University of Zurich^UZH

MASTER THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

Representation of Privacy Notices in Decentralized Applications

Duanran Jing
Zurich, Switzerland
Student ID: 20-752-432

Supervisor: Daria Schumm, Thomas Grübl, Prof. Dr. Burkhard Stiller
Date of Submission: April 30, 2025

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

Master Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmuehlestrasse 14, CH-8050 Zurich, Switzerland
URL: http://www.csg.uzh.ch/

Declaration of Independence

I hereby declare that I have composed this work independently and without the use of any aids other than those declared (including generative AI such as ChatGPT). I am aware that I take full responsibility for the scientific character of the submitted text myself, even if AI aids were used and declared (after written confirmation by the supervising professor). All passages taken verbatim or in sense from published or unpublished writings are identified as such. The work has not yet been submitted in the same or similar form or in excerpts as part of another examination.

The declared tool used in this thesis is:

- Grammarly: for typo fixing and phrasing in writing.

Zürich, 30.04.2025

Signature of student

Abstract

Self-sovereign identity (SSI) is a user-centric and decentralized approach that ensures that individuals have full control over their identity data without relying on a central authority. This concept aims to protect user privacy by using decentralized identifiers and requiring user consent before any data sharing occurs. However, many users often experience “consent fatigue” due to cumbersome privacy notices, leading them to consent without fully reading or understanding what they are agreeing to. As a result, users may not be aware of the specifics of their consent, and if a verifier requests more data than is necessary, it can result in excessive information disclosure, undermining the benefits of SSI.

This thesis explores a more effective representation of privacy notices in SSI applications to improve user awareness and trust. Building on existing guidelines and best practices, a new SSI application has been developed featuring an improved privacy notice that clearly presents key privacy attributes. A user study with ten participants showed that this new representation of the privacy notice significantly improved understanding of privacy-related aspects and noticeably increased user trust in the application.

Die souveräne Identität (SSI) ist ein nutzerzentrierter und dezentraler Ansatz, der sicherstellt, dass Einzelpersonen die volle Kontrolle über ihre Identitätsdaten haben, ohne sich auf eine zentrale Behörde zu verlassen. Dieses Konzept zielt darauf ab, die Privatsphäre der Benutzer zu schützen, indem dezentrale Identifikatoren verwendet werden und die Zustimmung des Benutzers erforderlich ist, bevor eine gemeinsame Nutzung von Daten erfolgt. Viele Benutzer sind jedoch aufgrund umständlicher Datenschutzhinweise oft "einwilligungsmüde", was sie dazu verleitet, ihre Zustimmung zu erteilen, ohne sie vollständig zu lesen oder zu verstehen, wozu sie sich bereit erklären. Infolgedessen sind sich die Nutzer möglicherweise nicht über die Einzelheiten ihrer Zustimmung im Klaren, und wenn ein Prüfer mehr Daten als nötig anfordert, kann dies zu einer übermäßigen Offenlegung von Informationen führen, was die Vorteile der SSI untergräbt.

In dieser Arbeit wird eine effektivere Darstellung von Datenschutzhinweisen in SSI-Anwendungen untersucht, um das Bewusstsein und das Vertrauen der Nutzer zu verbessern. Auf der Grundlage bestehender Richtlinien und bewährter Verfahren wurde eine neue SSI-Anwendung mit einem verbesserten Datenschutzhinweis entwickelt, der die wichtigsten Datenschutzmerkmale klar darstellt. Eine Nutzerstudie mit zehn Teilnehmern zeigte, dass diese neue Darstellung des Datenschutzhinweises das Verständnis für datenschutzrelevante Aspekte deutlich verbessert und das Vertrauen der Nutzer in die Anwendung spürbar erhöht.

Acknowledgments

I would like to express my sincere gratitude to my supervisors, Daria Schumm, Thomas Grübl and Prof. Dr. Burkhard Stiller, for their guidance, support, and profound expertise throughout the course of my thesis. Their insightful feedback, constructive suggestions, and constant encouragement were instrumental in shaping this research.

I am also deeply grateful to all the individuals who participated in the pilot study and user study. Their valuable engagement, thoughtful input, and diverse perspectives significantly contributed to this thesis.

Finally, I would like to thank my husband, Theo Weidmann, for his continuous support throughout this thesis. His thoughtful suggestions, careful proofreading, and our many discussions about my work provided valuable input and helped me improve this thesis a lot.

Contents

Chapter 1

Introduction

This chapter outlines the motivation for the thesis and explains the relevance and significance of the research topic in the context of self-sovereign identity applications, privacy notices, and user experience. It then details the goals of the thesis, emphasizing the key objectives of the research. Additionally, this chapter discusses the methodology employed to achieve these goals. Finally, the thesis outline presents the structure of the work.

1.1 Motivation

Self-Sovereign Identity (SSI) is a decentralized and user-centric approach that prioritizes users in the management of their identities [74]. It allows individuals to own and control their personal data without relying on central authorities. SSI is designed to protect user privacy. From a technical perspective, SSI employs decentralized identifiers (DIDs) and verifiable credentials (VCs) [32]. In some cases, the verification process is enhanced with zero-knowledge proofs to further safeguard user privacy [32]. To ensure user control, Christopher Allen proposed ten principles of SSI [74]. One key principle is consent, which stipulates that users must agree to the use of their identity [74]. Data sharing should only occur with the explicit consent of the users [74].

Unlike physical identity, VCs in SSI are digital, which means users do not need to worry about losing their identity and compromising their privacy [72]. Centralized identity systems raise ethical, security, and privacy concerns, as these centralized databases can often be targeted by hackers [72]. While federated identity allows users to maintain the same identity across multiple platforms, the organization providing this service still functions as a centralized authority [74]. In contrast, SSI offers a more secure identity solution that better protects users' privacy compared to physical identity, centralized identity, and federated identity.

However, several studies have shown that one problem in SSI applications is that sometimes users may give consent without fully understanding what they are agreeing to [20, 41, 63]. If the verifier requests more information than necessary and users consent to this data sharing without comprehension, it can result in excessive information disclosure [20, 51]. This situation undermines the benefits that SSI is intended to provide.

The phenomenon of users giving their consent without fully reading or understanding the privacy notice is known as consent fatigue. This often occurs when users are repeatedly asked for their consent [24, 33, 76]. [76] suggested that research on consent management, presentation and enforcement could be beneficial in addressing this problem.

This thesis addresses the problem of consent fatigue encountered by users of SSI applications. The goal is to create an improved way of representing privacy notices in SSI applications to enhance users' awareness and understanding of privacy-related issues. A new SSI application has been developed where privacy information is presented in a more effective and user-friendly manner. This approach helps users make informed decisions about their data-sharing practices while still benefiting from the privacy advantages offered by SSI.

1.2 Thesis Goals

The primary objective of this thesis is to identify a more effective way to enhance user awareness of their data privacy. To address the research question, the following intermediate objectives have been defined:

- **Fundamental Research on the Background.** To fully understand the current challenges related to privacy notices, it is crucial to first understand foundational concepts such as SSI, UX, privacy, and consent fatigue. This involves examining how SSI empowers users to manage their own identity data, while also recognizing the limitations that poor UX design can introduce in privacy-related interactions. Additionally, it is important to investigate the role of usability and UX in shaping user trust and perceptions of transparency, especially in the context of privacy notifications.

- **A Review of Literature on Guidelines for SSI Applications and Privacy Notices.** To ensure a positive UX in SSI applications and to develop a new and effective representation of privacy notices, it is essential to identify recommendations, best practices, and design guidelines that are specifically relevant to SSI applications and privacy notices.

- **Assessing Privacy Notice Usability in Existing SSI Solutions.** To gain a comprehensive understanding of the current state of SSI applications, it is essential to conduct a testing of existing SSI applications available in the market. This process should focus specifically on how these applications present privacy notices, and how effectively they inform users about data privacy.

- **Design and Implement a New SSI Application.** Based on the findings from the literature review and the evaluation of existing SSI applications, a prototype for an SSI application that ensures a positive and user-friendly experience is designed and implemented. This prototype should not only focus on improving usability, but also introduce a new and enhanced representation for privacy notices, based on the summarized guidelines and best practices identified in the research.

- **Evaluation of the New SSI Application.** In the end, the effectiveness of the new SSI application will be evaluated through a comparative analysis with an existing SSI application. The evaluation will focus on key aspects such as UX, privacy awareness, and user trust.

1.3 Methodology

This thesis employs several methodologies to understand the problem, identify possible solutions, improve the design of a new SSI application, and evaluate its effectiveness.

The literature review was conducted to comprehend the fundamental concepts related to the thesis topic and to gain insights into SSI, UX, privacy, and consent fatigue. This review emphasized the importance of addressing the problem and helped identify its underlying causes. The literature was later revisited to explore potential solutions to the issues identified.

In addition to the literature review, field research was conducted to assess the current state of SSI applications. Various existing applications available on the market were tested with guidance from the instructions and tutorials provided by the companies. The goal of this process was to understand how these applications present their privacy notices.

During the design and implementation of the new SSI application, BetterID, a one-round iterative method was used. After the completion of the initial BetterID design and preparation for the user study, a pilot study was conducted. Based on the results and feedback from this pilot study, several modifications were made to enhance the design.

To evaluate user experience, privacy awareness, and trust, a user study employing a within-subject design was conducted. In this study, participants interacted with two different SSI applications, completing two tasks within each application. Following their interactions, they filled out a questionnaire. Data were collected from both questionnaire responses and interactions recordings.

1.4 Thesis Outline

The structure of the thesis is organized as follows:

- **Chapter** 2 explores the fundamental concepts related to the topic of this thesis. It examines useful design principles applicable to decentralized applications and effective design principles for privacy notices drawn from literature. Additionally, it presents the results of a test conducted on existing SSI applications.

- **Chapter 3** focuses on the methodology used in this thesis. It explains how the literature review and field research were conducted. Additionally, it details the design iteration method employed, along with the pilot study, and describes the user study conducted to evaluate the new SSI application, BetterID.

- **Chapter 4** summarizes the requirements for an SSI application and describes the interaction flows within BetterID. It then explores how the design principles derived from the literature were incorporated into the initial design of BetterID. Additionally, the chapter discusses the refinements made to the user interface, driven by feedback from a pilot study.

- **Chapter 5** outlines the technology stack used in the implementation. It presents the overall architecture of BetterID, including the pages and key components. Also, it details the implementation of state management. Finally, it presents the final version of the UI of BetterID.

- **Chapter 6** outlines the design and methodology of the user study, providing a detailed account of its structure and objectives. It presents the results from both the pilot study and the main user study, followed by a thorough discussion of the findings.

- **Chapter 7** concludes the research by summarizing the key findings and their implications. It also suggests potential directions for future work, identifying areas for further exploration and development.

Chapter 2

Fundamentals

This chapter explores the fundamental concepts essential for understanding this thesis. It provides background information on SSI, privacy, UX, and consent fatigue. Additionally, the chapter presents literature closely related to this research. It begins by discussing design principles that can be applied to decentralized applications in order to improve communication. Next, it outlines design principles specifically aimed at enhancing privacy notices. Finally, it presents the results from the testing of existing SSI applications.

2.1 Background

2.1.1 Self-Sovereign Identity

Traditional identity systems have historically depended on centralized databases managed by governments or corporations. This reliance raised privacy concerns and led to data breaches [72]. With the acceleration of digitization, the demand for more secure, transparent, and user-controlled identity systems became clear. Self-sovereign identity (SSI) emerged as a solution to these issues, utilizing blockchain technology to ensure data integrity, traceability, and security without the need for a central authority [80]. The introduction of decentralized identifiers (DIDs) and verifiable credentials (VCs) has further advanced the development of SSI, enabling individuals to manage their identities in a secure and privacy-preserving manner [32].

SSI is a decentralized identity approach that allows individuals to own and control their personal data without relying on central authorities or intermediaries [80]. There are three key components in SSI applications: issuer, identity holder, and verifier. The issuer is either a reputed person or an organization known by its public key, an entity that attests to certain attributes of the identity holder by issuing the digital signing [73]. The identity holder is an entity that is responsible for obtaining, storing, managing, controlling, and sharing its identity data/attributes with other entities [23]. The verifier is an entity that requests a proof of identity from the identity holder to identify and verify the holder's identity and provide them with a (digital) service or product [23]. Figure 2.1 is a summary of the interaction and data flow of SSI applications.

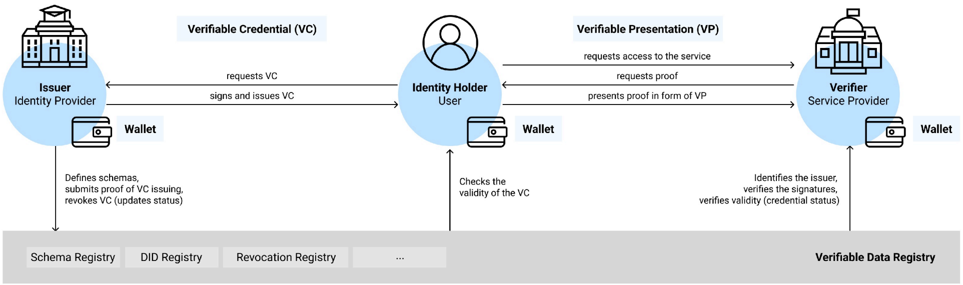


Figure 2.1: The interaction and data flow in SSI applications[18]

In 2016, C. Allen proposed ten principles of SSI, which were intended to ensure user control. He stated that the key properties of the SSI system are Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimalization, and Protection [80]. Over the years, many studies tried to examine or expand these principles [19, 28, 81]. Even though there are open challenges in SSI applications, which cannot be addressed by these ten principles, these ten principles are still viewed as a set of requirements that SSI systems should achieve, and they are very useful at evaluating if an SSI application is user-centric [19].

As SSI continues to develop, several challenges have emerged. [20] published an article highlighting seven flaws in identity management systems, focusing on challenges related to both usability and security. One notable flaw is that "user consent could lead to maximum information disclosure." The authors pointed out that when users encounter privacy policies, they often skim the text quickly and rarely take the time to fully understand what they are consenting to [20].

Some studies also focus on usability issues in SSI applications. [47] conducted a study that revealed that the interactions with identity wallets often do not align with users' mental models during the credential sharing process [47]. Furthermore, there are usability issues with decentralized wallets [56, 69], such as the fact that the concepts of decentralized identity are not adequately explained to end users [45]. [69] identified usability problems in fundamental tasks through cognitive walkthroughs and proposed solutions to improve usability and accessibility [69].

2.1.2 Privacy

According to Alan Westin, privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [90]. Today, online services want to collect more user data and with the help of machine learning, they can discover hidden patterns, links, behaviors, and other practical knowledge [6]. Under limited choices and dark design patterns, users might give up on their privacy to use the service [63, 70, 79]. To protect people and their data, the General Data Protection Regulation (GDPR) is created in Europe. GDPR requires companies to explain the controller's identity, what kind of data will be processed, how it will be used, and the purpose of the processing operations in the consent [30].

SSI applications are designed to provide digital identities while preserving privacy [72, 80]. Each identity is associated with one or more DIDs, which are universally unique and do not require any centralized registration authority [58, 59]. Furthermore, zero-knowledge proofs can be used to disclose only the necessary information during interactions [72].

One challenge that SSI applications face is that user consent can lead to maximum information disclosure, which contradicts the core design principles of SSI applications [20]. This issue arises because users often skim through or become habitual of warnings after encountering them multiple times [20]. Therefore, it is essential to design effective privacy notices that clearly convey important information, alert users to risky behaviors, and obtain user consent in SSI applications.

2.1.3 User Experience

The ISO 9241-11 standard defines user experience as "user perceptions and responses that result from the use and/or anticipated use of a system, product or service" [38]. Information on user experience is very important during the design and development of an application [7]. The tool or means with which users interact and enable the achievement of user goals is the user interface (UI). The objective of UI design is to make the UX as simple, intuitive, and efficient as possible to achieve user goals and expectations [18]. For decentralized applications, users often struggle to comprehend the concepts involved, making it challenging for them to recognize their intrinsic value. Therefore, it is essential to provide value to users by ensuring good usability and improving user experience [39].

UX is essential to improve trust and protect user privacy, especially when users lack alternative options for a system [18, 63, 79]. [63] explored the relationship between UX and user privacy, identifying two layers: a visible layer and an invisible layer. The visible layer refers to the UI. To protect user privacy, the UI should clearly inform users about the types and amounts of data collected, as well as obtain their consent [63]. The invisible layer involves the design patterns underlying the UI, which significantly influence whether the UX is privacy-friendly or invasive. When users experience dark patterns, they may give their consent without knowing how the data is collected and used [13, 14]. For effective UX, privacy notices should be concise, clear, and appealing, and all options must be presented fairly [63].

2.1.4 Consent Fatigue

Numerous studies have highlighted the growing concerns among users about their privacy while online. In response to these concerns, privacy notices have become widespread [41]. In SSI applications, users must understand these privacy notices and provide their consent. However, the requirement to consent to multiple privacy notices has led to a phenomenon known as consent fatigue [76]. As a result, users can accept terms and conditions without fully understanding the implications, which decreases the effectiveness of consent mechanisms and can compromise user autonomy and privacy [71]. Previous research has identified three main factors that contribute to consent fatigue: 1) the complexity of privacy notices; 2) their length; and 3) the language and presentation of these notices, which are often dull, dense, and inaccessible [6, 41, 70].

2.2 Related Work

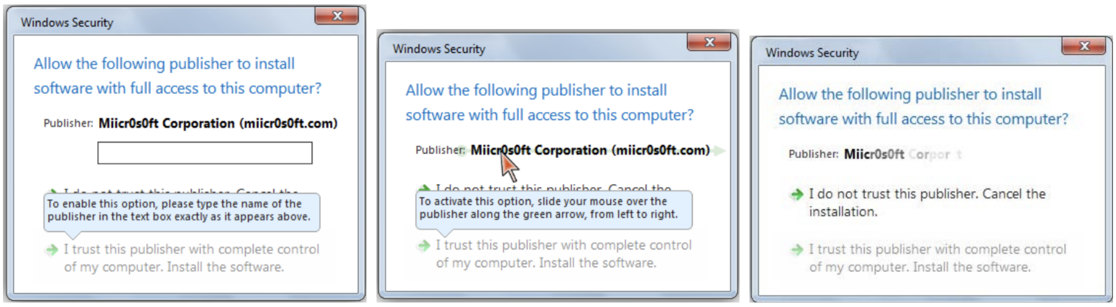
2.2.1 Design Principles for Efficient Communication

To understand how to improve user's trust and make users aware of privacy issues in SSI applications, a top-down approach was adopted. A research on the general design principles for communicating with users more efficiently was conducted at first. The goal is to find out some general design principles, that can be applied to decentralized applications and can also enhance the communication between the system and the user. Here is a summary of the principles and approaches that have been tested in the past.

Concise and Simple Language. As mentioned in many studies, one challenge to improve user trust in decentralization applications is that the terms are always obscure and it is difficult for users to understand all the terms [39, 45, 56, 63]. In this case, users might have difficulty understanding the application and its value [39]. Therefore, several studies have tried to use a simple language in decentralized applications and it turned out that it can enhance user understanding and trust [11, 33, 88].

Selective Disclosure. Dark patterns refer to UI and UX strategies intentionally designed to trick, manipulate, or coerce users into making decisions that may not be in their best interest, often benefiting the service provider instead [63]. Dark patterns include obscuring data sharing, preselected options, hard-to-find settings and so on [63]. The use of dark patterns can affect UX and harm user trust [13, 63]. Prior research have pointed out that one big problem caused by dark patterns is that consenting to data collection and use was easy, but it is difficult to withhold or revoke [14]. For applications which are designed with dark patterns, there is always a default setting in the notice, which makes users feel intrusive, and when users want to reject or withhold consent, it becomes difficult. As a result, it is cumbersome to preserve privacy [14, 63, 70]. In many cases, users can read the privacy notice, but there are very little choices offered to users, so users are left with a take-it-or-leave-it choice, and they can either give up on their privacy or go somewhere else [64]. Privacy notices can only be effective if they are actionable and offer meaningful choices to users [17].

The Least Surprise Principle. A mental model is a user's internal understanding of how a system works, how people perceive and predict how to interact with something based on past experience, expectations, and available information [34]. A mental model helps users understand how systems operate and predict their outcomes [39]. As mentioned in the previous section, [47] highlighted that the design of the credentials-sharing process



Windows Security

Allow the following publisher to install software with full access to this computer?

Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)

To enable this option, please type the name of the publisher in the text box exactly as it appears above.

I trust this publisher with complete control of my computer. Install the software.

(a) Type attractor [10]

Windows Security

Allow the following publisher to install software with full access to this computer?

Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)

To activate this option, slide your mouse over the publisher along the green arrow, from left to right.

I trust this publisher with complete control of my computer. Install the software.

(b) Swipe attractor [10]

Windows Security

Allow the following publisher to install software with full access to this computer?

Publisher: Miicr0s0ft Corpor t

I do not trust this publisher. Cancel the installation.

I trust this publisher with complete control of my computer. Install the software.

(c) Reveal attractor [10]

Figure 2.2: Examples of Attractor from [10]

does not align with the mental models of the users [47]. Furthermore, [39] emphasized the importance of developing an accurate mental model, arguing that it is essential to address usability issues in decentralized applications [39]. When designing the interaction in decentralized application, it can be helpful to refer to other applications which users interact more often, so that the interaction in decentralized application can fit with users' mental model better [39].

The use of intervention. Previous research have shown that users' trust in a company is closely related to the perception of how well a company respects or does not respect their privacy [24, 49, 93]. Therefore, the use of privacy notice and intervention to warn users about the privacy risks can contribute to improve users' trust [21, 79]. The details of designing privacy notices will be discussed in the next section, and here the use of intervention will be discussed.

Common types of interventions include nudges, fear appeals, warnings, polymorphic warnings, and attractors. [21] provide a detailed explanation of each intervention in their paper, analyzing both the positive and negative effects these interventions have on users. In Figure 2.2, there are three examples of attractor designed by [10].

On the one hand, interventions can positively influence users when making privacy decisions and help users avoid habituation. For example, [79] implemented a counter, sensitivity score, and privacy smiley to increase users' privacy concerns during decision making. Additionally, [9] conducted a study comparing the effectiveness of various attractors in preventing pop-up fatigue. Their findings indicated that both swipe attractors and type attractors remained effective even after multiple exposures [9]. Prior research have reported several approaches, which are resistant to habituation, such as polymorphic dialogues, opinionated design, and the use of attractors [2, 9, 86].

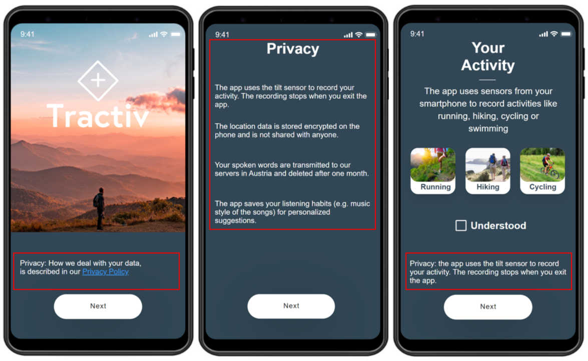
However, excessive use of interventions can become a burden for users. [9] discovered that while type attractors performed the best, they also imposed the greatest usability burden. Furthermore, [20] suggested that developers limit the use of warnings, dialogues, and indicators intended to acquire user consent. While interventions can effectively alert users, they also risk overwhelming them, which could lead to consent fatigue [20].

2.2.2 Design Principles for Privacy Notice

After gaining an understanding of the general design principles for better communication, the focus was narrowed to the privacy notice. Research on the design of privacy notices in SSI applications is still in its early stages. To gain a broader understanding, the scope was widened to include not only SSI applications, but also a diverse range of other application types, with a particular emphasis on decentralized applications. In this section, a summary of the design principles that have been identified in the existing literature is presented.

Integrate Privacy Notice Into the System. As [70] pointed out in their study, one problem of privacy notices is that they are rarely integrate into the system [70]. When users need to go to a separate website to learn about privacy notices, it is less likely that they will read them [62, 70]. To make users read privacy notices, it is necessary to present privacy notices in the system, not in setting, sub-menu or a separate website.

Increase the Saliency Level. [24] studied the effectiveness of three different ways of presenting privacy notice (click, exclusive, and embedded, as shown in Figure 2.3) and discovered that increasing the saliency level of the notices had a significant effect on raising users' awareness on privacy notice. Compared to the other two representations, presenting privacy notices exclusively on a screen is the most effective way to make users read and pay attention on the content, because the privacy notice is neither decoupled (for example, the click design) nor combined with other irrelevant information (for example, the embedded design) [24].



Privacy: How we deal with your data, is described in our Privacy Policy

The app uses the tilt sensor to record your activity. The recording stops when you exit the app.

The location data is stored encrypted on the phone and is not shared with anyone.

Your spoken words are transmitted to our servers in Austria and deleted after one month.

The app saves your listening habits (e.g. music style of the songs) for personalized suggestions.

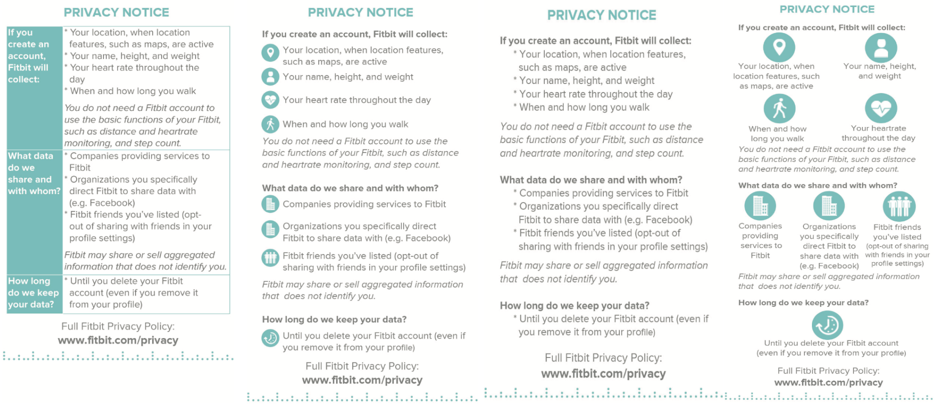
The app uses sensors from your smartphone to record activities like running, hiking, cycling or swimming

Privacy: the app uses the tilt sensor to record your activity. The recording stops when you exit the app.

Figure 2.3: Three representations of privacy notices: click(left), exclusive(middle), embedded(right) from [24]

Include More Meaningful Content. One problem of privacy policy is that there is always a mismatch between the issues that business wants to address in the policy and the issues users really want to know about [13]. Based on interviews with users and experts, [6] provided a ranked list of privacy attributes. It turned out that the content in privacy notice should go beyond data collection and processing. The three most important privacy attributes are: 1) collection: What data is being collected? 2) sharing: Is any of the collected data leaving the ownership of the service provider? 3) sale: Are any of the collected data being sold to third parties? [6]

Keep It Short. As discussed previously, the length of privacy notices is a key factor which caused consent fatigue. [70] pointed out that it is not necessary to list all data practices of the business. Instead, privacy notice can be implemented with short notice [24, 70]. Moreover, many studies have demonstrated that standardized short-form privacy notices can improve users' awareness of privacy practices in different disciplines [4, 24, 43, 44]. For example, in Figure 2.4, there are four different formats of short-form privacy notices designed by [33]: table format, bulleted icon format, bulleted format, and icon format. Through a user study, they found that these short-form notices effectively improve awareness of privacy practices [33].



PRIVACY NOTICE

If you create an account, Fitbit will collect:	* Your location, when location features, such as maps, are active * Your name, height, and weight * Your heart rate throughout the day * When and how long you walk *You do not need a Fitbit account to use the basic functions of your Fitbit, such as distance and heartrate monitoring, and step count.*
What data do we share and with whom?	* Companies providing services to Fitbit * Organizations you specifically direct Fitbit to share data with (e.g. Facebook) * Fitbit friends you've listed (opt-out of sharing with friends in your profile settings) *Fitbit may share or sell aggregated information that does not identify you.*
How long do we keep your data?	* Until you delete your Fitbit account (even if you remove it from your profile)

Full Fitbit Privacy Policy:
www.fitbit.com/privacy

PRIVACY NOTICE

If you create an account, Fitbit will collect:

Your location, when location features, such as maps, are active

Your name, height, and weight

Your heart rate throughout the day

When and how long you walk

You do not need a Fitbit account to use the basic functions of your Fitbit, such as distance and heartrate monitoring, and step count.

What data do we share and with whom?

Companies providing services to Fitbit

Organizations you specifically direct Fitbit to share data with (e.g. Facebook)

Fitbit friends you've listed (opt-out of sharing with friends in your profile settings)

Fitbit may share or sell aggregated information that does not identify you.

How long do we keep your data?

Until you delete your Fitbit account (even if you remove it from your profile)

Full Fitbit Privacy Policy:
www.fitbit.com/privacy

PRIVACY NOTICE

If you create an account, Fitbit will collect:

* Your location, when location features, such as maps, are active
* Your name, height, and weight
* Your heart rate throughout the day
* When and how long you walk

You do not need a Fitbit account to use the basic functions of your Fitbit, such as distance and heartrate monitoring, and step count.

What data do we share and with whom?

* Companies providing services to Fitbit
* Organizations you specifically direct Fitbit to share data with (e.g. Facebook)
* Fitbit friends you've listed (opt-out of sharing with friends in your profile settings)

Fitbit may share or sell aggregated information that does not identify you.

How long do we keep your data?

* Until you delete your Fitbit account (even if you remove it from your profile)

Full Fitbit Privacy Policy:
www.fitbit.com/privacy

PRIVACY NOTICE

If you create an account, Fitbit will collect:

Your location, when location features, such as maps, are active

Your name, height, and weight

When and how long you walk

Your heartrate throughout the day

You do not need a Fitbit account to use the basic functions of your Fitbit, such as distance and heartrate monitoring, and step count.

What data do we share and with whom?

Companies providing services to Fitbit

Organizations you specifically direct Fitbit to share data with (e.g. Facebook)

Fitbit friends you've listed (opt-out of sharing with friends in your profile settings)

Fitbit may share or sell aggregated information that does not identify you.

How long do we keep your data?

Until you delete your Fitbit account (even if you remove it from your profile)

Full Fitbit Privacy Policy:
www.fitbit.com/privacy

Figure 2.4: Four different format of short-term notice designed by [33]

[88] recognized that users also experience consent fatigue when required to read the end user license agreement (EULA) for applications. To address this issue, they paraphrased the EULA into a bullet-point format using simpler language and condensed its length. The results from their user study indicated that participants spent more time engaging with the paraphrased EULA and reported a more positive attitude toward it [88].

Use Privacy Visualization. To effectively communicate privacy risks to users, researchers and regulators have advocated for clearer, more visual representations of privacy notices [6]. In the United States, the Federal Trade Commission has been promoting the use of tabular privacy notices, similar to nutrition labels, since 2001 [6]. Similarly, in Europe, GDPR recommends the inclusion of "standardized icons" in overviews of data processing. Even though the effect of using icon is still not clear yet.

[6] have reviewed various privacy visualizations and guidelines for privacy by design. Currently, only CLEVER°FRANKE [16], DaPIS [67], and privacylabel.org [66] are still in development for privacy visualization. The authors suggested that adopting these labeling systems could benefit users, although there may be associated costs for service providers [6, 13].

Tailor the Notices According to Audience. [70] recognized the lack of guidance on designing effective privacy notices and developed a framework by identifying key dimensions, as illustrated in Figure 2.5. Their paper offers numerous valuable suggestions, particularly emphasizing the importance of tailoring notices for different audiences and employing multilayered notices [70]. To design an effective privacy notice, designers should consider the time when the privacy notice is presented, the channel where the privacy notice is delivered, the visual design, and how to integrate user choices and consent into the notices [70].

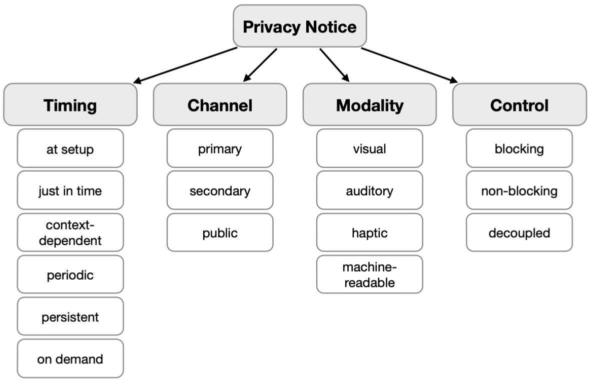


Figure 2.5: The design space of privacy notice proposed by [70]

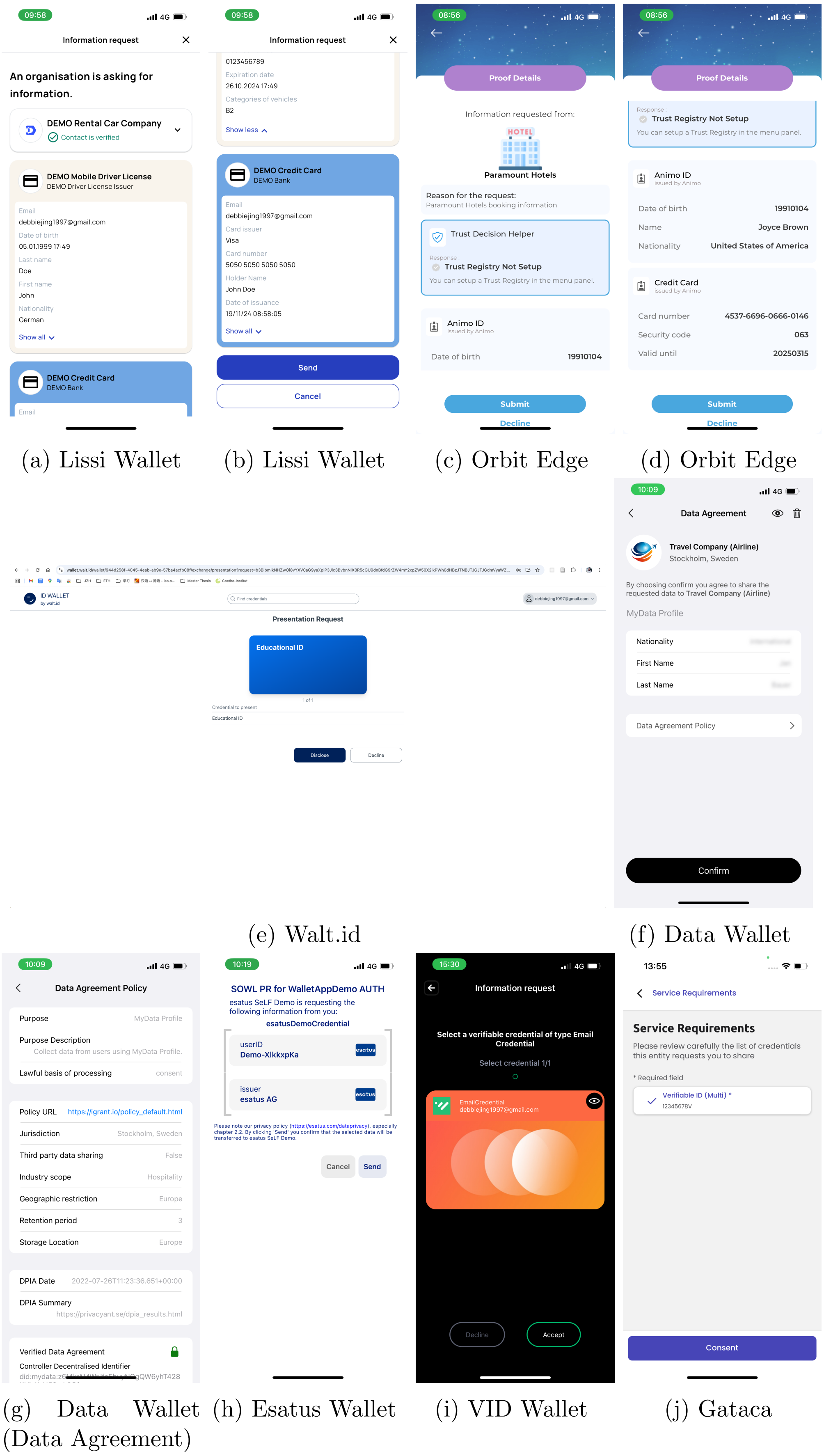
2.2.3 Privacy Notices in the Existing SSI Systems

To evaluate the current state of privacy notices in SSI applications, a test on several popular apps was conducted. From a list provided by the European Blockchain Association [26], several SSI applications were identified and more SSI applications were found by additional online searches. The selection criteria were based on two main points: 1) the application must be free to use, and 2) the application should offer a demo or tutorial to mock the process of getting credentials and sharing credentials. Two well-known SSI applications, provided by Sovrin [77] and Civic [15] were excluded, because they are not free to use.

During the testing period, there were various issues, such as some applications being unavailable in the region (e.g., Jolocom [42]), difficulties in signing up due to unclear reasons (e.g., Trinsic [82]), and underdeveloped functionality (e.g., WorldID [92]). Ultimately, the following candidates were identified for the assessment: Lissi Wallet [50], Orbit Edge [3], Walt.id [89], Data Wallet [37], Esatus Wallet [25], VID Wallet [85] and Gataca [29].

Lissi Wallet In Lissi Wallet, a demo designed for renting a car is provided. In the application, users are asked to provide the driver's license and credit card information. However, during the data-sharing process, there was no privacy notice provided. Additionally, only the entire credit card could be selected, even though some of the information on it was unnecessary.

Orbit Edge In Orbit Edge, the demo focuses on booking a hotel room. Users need to connect with a hotel and provide ID card and credit card information. While it's possible to set up the trust registry in the application, there was no privacy notice provided when sharing the data.



Information request

An organisation is asking for information.

DEMO Rental Car Company
Contact is verified

DEMO Mobile Driver License
DEMO Driver License Issuer

Email
debbiejing1997@gmail.com
Date of birth
05.01.1999 17:49
Last name
Doe
First name
John
Nationality
German
Show all

DEMO Credit Card
DEMO Bank
Email

(a) Lissi Wallet

Information request

0123456789
Expiration date
26.10.2024 17:49
Categories of vehicles
B2
Show less

DEMO Credit Card
DEMO Bank

Email
debbiejing1997@gmail.com
Card issuer
Visa
Card number
5050 5050 5050 5050
Holder Name
John Doe
Date of issuance
19/11/24 08:58:05
Show all

Send
Cancel

(b) Lissi Wallet

Proof Details

Information requested from:
Paramount Hotels

Reason for the request:
Paramount Hotels booking information

Trust Decision Helper
Response :
Trust Registry Not Setup
You can setup a Trust Registry in the menu panel.

Animo ID
issued by Animo
Date of birth 19910104

Submit
Decline

(c) Orbit Edge

Proof Details

Response :
Trust Registry Not Setup
You can setup a Trust Registry in the menu panel.

Animo ID
issued by Animo
Date of birth 19910104
Name Joyce Brown
Nationality United States of America

Credit Card
issued by Animo
Card number 4537-6696-0666-0146
Security code 063
Valid until 20250315

Submit
Decline

(d) Orbit Edge

ID WALLET
by walt.id
Find credentials
debbiejing1997@gmail.com

Presentation Request

Educational ID
1 of 1
Credential to present
Educational ID

Disclose
Decline

(e) Walt.id

Data Agreement

Travel Company (Airline)
Stockholm, Sweden

By choosing confirm you agree to share the requested data to Travel Company (Airline)

MyData Profile
Nationality
First Name
Last Name

Data Agreement Policy

Confirm

(f) Data Wallet

Data Agreement Policy

Purpose MyData Profile
Purpose Description
Collect data from users using MyData Profile.
Lawful basis of processing consent

Policy URL https://igrant.io/policy_default.html
Jurisdiction Stockholm, Sweden
Third party data sharing False
Industry scope Hospitality
Geographic restriction Europe
Retention period 3
Storage Location Europe

DPIA Date 2022-07-26T11:23:36.651+00:00
DPIA Summary
https://privacyant.se/dpia_results.html

Verified Data Agreement
Controller Decentralised Identifier
did:mydata:z6...jQW6yhT428

(g) Data Wallet (Data Agreement)

SOWL PR for WalletAppDemo AUTH
esatus SeLF Demo is requesting the following information from you:
esatusDemoCredential

userID
Demo-XlkkxpKa

issuer
esatus AG

Please note our privacy policy (https://esatus.com/dataprivacy), especially chapter 2.2. By clicking 'Send' you confirm that the selected data will be transferred to esatus SeLF Demo.

Cancel
Send

(h) Esatus Wallet

Information request

Select a verifiable credential of type Email Credential

Select credential 1/1

EmailCredential
debbiejing1997@gmail.com

Decline
Accept

(i) VID Wallet

Service Requirements

Service Requirements
Please review carefully the list of credentials this entity requests you to share

* Required field
Verifiable ID (Multi) *
12345678V

Consent

(j) Gataca

Figure 2.6: Screenshots From Testing

Walt.id Unlike the other applications tested, Walt.id is a web-based SSI application. The demo did not include a specific scenario; instead, it focused more on the features. With Walt.id, users can add an educational ID and share it when requested. The interface and overall application are simple. Although there was no privacy notice, it was indicated that the verified party had been authenticated and several policies were presented.

Data Wallet In Data Wallet, users need to share the personal data (first name, last name, nationality) with a travel company in the demo. Data Wallet provided a privacy notice at the time of sharing, as illustrated in Figure 2.6f. By clicking on the data agreement policy, additional information about privacy can be assessed, as shown in Figure 2.6g.

Esatus Wallet In the Esatus Wallet, on the data sharing page, there is a link to the privacy policy along with a reference to the relevant chapter. When users click on the link, the privacy policy website opens in the browser, and users will need to navigate to the specific chapter ourselves.

VID Wallet VID Wallet offered a demo that involves users sharing their ID to enroll in a university. During this data sharing process, users can see which credentials and information are being shared. However, there was no privacy notice provided.

Gataca During the data sharing process in Gataca, users were reminded to carefully review the credentials they were sharing. However, a privacy notice was absent.

The testing revealed that 5 out of 7 applications evaluated do not provide a privacy notice when users receive a request to submit their credentials. Two applications (Data Wallet and Esatus Wallet) address privacy concerns when users are asked to share their credentials. Data Wallet is the only one, who provides a page (see 2.6g) summarizing the data agreement policy. Although Esatus Wallet includes a reminder under the requested credentials, and provide a link to their privacy policy page, this type of decoupled notice makes it less likely that users will read it [70].

Similarly, for the applications who do not provide a notice during data sharing process, most of they also provide the link of privacy notice in the setting of the application. All of these decoupled notices make it cumbersome for users to learn about the information regarding their data and are not effective to let users know about the potential risks.

2.3 Problem Statement

As pointed out previously, consent is an important principle of SSI application, as it requires users to agree to the use of their identity [80]. To give the consent, users must understand what they are consenting to. However, many studies have revealed that sometimes users give their consent without knowing how the data is collected and used, which can lead to severe privacy issues. The reasons behind this behavior are: users habitual behaviors, dark patterns in design, the complexity of the notices and the decoupling between the notice and the system [6, 13, 14, 20, 41, 45, 63]. Furthermore, from our testing on existing SSI applications, an important finding is that most of the applications do not warn users about privacy issues during the data sharing process, decoupled privacy notices are prevailed and the privacy notices are long and difficult to read. Although literature already outlined the problems and provided possible solutions, in reality the privacy notices are still not presented in an effective way.

This gap between the design principle and the actual implementation of SSI applications motivated this research. The goal of this thesis is to answer the question: **How can we effectively make a user aware of their data privacy?** In response, a new prototype of an SSI application that focuses on enhancing users' awareness and understanding of how their identity and data are used was developed, along with other essential privacy-related information they care about, by improving the UX in SSI applications.

Chapter 3

Methodology

This chapter outlines the methodological approach adopted in this thesis. The methodology consists of four components: literature review to establish a theoretical foundation and explore design principles and recommendations, field research to analyze the current state of privacy notices in existing SSI applications, a design iteration including a pilot study, and a user study to evaluate the new SSI application.

3.1 Literature Review

In this thesis, the literature review was conducted twice for different purposes. Initially, the literature review aims to gain a general understanding of the topic, focusing on relevant concepts such as SSI, privacy, UX, and consent fatigue. To identify relevant literature, the keywords "SSI privacy," "SSI UX," and "SSI consent fatigue" were used. Given that research on SSI is still in its early stages, the scope was expanded to include blockchain applications and distributed systems in order to find additional literature. Thus, the keywords "Blockchain UX", "Blockchain privacy", "Distributed system UX", and "Distributed system privacy" were employed. The literature gathered from these keywords served as seeds for conducting forward and backward snowball searches to uncover more relevant studies related to the thesis topic. Through this literature review, a comprehensive understanding of what SSI is and how it operates was developed, along with insights into the UX challenges present in SSI applications. Additionally, the review helped to identify potential privacy issues and the causes of consent fatigue within these applications.

After establishing a foundational understanding, a second literature review was conducted to search for design principles, best practices, and recommendations for creating distributed systems and more effective privacy notices. Initially, the keywords "SSI design", "Blockchain design", "SSI design principles", and "SSI privacy notice" were used. Subsequently, the term "Privacy notice" was applied to discover further literature related to the design of privacy notices across various applications.

3.2 Field Research

To evaluate the current state of SSI applications, field research was conducted to assess the SSI applications available on the market. The focus of the field research is to study how SSI applications present their privacy notice, and if and how they remind users of privacy-related issues during the data sharing process. The selection criteria were as follows:

- The application must be free to use.
- The application should offer a demo or tutorial to mock the process of getting and sharing credentials.

The evaluation began with the SSI applications listed by the European Blockchain Association [26]. Subsequently, additional SSI applications mentioned in relevant literature were also assessed.

3.3 Design Iteration With a Pilot Study

A pilot study was conducted with a small group of participants to test the initial design and prepare for the formal user study. The pilot served as a crucial step in validating both the functionality and the overall research setup. The main goals of the pilot study were to:

- Validate the design of the user study: Confirm that the study structure, including the task instructions, questionnaire flow, and timing, was reasonable and intuitive for participants to follow.
- Identify usability issues and confusing elements in the interface: Observe participants behavior to detect areas where participants hesitated, misunderstood information, or became disengaged. These insights were essential for improving both the clarity and usability of the interface.

The pilot study provided valuable insights into both the UX and the logistics of the user study. Participants provided verbal feedback and completed post-task questionnaires, allowing for the identification of interface elements that required clarification or redesign.

More details on the user study design, and a summary of the results from the pilot study can be found in Chapter 6, and the modifications made to the user interface can be found in Chapter 4.

3.4 User Study

To evaluate the newly developed SSI application and assess whether its redesigned privacy notice more effectively informs users about privacy-related issues, a user study was conducted. The study employed a within-subject design, allowing each participant to interact with both the new SSI application and an existing SSI application from the market. This approach enabled a direct comparison of user responses across the two applications under consistent conditions. The primary goals of the user study were to:

- Evaluate and compare the UX in the two SSI applications.
- Assess whether users read and engaged with the privacy notice more attentively in the new SSI application.
- Determine whether users were able to recall key privacy attributes related to the connections they made.
- Examine whether there was a difference in self-reported trust levels between the two applications.
- Collect feedback for further improvements to the new SSI application.

The results of the user study are presented using visualizations such as charts, followed by statistical analyses to determine whether the observed differences between the two SSI applications are statistically significant. Chapter 6 provides a comprehensive overview of the user study, including the procedure, tasks, and data collection methods, along with a detailed presentation of the results and a discussion of the findings.

Chapter 4

Design

This chapter details the design process of the new SSI application prototype, structured into four main sections. It begins by summarizing the system requirements, which were derived from the literature and current SSI applications. Next, it describes the interaction flows within the new application and introduces the concept of a dual-state architecture. The third section explains how established design principles from the literature were incorporated into the initial design. Finally, the chapter discusses the modifications made to the initial design based on insights gained from the pilot study.

4.1 User Story

To ensure user control, [80] proposed ten principles for SSI applications. Over the years, numerous studies have sought to expand upon these principles. However, the original set is still regarded as essential requirements that SSI systems should fulfill [19, 80]. Based on these principles, the user stories are developed. The details of the user stories can be found in Appendix B.

A study conducted by [18] identified common design patterns in SSI applications [18]. To ensure that the new SSI application, BetterID, includes the essential functionalities of an SSI application, the design patterns identified by [18] that have a frequency of occurrence higher than 60% are used as a reference to check if the user story covers the common design patterns, because the work by [18] provides an overview of what the common design patterns and functionalities most of the SSI application have. Common design patterns that have a frequency of at least 60% are: Restricted wallet access, QR code / link presentation, connection initiation, credential request, connection list, VCs archive, extended VC view, review connection, review credential, review presentation, notification, selective disclosure, self-tested attributes. An overview of user stories, with the common design patterns and the corresponding principles they satisfy, is presented in Table 4.1.

Principles	Requirement (User Story)	Design Patterns
Existence, Access	R1: Log in and register	Restricted wallet access
Control	R2: Receive credentials	Credential request, Self-Attested attributes
Control, Persistence, Portability, Transparency	R3: View credentials	VCs archive, Extended VC view
Control	R4: Delete credentials	Data Deletion
-	R5: Connect to a third party	Connection initiation, Link presentation
Minimalization	R6: Share credentials	Review presentation, Selective disclosure
Consent, Protection, Minimalization	R7: Privacy notice	-
Control	R8: Connection history	Connection list, Review connection
Interoperability	R9: Usability of credentials	-
Transparency	R10: Transparency of the System	-

Table 4.1: The table of user stories for the system with the principles and design patterns they matches

Since the new application is a web application, there are no specific user story and requirement that align with the notification design pattern. One key difference between the user story and the common SSI applications functionalities found in the literature is that there is no feature of offering a backup service. This decision stems from the fact that BetterID is only a frontend mock-up, primarily focused on informing users about privacy issues during the data-sharing process.

Through the testing of existing SSI applications, the focus has been on learning about how or if existing SSI applications warn users about privacy issues during data sharing, but also on gaining valuable insights into the current state of SSI applications and their functionalities. The main functionalities provided by the existing SSI applications are consistent with the result from [18].

4.2 Interaction Flow and State Design

Based on the user stories, the core interactions users can have with the application include obtaining and revoking credentials, reviewing previous connections, and establishing new connections with third-party organizations to share credentials and data. This section demonstrates the interaction flow of each function along with the design considerations for managing state.

4.2.1 Interaction Flow

On the credential management page, users can view the details of each credential, including the specific data it contains. If a credential is no longer needed, users have the option to delete it from their wallet.

The interaction flow for adding a new credential is illustrated as sequence diagram in Figure 4.1. After users select the credential they wish to add, they must enter the required information requested by the issuer. Using the information provided, the issuer can do input validation. If the provided information is correct, then the issuer can issue the new credential to the users. The new credential will be added to the persistent store.

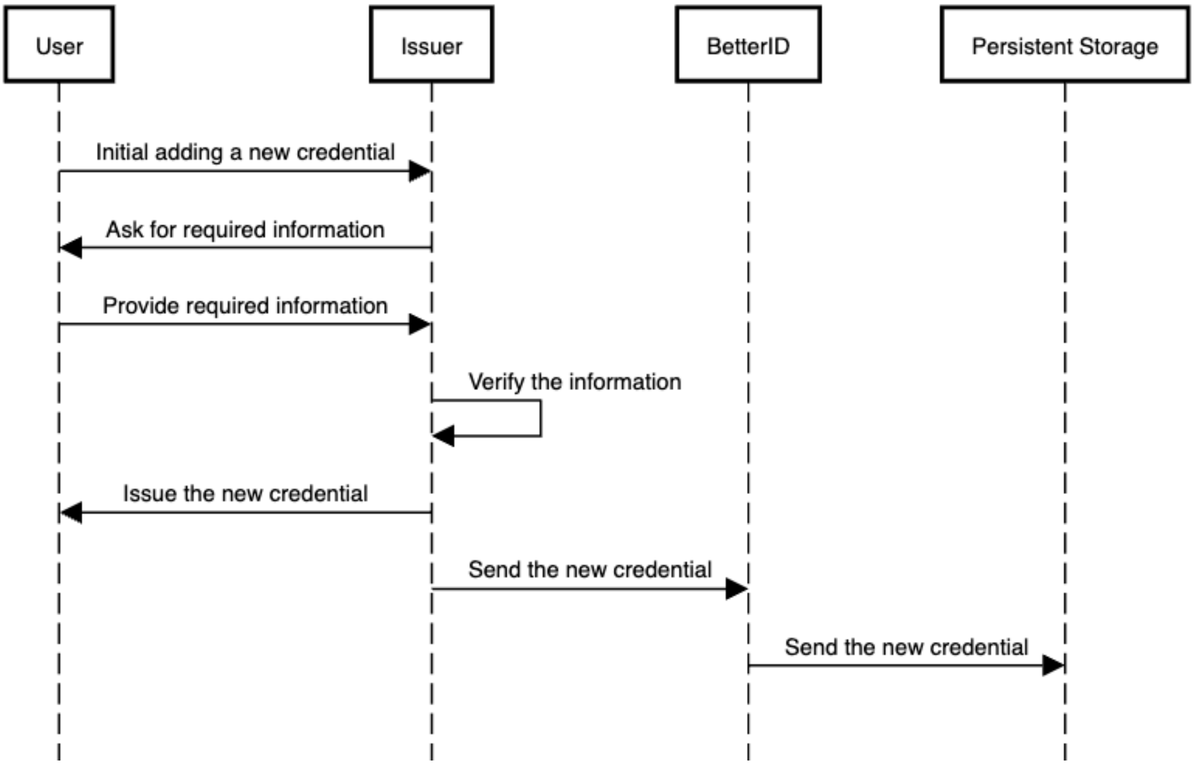


Figure 4.1: The sequence diagram of adding a new credential

Users can review their past connections in BetterID. They can view the organizations they were connected to, the date of each connection, and what credentials and data were shared during those connections.

Figure 4.2 illustrates the interaction flow for establishing a new connection. When users wish to create a new connection, they must first choose a third party (the verifier) that they want to connect with. The verifier will then request the necessary credentials and data from the users. Users have the option to select which data and credentials they want to share. The data they selected will be stored in the temporary store, so that BetterID can check if users select all the required data or if they select unnecessary data. If not all the required data are selected, there will be a warning message and users will not be able to proceed to the next step. If there is extra data selected, there will be a warning message as well, but users can still proceed to the next step. After making their selections, a privacy notice will be displayed in the application, and users are required to read it and provide their consent by typing the defined sentence. Once the consent is given, the selected data will be sent to the verifier. The information in the temporary store is cleared, and the detailed information of the connection is stored in the persistent store.

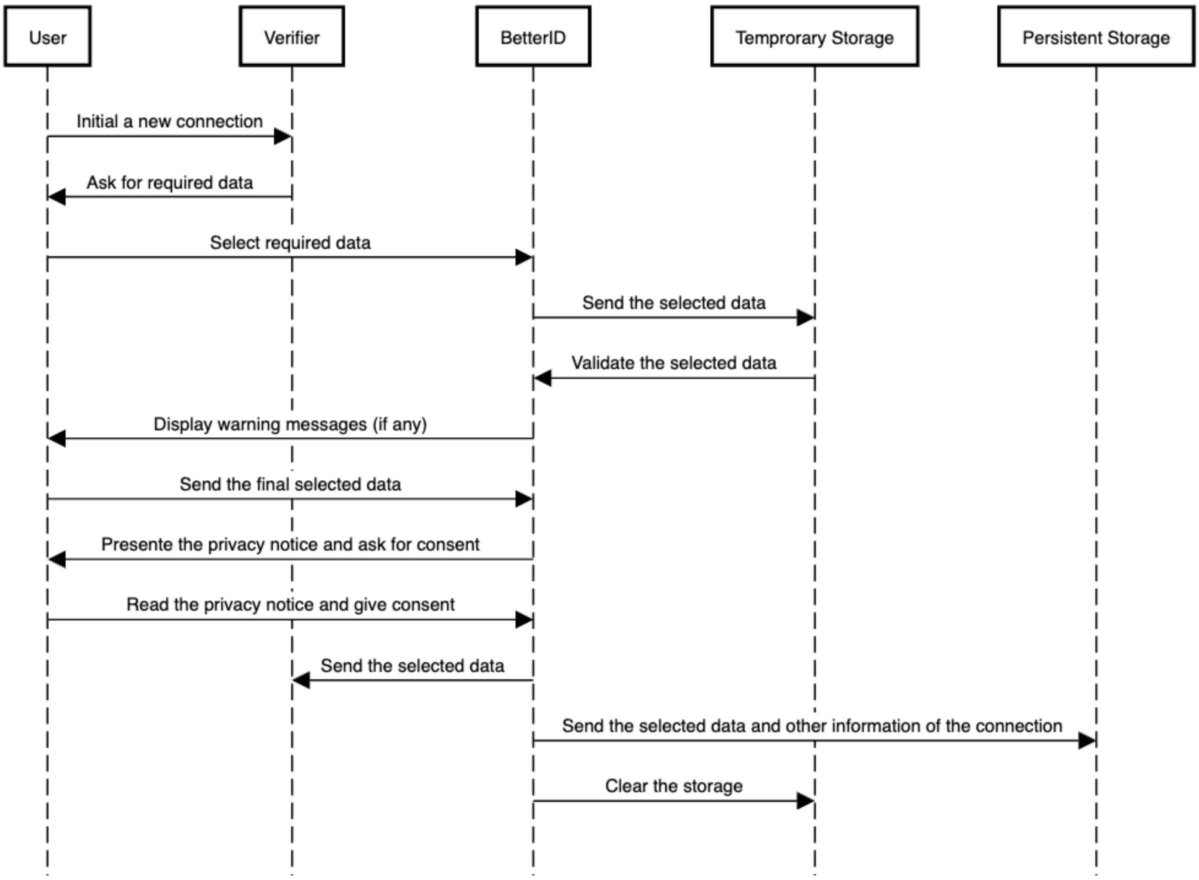

User
Verifier
BetterID
Temprorary Storage
Persistent Storage
Initial a new connection
Ask for required data
Select required data
Send the selected data
Validate the selected data
Display warning messages (if any)
Send the final selected data
Presente the privacy notice and ask for consent
Read the privacy notice and give consent
Send the selected data
Send the selected data and other information of the connection
Clear the storage

Figure 4.2: The sequence diagram of establishing a new connection

4.2.2 State Design

To ensure a clear and privacy-conscious interaction flow, BetterID employs a dual-state architecture managed with zustand. It features a global store that holds persistent information, such as previously acquired credentials and established connections. Additionally, there is a temporary store used exclusively during the data-sharing process. This temporary store tracks user selections and validates them, allowing the application to alert users if they have not selected the necessary data or if they have selected more data than required.

This separation of stores enables the system to handle transient user decisions carefully, preventing premature data commitment and providing a middleware-like step for real-time feedback and validation. Once the user confirms the sharing process and completes the new connection, relevant details, such as the selected data, the date of the connection, and the organization they connected with, are transferred to the persistent store as part of the user's connection history.

4.3 Application of Design Principles in the Initial Design

4.3.1 User Interface and Components

Color Scheme. Color scheme plays an important role in an application because it conveys the application's echos and enhance user engagement [27]. Typically, in decentralized applications, like blockchain applications, bold colors like purple are widely used to catch people's attention [54]. Studies have advocated the use of blue and green to convey transparent and trust in applications [27]. Also, [27] recommended using light themes and neutral colors in blockchain wallet to keep the application accessible and clear. Based on these recommendations, a neutral color scheme, consisting solely of black, white, and grey, is adopted for BetterID.

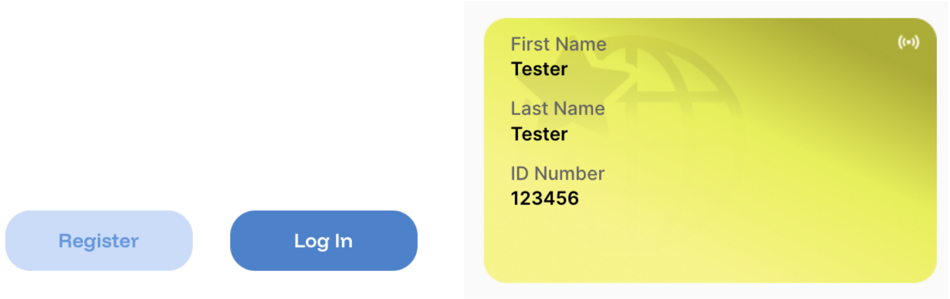
The Least Surprise Principle. As discussed in Chapter 2, the components and interactions in an application should align with the user's mental model [39]. This principle is implemented in two ways in BetterID.

First, a card-based design is used for the credentials. When people think of credentials or identity, they often envision ID cards. By using a card-based design, it fits better with users mental model and can reduce cognitive load [5, 8].

Second, the privacy notice is displayed after users select the required data. To make interactions in BetterID more predictable, the interaction in BetterID mimics other applications that users frequently interact with, such as e-banking and hotel booking apps. In these applications, users typically enter transaction details or select a date for hotel bookings first. Afterward, a summary of the information is displayed, allowing users to review the details before finalizing the transaction or confirming the booking. The privacy notice serves a similar purpose: to inform users about potential privacy issues and prompt them to review the data being shared. By mimicking the interaction style of these familiar systems, it is decided that the privacy notice should be shown after the data selection.

Hierarchy by Contrast. "Refactoring UI" by Adam Wathan is renowned for translating complex design concepts into actionable advice tailored for developers [1]. It emphasizes functionality and usability over mere aesthetics, making it easier for developers to implement effective design solutions without extensive design backgrounds. During the design of the user interface, some recommendations from "Refactoring UI" [1] were implemented.

For instance, contrast is used to establish a visual hierarchy, ensuring that only certain elements capture the user's attention. In Figure 4.3, two examples of how contrast can create the hierarchy are shown. One example features the buttons for registration and login, while the other highlights only the content of each field in credentials.



First Name
Tester

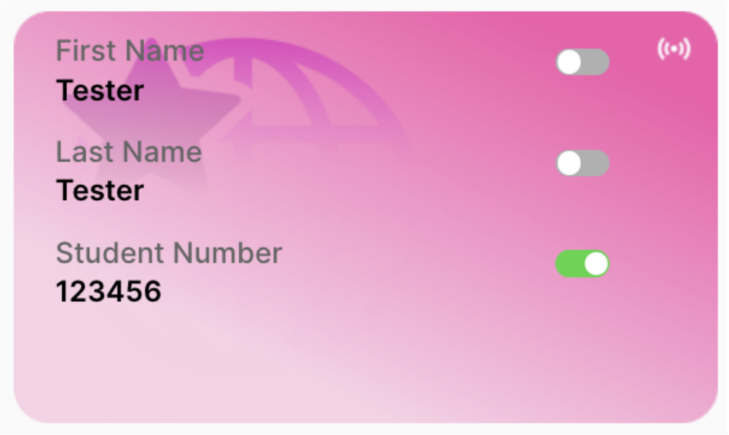
Last Name
Tester

ID Number
123456

(a) Buttons for register and login (b) Labels in credentials

Figure 4.3: Two Examples of Using Contrast to Provide Hierarchy

Selective Disclosure. To prevent the use of dark design patterns in the system, all choices will be presented equally, allowing users the right to select which data and credentials they wish to share. Selective disclosure is implemented during the data selection process for new connections, as illustrated in Figure 4.4. When an organization requests users to share specific data, users can choose the required information by clicking on a switch. When the switch is positioned to the right, it will have a green background, indicating that the data is selected. Unlike existing SSI applications on the market, the new SSI application allows users to share only the necessary data from a credential, without the requirement to disclose all information.



First Name
Tester

Last Name
Tester

Student Number
123456

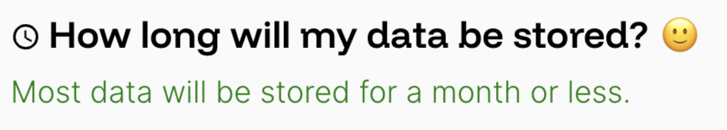
Figure 4.4: The implementation of selective disclosure in the initial design

4.3.2 Privacy Notice

The representation of the privacy notice is the most important aspect in the design, since the new SSI application aims at informing users about privacy issues more efficiently. As mentioned before, by referring to other systems, the privacy notice is displayed after users select the data to share. More design details of the new version of the privacy notice will be discussed in this section.

Integrate Into the System and Make It Obvious. Through the review of the literature and testing of the existing SSI application, one finding is that decoupled notices remain popular [70]. However, as [70] pointed out that this separate presentation of notices is not effective in communicating with users. Based on the design principles identified in the literature, a dedicated page for the privacy notice is created. This approach ensures that the notice is integrated into the system, and it is not combined with other information. In this way, the privacy notice will capture users' attention more effectively and the communication with users will be enhanced.

Keep It Short and Simple. Since short-form notices have been shown to be effective across various fields, the privacy notice in BetterID should also follow a short-form design. As [6] pointed out, CLEVER°FRANKE's, DAPIS and privacylabel.org are the only privacy visualization that are currently still being developed. After reviewing their design, only privacylabel.org [66] fits better with presenting a privacy notice in a short form. In line with these design principles, icons were incorporated for each piece of information. Instead of using terms like "Data Sales", a question-and-answer format is adopted, to clarify the key aspects of each connection in the initial design, as illustrated in Figure 4.5.



How long will my data be stored? 🙂

Most data will be stored for a month or less.

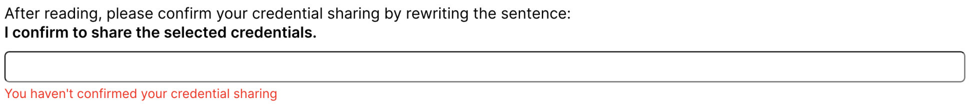
Figure 4.5: The question-and-answer format in BetterID in the initial design

Include The Desired Content. To determine the content for the privacy notice, the results from [6] are very beneficial. They interviewed users and experts to create a ranked list of the most important privacy attributes that people care about [6]. Additionally, an understanding of which privacy attributes should be included in the notices is gained by examining the privacy visualization provided by privacylabel.org [66] . To ensure that the privacy notice in BetterID aligns with the legal requirements, a review of the requirements from GDPR is conducted as well. Ultimately, the content in the privacy notice includes: 1) What data is collected? 2) Who will my data be shared with? 3) What is the purpose of data collection? 4) How long will my data be stored? 5) Where will my data be processed?

Color Code and Smiley Score. In BetterID, the Smiley Score, developed by [79], to provide users with a general impression of various aspects is implemented in the initial design. If users find it challenging to understand the content, the smiley score can offer some assistance. The smiley score features five expressions: angry, sad, indifferent, happy, and laughing. As shown in Figure 4.5, since most data will be stored for a month or less, a happy face is displayed. Additionally, a color code is used to highlight positive aspects in green and negative aspects in red.

Reading a page filled with text can be exhausting for users. By using the smiley score and color coding, users can quickly grasp the important elements of the content. Research shows that users tend to react more strongly to negative information [52]. Therefore, by drawing attention to negative aspects first, users are warned to be more cautious in their behavior.

Type Attractor. Using interventions like attractors can help in steering users away from their habitual behaviors. A study has shown that type attractors are particularly effective in drawing users' attention to essential information needed for decision-making [9]. In BetterID, a type attractor is implemented in the end of the privacy notice. Users are required to type, "I confirm that I want to share the selected credentials." to share their data and complete the connection, as illustrated in Figure 4.6. This approach is intended to ensure that users are at least aware of the data they have chosen to share, fostering a sense of responsibility regarding their decisions.



After reading, please confirm your credential sharing by rewriting the sentence:

I confirm to share the selected credentials.

You haven't confirmed your credential sharing

Figure 4.6: The type attractor in BetterID

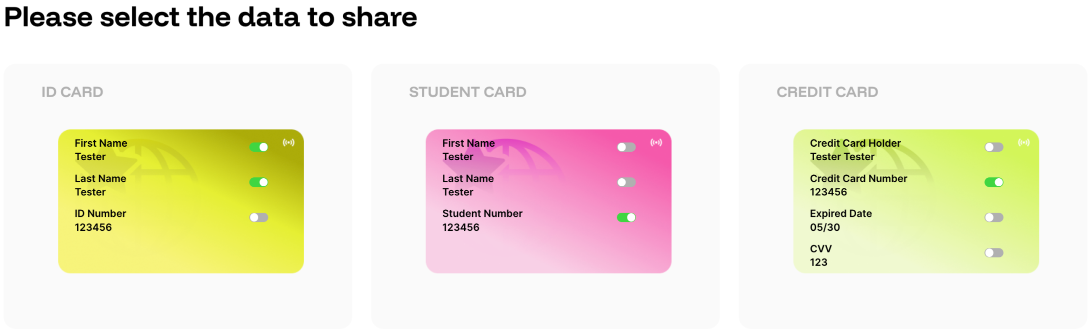
4.4 Modifications After the Pilot Study

After implementing the initial design of BetterID and designing the study, a pilot study to test the system's usability and gather feedback from various users is conducted. By observing user interactions with BetterID and considering their comments, several revisions were made to the initial design, which were incorporated into the final version of the system.

The results of the pilot study is presented in chapter 6. Based on the results from the pilot study, major changes were made in data selection in a new connection and the representation of the privacy notice.

4.4.0.1 Data Selection in a New Connection

Privacy by Design. A good observation from the study is that users do not want to share unnecessary credentials. In the initial design, all credentials were displayed in the data selection section when establishing a new connection, as shown in Figure 4.7. To protect users from sharing unnecessary information and to respect their preference against sharing unnecessary credentials, a major change is to only include the required credentials in the data selection process.



Please select the data to share

ID CARD

First Name
Tester

Last Name
Tester

ID Number
123456

STUDENT CARD

First Name
Tester

Last Name
Tester

Student Number
123456

CREDIT CARD

Credit Card Holder
Tester Tester

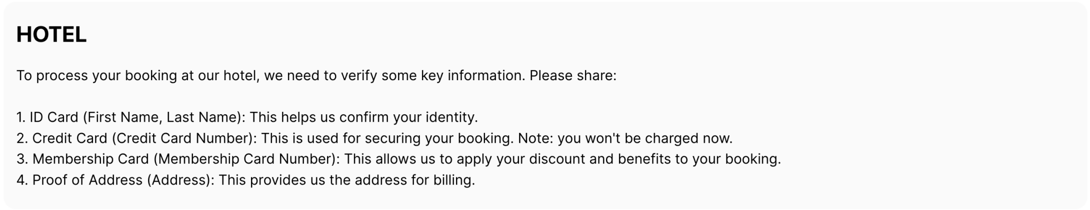
Credit Card Number
123456

Expired Date
05/30

CVV
123

Figure 4.7: The initial design of data selection in a new connection (with selective disclosure)

Required Data Checklist. One issue with the data selection process is that users often focus more on the credentials rather than on the required data. Once they understand a credential is needed, they often ignored the required data, and selected all the data on the credential. To remedy this, distractions should be minimized and users should be assisted in selecting only the necessary information. The problem stems from the initial design, which only included introductory text at the top to inform users about the required credentials and data, as illustrated in Figure 4.8. Additionally, there was no any variation in font weight to emphasize the required data. To improve this, a new design that combines the introduction with selective disclosure was proposed, as shown in Figure 4.9.



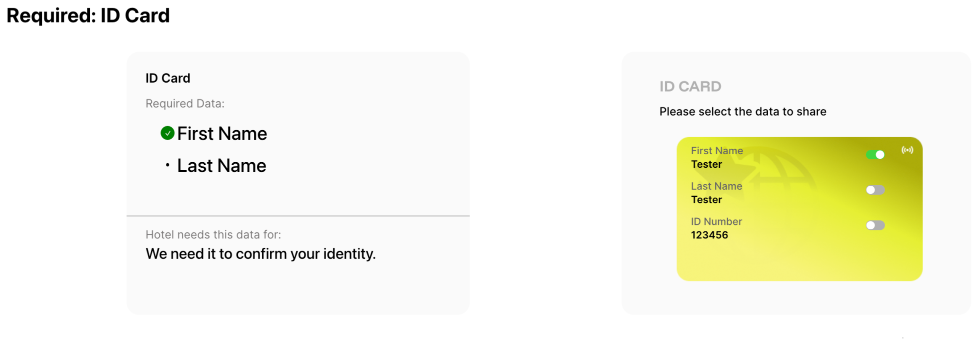
HOTEL

To process your booking at our hotel, we need to verify some key information. Please share:

1. ID Card (First Name, Last Name): This helps us confirm your identity.
2. Credit Card (Credit Card Number): This is used for securing your booking. Note: you won't be charged now.
3. Membership Card (Membership Card Number): This allows us to apply your discount and benefits to your booking.
4. Proof of Address (Address): This provides us the address for billing.

Figure 4.8: The initial design of the introduction text in a new connection

In the new design, the data sharing page is divided into distinct credential blocks. Each block contains only one required credential. On the left side, a card format is adopted to inform users about the necessary data and its purpose. The required data is emphasized by using the largest font size and increased font weight. Each required data point is preceded by a bullet point, which will change to a green check mark once the user selects the data, as illustrated in Figure 4.9.



Required: ID Card

ID Card

Required Data:

- ✓ First Name
- · Last Name

Hotel needs this data for:

We need it to confirm your identity.

ID CARD

Please select the data to share

First Name
Tester

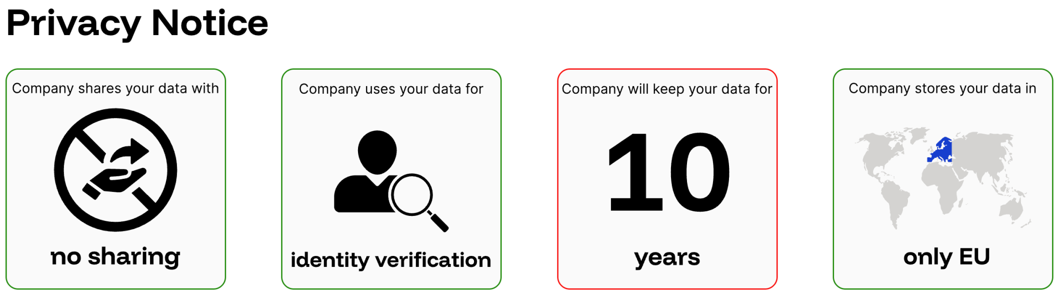
Last Name
Tester

ID Number
123456

Figure 4.9: The new design of a block in data selection, with card-based design on the left, including a check list to indicate if users select the required data and the purpose, and on the right, the original design of selective disclosure is preserved

4.4.0.2 Representation of Privacy Notice

Block-based Design with Icons. The tendency of users to ignore privacy notices indicates that the initial design of the notice is not ideal. One issue is that, although the overall content was short, it was still in a text format that users had to read. However, users typically do not enjoy reading textual privacy notices because they are cumbersome [53]. A novel representation was needed. GDPR and some studies advocated the use of icons to visually present privacy attributes [30, 63]. Therefore, the text format was abandoned and a block-based design is adopted instead. Each block represents a privacy attribute of the connection. In each block, icons are incorporated to convey information with minimal text, as illustrated in Figure 4.10.



Privacy Notice

Company shares your data with
no sharing

Company uses your data for
identity verification

Company will keep your data for
10
years

Company stores your data in
only EU

Figure 4.10: The new block-based design of privacy notice

Remove Distracting Element. In the initial design, both the color code and the smiley score were intended to draw users' attention to negative aspects, prompting them to be cautious. However, users reported that after reading the privacy notice, the only detail they could remember was the negative information. To address this issue, the smiley score is removed, as some users also found it difficult to understand.

In the new design, the color code is used solely as the border for each block. If a privacy attribute is concerning, the border will be red; otherwise, it will be green.

Animation. animations is implemented for each block of the privacy notice to help draw users' attention. With this feature, the blocks will appear one by one, allowing users enough time to read the content. According to the Nielsen Norman Group, utilizing animations can effectively capture users' attention [57].

Chapter 5

Implementation

This chapter examines the implementation of the new SSI application. It begins by outlining the technology stack and tools chosen to build the application. The chapter then describes the structure of the application, including its pages, key components, and the user flow within the application. It then explains the implementation of the state management. Finally, it presents the finalized user interface of the application.

5.1 Technology Stack

To implement the frontend of the SSI web application, the following technologies were employed:

- **React (Version 18.2.0):** A open-source JavaScript library for building user interfaces, developed and maintained by Meta. React enables developers to create dynamic and interactive UIs by using a component-based architecture, where reusable components manage their own state and render efficiently [55].

- **JavaScript:** A programming language that powers web development by enabling dynamic and interactive web experiences. As a core technology of the web, it allows developers to manipulate the DOM, handle user interactions, and communicate with servers [40].

- **zustand (Version 5.0.3):** A lightweight, high-performance, and scalable state management solution with minimal setup. Zustand features a comfy API based on hooks. It is not boilerplatey or opinionated, yet has enough conventions to be explicit and flux-like [65].

- **npm (Version 10.2.4):** A widely used package manager for JavaScript that simplifies the installation, management, and sharing of dependencies in web development [61].

5.2 Application Structure and User Flow

The application is structured as a single-page application built with React and managed using zustand for state management. It is composed of several main pages and components that correspond to core user actions. Navigation is handled via a router, and the application state is persisted in memory using zustand. The pages in the system are:

- **Dashboard**: All the function supported by the application is illustrated here and users can navigate to different pages.

- **Credential Management Page**: List of all the credentials that users already have. Users can review the details of each credential and delete the credential that they no longer need.

- **Adding New Credentials Page**: All the available credentials are categorized by the organizations who can issue them. The user can select the credentials they want to add.

- **Connections Page**: Users can select a third party to establish a new connection, and review the connections they had in the past.

- **Data Selection Page**: Users can see the required data as a checklist and they can select the data they want to share.

- **Privacy Notice Page**: After selecting data to share, the privacy notice with important privacy attributes are displayed in this page.

The main components in the application are credentials, organizations and connections. When a user adds a credential, it is saved in the zustand store and rendered in the credentials list. When a connection is initiated, a new connection object is created and updated based on the status of the verification process. Organizations are the entities who can issue a new credential to the user and ask the user to share data in a connection.

Figure 5.1 illustrates the interaction in the entire application between pages and component.

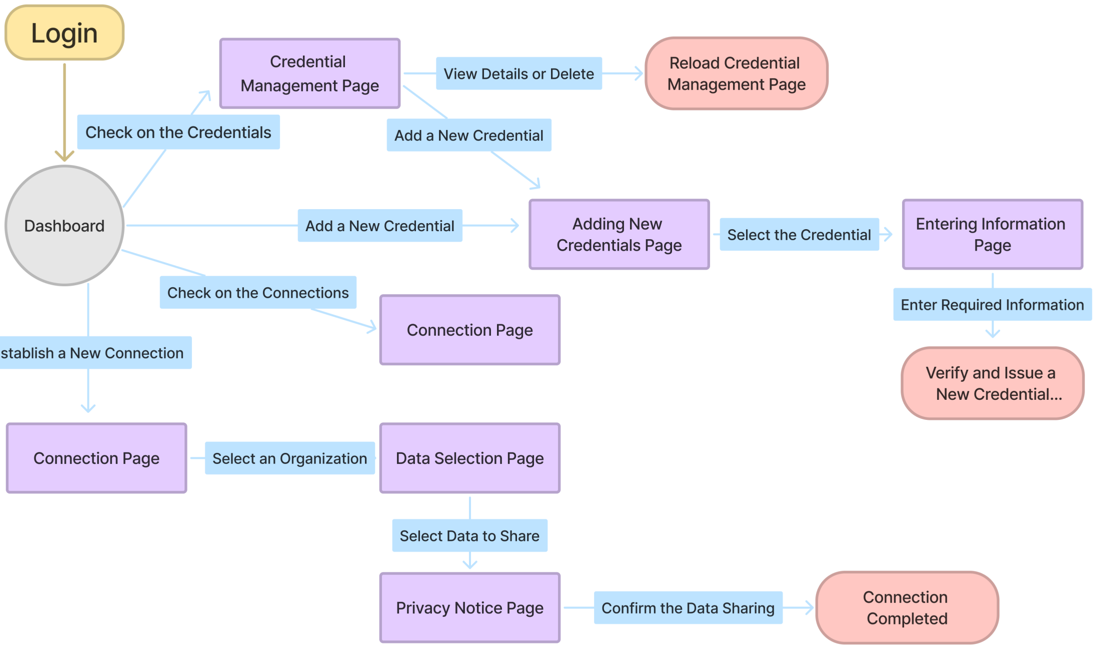


Figure 5.1: High-level user flow of the SSI application, illustrating the main pages, supported user actions (e.g., adding credentials, managing connections), and transitions between views. This diagram reflects how users navigate the system and how different components are logically connected.

5.3 State Management

Since the application is a frontend mock-up, there is no backend database to store all the credential and connection information. A key challenge is to implement the state management in the frontend to store the credential and connection information. To solve this problem, zustand is used as a global store to manage application-wide state. Here is the code how state management is implement in the application:

```
export const usePermanentStore = create(
    persist((set, get) => ({
            credentials: [
                {
                    "card_id": 1,
                    "card_name": "ID Card",
                    "card_color": "yellow",
                    "info": {
                        "First Name": "Tester",
                        "Last Name": "Tester",
                        "ID Number": "123456",
                    }
                },
                {
                    "card_id": 2,
                    "card_name": "Student Card",
                    "card_color": "pink",
                    "info": {
                        "First Name": "Tester",
                        "Last Name": "Tester",
                        "Student Number": "123456",
                    }
                }
            ],
            connections: [
                {
                    "connection_id": 1,
                    "connection_party": "University of Zurich",
                    "icon": "school",
                    "date": "04.12.2024",
                    "shared_credentials": [
                        "ID Card",
                        "Student Card"
                    ],
                    "shared_data": [
                        "First Name",
                        "Last Name",
                        "ID Number",
                        "Student Number",
                    ]
                },
                {
                    "connection_id": 2,
                    "connection_party": "Swiss Airline",
                    "icon": "plane",
                    "date": "16.12.2024",
                    "shared_credentials": [
                        "ID card",
                    ],
                    "shared_data": [
                        "First Name",
                        "Last Name",
                        "ID Number",
                    ]
                }
            ],

            initialCredentials() {
                set(() => ({credentials: [
                        {
                            "card_id": 1,
                            "card_name": "ID Card",
                            "card_color": "yellow",
                            "info": {
                                "First Name": "Tester",
                                "Last Name": "Tester",
                                "ID Number": "123456",
                            }
                        },
                        {
                            "card_id": 2,
                            "card_name": "Student Card",
                            "card_color": "pink",
                            "info": {
                                "First Name": "Tester",
                                "Last Name": "Tester",
                                "Student Number": "123456",
                            }
                        }
                    ]}))
            },
            initialConnections() {
                set(() => ({connections: [
                        {
                            "connection_id": 1,
                            "connection_party": "University of Zurich",
                            "icon": "school",
                            "date": "04.12.2024",
                            "shared_credentials": [
                                "ID Card",
                                "Student Card"
                            ],
                            "shared_data": [
                                "First Name",
                                "Last Name",
                                "ID Number",
                                "Student Number",
                            ]
                        },
                        {
                            "connection_id": 2,
                            "connection_party": "Swiss Airline",
                            "icon": "plane",
                            "date": "16.12.2024",
                            "shared_credentials": [
                                "ID card",
                            ],
                            "shared_data": [
                                "First Name",
                                "Last Name",
                                "ID Number",
                            ]
                        }
                    ]}))
            },
            addingCredential(cardObject) {
                set((state) => ({credentials: [...state.credentials,
                   cardObject]}));
            },
            deleteCredential(cardID) {
                set((state) => ({credentials: state.credentials.filter((
                   o) => o.card_id !== cardID)}));
            },
            addConnection(id, selectedCredentials, selectedData) {
```

```
        const newId = get().connections[get().connections.length - 1].connection_id + 1;
        const today = new Date();
        const yyyy = today.getFullYear();
        let mm = today.getMonth() + 1;
        let dd = today.getDate();
        set((state) => ({connections: [...state.connections, {
            "connection_id": newId,
            "connection_party": id === 'hotel' ? "Hotel" : "Job",
            "icon": id,
            "date": dd + "." + mm + "." + yyyy,
            "shared_credentials": selectedCredentials,
            "shared_data": selectedData,
          }]}))
      }
    }),
    {
      storage: createJSONStorage(() => localStorage),
    },
  )
)
```

Listing 5.1: Zustand store configuration used for managing global application state, including credentials and connections.

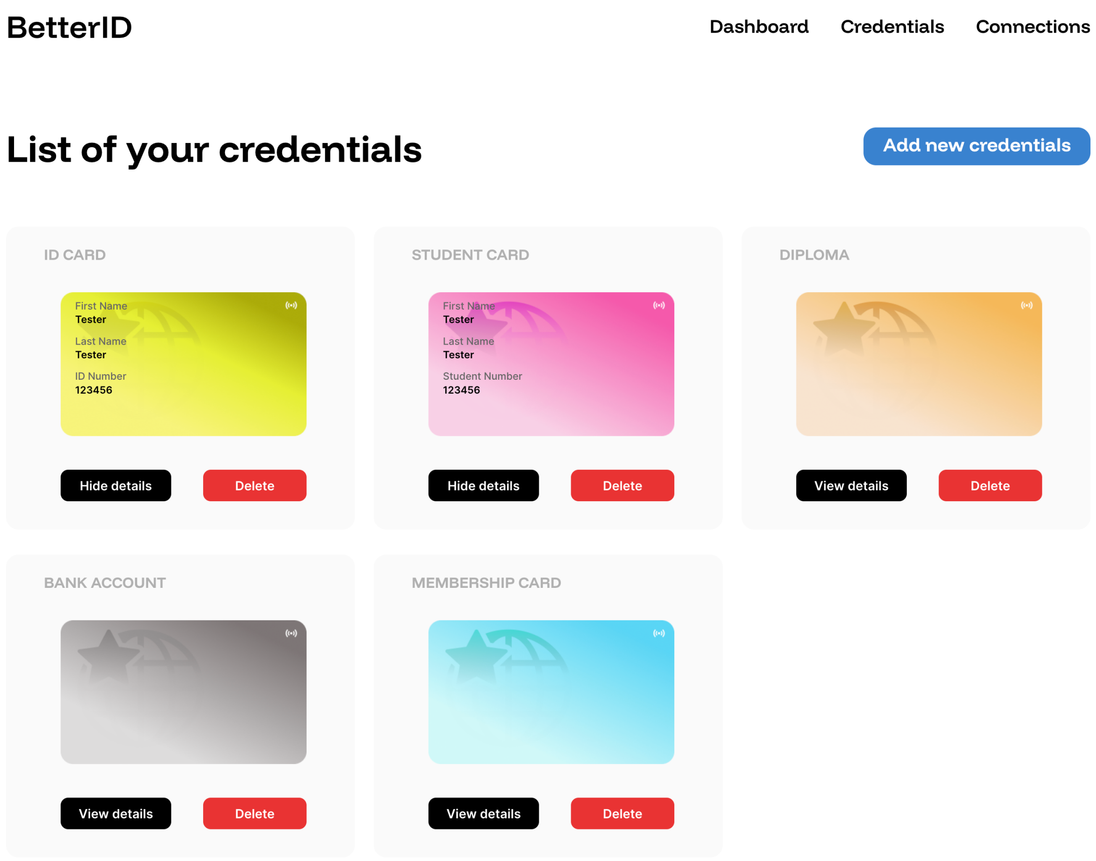
Once a user login to the application, the credentials and connections information will be initialized. Upon a new credential is added or a new connection is established, the storage will be updated.

5.4 User Interface

After implementing the changes identified in the pilot study, the work on BetterID implementation was completed. In this section, the result of the implementation will be presented.

5.4.1 Credential Management

In the "Credential Management" page (Figure 5.2), users can find all the credentials they already have and the information each credential contains. They can also delete the credential that they no longer needs by clicking on the delete button.



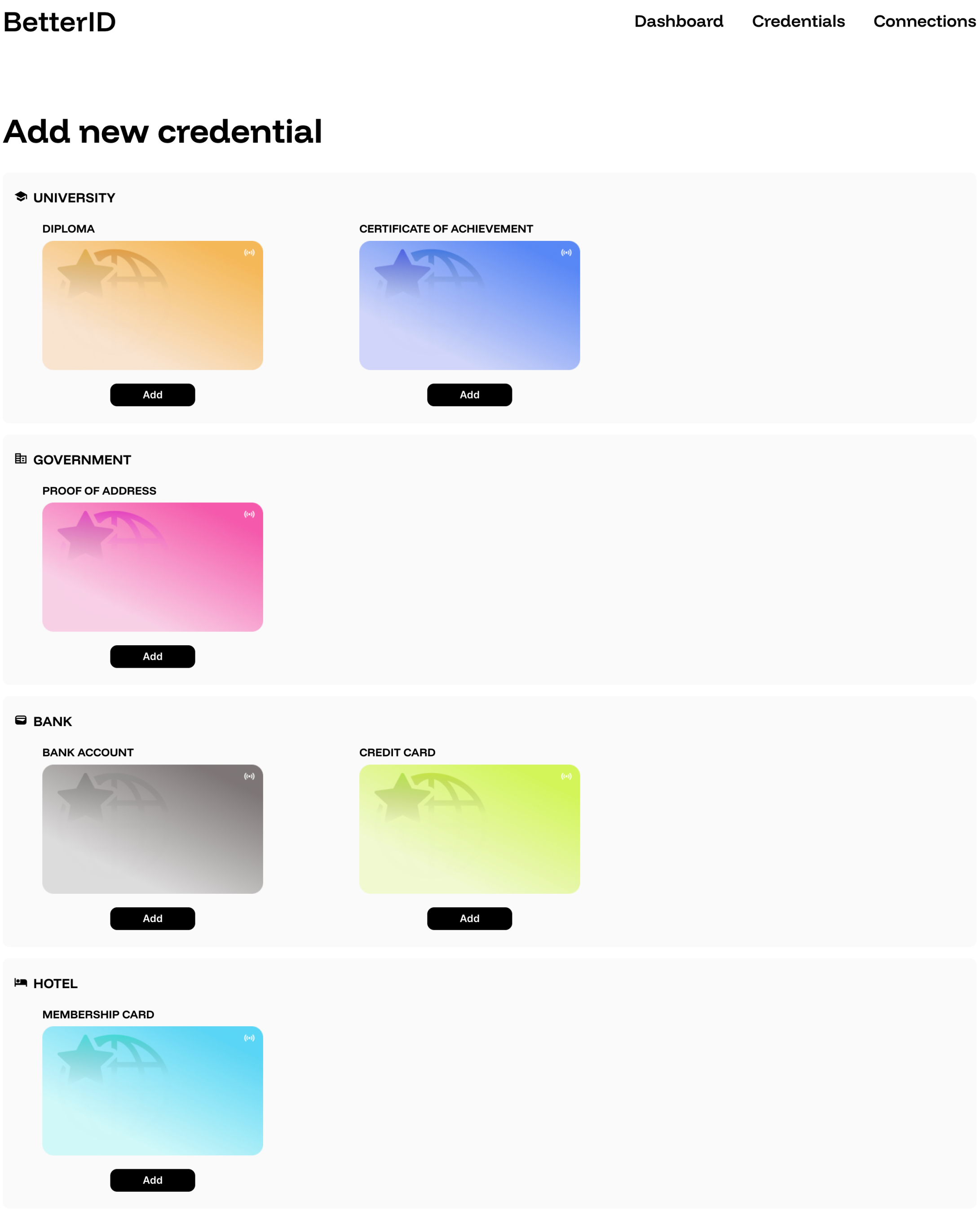
First Name
Tester
Last Name
Tester
ID Number
123456

First Name
Tester
Last Name
Tester
Student Number
123456

Figure 5.2: Credential management page

5.4.2 Add New Credentials

By clicking on the button “Add new credentials”, users will be redirected to “Adding New Credentials” page (Figure 5.3). All the available credentials are categorized by the organization. Users can click the add button to add the desired credential.



BetterID

Add new credential

UNIVERSITY

DIPLOMA

CERTIFICATE OF ACHIEVEMENT

GOVERNMENT

PROOF OF ADDRESS

BANK

BANK ACCOUNT

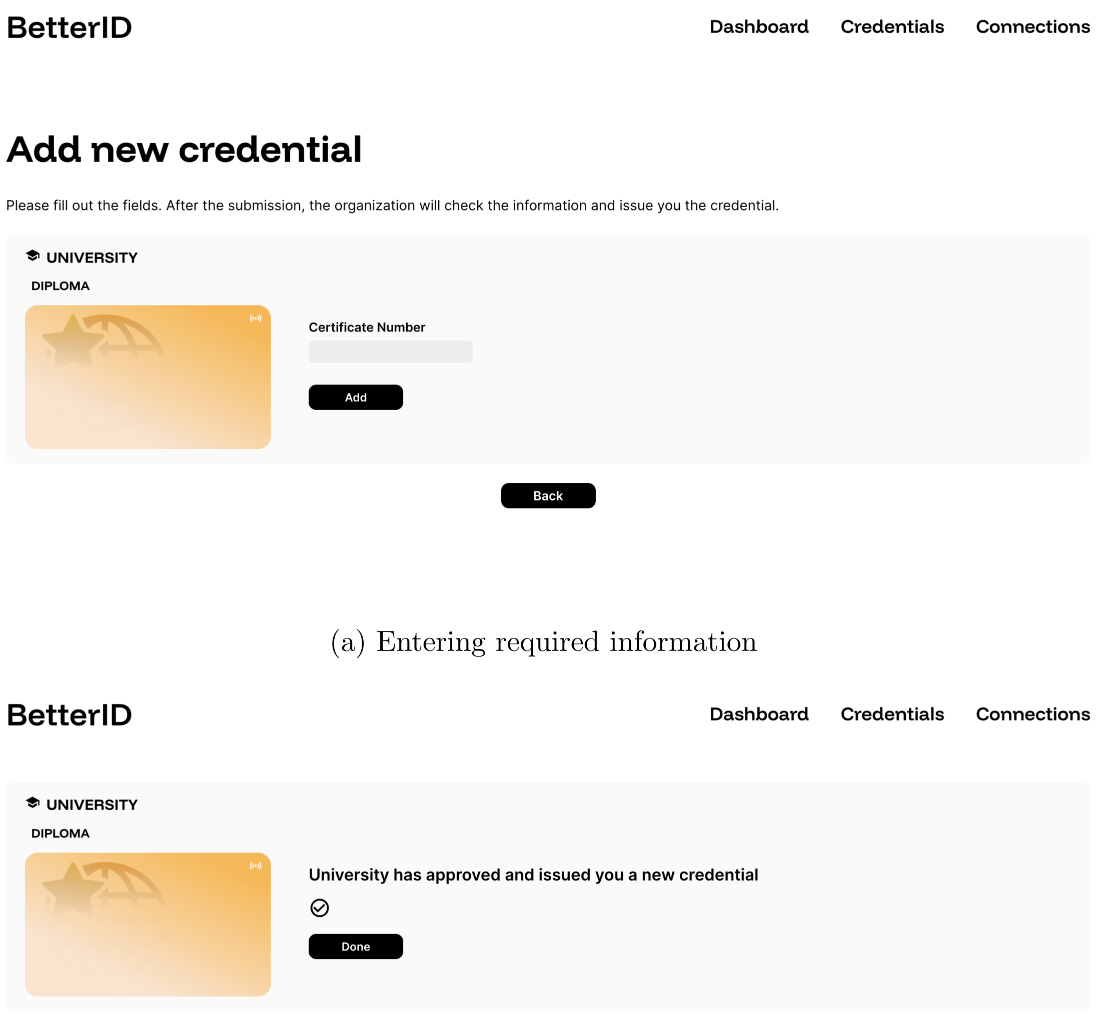
CREDIT CARD

HOTEL

MEMBERSHIP CARD

Figure 5.3: Add new credentials page

Consider the example of a diploma, in order to add the credential, users must submit the necessary information to the issuer, who will then verify the data and subsequently issue the credential to the user. (Figure 5.4).



Add new credential

Please fill out the fields. After the submission, the organization will check the information and issue you the credential.

Certificate Number

(a) Entering required information

University has approved and issued you a new credential

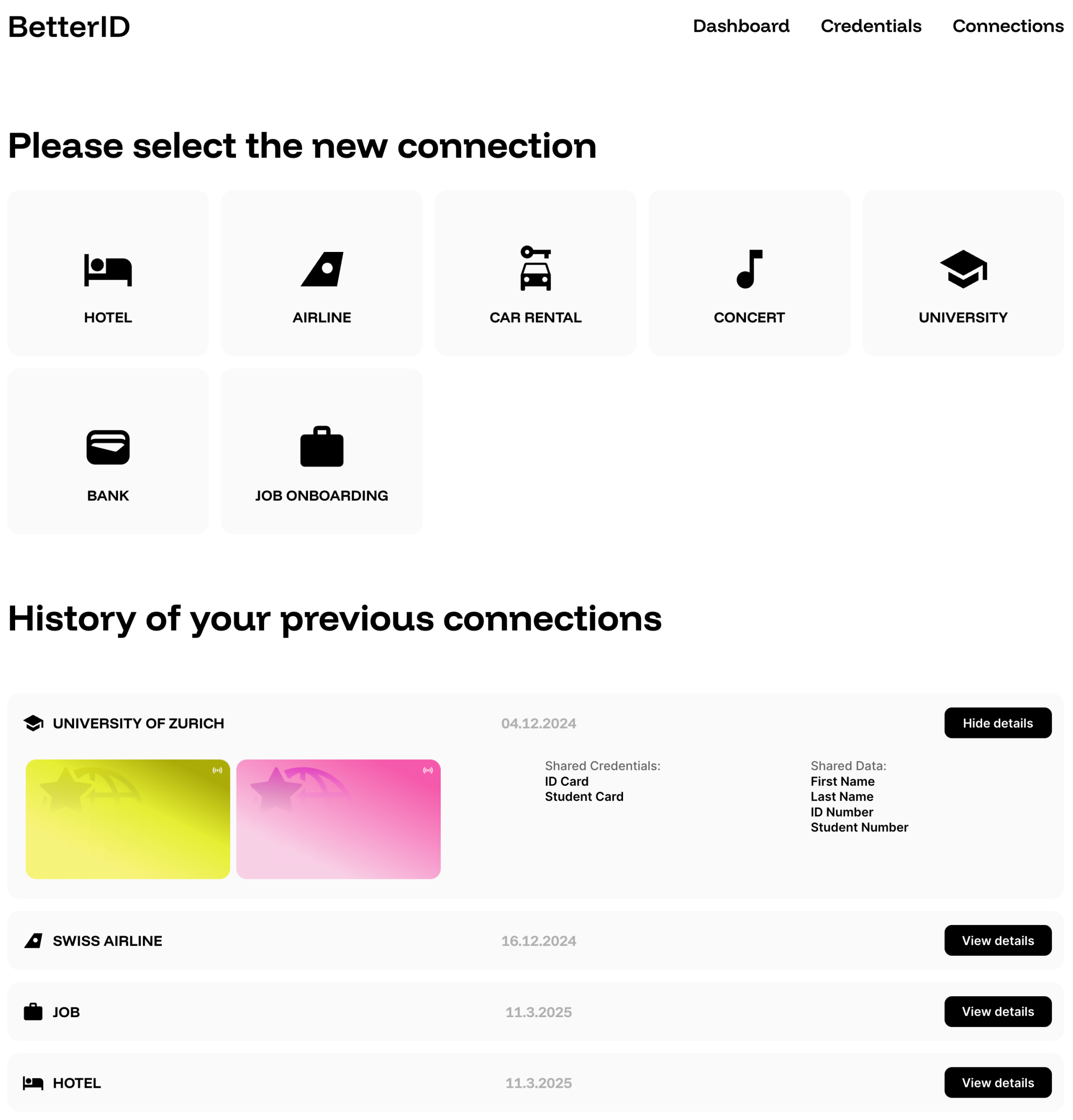
✓

(b) Adding the credential successfully

Figure 5.4: The process of adding a new credential

5.4.3 Connection

“Connection” page (Figure 5.5) is where users can start a new connection by clicking on the organization they want to connect with, and review the connections they had in the past.



Please select the new connection

History of your previous connections

UNIVERSITY OF ZURICH 04.12.2024

Shared Credentials:
ID Card
Student Card

Shared Data:
First Name
Last Name
ID Number
Student Number

SWISS AIRLINE 16.12.2024

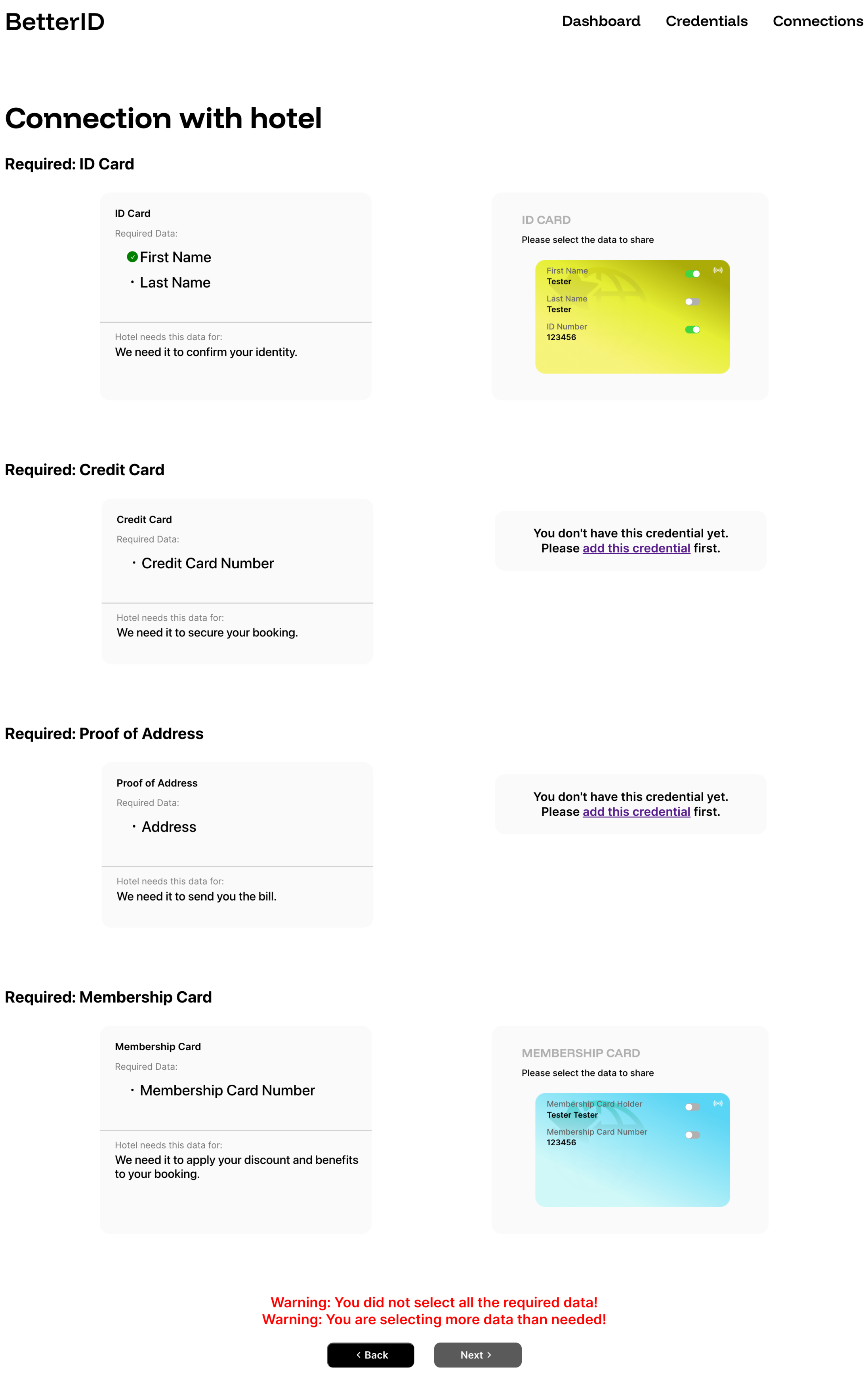
JOB 11.3.2025

HOTEL 11.3.2025

Figure 5.5: Connection page

5.4.4 Data Selection in a Connection

After a new connection is established, users need to select the data they want to share. Here (Figure 5.6) is the new design of the page for selecting data.



BetterID

Dashboard Credentials Connections

Connection with hotel

Required: ID Card

ID Card

Required Data:

- ✓ First Name
- Last Name

Hotel needs this data for:

We need it to confirm your identity.

ID CARD

Please select the data to share

First Name
Tester

Last Name
Tester

ID Number
123456

Required: Credit Card

Credit Card

Required Data:

- Credit Card Number

Hotel needs this data for:

We need it to secure your booking.

You don't have this credential yet.
Please add this credential first.

Required: Proof of Address

Proof of Address

Required Data:

- Address

Hotel needs this data for:

We need it to send you the bill.

You don't have this credential yet.
Please add this credential first.

Required: Membership Card

Membership Card

Required Data:

- Membership Card Number

Hotel needs this data for:

We need it to apply your discount and benefits to your booking.

MEMBERSHIP CARD

Please select the data to share

Membership Card Holder
Tester Tester

Membership Card Number
123456

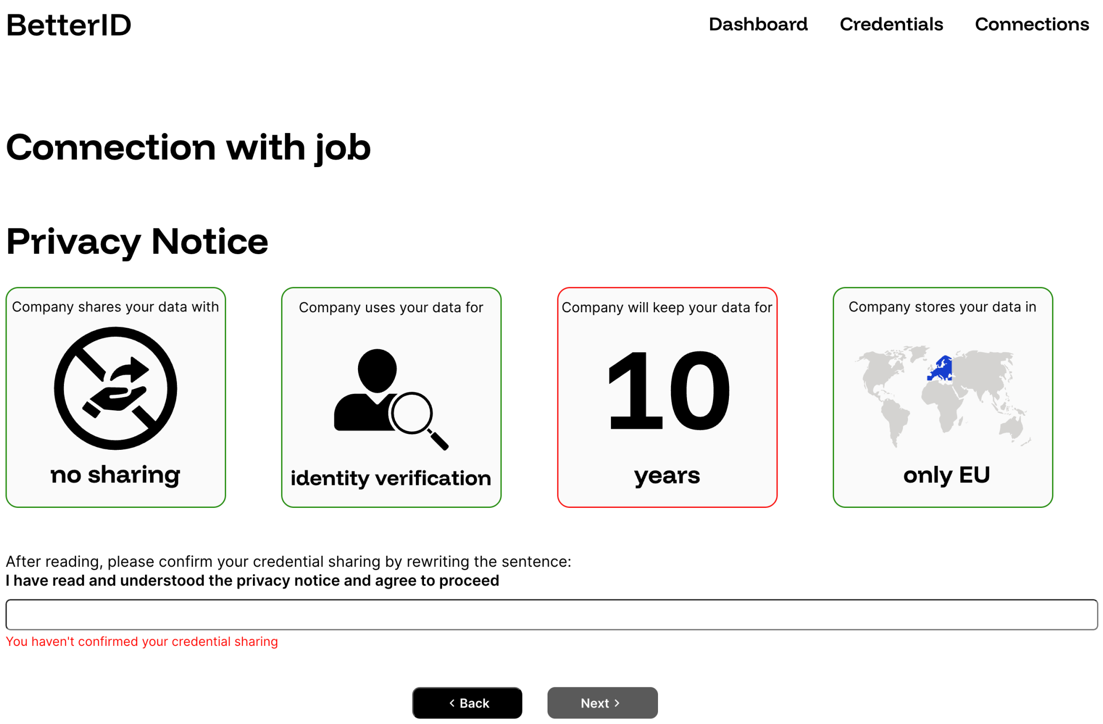
Warning: You did not select all the required data!
Warning: You are selecting more data than needed!

Figure 5.6: Data selection in a connection

As in Figure 5.6, if users do not have the required credential yet, they can click on the link to go to add it. If users have not selected all the required data, or they selected more data than required, warning messages will be displayed in the end, above the button for going to the next page.

5.4.5 Privacy Notice

After users select all the required data, the privacy notice (Figure 5.7) is shown.



Connection with job

Privacy Notice

Company shares your data with
no sharing

Company uses your data for
identity verification

Company will keep your data for
10
years

Company stores your data in
only EU

After reading, please confirm your credential sharing by rewriting the sentence:
I have read and understood the privacy notice and agree to proceed

You haven't confirmed your credential sharing

Figure 5.7: Privacy notice in a connection

Chapter 6

Evaluation

This chapter outlines the methodology used in the study. It further details the results of both the pilot study and the user study, including quantitative findings and user feedback. In addition, the chapter discusses these results in relation to the existing literature and potential future directions, while also identifying potential threats to validity.

6.1 Methods

6.1.1 User Study Design

6.1.1.1 Selection of SSI Application

To choose an appropriate SSI application as reference, the applications that were previously tested were reviewed again. The criteria for selecting the reference SSI application are as follows:

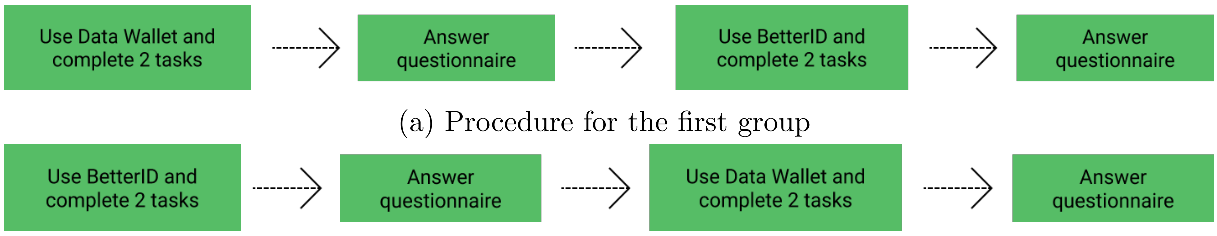
- The application must provide a privacy notice during the data sharing process.
- The application should include tutorials or demos that can provide some suitable scenarios for users to interact with it.

Based on these criteria, Data Wallet [37] is selected because it is the only application that meets the requirements.

6.1.1.2 Procedure

At the start of the study, participants will answer a pre-study questionnaire (see Appendix C)that gathers information about their background and their knowledge of SSI and UI design. If participants are unfamiliar with SSI, they will receive a brief introduction to its fundamental concepts and benefits.

The study employs a within-subject design, meaning that each participant will interact with both SSI applications. Participants were randomly divided into two groups to counterbalance any order effects. One group will interact with Data Wallet first and then with BetterID (as shown in Figure 6.1a), while the other group will interact with BetterID first and then with Data Wallet (as shown in Figure 6.1b). During each interaction, users will complete two tasks by following the provided instructions. After each interaction, participants will need to answer to a questionnaire (see Appendix D) regarding UX, their awareness of privacy and their trust in the system.


Use Data Wallet and complete 2 tasks
Answer questionnaire
Use BetterID and complete 2 tasks
Answer questionnaire
Use BetterID and complete 2 tasks
Answer questionnaire
Use Data Wallet and complete 2 tasks
Answer questionnaire

(a) Procedure for the first group

(b) Procedure for the second group

Figure 6.1: The procedure of the study for two groups

6.1.1.3 Tasks

In Data Wallet, two demonstrations from their website were selected. The first task involves requesting and receiving an e-receipt, which will then be shared with the accounting department [35]. The second task is to receive a COVID test result and share it with the airport [36].

Although COVID-19 test results are no longer universally required for travel, proof of vaccination remains a common requirement in some countries. Moreover, a typical use case for SSI applications involves presenting credentials at airports, such as boarding passes, which makes this scenario relevant and realistic. The process of sharing paper-based COVID-19 test results is also a familiar experience for many users, which helps them to better relate to the task. This familiarity enables a more intuitive understanding of the context and allows a meaningful comparison between traditional paper credentials and the digital process facilitated by SSI.

For BetterID, the first task requires users to share the required data with a company to complete the job onboarding process. In the second task, users will need to share the required data with a hotel to verify their booking. In both tasks, users must first request the necessary credentials.

The devices, step-by-step instructions and necessary documents are provided to help users complete all the tasks. If users feel confused by the instructions or find themselves stuck and unable to complete the tasks, then they can ask for assistance.

6.1.1.4 Questionnaire

The questionnaire is divided into four parts: UX, awareness of privacy, user trust and further feedback. To evaluate the UX of both applications, the User Experience Questionnaire (UEQ) [84] was selected due to its comprehensive coverage of key UX dimensions. While the UEQ includes six scales, it is allowed to only use the scales that are related to the research. Therefore, in the user study, two scales were excluded, and the remaining four scales that indicate pragmatic quality were selected:

- Attractiveness: Overall impression of the product. Do users like or dislike the product?
- Perspicuity: Is it easy to get familiar with the product? Is it easy to learn how to use the product?
- Efficiency: Can users solve their tasks without unnecessary effort?
- Dependability: Does the user feel in control of the interaction?

Each scale consists of several items, with participants rating their agreement or disagreement with each statement on a Likert scale (typically from 1 = “Strongly disagree” to 7 = “Strongly agree”). The responses are then averaged to provide a score for each scale, reflecting the user’s experience in each dimension.

Alternative tools such as the System Usability Scale [91] provide only a single usability score, offering limited insight into specific UX dimensions. NASA-TLX [60], meanwhile, focuses on cognitive workload and does not capture aspects like user satisfaction or clarity. Given these limitations, UEQ was the most suitable choice for obtaining a comprehensive yet focused assessment of user experience.

Since the purpose of privacy notices is to inform users about important privacy attributes, which is required by the law, users’ awareness of privacy is defined as the ability to recall each privacy attribute after the connections are completed in this study. The part for evaluating awareness of privacy includes seven questions. All of them are yes-or-no questions that ask users if they can still remember different aspects of the connections they just made:

- Did you read the privacy notice?
- Can you recall who you were sharing the data with?
- Can you recall what data you shared?
- Can you recall where your shared data will be processed?
- Can you recall the purpose of the data collection?
- Can you recall if your data will be sold to other parties?

- Can you recall how long your data will be stored?

Next, users' trust in the application is measured. Based on the literature [22, 46], in this study, trust is measured as the user's perceived confidence in the application's ability to handle their data responsibly, securely, and transparently. It was measured using a 5-point Likert scale question asking "Please rate how much you trust the system as:", where 1 as Not at all and 5 as Completely.

To study the possible improvement in the design of SSI applications, users are asked to provide feedback on other aspects they wish to learn about SSI and the connection. As a new concept, SSI applications sometimes fail to communicate with users in an effective way to make users understand it and its benefits [68]. The user's opinion on other interesting aspects can be integrated into the SSI applications, so that the user can gain more knowledge about the SSI. In addition, users are asked to provide feedback on the UI design so that the usability of the SSI application can be improved.

6.1.2 Data Collection

In the user study, demographic data and participants' self-reported knowledge levels in SSI and UI design were gathered through a pre-study survey. Their opinions on the UX, awareness of privacy and the trust in the system were collected using a questionnaire. Participants also provided suggestions for the UI of BetterID. Additionally, with their consent, their interactions while using BetterID was recorded.

6.1.3 Pilot Study Design

In the pilot study, participants were instructed in the same manner as they would be in the actual user study. They were randomly divided into two groups. Initially, they completed a pre-study survey. Next, they interacted with the first application, completing two defined tasks while following the provided instructions. Afterward, they interacted with the second application. Following each interaction, participants filled out a questionnaire. With their consent, while they interacted with BetterID, the screen is recorded to help identify any confusing elements and to inform future improvements. Additionally, participants were asked to provide suggestions for improving the UI design of BetterID.

6.2 Results

6.2.1 Results of the Pilot Study

6.2.1.1 Participants

Four individuals voluntarily participated in the pilot study, consisting of two males and two females. All participants were between 22 and 26 years of age. In particular, only one participant has a solid understanding of SSI and is able to explain it to others; the remaining participants have never heard of SSI. In terms of UI design experience, one participant has extensive expertise, while two are familiar with basic UI concepts but lack practical experience. The fourth participant has some experience in UI design or evaluation.

6.2.1.2 Identified Potential Improvements

In general, participants can complete the defined tasks without significant difficulties, indicating that the application is intuitive and user-friendly. Most participants expressed a positive overall impression of the application, which suggests that the initial design ensures core usability goals. However, a closer analysis of user behavior, particularly through the screen recordings captured during the study sessions, reveals several areas where the UX could be enhanced. Also, one of the participants has intensive UI design experiences and provided many valuable suggestions on how to improve the design to provide better UX. As a results, several potential improvements are concluded:

- **Clearer Representation of the Required Data in Data Selection Page.** The page that allows users to select the data they wish to share with verifiers, is based on the established guidelines, which recommend removing default settings and presenting all choices equally. However, in the pilot study, most of the participants were unfamiliar with SSI and often struggled to grasp the purposes and benefits of selective disclosure. Many tend to only focus on the required cards and end up sharing all the data on those cards, which results in sharing more information than necessary. Therefore, improving the design for selective disclosure to emphasize the necessary data and assist users in avoiding the sharing of excessive information was essential.

- **Remove Text and Offer a Novel Visual Representation of Privacy Notice.** The primary goal of BetterID is to more effectively inform users about privacy issues. The privacy notice is created based on effective suggestions and designs. However, in the pilot study, some of the participants still tended to overlook it, which indicated the initial design of the privacy notice was not ideal. Only shortening the text in the privacy notice was not effective enough. A novel representation of the privacy notice, that can draw users' attention was needed.

- **Other Minor Issues With the UI.** In the pilot study, some minor UI issues were identified with the help of participants. For instance, the menu bar in the initial design was found to be unappealing, and some participants reported that the items in the menu bar appeared to be disabled but actually they were not.

The pilot study provided valuable insights on how to improve the design of BetterID. The identified potential improvements were late implemented in the application. More details on the changes in the design and the implementation details of the modifications can be found in Chapter 4 and Chapter 5.

6.2.2 Demographic Results of the Participants in the User Study

Ten participants voluntarily participated in the user study without receiving any compensation, consisting of two men and eight women. All participants were between 22 and 31 years old. As illustrated in Figure 6.2, four participants had never heard of SSI before, one had a very good understanding of SSI, two had a basic understanding of SSI, and three had heard of SSI but did not know what it is. Regarding knowledge of UI design, as shown in Figure 6.3, five participants are familiar with basic UI concepts but lack practical experience, two have no knowledge of UI design, two have extensive experience in UI design, and one has some knowledge of UI design.

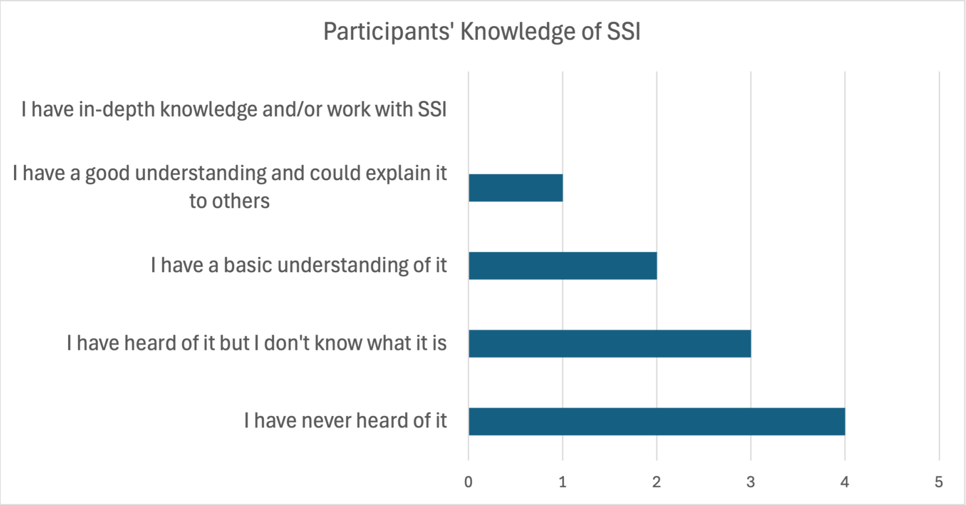


Figure 6.2: Distribution of participants' SSI knowledge levels: self-reported expertise in SSI prior to the study

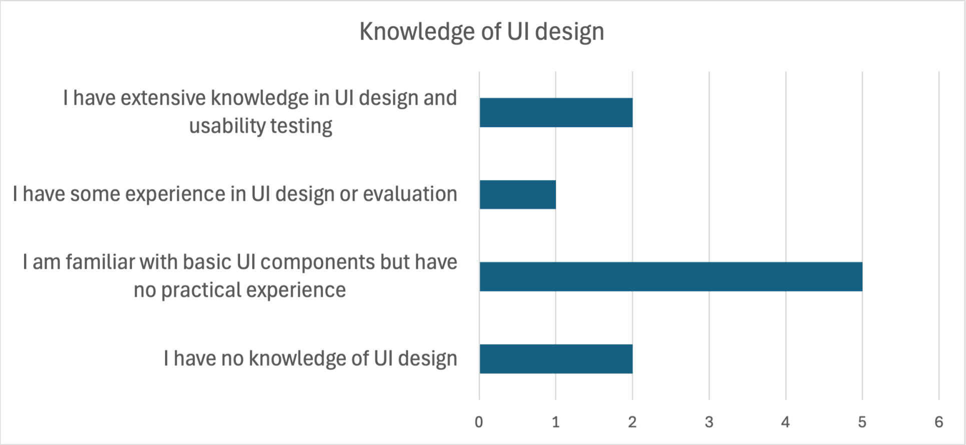


Figure 6.3: Distribution of participants' UI design knowledge levels: self-reported expertise in UI design prior to the study

6.2.3 Quantitative Outcomes in the User Study

6.2.3.1 UEQ

The results of UEQ in both BetterID and Data Wallet are presented in Figure 6.4, using the data analysis tool provided by the creators of UEQ.

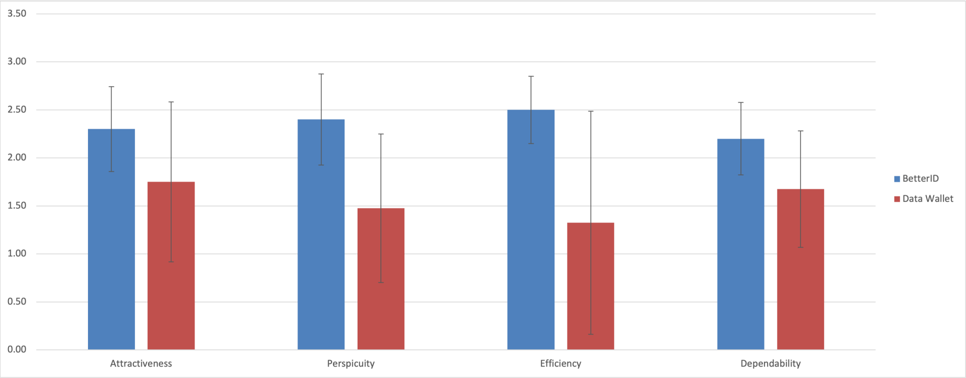


Figure 6.4: UEQ results: comparison of attractiveness, perspicuity, efficiency, and dependability between BetterID and Data Wallet

The UEQ handbook also provided benchmarks for each scale. The comparison between the results of BetterID and the benchmark is shown in Figure 6.5.

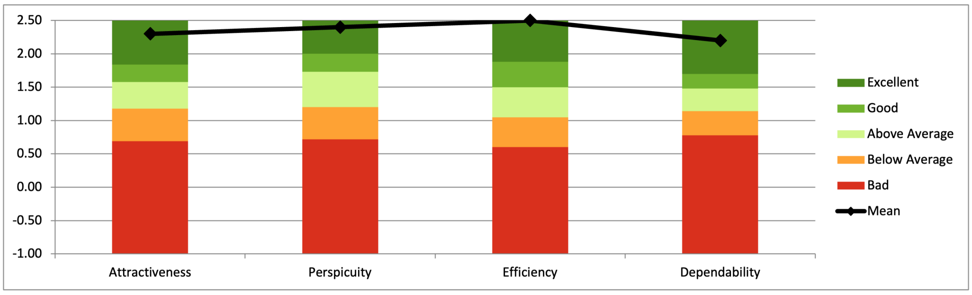


Figure 6.5: UEQ benchmark comparison: evaluation of BetterID's UX against standardized UEQ benchmarks across different scales

6.2.3.2 Privacy Awareness

Participants' awareness of privacy is assessed based on their responses to seven questions. The first question asks whether they have read the privacy notice. The remaining six questions focus on different aspects of data sharing, as discussed in the section 6.1.1. In Figure 6.6, the total number of "Yes" responses is presented for each question in both applications.

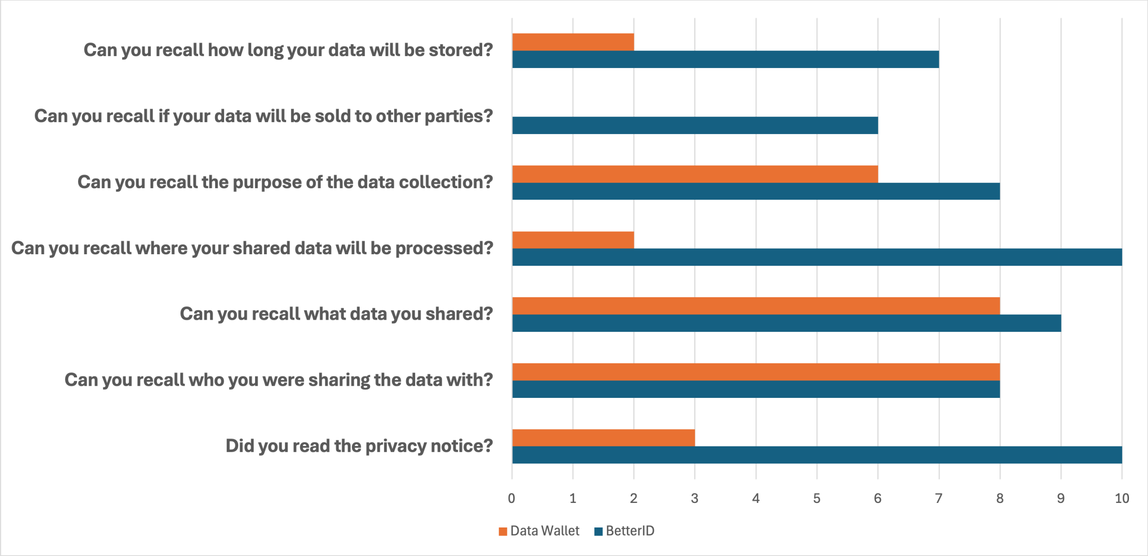


Figure 6.6: Comparison of "Yes" responses for privacy awareness questions: user recall of key privacy aspects in each SSI application.

In Figure 6.6, the data show that BetterID consistently received an equal or greater number of "Yes" responses compared to Data Wallet. To determine if this difference is statistically significant, a paired t-test on the overall responses related to privacy awareness is performed. A significance level of 0.05 was selected as it is widely used in empirical research [83]. A p-value of 0.013 indicates that the difference in privacy awareness between the two applications is statistically significant. When interacting with BetterID, users are able to recall various aspects of data sharing more effectively.

Furthermore, a paired t-test is performed for each question, to evaluate if the difference in the number of "Yes" responses is statistically significant. The result can be found in Table 6.1.

Question	T-statistic	p-value	Statistically Significant
Q1: Did you read the privacy notice?	-4.583	0.001	Yes
Q2: Can you recall who you were sharing the data with?	N/A	N/A	No
Q3: Can you recall what data you shared?	-0.557	0.591	No
Q4: Can you recall where your shared data will be processed?	-6.000	0.000	Yes
Q5: Can you recall the purpose of the data collection?	-0.802	0.443	No
Q6: Can you recall if your data will be sold to other parties?	-3.674	0.005	Yes
Q7: Can you recall how long your data will be stored?	-2.236	0.052	No

Table 6.1: The result from paired t-test for each question related to the awareness of privacy

For questions Q1, Q4, and Q6, the differences in responses between the two applications are statistically significant. For questions Q2, Q3, and Q5, most users can recall the required data, the organization with which they were connected, and the purpose of data collection in both applications. For question Q7, the difference between the two application is not statistically significant.

6.2.3.3 Trust Rating

Participants were also asked to rate their trust in each application using a five-point Likert scale: completely, very, moderately, slightly, or not at all. The self-reported trust levels for the two applications are shown in Figure 6.7.

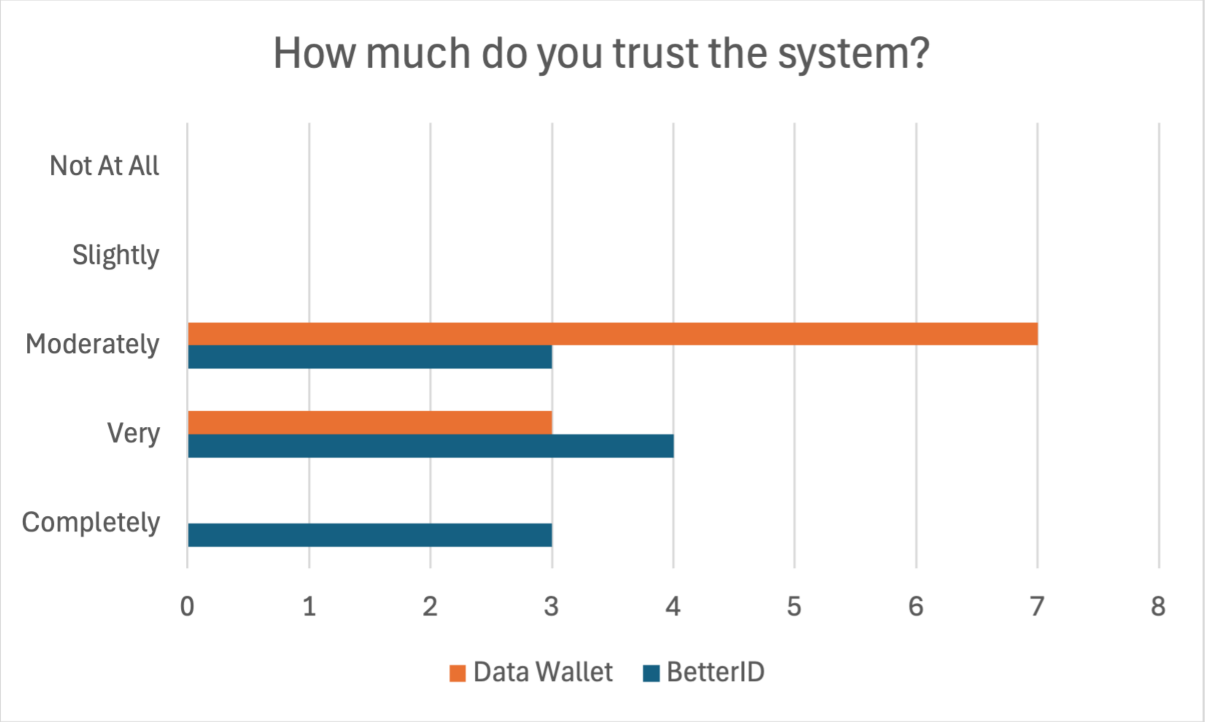


Figure 6.7: Distribution of trust ratings: participants' responses on a 5-Point Likert scale for each SSI application

Most of the participants trust BetterID more than Data Wallet, while the others trust both applications equally. To determine if the difference in the self-reported trust in the two SSI applications is statistically significant, a check on whether the data are normally distributed was firstly conducted by a Shapiro-Wilk test. The test resulted in a p-value of 0.015, indicating that the data is not normally distributed, with the significant level of 0.05. As the next step, a Wilcoxon signed-rank test is performed to assess whether the difference in trust levels between the two applications is significant. The Wilcoxon test produced a p-value of 0.019, which confirms that the difference in trust levels is statistically significant, with a significant level of 0.05.

6.2.4 Summary of Participants' Suggestions in the User Study

6.2.4.1 Data Sharing

In the user study, some participants expressed curiosity about how information is transmitted securely. For instance, one participant wanted to know how information is encrypted within the SSI application, while another inquired whether the information is transmitted over a standard encrypted TLS connection.

Additionally, many participants highlighted the crucial role of the verifier. They wanted to be sure that their information would be handled according to established standards. Participants questioned the reasons to trust the verifier and suggested that it would be beneficial for the SSI application to implement a ranking system for verifiers so that they can evaluate the level of trust they can place in each.

While many participants appreciated the advantages of selective disclosure, some raised concerns about their ability to withhold information from specific verifiers or to avoid sharing certain required details. They wondered if there could be an option to opt out of connections they did not wish to engage with.

6.2.4.2 UI Design

Participants provided feedback on the UI design of BetterID, suggesting several improvements. They recommended that the registration and login pages feature larger forms for easier use. Additionally, they noted that the switches for selecting data to share on the data selection page should also be enlarged for better visibility. Two participants mentioned that navigating between the new connection page and the add new credential page was somewhat complicated.

Regarding the type attractor feature, opinions varied among participants. Most indicated that the type attractor did not add any burden to their experience. Currently, users can copy and paste to rewrite the defined sentence, but some suggested that disabling this feature might enhance usability. However, one participant expressed difficulty understanding the type attractor and preferred a checkbox as an alternative option.

6.3 Discussion

6.3.1 Interpretation of Quantitative Outcomes

By comparing the UEQ results for BetterID and Data Wallet, it is clear that BetterID received high scores across all four scales. Furthermore, when compared to the benchmark provided by UEQ, BetterID also achieved an excellent rating on all four scales. In conclusion, BetterID offers users a good overall user experience.

As illustrated in Figure 6.6 and supported by the t-test results, participants were significantly better able to recall privacy attributes in BetterID. Presenting the privacy notice on a separate page effectively captures users' attention. This finding aligns with the research presented in [24].

For the questions "Did you read the privacy notice?", "Can you recall where your shared data will be processed?", and "Can you recall if your data will be sold to other parties?", the differences in participants' answers between Data Wallet and BetterID were statistically significant. This may be attributed to how the privacy notice was presented. The use of a separate page for the privacy notice, combined with icons and animations, likely encouraged users to read it more carefully.

However, for the question "Can you recall how long your data will be stored?", the difference was not statistically significant. Participants sometimes struggled to recall information from the privacy notice in BetterID, as they found it challenging to interpret the accompanying images. These observations highlight the difficulty in selecting appropriate visuals to convey information. Additionally, the disconnect between reading and understanding the privacy notice has been studied by researchers [48, 87], and the results from the user study have revealed similar gaps.

For the questions "Can you recall who you shared the data with?", "Can you recall what data you shared?", and "Can you recall the purpose of the data collection?", there was no statistically significant difference in responses between Data Wallet and BetterID. Participants read the instructions and selected the required data, allowing them to clearly recall this information even if they did not read the privacy notice. This raises a question about whether information users already know should be excluded from the privacy notice. According to GDPR, there is no obligation to provide information that the data subject already possesses [31]. This guideline is valuable for determining which information should be included in privacy notices, especially when users already possess some information. Removing information that users already know helps keep the privacy notice concise [24, 33, 70] and maintains users' attention on new information.

6.3.2 Implication from Participants Suggestions

The results from the user study revealed that participants have a desire for transparency regarding how their data is encrypted and transmitted, as well as a request for a ranking system to assess the trustworthiness of verifiers. These insights reflect a growing awareness among users about the privacy and security practices of SSI applications.

Several participants expressed interest in understanding the methods used to encrypt and transmit their personal information to verifiers. This demand aligns with one of the key design principles of SSI, which emphasizes transparency in systems and algorithms [80]. Although the terminology used in SSI can be complex and difficult for users to understand [39, 45, 56, 63], the "progressive disclosure" strategy, where users can choose to access more detailed explanations as needed, could be considered to be implemented in SSI applications [78].

Another significant finding was the users' desire for a ranking or reputation system for verifiers. This reflects a challenge in SSI noted by researchers, who pointed out that users often find it difficult to evaluate the trustworthiness of verifiers, as there is no organization that can guarantee a completely trusted system [20]. However, some researchers have attempted to develop a ranking system for verifiers based on GDPR requirements to help users assess their reliability [12]. The study on building ranking system for the verifier remains limited. However, feedback from participants and relevant literature suggest that it holds potential as a promising direction for future research.

Feedback from participants regarding the UI design of BetterID revealed several issues, such as navigation and form readability, which were overlooked during the design process. This feedback is valuable for future improvements.

The varying opinions on the use of the type attractor are noteworthy. Only one participant had difficulty understanding the type attractor and suggested replacing it with a checkbox. To better understand their perspective, a review of the interaction recording for this participant was conducted while they were interacting with BetterID. It was found that they overlooked the instructions, which led to confusion about what to type in the input box. Consequently, they had to ask for help, indicating they experienced consent fatigue. Given their desire to complete the task quickly, it's understandable that typing out a full sentence was more cumbersome than simply clicking a checkbox. For users suffering from consent fatigue, a checkbox is preferable. Since the goal is to mitigate consent fatigue and encourage users to focus on the privacy notice, it can be concluded that the type attractor is more effective than a checkbox.

Another valuable piece of feedback from participants was their suggestion of having a walkthrough feature in BetterID to help them familiarize themselves with the application's functionalities. This aligns with best practices noted by [75]. As SSI is still a relatively new concept for users, incorporating instructional content or a walkthrough into the application could be beneficial [75]. Therefore, the lack of instruction and a walkthrough in BetterID represents an area for improvement in future iterations.

6.3.3 Threats to Validity

While this study provides valuable insights into improving privacy notice representation in SSI applications, certain factors may have influenced the results. These threats to validity should be acknowledged to ensure a transparent interpretation of the findings.

6.3.3.1 Participant Bias

Most of the participants in both user study and pilot study were acquaintances, which introduces the potential for bias in their responses. One notable concern is social desirability bias, where participants may have provided more positive feedback than they really felt, to avoid hurting our feelings or to align with perceived expectations. This could have influenced their ratings, making the user experience of both applications appear more favorable than it actually was.

Although BetterID scored higher than Data Wallet across all UEQ scales, it is important to note that both applications received scores significantly above the benchmark. This trend suggests that social desirability bias may have played a role. Additionally, acquaintance bias could have further impacted the results, as some participants may have had prior knowledge about BetterID and the expectations for it. Their familiarity with the work might have subconsciously influenced their feedback.

6.3.3.2 Learning Effect

One potential issue in the study is the possibility of a learning effect. After users interact with the first SSI application and complete the questionnaire, they may realize that the ability of recalling details about the connections and whether they read the privacy notice are measured. As a result, when they interact with the second SSI application, they might pay more attention to the privacy notice and the privacy attributes requested.

From the results, five participants who began with Data Wallet did not read the privacy notice at all. Conversely, two of the five participants who started with BetterID later read the privacy notice when using Data Wallet. This indicates that the possibility of a learning effect influencing their responses cannot be dismissed.

In future studies, if the sample size is large enough, researchers should consider switching from a within-subject design to a between-subject design to mitigate the potential impact of this learning effect.

6.3.3.3 Sample Size and Representativeness

It is mentioned previously that all participants voluntarily participated in both user study and pilot study, all of whom were aged between 22 and 31 years. All the participants are students, majoring in a MINT field (Mathematics, Informatics, Natural sciences, and Technology). While the sample size is relatively small, it is important to note that the Nielsen Norman Group suggests that with only five participants, it is already sufficient to identify over 80% of UX issues, making the user study reasonably effective in uncovering usability challenges. However, to achieve statistically significant results in a quantitative study, it is generally recommended to have a sample size of 20 or more participants to ensure a higher level of reliability and generalizability.

Furthermore, the participant pool was limited to students, which may have influenced the results, as their familiarity with digital systems and technical concepts might differ from those of a more diverse population. This homogeneity could impact the extent to which the findings can be generalized to a broader audience, including individuals with different levels of technical expertise, professional backgrounds, and age groups.

In future research, expanding the participant pool to include a more diverse group from various educational backgrounds, professional sectors, and age groups would enhance the representativeness of the study. A more inclusive approach would not only improve the validity of the study but also ensure that the designed privacy notices are accessible and effective for a wider range of users.

6.3.3.4 Differences Between Web and Mobile Applications

An additional factor that may have influenced the results of the user study is the comparison between a mobile SSI application and a web SSI application. Since the goal was to evaluate the new SSI application against an existing one in the market, the options for selecting the suitable SSI application were limited. Among the existing SSI applications tested, only one was a web application, and it did not meet the requirements. As a result, a mobile SSI application is chosen.

The differences in interaction design between mobile and web applications, along with varying usability expectations, could have impacted participants' experiences and perceptions. Additionally, user familiarity with and preference for different platforms may have shaped their responses. Individual differences in prior experience could also have influenced their perceptions of usability, efficiency, and overall satisfaction with each system.

Future studies could reduce this potential bias by ensuring that both the tested and experimental systems are available on the same platform. This would allow for more direct comparisons and help mitigate the confounding effects of platform-specific usability factors.

Chapter 7

Final Considerations

This chapter begins with a concise summary of the research conducted throughout this thesis. It then presents the final conclusions drawn from the results. Finally, the chapter outlines several promising directions for future research, building on the insights gained and identifying areas where further exploration could enhance or extend the work presented.

7.1 Summary

In this thesis, a new SSI application with a new representation of privacy notices is proposed and its UX and effectiveness in improving users' awareness of privacy and trust, and conveying essential privacy attributes within an SSI application is evaluated.

In the beginning, the fundamental concepts of SSI, privacy, UX, and consent fatigue are discussed. Through an extensive literature review, it is clear that SSI enables users to have full control over their identity data. However, due to poor UX in privacy notices and inappropriate behavior by verifiers, users may experience consent fatigue and inadvertently share more data than necessary.

To identify a better representation of privacy notices that enhances UX, and protects user privacy, a research of relevant UI design principles applicable to decentralized applications, as well as effective design principles for privacy notices is conducted. Additionally, an analysis of existing SSI applications in the market is conducted, to assess how they present privacy notices. Specifically, whether these notices are displayed while users share data. Based on the findings, a prototype for a new SSI application, BetterID, is designed and implemented.

The design is iterated by conducting a pilot study with four participants. Observing their interactions with BetterID and gathering their feedback, minor UI adjustments are made and the data selection page and privacy notice are redesigned. In BetterID, the selective disclosure is offered to users and a checklist of required data is provided for their reference.

The privacy notice uses visuals and icons to effectively communicate the content related to each privacy attribute.

To evaluate whether BetterID offers a satisfactory UX and improves users' awareness of privacy and users' trust, a user study involving ten participants is conducted. Participants interacted with BetterID and Data Wallet to complete two tasks within each application, followed by a questionnaire that included the UEQ, seven yes-or-no questions about their recall of key privacy attributes, and a self-reported trust level measured on a five-point Likert scale. Finally, participants were asked to provide additional suggestions about the content in the application and the privacy notice, and the BetterID UI design.

7.2 Conclusions

The user study has provided valuable insights, leading us to conclude that BetterID significantly outperforms Data Wallet across several UX dimensions, including attractiveness, perspicuity, efficiency, and dependability. Furthermore, BetterID stands out as a SSI application with an excellent UX, compared to the UEQ benchmark.

During the study, participants not only read the privacy notice while interacting with BetterID, but they also demonstrated a remarkable ability to recall important privacy attributes afterward. Users expressed higher levels of trust in BetterID, suggesting that the effective UX and improved privacy notice design contribute to greater transparency and trust in the application.

Statistical analysis indicates that the differences in participants' ability to recall important privacy attributes and their trust levels between BetterID and Data Wallet are statistically significant. The new representation of the privacy notice in BetterID is proved to effectively educate users about privacy issues. These findings also suggest that a well-designed privacy notice, seamlessly integrated into the UI, can help reduce consent fatigue, improve user privacy awareness, and foster trust in SSI applications.

7.3 Future Work

While this study demonstrated the effectiveness of an improved privacy notice design for SSI applications, there are still opportunities to refine and expand upon these findings. Future research can further enhance UX, improve trust and transparency, and address remaining usability challenges. This section explores potential directions for extending the study, expanding system design, and incorporating new technologies to make privacy notices more effective and interactive.

7.3.1 Enhancing Usability for Novice

From both the pilot study and the user study, an main observation is that some users struggle to understand the benefits of SSI, which can lead to them sharing excessive information. Users with limited knowledge of SSI often mistakenly believe that sharing a credential means sharing all the data contained within it. This misunderstanding suggests that the concept of selective disclosure is not always intuitive for novice users.

To address this issue, a checklist aimed at helping users select only the necessary data was implemented. However, in the user study, two participants still shared too much information and reported that they either did not see or did not understand the checklist. This highlights the need for further improvements in the design of selective disclosure tools, ensuring they are more attractive, visible, intuitive, and accessible to users with little prior knowledge of SSI.

Moreover, the concept of SSI is still relatively new to many people. As one participant pointed out, providing a walkthrough of the application would help users become familiar with how an SSI application operates. And many participants expressed their interests in learning how the information is transmitted to the destination. A key direction for future work is to improve novices' understanding of SSI applications. It would be advantageous to explore various ways to integrate tutorials that educate users about SSI, or necessary knowledge that users find interesting, within the application, all while ensuring a positive UX.

7.3.2 Trustworthiness Ranking for Verifiers

An important area for future development is enhancing trust in SSI applications by implementing a ranking system for verifiers. Although privacy notices provide essential privacy attributes, users may still struggle to determine whether a verifier can be trusted. This uncertainty can result in hesitance to share credentials or, conversely, lead to excessive disclosure due to a lack of clear guidance.

To tackle this issue, a trustworthiness ranking system for verifiers could be established. This system would assess verifiers based on various factors, including transparency, security practices, reputation, and compliance with privacy standards. During each interaction, the trust score of a verifier could be displayed, enabling users to make more informed decisions about sharing their credentials. By integrating such a ranking system, SSI applications could further empower users, enhance transparency, and foster greater confidence in digital identity interactions.

7.3.3 AI-Generated Interactive Privacy Notices

During the design iteration, the privacy notice is redesigned into a block-based format, incorporating an image in each block to illustrate key concepts. While existing literature presents uncertainty on the effectiveness of images and icons in privacy notices, the user study revealed a statistically significant improvement in privacy awareness between the two SSI applications. This suggests that the redesigned privacy notice effectively enhances users' understanding of key privacy attributes.

However, beyond visual appeal, drawing users' attention to privacy notices remains a critical challenge. The inclusion of images and icons not only makes the notice more engaging but also serves as a visual attractor, encouraging users to stay on the page and absorb the content. To build on this approach, future work could explore AI-driven interactive privacy notices. This could involve AI generating adaptive explanations tailored to the user's knowledge level or context, ensuring a more personalized and engaging experience. Potential features could include interactive elements, dynamic summaries, or chatbot-based explanations to improve user comprehension and foster greater trust in SSI applications.

The observations indicate that users often avoid reading text. A key challenge in this approach is effectively translating AI-generated insights into engaging and interactive elements that capture users' attention. Future work should also focus on designing visually appealing, intuitive representations of privacy attributes based on AI insights, allowing users to effortlessly engage with and understand key privacy information with minimal cognitive effort.

7.3.4 Scaling the Study with Eye-Tracking Analysis

As discussed in the section 6.3.3, the user study had a relatively small sample size, and the representativeness of the sample could be improved. To enhance the generalizability of the findings, future research should aim to scale the study by including a larger and more diverse participant pool drawn from various demographic and professional backgrounds. This would provide a broader understanding of how different user groups interact with and comprehend privacy notices in SSI applications.

In the user study, users' awareness of privacy attributes is assessed by asking them to recall specific details from the privacy notice. While this method offers valuable insights, future research could incorporate additional tools, such as eye-tracking technology, to better understand user engagement with the privacy notice. By measuring the amount of time users spend reading the notice and determining whether they focus on the key elements, researchers can gather more accurate and detailed data on how effectively users engage with privacy information. Combining these objective measures with subjective recall assessments would provide a more comprehensive evaluation of the effectiveness of privacy notices.

Bibliography

[1] Adam Wathan and Steve Schoger. *Refactoring UI - Design for Developers*. n.d. URL: https://www.refactoringui.com/.

[2] Bonnie Brinton Anderson et al. "How Polymorphic Warnings Reduce Habituation in the Brain: Insights from an fMRI Study". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. CHI '15. 2015, 2883â2892.

[3] Animo Solutions. *Animo Demo - Digital Identity Demonstration*. n.d. URL: https://demo.animo.id/demo.

[4] A.I. Anton et al. "Financial privacy policies and the need for standardization". In: *IEEE Security Privacy* 2.2 (2004), pp. 36–45.

[5] Nick Babich. *Designing Card-Based User Interfaces*. 2016. URL: https://www.smashingmagazine.com/2016/10/designing-card-based-user-interfaces/.

[6] Susanne Barth, Dan Ionita, and Pieter Hartel. "Understanding Online PrivacyâA Systematic Review of Privacy Visualizations and Privacy by Design Guidelines". In: *ACM Comput. Surv.* 55.3 (Feb. 2022).

[7] Nigel Bevan. "What is the difference between the purpose of usability and user experience evaluation methods". In: *Proceedings of the Workshop UXEM*. Vol. 9. 1. Citeseer. 2009, pp. 1–4.

[8] Masum Billal. *The Power of Mental Models in UX Design*. 2021. URL: https://masumux.medium.com/the-power-of-mental-models-in-ux-design-85d27f59ee39.

[9] Cristian Bravo-Lillo et al. "Harder to ignore?" In: *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*. SOUPS '14. 2014, 105â111.

[10] Cristian Bravo-Lillo et al. "Your attention please: designing security-decision UIs to make genuine risks harder to ignore". In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*. SOUPS '13. 2013.

[11] José Carlos Brustoloni and Ricardo Villamarín-Salomón. "Improving security decisions with polymorphic and audited dialogs". In: *Proceedings of the 3rd Symposium on Usable Privacy and Security*. SOUPS '07. 2007, 76â85.

[12] David W. Chadwick et al. "Establishing Trust in SSI Verifiers". In: *Open Identity Summit 2023*. 2023, pp. 15–26.

[13] George Chalhoub and Ivan Flechais. "Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives". In: *Proc. ACM Hum.-Comput. Interact.* 6.CSCW2 (Nov. 2022).

[14] George Chalhoub et al. "âIt did not give me an option to declineâ: A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products".

In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI ’21. 2021.

[15] Civic Technologies. *Civic - Secure Identity Verification*. n.d. URL: https://www.civic.com/.

[16] CleverÂ°Franke. *CleverÂ°Franke - Data-Driven Design and Experiences*. n.d. URL: https://www.cleverfranke.com/.

[17] Lorrie Cranor. “Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice”. In: (Dec. 2012).

[18] Špela Čučko, Vid KerÅ¡iÄ, and Muhamed TurkanoviÄ. “Towards a Catalogue of Self-Sovereign Identity Design Patterns”. In: *Applied Sciences* 13.9 (2023).

[19] Špela Čučko et al. “Towards the Classification of Self-Sovereign Identity Properties”. In: *IEEE Access* 10 (2022), pp. 88306–88329.

[20] Rachna Dhamija and Lisa Dusseault. “The Seven Flaws of Identity Management: Usability and Security Challenges”. In: *IEEE Security Privacy* 6.2 (2008), pp. 24–29.

[21] Verena Distler et al. “The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely”. In: *Proceedings of the New Security Paradigms Workshop 2020*. NSPW ’20. 2021, 45â58.

[22] Ernie Djaenudin and Sugeng Prastowo. “The Influence of Digital Platform Quality and Security on Decision and Satisfaction through Trust in the DANA Digital Wallet”. In: *International Journal of Business, Law, and Education* 5 (Sept. 2024), pp. 2314–2323.

[23] Dock.io. *Self-Sovereign Identity: A Comprehensive Overview*. n.d. URL: https://www.dock.io/post/self-sovereign-identity.

[24] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. “Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices”. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI ’21. 2021.

[25] Esatus AG. *Digital Identity - Esatus AG*. n.d. URL: https://esatus.com/en/digital-identity/.

[26] European Blockchain Association. *SSI Wallets*. n.d. URL: https://europeanblockchainassociation.org/ssi-wallets/.

[27] Javad Farahani. *Web3 Design: Principles, Values, and Best Practices from Leading Platforms*. Feb. 2025.

[28] Md. Sadek Ferdous, Farida Chowdhury, and Madini Alassafi. “In Search of Self-Sovereign Identity Leveraging Blockchain Technology”. In: *IEEE Access* 7 (July 2019), pp. 1–1.

[29] Gataca. *Gataca Demo - Secure Digital Identity Solutions*. n.d. URL: https://gataca.io/demo.

[30] GDPR Info. *Personal Data - General Data Protection Regulation (GDPR)*. n.d. URL: https://gdpr-info.eu/issues/personal-data/.

[31] GDPR-info.eu. *GDPR Recital 62 â Information to be Provided Where Personal Data Have Not Been Obtained from the Data Subject*. n.d. URL: https://gdpr-info.eu/recitals/no-62/.

[32] F. Ghaffari et al. “Identity and Access Management Using Distributed Ledger Technology: A Survey”. In: *International Journal of Network Management* 31.4 (2021), e2180.

[33] Joshua Gluck et al. “How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices”. In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. June 2016, pp. 321–340.

[34] Rex Hartson and Partha S. Pyla. “Chapter 8 - Mental Models and Conceptual Design”. In: *The UX Book*. Ed. by Rex Hartson and Partha S. Pyla. 2012, pp. 299–332.

[35] iGrant.io. *Data4Receipts - Enabling Privacy-Preserving Digital Receipts*. n.d. URL: https://igrant.io/data4receipts.html.

[36] iGrant.io. *Data4Travel - Enabling Privacy-Preserving Travel Data Sharing*. n.d. URL: https://igrant.io/data4travel.html.

[37] iGrant.io. *iGrant.io - Enabling Trusted Data Sharing*. n.d. URL: https://igrant.io/index.html.

[38] International Organization for Standardization (ISO). *ISO 9241-11: Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts*. n.d. URL: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en.

[39] Hyeji Jang, Sung H. Han, and Ju Hwan Kim. “User Perspectives on Blockchain Technology: User-Centered Evaluation and Design Strategies for DApps”. In: *IEEE Access* 8 (2020), pp. 226213–226223.

[40] JavaScript.com. *JavaScript.com - Learn JavaScript Programming*. n.d. URL: https://www.javascript.com/.

[41] Carlos Jensen and Colin Potts. “Privacy policies as decision-making tools: an evaluation of online privacy notices”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’04. 2004, 471â478.

[42] Jolocom. *Jolocom Stories - Insights on Self-Sovereign Identity*. n.d. URL: https://stories.jolocom.com/.

[43] Patrick Gage Kelley et al. “A ”nutrition label” for privacy”. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. SOUPS ’09. 2009.

[44] Patrick Gage Kelley et al. “Standardizing privacy notices: an online study of the nutrition label approach”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’10. 2010, 1573â1582.

[45] Alina Khayretdinova et al. “Conducting a Usability Evaluation of Decentralized Identity Management Solutions”. In: *Selbstbestimmung, Privatheit und Datenschutz : Gestaltungsoptionen für einen europäischen Weg*. Ed. by Michael Friedewald, Michael Kreutzer, and Marit Hansen. 2022, pp. 389–406.

[46] Jiet Ping Kiew et al. “Perceived Trust, Convenience and Promotion For the Adoption of e-Wallet”. In: *International Journal of Academic Research in Business and Social Sciences* 12 (Sept. 2022).

[47] Maina Korir, Simon Parkin, and Paul Dunphy. “An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control”. In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Aug. 2022, pp. 195–211.

[48] Jana Korunovska, Bernadette Kamleitner, and Sarah Spiekermann. “The Challenges and Impact of Privacy Policy Comprehension”. In: *CoRR* abs/2005.08967 (2020).

[49] Thomas Lauer and Xiaodong Deng. “Building online trust through privacy practices”. In: *Int. J. Inf. Sec.* 6 (Aug. 2007), pp. 323–331.

[50] Lissi. *Lissi - Enabling Digital Identities*. n.d. URL: https://www.lissi.id/.

[51] Junliang Liu, Zhiyao Liang, and Qiuyun Lyu. “Empowering Privacy Through Peer-Supervised Self-Sovereign Identity: Integrating Zero-Knowledge Proofs, Blockchain Oversight, and Peer Review Mechanism”. In: *Sensors* 24.24 (2024).

[52] Loranger. *Negativity Bias in User Experience*. Nielsen Norman Group. 2022.

[53] Yannic Meier, Johanna BÃ¶rsting, and Nicole KrÃ¤mer. “The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making”. In: *Media and Communication* 8 (June 2020), p. 291.

[54] Merge. *10 Web3 Design Trends for 2024*. 2024. URL: https://merge.rocks/blog/10-web3-design-trends-for-2024.

[55] Meta Open Source. *React - A JavaScript Library for Building User Interfaces*. n.d. URL: https://react.dev/.

[56] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. “Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets”. In: *Cyber Security and Computer Science*. Ed. by Touhid Bhuiyan, Md. Mostafijur Rahman, and Md. Asraf Ali. 2020, pp. 631–643.

[57] Kate Moran. *Animation in UX: The Purpose of Motion*. 2017. URL: https://www.nngroup.com/articles/animation-purpose-ux/.

[58] Nitin Naik and Paul Jenkins. “Is Self-Sovereign Identity Really Sovereign?” In: *2022 IEEE International Symposium on Systems Engineering (ISSE)*. 2022, pp. 1–7.

[59] Nitin Naik and Paul Jenkins. “Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity”. In: *2020 7th International Conference on Behavioural and Social Computing (BESC)*. 2020, pp. 1–6.

[60] NASA Human Systems Integration Division. *NASA Task Load Index (TLX)*. 2024. URL: https://humansystems.arc.nasa.gov/groups/tlx/.

[61] NPM, Inc. *NPM - Node Package Manager*. n.d. URL: https://www.npmjs.com/.

[62] Jonathan A. Obar and Anne Oeldorf-Hirsch. “The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services”. In: *Information, Communication & Society* 23.1 (2020), pp. 128–147.

[63] Davide M. Parrilli and Rodrigo Hernández-Ramírez. “Building a Privacy Oriented UI and UX Design: An Introduction to Its Foundations and Potential Developments”. In: *Advances in Design and Digital Communication II*. Ed. by Nuno Martins and Daniel Brandão. 2022, pp. 16–30.

[64] DANIEL J. SOLOV PAUL M. SCHWARTZâ. *THE PII PROBLEM: PRIVACY AND A NEW CONCEPT OF PERSONALLY IDENTIFIABLE INFORMATION*. 2011. URL: https://www.law.berkeley.edu/files/bclt_Schwartz-Solove_NYU_Final_Print.pdf.

[65] PMND.rs. *Zustand Demo - Bearishly Good State Management*. n.d. URL: https://zustand-demo.pmnd.rs/.

[66] Privacy Label. *Learn - Privacy Label: Simplifying Privacy Communication*. n.d. URL: https://www.privacylabel.org/learn/.

[67] Arianna Rossi and Monica Palmirani. “DAPIS: An Ontology-Based Data Protection Icon Set”. In: *Knowledge of the Law in the Big Data Age*. Ed. by Ginevra Peruginelli and Sebastiano Faro. 2019, pp. 181–195.

[68] Sebastian Sartor et al. “Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets”. In: Apr. 2022.

[69] Abylay Satybaldy. “Usability Evaluation ofÂ SSI Digital Wallets”. In: *Privacy and Identity Management*. Ed. by Felix Bieker et al. 2023, pp. 101–117.

[70] Florian Schaub et al. "A Design Space for Effective Privacy Notices". In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. July 2015, pp. 1–17.

[71] Karl van der Schyff et al. "Online Privacy Fatigue: A Scoping Review and Research Agenda". In: *Future Internet* 15.5 (2023).

[72] Johannes Sedlmeir et al. "Digital Identities and Verifiable Credentials". In: *Business & Information Systems Engineering* 63.5 (Oct. 2021), pp. 603–613.

[73] Johannes Sedlmeir et al. "Transition pathways towards design principles of self-sovereign identity". In: Sept. 2022.

[74] *Self-Sovereign Identity: 5 Years On.* `https://www.lifewithalacrity.com/article/SSI-5-Years-On/`.

[75] Rachelle Sellung and Michael Kubach. "Research on User Experience for Digital IdentityWallets: State-of-the-Art and Recommendations". In: *Open Identity Summit 2023*. 2023, pp. 39–50.

[76] Reza Soltani, Uyen Trang Nguyen, and Aijun An. "A Survey of Self-Sovereign Identity Ecosystem". In: *Security and Communication Networks* 2021 (July 2021). Ed. by Clemente Galdi, 1â26.

[77] Sovrin Foundation. *Sovrin - The Foundation for Self-Sovereign Identity.* n.d. URL: `https://sovrin.org/`.

[78] Aaron Springer and Steve Whittaker. "Progressive Disclosure: When, Why, and How Do Users Want Algorithmic Transparency Information?" In: *ACM Trans. Interact. Intell. Syst.* 10.4 (Oct. 2020).

[79] Moritz Teuschel et al. "âDonât Annoy Me With Privacy Decisions!â â Designing Privacy-Preserving User Interfaces for SSI Wallets on Smartphones". In: *IEEE Access* 11 (2023), pp. 131814–131835.

[80] *The Path to Self-Sovereign Identity.* `https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/`.

[81] Kalman Toth and Alan Anderson-Priddy. "Self-Sovereign Digital Identity: A Paradigm Shift for Identity". In: *IEEE Security Privacy* 17 (May 2019), pp. 17–27.

[82] Trinsic. *Trinsic - Building the Future of Digital Identity.* n.d. URL: `https://trinsic.id/`.

[83] JuliÃ¡n Urbano, Harlley Lima, and Alan Hanjalic. "Statistical Significance Testing in Information Retrieval: An Empirical Analysis of Type I, Type II and Type III Errors". In: *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval.* SIGIR â19. July 2019, 505â514.

[84] User Experience Questionnaire (UEQ). *User Experience Questionnaire (UEQ) - Measuring User Experience.* n.d. URL: `https://www.ueq-online.org/`.

[85] Validated ID. *VIDwallet - Digital Identity Wallet by Validated ID.* n.d. URL: `https://www.validatedid.com/en/identity/vidwallet`.

[86] Anthony Vance et al. "What Do We Really Know about How Habituation to Warnings Occurs Over Time? A Longitudinal fMRI Study of Habituation and Polymorphic Warnings". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* CHI '17. 2017, 2215â2227.

[87] Kim-Phuong L. Vu et al. "How Users Read and Comprehend Privacy Policies". In: *Human Interface and the Management of Information. Interacting in Information Environments.* Ed. by Michael J. Smith and Gavriel Salvendy. 2007, pp. 802–811.

[88] T. Franklin Waddell, Joshua R. Auriemma, and S. Shyam Sundar. "Make it Simple, or Force Users to Read? Paraphrased Design Improves Comprehension of End User

License Agreements”. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI ’16. 2016, 5252â5256.

[89] Walt.id. *Walt.id - Empowering Decentralized Identity and Privacy*. n.d. URL: https://walt.id/.

[90] Alan Westin. *Privacy and Freedom*. 1967.

[91] Wikipedia contributors. *System usability scale — Wikipedia, The Free Encyclopedia*. 2024. URL: https://en.wikipedia.org/wiki/System_usability_scale.

[92] World ID. *World ID - Decentralized Identity for Everyone*. n.d. URL: https://zh-cn.world.org/world-id.

[93] Kuang-Wen Wu et al. “The effect of online privacy policy on consumer privacy concern and trust”. In: *Computers in Human Behavior* 28.3 (2012), pp. 889–897.

Abbreviations

SSI	Self-Sovereign Identity
VC	Verifiable Credential
DID	Decentralized Identifier
UX	User Experience
UI	User Interface
GDPR	General Data Protection Regulation
EULA	End User License Agreement

List of Figures

List of Tables

Listings

Appendix A

Contents of the Repository

The code repository is on BetterID repository. The code repository contains the following content:

Operation

In the project directory, you can run:

```
npm start
```

Runs the app in the development mode. Open http://localhost:3000 to view it in your browser.

The page will reload when you make changes. You may also see any lint errors in the console.

```
npm test
```

Launches the test runner in the interactive watch mode. See the section about running tests for more information.

```
npm build
```

Builds the app for production to the build folder. It correctly bundles React in production mode and optimizes the build for the best performance.

The build is minified and the filenames include the hashes. Your app is ready to be deployed!

Folder Structure The folder structure of the entire project is:

- .idea: Workspace configuration, code style settings, and other IDE-related files.
- public: Holds static assets that are publicly accessible and not processed by Webpack.
- src: Contains the source code for BetterID.

- .gitignore: Specifies intentionally untracked files to ignore.
- README.md: Provides an overview of the project, including setup instructions, usage guidelines, and other relevant information to help users and contributors understand and work with the repository.
- package-lock.json: Records the exact versions of installed dependencies, ensuring consistent installs across environments.
- package.json: Lists project dependencies, scripts, and metadata.

In the scr folder, where contains the source code, the folder structure is:

- components: Contains all the reusable components, like menu bar.
- data: Contains all the mock-up data for credentials and connections.
- functions: Contains all the functions that are called in the application.
- images: Contains all the images that are used in the application.
- pages: Contains all the webpage.
- state: Contains the implementation of the state management.
- styles: Contains all the css files for styling the applications.
- utils: Contains reusable pieces of logic that support the main application.

Appendix B

User Story

Register and Log In
Priority: High
Property: Existence, Access
User Story: As an unregistered user, I want to register in the app so that I can have my own account. And as a registered user, I want to log in to my account.

Receive Credentials
Priority: High
Property: Control
User Story: As a user, I want to receive credentials to prove my identity, so that I can share it when needed.

View Credentials
Priority: Medium
Property: Control, Persistence, Portability, Transparency
User Story: As a user, I want to see credentials I've gotten, so that I know which credentials I own on the app.

Delete Credentials
Priority: High
Property: Control
User Story: As a user, I want to be able to delete credentials, so that if a credential is not useful anymore, it can be deleted from the app.

Connect to A Third Party
Priority: High
Property: -
User Story: As a user, I want to connect to a third party, when this third party is asking me to give me identity, so that I can share the asked data on the app.

Share Credentials
Priority: High
Property: Minimalization
User Story: As a user, I want to select which credentials or which data I want to share

with the third party, when I am connecting to the third party, so that I can have the control of data sharing.

Privacy Notice
Priority: High
Property: Consent, Protection, Minimalization
User Story: As a user, I want to be informed about privacy issue when I am sharing my credentials. As a privacy notice, it should include aspects: 1) collection: which data are collected? 2) sharing: does any of the collected data leave the ownership of the service provider? 3) sale: are any of the data sold to third parties?

Connection History
Priority: Low
Property: Control, Usability Issue User Story: As a user, I want to see the history of my connection, so that I can see who I have connected to and which data I have shared.

Usability of the Identities
Priority: Medium
Property: Interoperability
User Story: As a identity/credential, I want to be useful as widely as possible, which means I can be used in several connections, so that I am more useful to users.

Transparency of the System
Priority: Medium
Property: Transparency
User Story: As a system, the administration and operation of the identities are open, which means the implementation of the system and credential should be open sourced, so that users know how they function, how they are managed and updated.

Appendix C

Pre-study Questionnaire

What is your gender?
What is your age?
How familiar are you with the concept of Self-Sovereign Identity (SSI)?
I have never heard of it/I have heard of it but don't know what it is/I have a basic understanding of it/I have a good understanding and could explain it to others/I have in-depth knowledge and/or work with SSI
How would you rate your knowledge of user interface (UI) design and usability principles?
I have no knowledge of UI design/I am familiar with basic UI concepts but have no practical experience/I have some experience in UI design or evaluation/I have extensive experience in UI design or usability testing
Please confirm to participate in the study by checking the box

Appendix D

User Study Questionnaire

User experience (based on UEQ)
Attractiveness
Please rate the user interface of the application:
Scale 1 (as annoying) to 7 (as enjoyable)
Scale 1 (as bad) to 7 (as good)
Scale 1 (as unlikable) to 7 (as likable)
Scale 1 (as unpleasant) to 7 (as pleasant)
Scale 1 (as unattractive) to 7 (as attractive)
Scale 1 (as unfriendly) to 7 (as friendly)

Perspicuity
Based on your interaction with the system, please rate the system:
Scale 1 (as not understandable) to 7 (as understandable)
Scale 1 (as difficult to learn) to 7 (as easy to learn)
Scale 1 (as complicated) to 7 (as easy)
Scale 1 (as confusing) to 7 (as clear)

Dependability
Based on how you used the system to complete the tasks, please rate the system:
Scale 1 (as unpredictable) to 7 (as predictable)
Scale 1 (as obstructive) to 7 (as supportive)
Scale 1 (as not secure) to 7 (as secure)
Scale 1 (as does not meet expectations) to 7 (as meets expectations)

Efficiency
Considering the efforts in completing the tasks, please rate the system:
Scale 1 (as slow) to 7 (as fast)
Scale 1 (as inefficient) to 7 (as efficient)
Scale 1 (as impractical) to 7 (as practical)
Scale 1 (as cluttered) to 7 (as organized)

Awareness of privacy (based on the content in privacy notice)
Did you read the privacy notice/data agreement policy? (Y/N)

Can you recall who you were sharing the data with? (Y/N)
Can you recall what data you shared? (Y/N)
Can you recall where the organization will process your data? (Y/N)
Can you recall the purpose of the data collection? (Y/N)
Can you recall if your data will be sold to other parties? (Y/N)
Can you recall how long your data will be stored? (Y/N)

Trust in the System
Please rate how much you trust the system: Not at all, Slightly, Moderately, Very, Completely

Feedback
Is there anything else that you want to know regarding the data you shared?
Do you have any suggestion on the design of user interface and the design of privacy notice? (Only in BetterID)