the app are inversely related.
The results of the One-Way ANOVA for the HCTM surveys show that the difference in means is unlikely to be due to random chance alone. Therefore, it can be concluded that there are statistically significant differences between at least some of the group means in the group variable. In contrast, for the SUS surveys there is no evidence of a statistically significant difference in the average SUS scores among the three phases.
Reflecting the findings of this thesis compared to the related literature, the results answer the research questions confirming that: beside enhanced security measures, the core of trust lies on the chosen wallet operator [24] and a higher level of usability is associated with a higher level of trust [2]. Furthermore, the results show that both trust and flow experience have a significant impact on the intention to use wallet apps [62], and that providing reputational information about the operator significantly improved perceived trustworthiness [63].

6.2 Discussion of the Results of the Individual Phases

The analysed answers to the open questions in the first phase provided facts about the aspects in which users were satisfied and in which they were concerned with the wallet app. The concerns show how important security, data protection and user control over their data are for trust in the wallet app. The results of the HCTM questionnaire in the first phase reveal a highly favourable user perception of the wallet app. The satisfaction score of 76.3% indicates a positive and contented experience with the system. The low perception of risk contributed significantly to the overall trust users place in the system's functionality and security. Users in phase one believed that the system operates with genuine benevolence and concern for their best interests. The high competence score indicates that users trust the system's ability to perform its functions effectively and reliably. The average SUS score here standing impressively at 90.00 attests to a high level of ease of use.
Interestingly, despite the slight deterioration in usability, user trust has improved considerably in the second phase. The adjustments made to the prototype in response to user feedback from the initial phase evidently had a favourable impact on users' trust perceptions. User satisfaction with the app improved slightly with a score of 79.6%, compared to the first phase. This suggests that users were even more satisfied with the app after the proposed improvements in terms of security measures, support and informative aspects had been implemented. In this second phase, risk perception decreased very slightly compared to the first phase. This signifies

that users perceived the app as less risky after the changes, although the difference is minimal. The high level of benevolence and competence at this stage is evidence that users believe that the app primarily pursues their interests and that they perceive the app to be very powerful and effective in terms of its intended functions. In this phase, users' evaluations of usability continued to be positive, although there was a decrease in usability scores compared to the first phase. This change could be attributed to the introduction of the new features. While some users found these additions beneficial, others may have encountered a learning curve. The average SUS score of 88.00 suggests that there may have been some challenges or aspects in the updated prototype that users found less intuitive.

The results of the third phase showed that the majority of users expressed a high level of trust in the app, particularly because it is operated by the state. The participants believed that government involvement ensures a higher level of security and minimises the risk of data misuse. The user satisfaction rate of 80.3% recorded in the HCTM survey showed an improvement compared to the first and second phases, which indicates that the state as the wallet operator had a positive influence on user satisfaction. In this context, the wallet app continued to receive high ratings for its benevolence and competence. In particular, a significant decrease in perceived risk was noted. This result demonstrates a positive change in user trust compared to previous phases and emphasises the effectiveness of the changes made in relation to the wallet operator. As a conclusion, trust in the app was bolstered by its state origin, contributing to users' trust in data security. The maximum SUS rating of A+ achieved in the final phase confirms the high level of user-friendliness and the positive experience that users have had when interacting with the wallet app.

7 Conclusion

This concluding chapter provides both a retrospective overview and forward-looking guidelines for further progress in this area. It summarizes key findings and contributions, limitations, and suggests future research directions. Finally, the chapter ends with practical recommendations for strengthening trust in digital identity wallet apps.

7.1 Summary of the Study

In this thesis, a comprehensive examination of user trust and usability in a digital identity wallet app concept was conducted. The research aimed to understand how users perceive and interact with these apps and to identify factors influencing their trust. A multi-phase approach, including interviews and surveys, was employed to collect data from a diverse participant group. The study primarily focused on assessing users' trust in a particular digital identity wallet app concept based on perceived risk, benevolence, and competence. Throughout the three phases, participants demonstrated a consistent and high level of trust in the app. Valuable insights into the dynamics of trust in such apps were gained, highlighting user expectations and challenges.
In addition to assessing user trust, the study also examined the usability of the digital identity wallet app. The results on usability were consistently positive in all three phases. Participants frequently described the app as intuitive, user-friendly, and easy to navigate. These usability findings are consistent with the high overall user satisfaction scores obtained in the study, further underscoring the app's potential for widespread adoption and use.

7.2 Key Findings and Contributions

One of the primary findings of this study was the substantial user satisfaction with the digital identity wallet app under investigation, which reached an optimum score of 82.3% in the HCTM survey and a peak score of 90.33 in the SUS survey. These values are results of the third phase of the user studies. This suggests that the wallet operator has a greater influence on the trust score than adding features that improve security measures, support users and inform about data policies. Especially the addition of further functions to the wallet app led to a slight decrease in usability.

Users expressed confidence in the app's competence and benevolence, attributing this trust partly to the app's association with the state. However, concerns about potential negative consequences and the need for additional support when using the app were identified. Notably, this study contributes to the field by providing insights into how trust is built and maintained in digital identity wallet apps, emphasizing the significance of both usability and trust factors.

7.3 Limitations and Future Research Directions

While this thesis offers valuable insights, it is not without limitations. The study's limitations include challenges in involving rural inhabitants, elderly individuals, and disabled people. These groups were underrepresented, potentially affecting insights into their experiences. Additionally, the focus on digitally literate participants might introduce bias, neglecting those less comfortable with technology. The sample size, while diverse, may not fully represent all user demographics. Broadening demographic inclusion would enhance the overall understanding of digital identity experiences.
Additionally, this thesis focused on a specific wallet app prototype, limiting generalizability. Future research could involve larger and more diverse samples, encompassing various digital identity wallet apps. It would also be beneficial to explore trust dynamics in different cultural contexts. Further investigations could go deeper into the impact of specific features, such as data encryption, biometric authentication or multifactor authentication on user trust. Additionally, longitudinal studies could assess how trust evolves over time.

7.4 Practical Recommendations for Improving User Trust in Digital Identity Wallet Apps

Based on the findings, several practical recommendations are proposed for enhancing user trust in digital identity wallet apps. Firstly, developers should prioritize simple user interfaces with clear and concise instructions to alleviate concerns about app usage. Secondly, integrating multifactor authentication and encryption can bolster the app's security, addressing user fears of potential negative consequences. Moreover, app operators should consider strategies to emphasize benevolence, such as transparent data handling policies. Lastly, in-app educational materials could inform users about the app's security features, its benefits, and best practices for protecting their digital identities to encourage wider adoption.

References

[1] Abras, C., Maloney-Krichmar, D., & Preece, J. (2004). User-centered design. Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications, 37(4), 445-456.

[2] Acemyan, C. Z., & Kortum, P. (2012, September). The relationship between trust and usability in systems. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 56, No. 1, pp. 1842-1846). Sage CA: Los Angeles, CA: SAGE Publications.

[3] Aljazzaf, Z. M., Perry, M., & Capretz, M. A. (2010, September). Online trust: Definition and principles. In 2010 Fifth International Multi-conference on Computing in the Global Information Technology (pp. 163-168). IEEE.

[4] Bachmann, R., Gillespie, N., & Priem, R. (2015). Repairing trust in organizations and institutions: Toward a conceptual framework. Organization Studies, 36(9), 1123-1142.

[5] Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. Intl. Journal of Human–Computer Interaction, 24(6), 574-594.

[6] Boyd, J. (2003). The rhetorical construction of trust online. Communication Theory, 13(4), 392-410.

[7] Brooke, J. (1996). Sus: a "quick and dirty" usability scale. Usability evaluation in industry, 189(3), 189-194.

[8] Brooke, J. (2013). SUS: a retrospective. Journal of usability studies, 8(2), 29-40.

[9] Cameron, K. (2005). The laws of identity. Microsoft Corp, 12, 8-11.

[10] Charalambous, G., Fletcher, S., & Webb, P. (2016). The development of a scale to evaluate trust in industrial human-robot collaboration. International Journal of Social Robotics, 8, 193-209.

[11] Chuttur, M. (2009). Overview of the technology acceptance model: Origins, developments and future directions.

[12] Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results (Doctoral dissertation, Massachusetts Institute of Technology).

[13] Dib, O., & Toumi, K. (2020). Decentralized identity systems: Architecture, challenges, solutions and future directions. Annals of Emerging Technologies in Computing (AETiC), Print ISSN, 2516-0281.

[14] Digital Identity Working Group of the Secure Identity Alliance (SIA). (2022). On the road to User-Centricity: Digital Identity in the Electronic Wallet era. An SIA guide exploring usages, policies, models and best practices. Retrieved from https://secureidentityalliance.org/publications-docman/public/268-on-the-road-to-user-centricity-digital-identity-in-the-electronic-wallet-era/file.

[15] Faranello, S. (2012). Balsamiq wireframes quickstart guide. Packt Publishing.

[16] Ferrario, A., Loi, M., & Viganò, E. (2020). In AI we trust incrementally: A multi-layer model of trust to analyze human-artificial intelligence interactions. Philosophy & Technology, 33, 523-539.

[17] Giovannini, C. J., Ferreira, J. B., Silva, J. F. D., & Ferreira, D. B. (2015). The effects of trust transference, mobile attributes and enjoyment on mobile trust. BAR-Brazilian Administration Review, 12, 88-108.

[18] Google Trends. (n.d.). Digital Identity. Retrieved from https://trends.google.com/trends/explore?date=all&q=Digital%20Identity&hl=en. Access: 18.09.2023.

[19] Gulati, S., Sousa, S., & Lamas, D. (2017). Modelling trust: An empirical assessment. In Human-Computer Interaction–INTERACT 2017: 16th IFIP TC 13 International Conference, Mumbai, India, September 25-29, 2017, Proceedings, Part IV 16 (pp. 40-61). Springer International Publishing.

[20] Gulati, S., Sousa, S., & Lamas, D. (2018, December). Modelling trust in human-like technologies. In Proceedings of the 9th Indian Conference on Human-Computer Interaction (pp. 1-10).

[21] Gulati, S., Sousa, S., & Lamas, D. (2019). Design, development and evaluation of a human-computer trust scale. Behaviour & Information Technology, 38(10), 1004-1015.

[22] Islam, M. T., Hoque, M. R., & Sorwar, G. (2016, December). Understanding customers' intention to use e-commerce in Bangladesh: An application of the technology acceptance model (TAM). In 2016 19th International Conference on Computer and Information Technology (ICCIT) (pp. 512-516). IEEE.

[23] Klug, B. (2017). An overview of the system usability scale in library website and system usability testing. Weave: Journal of Library User Experience, 1(6).

[24] Kostic, S., & Poikela, M. (2022). 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 (pp. 195-211).

[25] Laurent, M., Denouël, J., Levallois-Barth, C., & Waelbroeck, P. (2015). Digital identity. In Digital identity management (pp. 1-45). Elsevier.

[26] Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. Human factors, 46(1), 50-80.

[27] Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. Social forces, 63(4), 967-985.

[28] Lewis, J. R. (2018). The system usability scale: past, present, and future. International Journal of Human–Computer Interaction, 34(7), 577-590.

[29] Lewis, J. R., & Sauro, J. (2009). The factor structure of the system usability scale. In Human Centered Design: First International Conference, HCD 2009, Held as Part of HCI International 2009, San Diego, CA, USA, July 19-24, 2009 Proceedings 1 (pp. 94-103). Springer Berlin Heidelberg.

[30] Lewis, J. R., & Sauro, J. (2018). Item benchmarks for the system usability scale. Journal of Usability Studies, 13(3).

[31] Lindgren, I., Madsen, C. Ø., Hofmann, S., & Melin, U. (2019). Close encounters of the digital kind: A research agenda for the digitalization of public services. Government information quarterly, 36(3), 427-436.

[32] Lule, I., Omwansa, T. K., & Waema, T. M. (2012). Application of technology acceptance model (TAM) in m-banking adoption in Kenya. International journal of computing & ICT research, 6(1).

[33] Madsen, M., & Gregor, S. (2000, December). Measuring human-computer trust. In 11th australasian conference on information systems (Vol. 53, pp. 6-8).

[34] Mishra, P., Pandey, C. M., Singh, U., Gupta, A., Sahu, C., & Keshri, A. (2019). Descriptive statistics and normality tests for statistical data. Annals of cardiac anaesthesia, 22(1), 67.

[35] Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. Information systems research, 2(3), 192-222.

[36] Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80-86.

[37] Naik, N., & Jenkins, P. (2020, August). Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology. In 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) (pp. 90-95). IEEE.

[38] Naik, N., & Jenkins, P. (2020, November). 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) (pp. 1-6). IEEE.

[39] Naik, N., & Jenkins, P. (2021, September). Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology. In 2021 IEEE International Symposium on Systems Engineering (ISSE) (pp. 1-7). IEEE.

[40] Pikos, A. (2022). Restoring trust in an organization after a business school rankings scandal. Polish Sociological Review, 217(1), 93-114.

[41] Pinto, A., Sousa, S., Simões, A., & Santos, J. (2022). A Trust Scale for Human-Robot Interaction: Translation, Adaptation, and Validation of a Human Computer Trust Scale. Human Behavior and Emerging Technologies, 2022.

[42] Podgorelec, B., Alber, L., & Zefferer, T. (2022, June). What is a (digital) identity wallet? a systematic literature review. In 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 809-818). IEEE.

[43] Pranam, A., & Pranam, A. (2018). Rapid Prototyping. Product Management Essentials: Tools and Techniques for Becoming an Effective Technical Product Manager, 97-123.

[44] Rountree, D. (2012). Federated identity primer. Newnes.

[45] Sadiku, M. N., Shadare, A. E., & Musa, S. M. (2016). Digital identity. International Journal of Innovative Science, Engineering & Technology, 3(12), 192-193.

[46] Seigneur, J. M., & El Maliki, T. (2009). Identity Management. In Computer and Information Security Handbook (pp. 269-292). Morgan Kaufmann.

[47] Setyadi, R. (2021, March). Analysing tourism application using information technology governance trust model in COVID-19 pandemic situation. In Journal of Physics: Conference Series (Vol. 1842, No. 1, p. 012006). IOP Publishing.

[48] Singh, N., & Sinha, N. (2020). How perceived trust mediates merchant's intention to use a mobile wallet technology. Journal of Retailing and Consumer Services, 52, 101894.

[49] Soltani, R., Nguyen, U. T., & An, A. (2021). A survey of self-sovereign identity ecosystem. Security and Communication Networks, 2021, 1-26.

[50] Sousa, S., & Beltrao, G. (2021). Factors influencing trust assessment in technology. In Human-Computer Interaction–INTERACT 2021: 18th IFIP TC 13 International Conference, Bari, Italy, August 30–September 3, 2021, Proceedings, Part V 18 (pp. 416-420). Springer International Publishing.

[51] Sousa, S., Martins, P., & Cravino, J. (2021). Measuring Trust in Technology: A Survey Tool to Assess Users' Trust Experiences.

[52] Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., ... & Völter, F. (2021). Self-Sovereign Identity: Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten.

[53] Taherdoost, H. (2016). How to design and create an effective survey/questionnaire; A step by step guide. International Journal of Academic Research in Management (IJARM), 5(4), 37-41.

[54] Tan, P. N., Steinbach, M., & Kumar, V. (2016). Introduction to data mining. Pearson Education India.

[55] Theodorou, P., Tsiligkos, K., Meliones, A., & Filios, C. (2022). A training smartphone application for the simulation of outdoor blind pedestrian navigation: usability, UX evaluation, sentiment analysis. Sensors, 23(1), 367.

[56] Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. The Sovrin Foundation, 29(2016), 18.

[57] Urban, G. L., Amyx, C., & Lorenzon, A. (2009). Online trust: state of the art, new frontiers, and research potential. Journal of interactive marketing, 23(2), 179-190.

[58] Ward, R. (2013). The application of technology acceptance and diffusion of innovation models in healthcare informatics. health Policy and Technology, 2(4), 222-228.

[59] Van Someren, M., Barnard, Y. F., & Sandberg, J. (1994). The think aloud method: a practical approach to modelling cognitive. London: AcademicPress, 11, 29-41.

[60] Willomitzer, J., Heinemann, A., & Margraf, M. (2016). Zur Benutzbarkeit der AusweisApp2. Mensch und Computer 2016–Workshopband.

[61] Yan, Z., Kantola, R., & Zhang, P. (2011, November). A research model for human-computer trust interaction. In 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 274-281). IEEE.

[62] Zhou, T. (2012). Examining mobile banking user adoption from the perspectives of trust and flow experience. Information Technology and Management, 13, 27-37.

[63] Zloteanu, M., Harvey, N., Tuckett, D., & Livan, G. (2018). Digital Identity: The effect of trust and reputation information on user judgement in the Sharing Economy. PloS one, 13(12), e0209071.

[64] Zwattendorfer, B., Zefferer, T., & Stranacher, K. (2014). An Overview of Cloud Identity Management-Models. WEBIST (1), 82-92.

List of Figures

List of Tables

List of Abbreviations

RQ	Research Question
IdP	Identity Provider
SP	Service Provider
SSI	Self-Sovereign Identity
SUS	System Usability Scale
DEC	Digital Equipment Corporation
TAM	Technology Acceptance Model
HCT	Human-Computer Trust
HCTM	Human-Computer Trust Measure
HCTS	Human-Computer Trust Scale
DID	Digital Identity
eID	Electronic Identity
Id	Identity
PAD	Personal Authentication Device
HRC	Human-Robot Collaboration
ITGT	IT Governance Trust
IDM	Identity Management
FAQ	Frequently Asked Questions
VC	Verifiable Credentials

Appendix

The appendix contains supplementary materials that were important for the research process. It contains the interview sheet and the questionnaire questions used for the user studies. These documents provide valuable insights into the methodology of this thesis.

The Research Interview Sheet

The Digital Identity Wallet – Interview

My name is Doruntina Murtezaj, and I am a Computer Science student at Freie Universität Berlin. I am currently working on my master's thesis, which focuses on the so-called Digital Identity Wallet app. The purpose of this interview is to gather information and perspectives related to the storage of multiple digital identities in one app, so that users can identify themselves online with different levels of assurance.
Your input will greatly contribute to the depth and richness of my study. Please feel free to share your thoughts openly, as all information will be treated confidentially and used for research purposes only. Before we begin, I want to assure you that your participation is voluntary, and you are free to withdraw at any point or decline to answer any specific questions if you prefer.
With your permission, I would like to begin the interview and record our conversation for accurate documentation. Is that alright with you?

Task 1: Setting up the app
Please open the ID Wallet app and follow the instructions to set up the app.

Task 2: Creation of a digital identity card
You have set up the ID Wallet app. Since you want to identify yourself to another service, you now need a digital identity. Please create the digital identity card.

Task 3: Registration to the library app (App-to-App Communication)
In addition to the digital ID card, you can also enter data manually and store it in your ID Wallet. Now you want to read the new bestseller book and have discovered a library where you can also create a digital library card and store it in your wallet. Your task now is to create this card.

Task 4: Creation of a digital driver's license (Web-to-App Communication)
You have discovered the service that you can digitally store not only the ID card and a library card, but also the driver's license on your smartphone. To do this, you call up the service via your PC in the web browser. Your task now is to create the digital driver's license.

Task 5 [Only in Phase 2]: Explore App Features
You are a new user of the ID Wallet app. Let's explore the features of the app and get familiar with the available menu options.

1. You know one of your cards is expiring this month, but you are not sure which one it is. Where can you check if you have expired cards in your ID Wallet?
2. You want to find out what actions you have taken with your ID Wallet recently. Where would you look?
3. You have a question and need customer support. How would you ask for help?
4. You are used to changing your passwords regularly. Where can you change the protection mechanism of your ID Wallet?
5. You want to find out how the wallet provider manages your data. Where would you look for this information?

[Only in Phase 1]

1. **Overall Experience:**

- How would you define the term "digital identity" in one sentence?
- How would you describe your overall experience with this app?
- Which aspects of this app impressed you the most and which disappointed you?

2. **Functionality and Features:**

- Did this app meet your expectations in terms of functionality? Please elaborate!
- What features or functions did you find particularly useful or lacking?
- Were there specific parts where you felt the app could be even more efficient?

3. **Usability:**

- Which features and functions of this app were not clear to you?
- What difficulties or confusion did you encounter while using this app?
- What do you think of the navigation in the app?

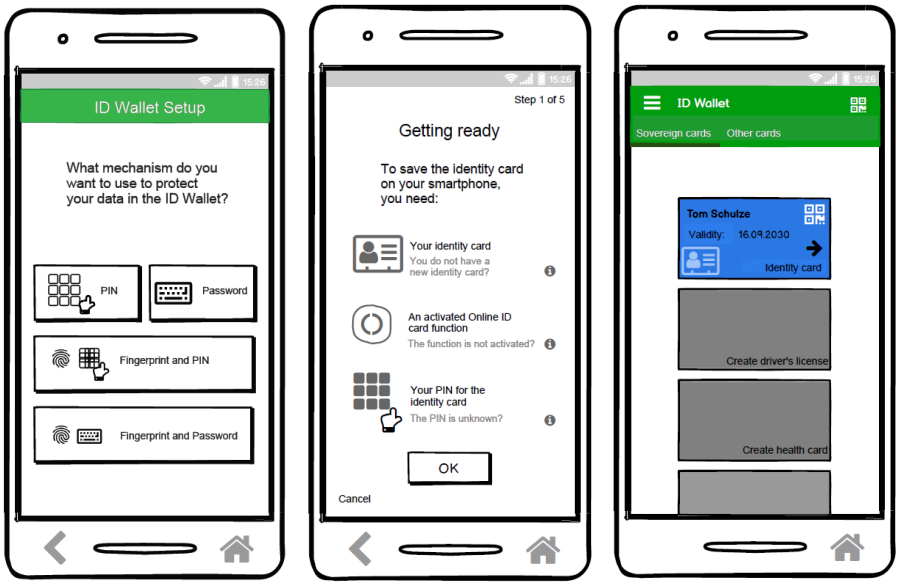
4. **Visual Design:**

- How would you rate the visual design of this app, e.g. aesthetics, layout, colour scheme? (1 - very dissatisfied; 5 - very satisfied)

- To what extent do you think the visual design matches the purpose of this app?
- Did the visual design enhance or hinder your overall experience with this app? How?

5. **User Trust:**

- Please select the most trusted screen for you. What did you take into consideration?



- Can you think of any visible feature or basic criteria that would make you not trust this app?
- This app can be operated by the state or by a private company. Who would you rather trust with your data and why?

6. **User Feedback and Preference:**

- What would you like to add, change, or remove from this app to better meet your needs and improve your experience with the app?
- You now have the digital ID card in addition to your physical ID card. Which of these two ID cards would you now use for in-person identification and why?
- Have you used similar apps in the past? If so, which ones and how do they compare to this app?

The Research Questionnaires

The Human Computer Trust Measure

1. I believe that there could be negative consequences from using the ID Wallet app.
2. I feel I must be cautious when using the ID Wallet app.
3. It is risky to use the ID Wallet app.
4. I believe the ID Wallet app will act in my best interest.
5. I believe that the ID Wallet app will do its best to help me if I need help.
6. I believe that the ID Wallet app is interested in understanding my needs and preferences.
7. I think that the ID Wallet app is competent and effective.
8. I think that the ID Wallet app has all the functionalities I would expect from it.
9. I think that the ID Wallet app performs its role very well.

The System Usability Scale

1. I think that I would like to use the app frequently.
2. I found the app unnecessarily complex.
3. I thought the app was easy to use.
4. I think that I would need the support of a technical person to be able to use the app.
5. I found the various functions in the app were well integrated.
6. I thought there was too much inconsistency in the app.
7. I would imagine that most people would learn to use the app very quickly.
8. I found the app very cumbersome to use.
9. I felt very confident using the app.
10. I needed to learn a lot of things before I could get going with the app.