Freie Universität Berlin
Institut für Informatik

Bachelorarbeit

User perception of credentials with regard to operator preference in digital wallets

Johannes Ehrich

1. Gutachter:	Prof. Dr. Marian Margraf
2. Gutachterin:	Jun.-Prof. Dr.-Ing. Maija Poikela
Betreuerin:	Sandra Kostic
Semester:	Sommersemester 2024
Verfasser:	Johannes Ehrich
Matrikel-Nr.:	5416380
Email:	johannee97@zedat.fu-berlin.de

Berlin den 21. Mai 2024

Abstract

Digital identity wallets offer a solution to the requirement of storing, managing and using digitized credentials. Private companies and governmental organs work on applications to provide their digital identity wallets to users. These applications can store both sovereign documents and non-sovereign documents alike. However, sovereign credentials, such as drivers licenses and passports, possess different properties compared to other credentials. Users have a choice to make regarding the credentials they want to store and who provides and operates the application they use. The purpose of this thesis is to investigate the influence of the credentials that users can store in the wallet on the choice of a provider. The conducted study focused on comparing sovereign credentials to non-sovereign credentials and investigating the differences in user preference regarding the provider for individual credentials. A pilot study and an online survey were used to investigate the topic. The conducted survey collected data on individual credentials and the correlating user preference. The study examined users both collectively and separately based on gender in order to also gather further insight into gender-specific preferences. The results conclude that the sovereignty of credentials leads to a significant preference towards a governmental provider. Furthermore, the study found that non-sovereign credentials sharing certain properties with sovereign credentials were also preferred to be stored in a governmentally provided digital identity wallet. Participants also expressed sovereignty as one of the arguments for a governmental provider. Male and female participants chose similar preferences for the individual credentials. However, male participants tended to express a stronger preference towards the provider they chose than female participants.

Selbstständigkeitserklärung

Ich erkläre gegenüber der Freien Universität Berlin, dass ich die vorliegende Bachelorarbeit 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, den 21. Mai 2024

Johannes Ehrich

Acknowledgements

First, I want to express my gratidue to my supervisor Sandra Kostic for guiding and helping me through conducting a study and writing a thesis. Furthermore, I would like to say thanks to the participants of the survey for providing me with their input on the topic. Finally I want to thank my wife for supporting me throughout not only the writing of this thesis but my all of my studies.

Johannes Ehrich

Contents

1 Introduction

This first chapter is intended to set the stage for the thesis and the correlating research by providing an introduction to the topic of digital identity wallets. Furthermore, it outlines the motivation upon which this thesis is based and the goals of the study.

In an increasingly digitized world, where transactions, communications, and interactions can be conducted online, the topic of digital identity is increasingly discussed [21]. Individuals can use their physical credentials ,whether to gain access to an institution with a corresponding key card, to pay in a shop with their credit card or to prove they have a certain right, for example the right to drive a car by presenting their drivers license [8]. The personal data contained in these credentials, such as a persons name or their date of birth, represents their unique identity and is commonly used by governments and companies to verify it. Whereas a physical credential and its data can be used to verify their identity in person, in the digital world a so-called digital identity is needed for identification online [18]. As with identities in the physical world, a digital identity can be verified using credentials. These credentials can be used in various scenarios similarly to their physical equivalent with the difference, however, that users of a digital identity may choose to only disclose data required for a transaction without being forced to reveal more [8].

A Digital Identity Wallet (DIW) offers a place that can be used to securely store digital credentials and other data belonging to the users digital identity as well as providing a way to manage this data or share it [3]. They offer a unified storage location for a significant amount of documents, credentials and certificates for all purposes. DIWs are increasingly realized in form of mobile applications as mobile devices have become a crucial part of modern day interaction [8]. These applications, apart from storing data, enable users to have more control over their data. However the core of DIWs lies within the ability to access important credentials or other relevant identity information under a secure digital format.

1.1 Motivation

The motivation behind this thesis stems from the increasing discussion about digital identity. As researchers predict the amount of users of digital identity documents to exceed 6.5 billion [22], digital identity wallet applications, relevant for the secure storage and use of the credentials, have to come into the focus. Governments and private companies all around the world have worked on establishing digital identities or launched their DIWs. Estonia and Luxembourg started testing and analysis in a pilot project for a European DIW in 2023 [12] and within the European Union (EU), the provision of a digital identity wallet has been made mandatory with a deadline of 2026 [27]. Furthermore, the EUs political program 2030 for the digital decade strives to ensure that all significant public services are available online by 2030 at the latest [10].
Whereas EU member states have to issue at least one DIW in the next two years, private companies have already launched their own DIWs or announced a future launch as well. Apple offers their „Apple Wallet“ [1] as their DIW, an app that was launched in 2012 under the name of „Passbook“ and is an integral part of the operating system of their smartphones as it comes pre-installed. The „Samsung Wallet“ [2] provided by Samsung was launched in 2022, the same year in which Meta launched their DIW [6].
Considering the continuous strive of the EU to integrate a European DIW and the various DIWs provided by private companies, users have a variety of DIWs to choose from. One of the aspects of that choice is whether to choose a governmentally provided DIW or one provided by a private company. This is a considerable choice as sovereign or otherwise significant credentials and certificates would then be stored in an application provided and operated by one of the previously mentioned companies or the government.

1.2 Goal

Digital identity is increasingly integrated into everyday life and different providers, private and governmental, offer their DIWs to potential users. [2] Various credentials and documents can be digitized to be used in a DIW. Considering the different properties of these credentials and the variety of DIWs

[1] `https://www.apple.com/wallet/`
[2] `https://www.samsung.com/de/apps/samsung-wallet/`

available to users currently or in the future, understanding the preferences of users regarding a potential provider of said DIWs becomes an important task. The main goal of this research is to discover the possible correlation between certain credential properties, notably sovereign credentials, and the users' preferred provider. The following research questions will be investigated:

RQ1: How does the sovereignty of a document affect the user's preference regarding the provider?

RQ2: What role does gender play in choosing a DIW provider?

Another focus of this thesis is to understand which properties of sovereign or non-sovereign credentials influence users' preference towards a certain DIW provider and to gain further insight in users' reasoning behind their preference. By gaining insights into these potentially influential factors, this study strives to contribute to a better understanding of users' needs and highlight aspects affecting their opinions. A comprehensive understanding of these affecting aspects could enable providers of digital identity wallets to further understand their responsibilities and potentially cater to their users' needs.

1.3 Structure of the Work

This thesis' structure is designed to offer an insight into the interplay of credentials' properties and users' views on the different types of DIW provider. First,Chapter 1 offered an introduction to the topic of Digital Identity Wallets and outlined the motivation and goals of the study. The following Chapter 2 will address related work that has been done on the subject of user perception regarding digital identity wallets. Chapter 3 provides a detailed description of the process and design structure behind the study, as well as the conducted survey which was used for this thesis. In Chapter 4 the results of the study are presented. The findings derived of the researches results are discussed in Chapter 5 where the results are interpreted in context of this thesis' goals. Lastly Chapter 6 summarizes the findings and highlights significant insights gained by the interpretation of the researches results. Furthermore the last chapter offers recommendations for future research.

2 Related Work

This chapters intent is to give an overview of previous research done in the context of user perception on digital identity wallets. This overview offers an insight on different researchers' focus regarding the topic and offers context to the focus of this thesis.

Various work has been done on the subject of user perception in regard to digital identity wallets [17][20][25]. The research focuses on different aspects of user perception in this context. A study by Sjöholm [25] analyzed aspects of user trust in the context of the European DIW and therefore discussed user perception on governmental DIW providers. Sjöholm discussed potentially influential factors regarding users' trust in governments in the context of digitization. Notably participants of this study mentioned Germany as an example of a country in which citizens might distrust governmental authorities when it comes to digital matters, a sentiment which might stem from previous digitization attempts in which German authorities struggled to accomplish their goals [24].

Another work, done by Murtezaj [20] offered some insight into potentially influential aspects of DIW applications in relation to users' perception. The study focused on different aspects of possible DIW applications and their influence on user perception, notably user trust and perceived usability. Other than in Sjöholms work, this study provided insight into the differences in trust, based on whether the provider of an application was the government or not. Murtezaj found users to trust an application operated by a governmental provider more than one that was not. However credentials used as exemplary use cases for the study were not separately examined and two of the overall used credentials were sovereign credentials.

Lastly, a study by S. Kostic [17] focused more in depth on user preference regarding a DIW provider. Their research also factors in potentially different user perception for sovereign and non-sovereign credentials. The study found a general preference towards a governmental DIW provider. The direct referencing of sovereign credentials was avoided in the beginning of the survey and participants were asked, after answering their provider preference, whether they would change their answer knowing that sovereign credentials were also supported which the majority declined. Based on their results, the study conclusively assumed that the general governmental preference was not affected by the ability to store sovereign credentials in the application.

Kostic [17] mentions the potential influence of sovereign credentials and, as well as Murtezaj [20], focuses on factors which might have an impact on whether a private or a governmental provider is preferred by users. However, other research in the field of user perception on digital identity wallets focuses on user perception in relation to the concept of the wallet or technical aspects [2]. Research in this field does not examine the individual credentials and their possible effect on user preference, which is where the focus of this thesis lies.

3 Research Methodology

This chapter provides an insight into the methodological approach of this study. It offers a discussion of used instruments and an explanation of their choice. Moreover it includes a structured analysis of the design of both the research and the conducted survey respectively, as well as a short overview of the implementation of the survey.

3.1 Online Survey

This study chose an online survey as method of data collection. Advantages of this method are manifold [11]. Conducting an online survey offered a rapid collection of a significant sample, as time to conduct the survey and the collection of response data are comparatively little. In comparison to personal surveys, where researchers are present, online surveys offer a greater guarantee to avoid bias caused by the interviewer [11]. Lastly this method facilitates the implementation of multimedia in the survey as well as the provision of engaging answering methods such as sliders.

3.2 Pilot Interviews

In order to test out the survey before deployment various pilot interviews were conducted. This method was chosen to provide the opportunity for adaptation to potential participant needs for introduction or explanation. Furthermore conducting pilot interviews gives the researcher valuable insight on how the topic of the study is perceived by the participants [16]. For this study the pilot interviews were deemed necessary in order to enable the seamless conduction of the study after deployment and to potentially modify or streamline questions.

3.3 Research Design

The user study was conducted in three phases, with the third and final phase being the quantitatively most significant. Initially only two phases were planned to be conducted, with the study consisting of a pilot phase and a main phase. However, another pilot phase was conducted beforehand in order to further assure the validity and usability of the final results. This change in the research design was made based on the recognition that there might be a knowledge gap regarding the concept of digital identity wallets among the participants and the importance of the ability to conduct the final survey remotely.

3.3.1 Pilot phase 1

The first phase was conducted in order to verify that the concept of DIWs was sufficiently explained to the participants of the study. A short sequence of slides, explaining the concept, were shown to the participants. During the first pilot phase a moderator was present in order to verify that the explanation would lead to a sufficient understanding of the topic in order to correctly answer the following questions. The phase consisted of 3 separate interviews, in which the participants were shown the slides before asking them about their opinion about the concept of DWIs. Based on the results, no further modifications were made to the explanation slides. Figure 1 shows the slides as they appeared in the survey. The slides were then used as an introduction to the survey, which was used for phase two and three. The participants of the first pilot phase were not used as participants in the main survey.

Figure 1: Explanatory slides

3.3.2 Pilot phase 2

During the second pilot phase, five participants answered the survey with a moderator present in order to ensure the understandability of the survey questions and to discover whether the survey could be remotely conducted without a researcher present. Participants were encouraged to vocalize their thoughts on the questions and the survey itself. This think-aloud method [9] allowed for an insight into their views on the survey design and their understanding of the topic. Based on comments given by the participants regarding the survey, minor changes were made to the phrasing of some questions. After thorough deliberation, the five participants of pilot phase two were taken into account for the final evaluation of the data since the changes implemented did not affect the survey other than slightly increasing usability. Furthermore, the moderator did not influence the participants by answering questions or giving any instructions apart from encouraging the participants to vocalize their thoughts.

3.3.3 Phase 3

In the final phase, the survey was conducted remotely and unsupervised. The survey was open to the public for two weeks, in which the web-link and a corresponding QR-code were distributed over multiple channels.

3.4 Survey Design

In the survey design, it was essential to keep in line with best practices [26], such as facilitating comprehension by keeping the survey simple or avoiding leading participants to certain answers. Furthermore, the survey was designed to be quick and intuitive, especially in regard to the first batch of questions.

In order to question a sufficient amount of participants, an online survey was chosen as a medium for the study. This medium offered the advantage of a quick and efficient distribution via web-link and corresponding QR-Code. Furthermore, it enabled participants to access and answer the survey on their mobile devices facilitating a higher willingness to partake in the study.
As mentioned in chapter 3.3, two pilot phases were conducted to assure that the study could be conducted remotely. After the initial explanatory slides established in phase one, the first batch of questions asked participants about their preference for individual credentials in a DIW and which provider they preferred for each one. Instead of a Likert scale a slider was used to answer the questions, to accommodate the nuances of possible answers and to further encourage intuitive answers by the participants [5]. To mitigate potential drawbacks of using a slider instead of a traditional answering method, an introductory slide was shown before the questions. Furthermore, an explanation of a private provider was added. The explanation underwent multiple drafts in an attempt to avoid bias and confusion. The final draft included the option of a global or national company in order to not be specific. As an example, the company SAP was chosen. SAP represented a globally active company, based in Germany. The decision to include a known German company was made based on the study of S. Kostic [17], in which a known German private company was the second most preferred DIW provider.

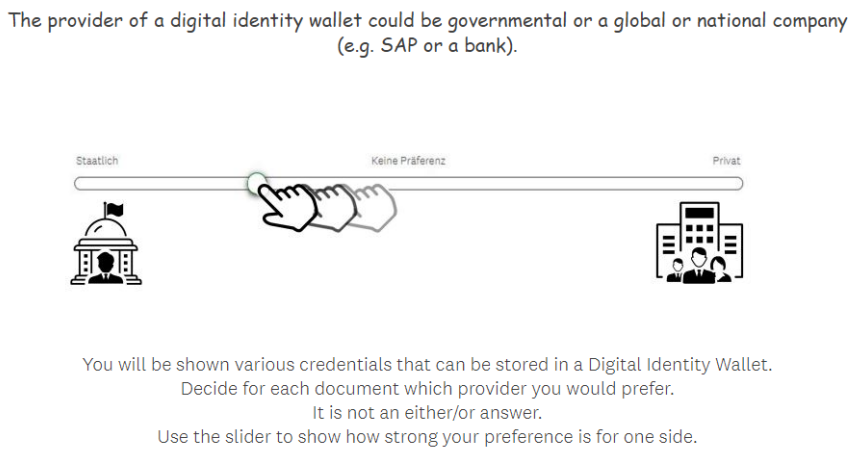

Figure 2: Slider Explanation

In the second batch of questions, the participants were given the opportunity to choose from the previous credentials for which they would definitely prefer a governmental provider and for which a private one. Another question was added, asking which credentials they would prefer not to be in a DIW at all. This question was added to differentiate neutral responses in the first question batch between not having a preferred provider and actively rejecting either one. In each of these questions, participants were given the option to give an explanatory open-ended answer as to why they chose the credentials. These answers account to the qualitative research in the study.
In the final questions, participants were asked whether they knew of the concept of DIWs and whether they would use a DIW, followed by demographical questions regarding age and gender.

3.5 Sample Selection and Implementing of User Study

In correlation to the three phases of research design, the user studies were carried out in three phases. The three participants of the first phase were chosen to represent three different age groups, different genders and varying technological knowledge. They were questioned over the course of three days.

The second phases participants were also chosen to vary in technological knowledge. While they also varied in regards to gender, all five participants were from the age group of 28 to 37. The participants were asked to complete the survey while vocalizing their thoughts on their answers, as well as the survey design while doing so. All interviews were conducted on the same day, albeit sequentially and separately to avoid interplay between the participants and enable uninfluenced results. Changes to the survey made after the second phase were minor, the most significant being the addition of the indication of optionality of open-ended answers, which was mentioned by three of the five participants. The lack of explanation needed on any of the questions and the vocalized deliberation on each question verified the ability of a remotely conducted survey.
Finally, for the third and final phase, the survey was made public in form of a web-link. The link was distributed over various channels, including publicly displaying a QR-code in medical practises and hospitals, as well as making the

link available on multiple media in order to collect participants for the study. There was no deliberate sample selection done for the third phase, in order to get a large and random sample. Answers were collected over two weeks during which potential participants could access the survey.

4 Results

In this chapter, the results of the user study will be presented. The chapter is divided into three subchapters. The first two subchapters contain results in relation to the two research questions outlined in chapter 1.2 . The third subchapter covers other results not mentioned in the first two subchapters. Considering the minority of the changes made to the survey after the second pilot phase, the five participants of the second phase of the study have been included in the total amount of participants and are not counted as a separate test group. Furthermore, one of the participants only answered the first batch of questions and is therefore not included in the second and third batch, including demographic questions. However, their responses for the first batch, which the participant completed, are considered valid in this study. Therefore, the total amount of 98 participants, used to calculate mean values for the first question batch, deviates from the total amount of participants in the latter question batches by one.
Within the two weeks of phase three 93 participants answered the online survey which, added to the five participants, total 98 participants for the study. The distribution of gender and age is shown below in Figure 3.

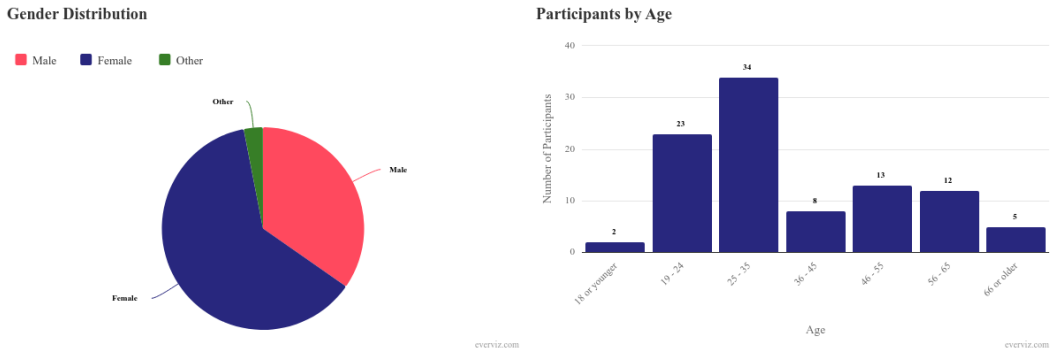

Figure 3: Gender and age distribution of the participants

Participants spanned across all available age groups, with two participants being 18 or younger and five participants being over 65 years old. With

34 participants, the age group between 25 and 35 represents the majority. Furthermore, 61 participants of the study were female and 34 male. Neither nationality nor technical knowledge were asked of the participants.

4.1 Sovereign and Non-Sovereign Credentials

The focus of RQ1 lies on discovering the effect of the sovereignty of credentials, stored in a DIW, on the users' preference of DIW provider. The participants were asked on their preference on the 16 credentials. Four of the credentials were classified as sovereign credentials and 12 were classified as non-sovereign. The credentials classified as sovereign were „ID Card“, „Passport“, „Drivers License“ and „Birth or Marriage Certificate“. Whereas the first three credentials are commonly mentioned as sovereign credentials [17], the classification of the credential „Birth or Marriage Certificate“ as sovereign derives from its status as a civil status certificate (German „Personenstandsurkunde“), which is established in German law [1].The non-sovereign credentials for the purpose of this study were „Organ Donor Card“, „Healthcare Card“, „Certificate of eligibility for social housing (CEH)“, „Student ID“, „School Certificate“, „Licenses (fishing license, hunting license, etc.)“, „Credit Card“, „Work ID / Company ID“, „Ticket (Travel)“, „Membership ID (e.g. gym card)“, „Ticket (Entry)“ and „Discount Card“. Possible ambiguity in the credential names, notably „Ticket“ and „Certificate“, only apply to English, as their German translations are unambiguous.

The responses for the first batch of questions were translated to numerical values resulting in a possible range from -100 to 100. Moving the slider towards the governmental provider resulted in a negative value and moving it towards the private provider resulted in a positive value. While these numerical values were not visible to the participants, they facilitate the visual representation of the results as well as their analysis. A frequently used term in this thesis is the term „mean“, a commonly used term in descriptive statistics [19]. The mean, also known as average, is calculated by adding up all the values in a set and dividing the result by the number of values.

The order in which participants were presented with the different credentials was chosen randomly during the survey design. However, each participant received them in the same order. Figure 4 shows the mean values for each of

the 16 credentials. For each sovereign credential the mean value was negative indicating a preference for a governmental DIW provider. For all four of these sovereign credentials the mean value was lower than -50, with the lowest value being the value for „Passport“ (-58,1).
Of the 12 non-sovereign credentials participants were shown six had a positive mean value indicating a preference towards a private provider with the highest two values given to „Membership ID (e.g. gym card)“ (64,2) and „Ticket“ (63,1). The mean value of the credential „Licenses (fishing license, hunting license, etc.)“ (-4,8) deviates least to either side. Furthermore, among the non-sovereign credentials, the mean value of the credential „Organ donor card“ at -51,0 indicates the strongest preference towards a governmental provider, similar to the lower values of the sovereign credentials. The other non-sovereign credentials with a negative mean value accounted to „Healthcare Card“, „Certificate of eligibility for social housing (CEH)“, „Student ID“, „School Certificate“ and the aforementioned „Licenses (fishing license, hunting license, etc.)“.

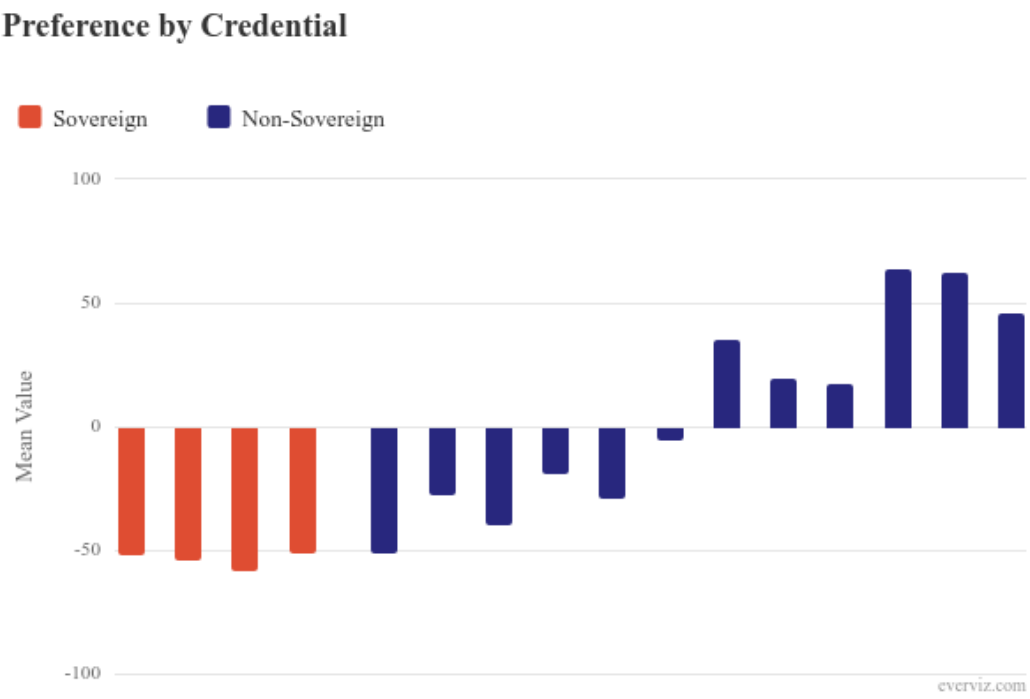

Figure 4: Mean values of all credentials

When asked to choose the credentials which they would definitely want a governmental DIW provider for from a list of the 16 credentials, the four

sovereign credentials were chosen most by the participants. The most picked credential „ID Card“ was picked by 79 of the participants. Furthermore the „Organ Donor Card“ credential, the most picked non-sovereign credential, was chosen by 52, more then half of the total amount of participants. Whereas the least chosen sovereign credential was picked by 65 of the participants 10 of the non-sovereign credentials were chosen 33 times or less. Eight participants did not choose any credential to be in a governmentally provided DIW.

36 participants chose to give an explanation for their choices in the open-ended section of this question. Of these 36 responses, 14 were related to the sovereignty of the credentials in question. These responses mentioned the governmental origin of the credentials as their main argument. One participant commented *„Because these are documents issued by the state and contain sensitive information“*. Another participant noted *„It feels natural to store things that come from the state in an app from the state, because then as few parties as possible have my data“*. 10 responses named privacy and data security as a reason for their choices, which they perceived as a reason to choose a governmental provider. A more detailed comment by one participant stated *„I fear that private operators can offer less secure platforms than the state. If the state is behind a feature, it automatically seems more secure to me because I trust the state. You would have to research private providers before entrusting them with data that is as vulnerable as your ID card.“* Furthermore 8 participants mentioned their distrust towards private corporations regarding the handling of their personal data. Participants stated they would definitely want a governmental DIW provider *„In order to avoid abuse by private providers.“* and voiced their concerns that *„private companies would find a way to sell this data“*.

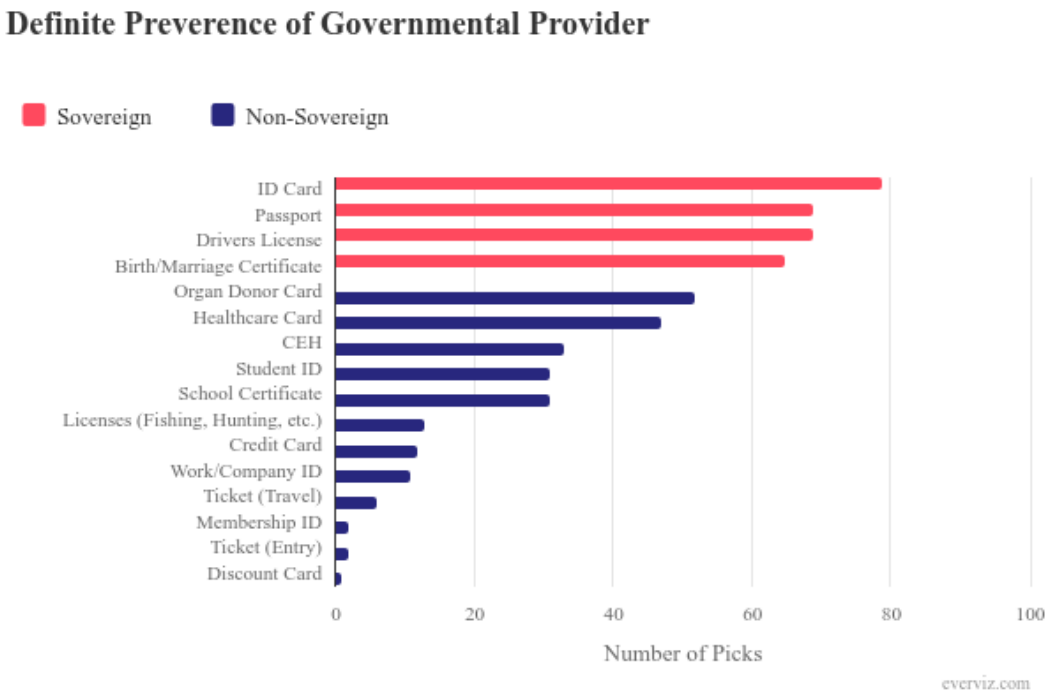

Figure 5: Number of picks for definite governmental preference

In the following question, participants were asked for which credentials of the same list they would definitely prefer a private DIW provider. The four sovereign credentials were picked less than 13 times each. „Organ Donor Card“ was chosen by only five participants and therefore the least of all credentials. Overall less credentials were chosen in this question than in the previous. Only two of the non-sovereign credentials, „Membership ID (e.g. gym card)“ (54) and „Ticket“ (53), were chosen by more than half of the participants. Furthermore 25 participants, more than a quarter of the total, did not pick any credential in this question. 21 participants gave an explanation in the optional section of the question. In the open-ended section, eight participants named the credentials' private commercial property as reason for their preference. One participant commented *„These are things that have to do with services and have nothing to do with state matters“* while another stated *„These are private commercial documents“*. Three participants mentioned an avoidance of governmental bureaucracy, such as one participant who stated *„Moreover, the state should not have to take care of everything, otherwise there will be a backlog of paperwork“* and one participant mentioned mistrust in governmental providers, commenting *„The state has nothing to do with these, nor should*

it; they depict a person's private life and are therefore data that could, in the worst case, be misused by the state. With fatal consequences for the individual. Therefore, the option should not be made available so easily.“

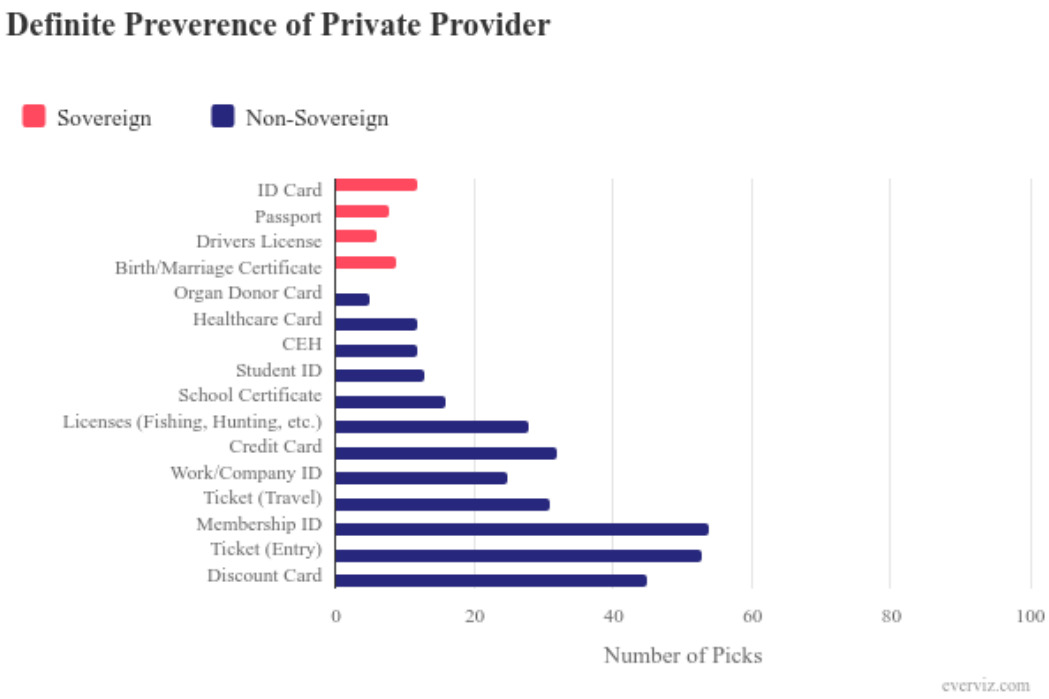

Figure 6: Number of picks for definite private preference

4.2 Gender

RQ2 focuses on understanding the effect of gender on the participants' preference towards either type of DIW provider. Figure 7 show the mean values for all credentials for each of the two compared genders. Although participants of other genders participated in this survey, the sample of only three participants was deemed to small to form a valid representation of this study.

Overall, female and male participants expressed similar preferences regarding which provider they wanted for each of the 16 credentials. The credential „Licenses (fishing license, hunting license, etc.)“ was the only credential for which the mean preference differed. Simultaneously this credential was also the one with the least deviation from zero for both genders. Whereas male participants

slightly preferred a governmental provider (-11), female participants preferred a private one (1). Furthermore, for 14 of the 16 credentials the mean values derived from the male participants' responses deviate further from zero than the females'. The highest differences in deviation occurred with the sovereign credentials „Student ID“ (male -42.8, female -3.1) with a difference of 39.7 and „ID Card“ (male -73.2, female -39.7) with a difference of 33.5. For the credential „Credit Card“ (male 35, female 35.8) the difference was 0.8 constituting lowest deviation difference. Furthermore, this credential was the only to have a higher deviation in female responses than in male responses.

Table 1: Mean values from male and female answers

Credential	Male	Female
ID Card	-73,2	-39,7
Passport	-76,0	-50
Drivers License	-69,1	-43,8
Birth/Marriage Certificate	-66,3	-43,4
Organ Donor Card	-55,2	-46,3
Healthcare Card	-49,3	-15
CEH	-56,3	-30,2
Student ID	-42,8	-3,1
School Certificate	-43,5	-17,3
Licenses (Fishing, Hunting, etc)	-11,6	1,3
Credit Card	35,0	35,8
Work/Company ID	24,1	19,9
Ticket (Travel)	23,7	18,0
Membership ID	70,1	61,7
Ticket (Entry)	68,0	60,2
Discount Card	56,3	43,6

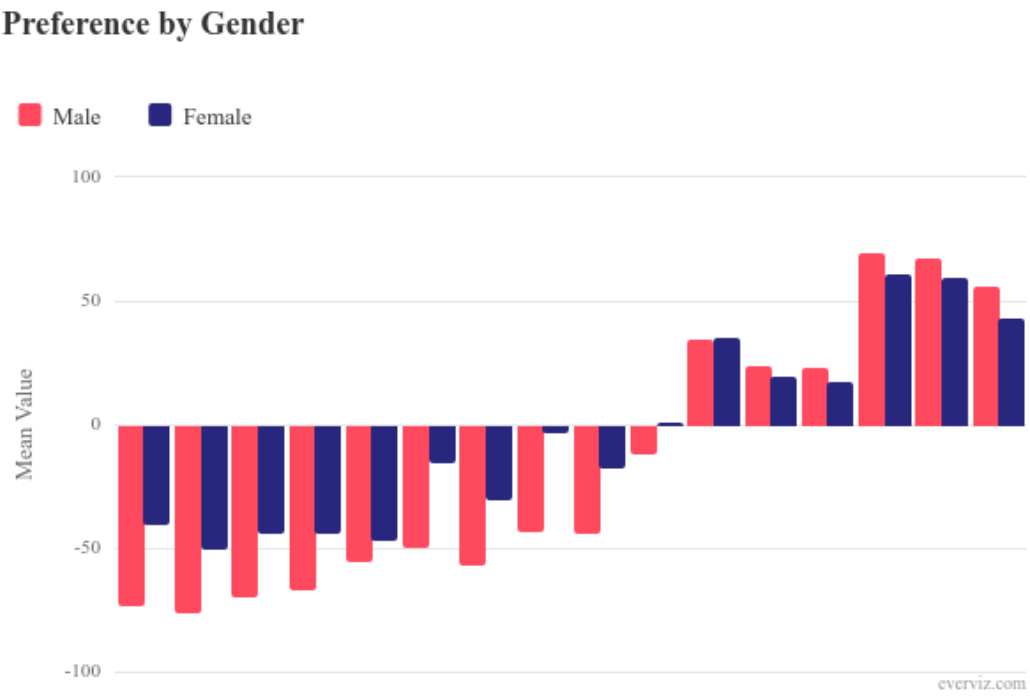

Figure 7: Mean preference values of male and female participants

As shown in Figure 8, the female and male participants chose similarly when prompted to pick credentials for which they would definitely want a governmental DIW provider. Both gender groups chose sovereign credentials more often than non-sovereign credentials. The most chosen non-sovereign credentials for both gender groups were „Healthcare Card“ and „Organ Donor Card“. All other credentials were picked by less than half of the participants respectively.

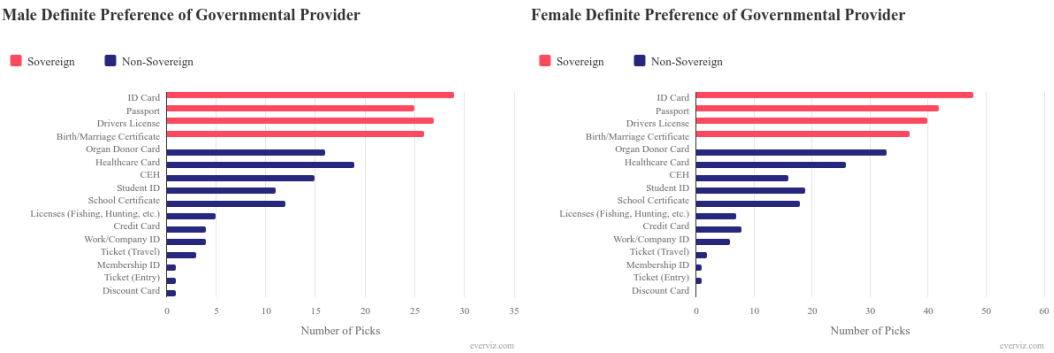

Figure 8: Picks for definite preference of a governmental provider male(left) and female(right)

Figure 9 depicts the female and male participants' choices in regard to which credentials they would definitely want a private provider for. Both female and male participants picked the non-sovereign credentials „Membership ID (e.g. gym card)“, „Ticket“ and „Discount Card“ as their most wanted credentials. The most chosen sovereign credential for both gender groups was „ID Card“, with three picks from the male participants and nine from the female participants.

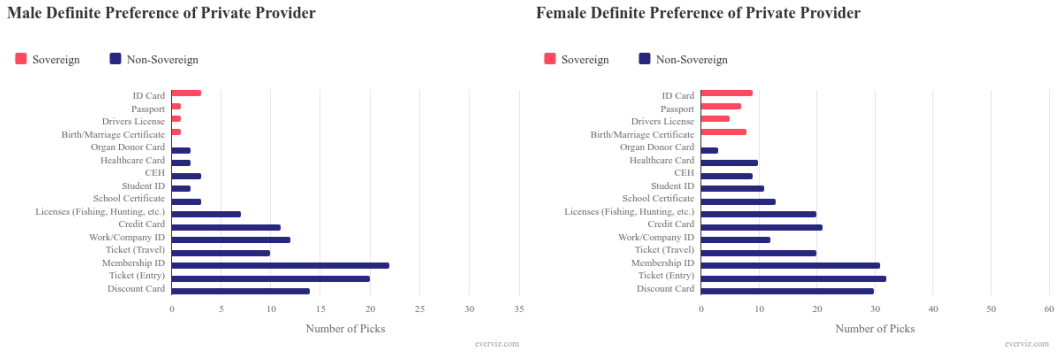

Figure 9: Picks for definite preference of a private provider male(left) and female(right)

4.3 Acceptance of Digtial Credentials and Digital Identity Wallets

The final question of batch two asked participants which credentials they would not want in a DIW at all. Responses were collected in the same manner as with the previous two questions. Figure 10 shows how often each credential was chosen. Results ranged from five picks, for the credential „Ticket (Travel)“, to 23 for the credential „Certificate (School, University, etc.)“. Overall, every credential was chosen by less than a quarter of the participants. 48 of the 97 participants did not pick any credential for this question. 10 of the 23 participants who gave an explanation named privacy as their reason. One participant commented „It's all too sensitive for me.“. Furthermore four participants mentioned „Fear of abuse“.

When asked whether they would use a Digital Identity Wallet, a majority of 72 answered „Yes“ and 24 answered „No“. Furthermore 43 participants expressed that they had heard of a DIW before but did not use one and 38

participants stated that they already use a DIW.

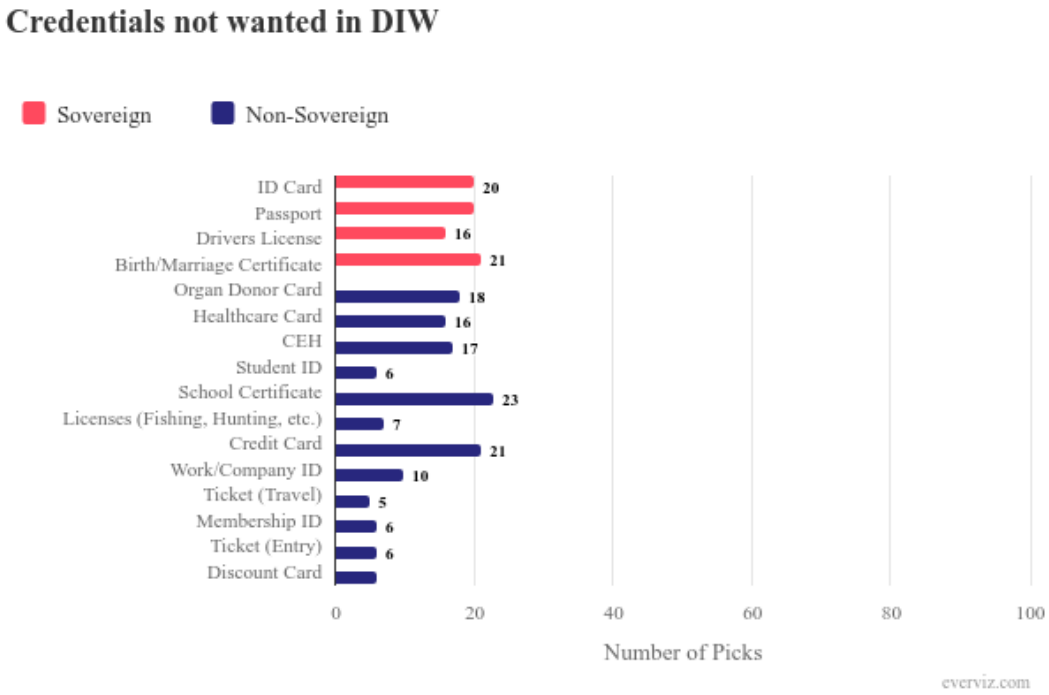

Figure 10: Picks for credentials not wanted in a DIW

5 Discussion

The intent of this chapter is a discussion of the research by reviewing its results and offering possible explanations, as well as interpretations. The chapter is divided into two subchapters, each focusing on one of the research questions RQ1 and RQ2.

5.1 Sovereignty

A significant insight constitutes the importance of certain credential properties and how they affect potential DIW users. The participants of this study have shown a significant preference towards governmental DIW providers for sovereign documents. This can be assumed based on the overall low mean values of -51,2, -53,7, -58,1 and -51,0 which rank them at the top of the credentials with governmental preference. However, their reasoning focuses on different properties of sovereign credentials. When addressing the sovereignty of the credentials the origin of the credential was significantly mentioned. Participants see the responsibility concerning credentials that were issued by the government with a governmental provider. This is further supported in this study by the responses given for credentials that are typically or predominantly issued by governmental authorities. „Certificate of eligibility for social housing“, „Student ID“, „Certificate (School, University, etc)“ and „Healthcare Card“ had mean values of -39,3, -18,4, -28,5 and -26,9 respectively. Whereas a „Certificate of eligibility for social housing“ is always issued by a governmental agency, schools, which issue student IDs as well as school certificates, and healthcare providers can be privately owned. However, schools in Germany are predominantly public [13] and a significant majority of the German population has a public healthcare provider [7] . Therefore, for a majority of the population, these credentials are issued by governmental authorities. For all of these credentials a governmental provider is preferred, as shown by the mean values derived from the answers, while for all but two of the remaining non-sovereign credentials it is not as can be assumed based on their positive mean values. This shows the significance of

the governmental origin of sovereign credentials for users' choice of provider.

Another inherent property of sovereign credentials, that has a considerable effect on potential DIW users, is the sensitivity of their data. Privacy and security concerns regarding sensitive data were mentioned by multiple participants of the study in the second batch of questions (see chapter 4.1). These concerns and the correlating fear of abuse were mentioned as an argument for choosing a governmental provider, as an argument for choosing a private provider, as well as an argument to not store credentials in a DIW at all. As other research has shown, mistrust towards the government, as well as private companies, has a significant effect on user perception in regards to privacy concerns [28][15]. However, certain types of data are perceived as more sensitive than others, as seen in a study by Gupta et al. [14], who offered a taxonomy of data types and measured sensitivity levels for each type. As sovereign credentials contain identity and even biometric data, users tend to see them as sensitive. As shown in this study (see Chapter 4.1), users prefer a governmental provider for documents containing such sensitive data. A finding further supported by the comparatively strong preference of a governmental DIW provider for credentials containing health related data, such as „Healthcare Card“ and „Organ Donor Card“, as health data is also considered one of the most sensitive data types according to Gupta et al. [14]. These two credentials were picked by 54 and 47 participants in the question regarding definite preference of a governmental provider, ranking 5th and 6th after the four sovereign credentials with 79, 69, 69 and 65 picks.

Overall, the results of the study not only show the impact sovereignty of credentials has on users' preference but also highlight specific inherent properties of sovereign credentials which cause users to also prefer a governmental DIW provider for other credentials sharing one or more of them. Furthermore, potential DIW users show a significant amount of privacy and security concerns affecting their acceptance of the storage of credentials containing sensitive data in a Digital Identity Wallet. Although mistrust towards both potential providers have been voiced in this study, more participants tended to mistrust private providers and more participants perceived a governmental provider to a be a more secure choice.

5.2 Gender

Another intent of this thesis is to gain further insight into potentially different preferences and opinions of different gender groups on DIW providers. As the results of the study show, in terms of general preference regarding sovereign and non-sovereign credentials female and male participants tended to choose similarly. (See Chapter 4.2) Both gender groups wanted the sovereign credentials to be in a governmentally provided DIW, as seen by their significantly negative mean values. Furthermore, the same properties of sovereign credentials, as discussed above (see Chapter 5.1), shared by some of the non-sovereign credentials influence their opinion on their choice of provider for each individual credential. The argument of sensitive data and a resulting preference towards a governmental DIW provider is notable in both groups, as it was mentioned by participants of both genders in the open-ended responses. Both male and female participants picked the credentials containing health data as their most preferred non-sovereign credentials for which they definitely want a governmental provider. The most chosen credentials of the remaining non-sovereign credentials consisted of the credentials issued mostly by governmental authorities, as discussed above (Chapter 5.1). In the scaled responses, the female and male participants chose the same provider preference on all but one credential in the study. The significance of this single credential „Licenses (fishing license, hunting license, etc.)“ not showing the same preference for both gender groups is comparatively low, considering it was picked by less than a quarter of the participants for either definite governmental preference, definite private preference or not wanted in a DIW at all, for which it was picked by 13, 28 and 7 participants respectively. Furthermore, this credential showed to have the mean value with the lowest deviation from zero for male participants, female participants and in total, with mean values deviating no more than by 11.6 for the male participants. This supports the suggestion of an overall comparatively low importance of the credential to users and therefore does not decrease the significance of the otherwise equal general preferences in male and female responses.

A key finding, when reviewing the surveys results, lies in the difference in deviation between male and female answers for the questions utilizing a

slider as answering method. As seen in chapter 4.2 the mean values of male participants' answers tended to deviate further from zero than those of the female participants. For most of the credentials a clear difference in deviation could be examined, especially for sovereign credentials where deviation differed by over 22 for all four credentials. The resulting suggestion towards stronger preferences in male users requires further consideration of gender differences in survey questions with scale based answers.

In order to understand whether this difference is based on a difference in preference intensity or on the answering method given by the study, other factors of scale based survey answers need to be examined. The term „Extreme Response Style (ERS) refers to the tendency to prefer responding using extreme endpoints on rating scales.“ (John H. Batchelor) [4] As research suggests, the more „extreme“ responses of one gender group in the survey might be attributed to participants' demographic properties including gender. In his study, Batchelor noted that, whereas some studies found no significant differences between the two examined gender groups, those studies who reported a difference found females to engage in ERS more than males[4]. Considering these findings on ERS, the more „extreme“ values of this studies male participants appears to not be attributed to ERS based on gender. Other attributing factors to ERS, notably participants' ethnicity and intelligence have not been collected in this survey and therefore can not be taken into account.

Based on these considerations, this thesis' underlying study found that although potential male and female DIW users generally agree on their preference regarding which DIW provider they prefer for different credentials, male participants tend to express a stronger preference towards their chosen provider. This is especially the case for sovereign credentials, considering the high difference in deviation seen in this study.

6 Limitations

This chapter is meant to address some limitations to the study and its findings. First, the surveys results only reflect the opinion of German users. Although German nationals were not exclusively addressed, the survey was only available in the German language. Although digital identity wallets are a subject of international interest, each country represents an individual governmental provider and citizens trust in their government in general or in regards to digital matters specifically can differ [25]. Moreover, properties of individual credentials, especially sovereign credentials also vary based on the country. The credential „Birth or Marriage Certificate“ offers some insight to this variation. Whereas in Germany a birth certificate contains the gender of the child, it does not contain this data in Switzerland. In Germany, a birth certificate constitutes a sovereign document by German law [1]. In Sweden a birth certificate does not exist at all. Therefore, the decision of limiting the scope to German participants in order to examine credential properties and their effect was made.

Second, studies on sliders as an answering method in surveys have suggested a higher potential for misunderstanding among participants [23]. This study attempted to mitigate this potential by expressively explaining the answer format in the survey, in form of an explanatory slide shown before the questions. On the slide participants were informed that their answering option was scaled and not a simple „either-or“ answer. Furthermore, a supervised pilot phase was conducted in order to verify the resulting mitigation. As none of the pilot phases participants voiced confusion and used the sliders as intended, the explanatory slide was assumed to be sufficient.

Lastly, the chosen credentials represent only a fraction of those possible to store and use in a digital identity wallet and therefore, other credential properties influencing users' preference might not be represented in this thesis. The sample chosen for the study contained the four credentials, which were

either mentioned to be sovereign by other sources or justifiable to be classified as sovereign. The 12 non-sovereign credentials were intended to represent multiple different use cases, data types and other properties, such as issuer. As such, some of the non-sovereign credentials were intended to overlap with sovereign credentials in regard to some of the listed differences.

7 Conclusion

This chapters is intended to present the conclusion of this thesis. It offers a a retrospective summary of the study, its contribution as well as key findings. Furthermore it provides suggestions for further research in this area, which may be of investigative interest.

7.1 Summary

The purpose of this thesis was to gain a comprehensive insight into the influence credentials, stored and used in digital identity wallets, and their properties, have on the potential users preference of digital identity wallet providers. The research focused on the effect of credentials' sovereignty and the underlying properties inherent in sovereign credentials. This effect was researched both on users overall, as well as on male and female users separately. An unsupervised and remotely conducted survey was employed in order to collect data from a diverse group of participants. Two supervised pilot phases were implemented prior to the final main study phase in order to ensure the validity of the unsupervised surveys results. Through the study, valuable insights were gained regarding the significance of sovereign credentials for users' preferred choice of DIW provider. Further insight was gained into specific properties of credentials, which affect this choice as well. Additionally this study observed gender based differences in the context of preferences regarding DIW providers.

7.2 Key Findings

One of the key findings derived from this study is the significant impact the sovereignty of a credential had on the participants' choice of a preferred provider. Throughout the study, participants consistently expressed their preference towards a governmental DIW provider when concerned with a sovereign credential. The four sovereign credentials offered by the study ranked highest in governmental preference mean values and were also the four most chosen

credentials for a definite governmental provider preference. Furthermore 38,8% of the open-ended responses in regard to governmental preference named the fact that the credentials were issued by the government as their reason for a governmental preference. This property of sovereign credentials, as well as the property of containing sensitive personal data, which was named second most in the same question, was found to be the driving factor behind the preference of a governmentally provided DIW for these credentials. This key finding was further supported by credentials, fulfilling one or both of these properties, to be ranked highest among the non-sovereign credentials' governmental preference value. Especially for credentials containing health related data a governmental preference was expressed, despite them not being issued by the government.
When examining differences in provider preference based on gender, this study found both male and female participants generally agreeing on their choice of provider for the different credentials. Sovereign credentials showed the highest preference towards governmental providers in both groups, followed by the non-sovereign credentials sharing inherent properties with them. A key insight, however, lies in the difference of preference intensity in the different gender groups. Results found male participants to generally express a stronger preference towards the chosen provider than female participants. After considerations of a potential reason behind this difference related to the format of the study and the corresponding potential of ERS-based differences in male and female answers, the occurrence of a stronger expressed male preference was found to be significant. As ERS was ruled out as the cause of the difference, these findings suggest male users to feel more strongly about their preference to either possible provider.

7.3 Future Research Directions and Recommendations

This thesis focused on the influence of sovereignty of credentials on user preference. Whilst examining the interplay of sovereign credentials and DIW provider preference, the study discovered inherent credential properties which influence preference regardless of sovereignty. Future research could delve further into this direction by examining other properties of credentials which might influence users' preference further. A useful guideline might be to understand more properties of sovereign credentials, in order to examine them individually.

Furthermore, non-sovereign credentials for which a stronger preference towards private DIW providers was expressed, could be examined similarly to gain insight on their influential properties.

Moreover, further research could be done with additional or different demographic parameters in focus. Age and technical knowledge as focus could be of interest, as well as nationality. This last demographic detail could be of particular significance considering the EUs European digital identity wallet project and the corresponding regulations for member states. As this project entails an expansion of cross-border authentication, the interplay of sovereignty of credentials and nationality might provide relevant insights into users' perception on the topic.

References

1. [n.d.]. §55 PStG https://www.gesetze-im-internet.de/pstg/__55.html.

2. Ansaroudi, Z. E., Carbone, R., Sciarretta, G. and Ranise, S. [2023], Control is nothing without trust a first look into digital identity wallet trends, *in* 'IFIP Annual Conference on Data and Applications Security and Privacy', Springer, pp. 113–132.

3. Attoresi, M. [n.d.], 'Digital identity wallet'. https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/digital-identity-wallet_en [Access: 20.05.2024].

4. Batchelor, J. and Miao, C. [2016], 'Extreme response style: A meta-analysis', *Journal of Organizational Psychology* .

5. Betella, A. and Verschure, P. F. [2016], 'The affective slider: A digital self-assessment scale for the measurement of human emotions', *PloS one* **11**(2), e0148037.

6. Counsil, B. [n.d.], 'Meta set to launch digital wallet for metaverse users'. https://www.blockchain-council.org/news/meta-set-to-launch-digital-wallet-for-metaverse-users/ [Access: 20.05.2024].

7. *Destatis, Krankenversicherungsschutz* [n.d.]. https://www.destatis.de/DE/Themen/Arbeit/Arbeitsmarkt/Qualitaet-Arbeit/Dimension-2/krankenversicherungsschutz.html [Access: 20.05.2024].

8. *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.* [n.d.]. Retrieved from https://secureidentityalliance.org/publicationsdocman/public/268-on-the-road-to-user-centricity-digital-identity-inthe-electronic-wallet-era/file.

9. Eccles, D. W. and Arsal, G. [2017], 'The think aloud method: what is it and how do i use it?', *Qualitative Research in Sport, Exercise and Health* **9**(4), 514–531.

10. *Europe's Digital Decade* [n.d.]. `https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade` [Access: 20.05.2024].

11. Evans, J. R. and Mathur, A. [2005], 'The value of online surveys', *Internet research* **15**(2), 195–219.

12. Gonzalez, B. [n.d.], 'European digital id wallets piloted in estonia and luxembourg'. `https://www.biometricupdate.com/202311/european-digital-id-wallets-piloted-in-estonia-and-luxembourg` [Access: 20.05.2024].

13. Grossarth-Maticek, J., Kann, K. and Koufen, S. [2020], 'Destatis kontext. privatschulen in deutschland–fakten und hintergründe'.

14. Gupta, S. D., Kaplan, S., Nygaard, A. and Ghanavati, S. [2021], A two-fold study to investigate users' perception of iot information sensitivity levels and their willingness to share the information, *in* 'International Symposium on Emerging Information Security and Applications', Springer, pp. 87–107.

15. Haney, J., Acar, Y. and Furman, S. [2021], " it's the company, the government, you and i": User perceptions of responsibility for smart home privacy and security, *in* '30th USENIX Security Symposium (USENIX Security 21)', pp. 411–428.

16. Kim, Y. [2011], 'The pilot study in qualitative inquiry: Identifying issues and learning lessons for culturally competent research', *Qualitative Social Work* **10**(2), 190–206.

17. Kostic, S. [2024], Who is the better operator of an identity wallet prioritised by the user?-a quantitative survey between state and company, *in* 'Extended Abstracts of the CHI Conference on Human Factors in Computing Systems', pp. 1–7.

18. Kostic, S. and 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.

19. Mishra, P., Pandey, C. M., Singh, U., Gupta, A., Sahu, C. and Keshri, A. [2019], 'Descriptive statistics and normality tests for statistical data', *Annals of cardiac anaesthesia* **22**(1), 67–72.

20. Murtezaj, D. [2023], Unlocking Digital Trust: A Study of User Trust and Usability in a Digital Identity Wallet Concept, PhD thesis, Freie Universität Berlin.

21. Podgorelec, B., Alber, L. and Zefferer, T. [2022], What is a (digital) identity wallet? a systematic literature review, *in* '2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)', IEEE, pp. 809–818.

22. Research, J. [2023], *Digital Identity: Solutions Assessment, Regional Analysis Market Forecasts 2023–2027*. `https://www.juniperresearch.com/press/users-of-digital-identity-documents-to-exceed/`.

23. Roster, C. A., Lucianetti, L. and Albaum, G. [2015], 'Exploring slider vs. categorical response formats in web-based surveys', *Journal of Research Practice* **11**(1), D1–D1.

24. Schwab, C., Kuhlmann, S., Bogumil, J. and Gerber, S. [2019], *Digitalisierung der Bürgerämter in Deutschland*, number 427, Study der Hans-Böckler-Stiftung.

25. Sjöholm, M. [2023], 'Designing a trustworthy eu digital identity wallet: A study of user needs and preferences'.

26. 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.

27. *The European Digital Identity Regulation* [n.d.]. `https://www.european-digital-identity-regulation.com/` [Access: 20.05.2024].

28. Zeng, E., Mare, S. and Roesner, F. [2017], End user security and privacy concerns with smart homes, *in* 'thirteenth symposium on usable privacy and security (SOUPS 2017)', pp. 65–80.

List of Figures

List of Tables