Master's Thesis

Designing Self-Sovereign Identities to Retain Personal Data Sovereignty in LMIC Health Data Ecosystem

Written by:

Giovanni Nian Gani

Management of Technology

2024

TU Delft lpdp NLC

Designing Self-Sovereign Identities to Retain Personal Data Sovereignty in LMIC Health Data Ecosystem

By

Giovanni Nian Gani (5706920)

In partial fulfilment of the requirements for the degree of

Master of Science

in Management of Technology

Faculty of Technology, Policy and Management

At the Delft University of Technology

To be defended publicly on Thursday, August 29th, 2024

Committee Chair	**:** DR. Ir. G.A. (Mark) dark de Reuver
1st Supervisor	**:** DR. Ir. G.A. (Mark) dark de Reuver
2nd Supervisor	**:** P.J. (Perla) Marang-van de Mheen PhD
Advisor	**:** Antragama Ewa Abbas
Company Supervisor (NLC)	**:** Irni Gemzon
Master Program	**:** Management of Technology
Faculty	**:** Faculty of Technology, Policy and Management

Acknowledgements

First of all, I would like to express my immense gratitude to Allah Almighty, who has blessed me throughout my life with so many precious gifts. Being born into a family where everyone pursued higher education abroad has undoubtedly influenced my own academic journey. Looking back to 2018, when I first considered continuing my studies, I embarked on a journey to find a suitable program. This journey has been supported by my family—my mom, late dad, and big brother. Thank you so much for the love and care that have shaped me into the person I am today.

This thesis would not have come to fruition without the insightful discussions I had with Mas Antragama Ewa Abbas during the ICT Service Design class in 2023. Thank you so much for introducing me to design science research, for your willingness to be an advisor for this research, and for answering the myriad questions that arose throughout this journey. My gratitude also extends to NLC and its team for allowing me to conduct my thesis internship there, particularly to Irni Gemzon—thank you for your unwavering support and for sticking with me until the very end.

I also wish to express my sincere thanks to the members of my graduation committee. Dr. Ir. G.A. (Mark) de Reuver, my first supervisor and chairman of my committee, your insights and support were invaluable, enabling me to graduate on time. I deeply appreciate the time and effort you dedicated to guiding me. To P.J. (Perla) Marang-van de Mheen, PhD, my second supervisor, thank you for your detailed feedback on my work, which provided clear direction for improving my research report. Both Mark and Perla have given me immense support, especially during the final months of this study. While I wish I could have delivered even better results, I acknowledge that certain circumstances limited my performance. I am truly grateful for your patience and guidance.

As I mark two years of living in the Netherlands, I want to thank every friend I've made here. To Skullers Belanda, my friends from my bachelor years—Suwig and Unggul, thank you for always providing a place to retreat from the pressures of life. Rezzy, Hanif, and Lucas, thank you for listening to my stories here in the Netherlands. To the Indonesian students in MOT 2022, thank you for the late-night karaoke sessions, sleepovers, and shared meals over the past two years; these moments have been incredibly enjoyable. To the other Indonesian students in Delft, thank you for all the jokes, events, dinners, and memories that made my life here more pleasant. To Shounak and Simona, thank you for the delicious food and meaningful conversations we've shared.

My gratitude also goes to LPDP (Indonesia Endowment Fund for Education) for selecting me as a scholarship awardee and providing me with the most valuable gift: opportunity. Without your generous support, I would not have had the chance to pursue this path.

Last but certainly not least, I want to express my deepest gratitude to my wife, Yasmin Aruni. Over the past two years, our journey has been filled with challenges, yet your unwavering support, encouragement, and love have never faltered, even during the toughest times. Thank you for your patience, understanding, and for the sacrifices you made while I was absorbed in my studies. Your belief in me and in what we have has been a constant source of strength, motivating me to persevere and keep moving forward, always with the thought of returning to you. I am immensely grateful and blessed to have you by my side. I love you more than words can express.

As I present this thesis, I hope you find it enlightening and that it reflects the dedication and effort that have gone into it. If any unintentional errors remain, I kindly ask for your understanding and forgiveness.

To conclude, I would like to share one of my favorite quotes from Andrea Hirata's novel: "Dream, for God will embrace those dreams."

Giovanni Nian Gani

Delft, August 2024

Executive Summary

Background

Integrated data within an established health data ecosystem (HDE) is critical to the improvement of a country's quality of healthcare as it enables stakeholders to gain a more holistic view of healthcare landscape. Individuals are a key part of the HDE as they are the customers providing health data that can be used by stakeholders such as the government, healthcare facilities, and insurance companies in developing policies, treatment, and products. However, individuals are also at risk of disempowerment due to data processing, as they often lose control of their data once it becomes a part of the data ecosystem. This study proposes Self Sovereign Identity (SSI) to address such concern. SSI is a decentralized blockchain-enabled system that allows individuals to gain control and ownership of their data, giving them power to decide what they will do with their own data, and to what extent they will let third parties use their information. Emphasis is being put on how SSI could influence an individuals' personal data sovereignty, or their ability to maintain control of their data. This study takes place in Indonesia, which is categorized as a Low- and Middle- Income Country (LMIC).

Question

Existing studies mostly focus on the more technical aspects of SSI implementation and development, such as discussing IT architecture and governance. Personal data sovereignty is a concept often being mentioned together with SSI, but no study has delved into how SSI influences an individual's data sovereignty. There is still a limited amount of research on SSI interface layer, which is a gap needs to be addressed as SSI is a user-centric model. This study aims to answer the following research question:

*"How should we **design functionalities in SSI artifacts** for a Low- and Middle-Income Country (LMIC) health data ecosystem that retains **user's personal data sovereignty**?"*

Approach

This study implements the Design Science Research (DSR) methodology, which is an approach to conducting research that focuses on creating and evaluating artifacts to advance knowledge and understanding in a particular domain, often within the context of Information Systems. This study implements Hevner's (2007) three DSR cycles: Relevance, Design, and Rigor, alongside Peffers et al. (2007) operationalization of DSR methodology that comprises of six stages: (1) Problem identification and motivation, (2) Define the objectives for a solution, (3) Design and development, (4) Demonstration, (5) Evaluation, and (6) Communication. Requirements for artifacts are developed following the requirements engineering process introduced by Boulanger (2016), focusing on the functionalities requirements for an SSI interface layer. Requirements are gathered from software documentation such as W3C, literature that discussed SSI artifact designs, and existing digital wallet. The development also explores the difference of users in LMIC and non-LMIC.

The SSI design artifacts were developed using UIZard, a user-friendly rapid prototyping tool, resulting in a clickable design artifact where user can test the artifact based on provided scenarios. This allows author to observe how users interact with interface layer and clarify user questions while using the artifact. Semi-structured interviews are conducted with fifteen respondents from Indonesia, comprising of five Indonesian students studying in TU Delft, and ten Indonesians residing in Indonesians. Indonesian-based respondents are all tested positive for socially stigmatized diseases such as HIV/AIDS and TB. They are included to ensure the inclusivity of this study, considering that people with socially stigmatized diseases are more sensitive and aware of their data. All interview data are anonymized, with minimum personal information gathered from respondents (i.e., short name, Indonesian, age cutoff of 18, disease name). Voice recording and interview transcripts are stored in TU Delft OneDrive to guard the privacy of respondents. Transcripts are analyzed using Atlas.ti through inductive and thematic coding process to extract insights. This study is qualitative in nature with a relatively small sample size of 15 respondents, allowing the exploration of individual experiences and provide deeper insights.

The findings are not generalizable to population at large but can provide a starting point for a future quantitative study on the same topic.

Results

The result of this study is a design artifact that is demonstrated and evaluated by selected respondents, which garners insight on how SSI functionalities can help LMIC users in retaining their personal data sovereignty (PDS). By comparing literature review and evaluation of user perspectives, it is found that the data revocation and data minimization are essential in addressing the values of ownership and control of a users' PDS. Data minimization allows user to share only the necessary data, whereas revocation allows users to withdraw from the data-sharing scheme. Users' perspective also showed that both functionalities can directly provide users with the feeling of control, whereas the feeling ownership is something that is more abstract and can only be attained by having control. In essence, the more control a user has over their data, the more ownership they feel over their data. In addition, the feeling of ownership can also be invoked by a relatively simple concept: the name of the user on an interface screen, together with all available credentials being safely stored inside an application.

This qualitative study found occurrences where people with affinity of the impact regarding data sharing influences the effectiveness of SSI functionalities; a user's level of digital literacy affects their perception of the interface, which influences how they perceive the effectiveness of data minimization in providing control. The higher the level of a user's affinity towards data sharing, the more critical they are of their data and consequences in sharing them, prompting them to demand a more complex interface that requires them to re-think their decision in accepting a data sharing request. On the other hand, people with limited affinity feels sufficient with a simpler interface, as they are less aware of the implications of sharing sensitive data. These findings might indicate the importance of improving user's affinity toward data sharing to empower them in retaining personal data sovereignty, which is a hypothesis that can be explored further using a quantitative approach. Lastly, trust and contractual agreement are found to be essential as a foundation of user's willingness to share data. This study suggests that the two concepts are prerequisites before a user would even consider participating in a data ecosystem, which is also a hypothesis that can be further explored using a quantitative approach. The key proposition of SSI is handing back control over data to its legitimate owner, and therefore the system needs to accommodate individuals with power and freedom of choice. Individuals should be provided with the good will of all stakeholders, placing them on the same level with organizations and entities, and not to be exploited.

Contribution

This study contributes to the growing research on SSI, particularly on the interface layer in the context of an LMIC. By taking a user-centric approach, this study delves into the link between SSI functionalities and individual's personal data sovereignty, a topic that is still understudied, and discover the possible interrelation between control and ownership. Conducting the research using the design science research methodology also provides an adequate basis for the development of design artifact. Moreover, the development of scenario in the design and development step also enables a more detailed artifact development process, which is also useful in the demonstration and evaluation of design artifacts by selected respondents. This study also ensures the inclusion of vulnerable population as represented by individuals with socially stigmatized diseases, where their concerns are also embedded in the development of design artifact. Lastly, this study could provide policymakers and stakeholders within the Indonesian healthcare ecosystem with insights on how SSI could be a key in increasing participation of citizens in the data ecosystem, while also considering the technical and resource limitations that need to be addressed before SSI can really be implemented at large.

Next steps

This study provides a starting point to the implementation of SSI in the context of a health data ecosystem in an LMIC, specifically in Indonesia. As this study only involves a limited number of respondents, the generalizability of this study should still be explored by including more respondents with varying socio-economic background that can better represent the Indonesian population and implementing a quantitative approach. The design artifact could further be enhanced according to the feedback of the users, while ensuring usability and the achievability of their personal data sovereignty.

Contents

List of figures

List of tables

1. Introduction

1.1. Background: Key components needed in a health data ecosystem to achieve quality health services

In 2019, the United Nations (UN) committed to achieving Universal Health Coverage (UHC) as a part of their Sustainable Development Goals. This goal aims to ensure that everyone, including those in Low-Middle Income Countries (LMIC), has access to a wide range of quality health services (Sahay et al., 2019). Achieving UHC does not only require strong political will but also an integrated health system that enables various stakeholders to collaborate efficiently (Bai et al., 2022). A key enabler in this effort is ensuring integrated data across the healthcare system, meaning that heterogeneous sources of health data are processed in a seamless way and distributed to different users (Peng et al., 2020). Integrated data is vital not only for front-line health workers in LMICs, such as those in small clinics and hospitals, but also for other stakeholders such as healthcare facilities and government to understand the effectiveness of their healthcare services, system, and policies. However, establishing an integrated data for health information system in LMICs faces challenges such as limited infrastructure and a lack of digital literacy (Sahay et al., 2019).

Integrated data is a crucial part of Health Data Ecosystems (HDE), which is defined as socio-technical networks that allow various community actors to engage in data-related activities like management, analysis, and sharing. HDE leverages cloud computing's scalability for secure data sharing, boosting research and encompassing diverse data under strict governance (Grossman, 2019; Marcelo et al., 2019). Research indicates that HDEs can enhance political and social facets, increase productivity, and create value in healthcare research (Marcelo et al., 2019). However, there are rising issues related to the nature of data sharing in HDE, particularly around data sovereignty, which is one's right to control and maintain their own data (Hummel, Braun, Tretter, et al., 2021). Purtova (2017) also highlights the risk of disempowerment of individuals as a negative consequence of data processing, as they cannot control what would be done with their data once it becomes a part of the data ecosystem.

A novel approach to addressing these concerns is Self-Sovereign Identity (SSI). SSI empowers individuals and entities to manage their identities independently, storing personal data either locally or on secure, distributed networks (Mühle et al., 2018). This system allows users to grant selective data access to trusted entities and retract data independently (Mukta et al., 2020; Vidal et al., 2021, 2022), bypassing intermediaries for authentication. Thus, SSI restores control and ownership of personal data to individuals (Mühle et al., 2018). This approach, enabled by blockchain technology, shifts data management from centralized to decentralized systems, where each network actor synchronizes and replicates their information (Anderson et al., 2023; Ferdous et al., 2019; Schlatt et al., 2021a).

The SSI model revolves around three principal roles: issuers, holders, and verifiers (Mühle et al., 2018; Preukschat et al., 2021) as depicted in Figure 1.1. Issuers issue Verifiable Credentials (VC), which is a digital representation of everyday attributes of one's identity document based on the holder's request. In this model, the holder stores all their VCs within a wallet, where they can manage and use them. The verifier will check the holder's credentials by requesting a Verifiable Presentation (VP), which is a duplicate of the VC with selectively disclosed information to be shared with the verifier. For instance, consider a scenario where a person applies for a driver's license at the Department of Motor Vehicles. Once the license is obtained, it becomes a VC. When renting a car, this license is presented as a VP for proof of identity and driving eligibility. All data is stored in a verifiable data registry. A Decentralized Identifier (DID) is used to verify the authenticity of VCs and the validity of the claims made in a VP by referencing the information stored in a verifiable data registry. This interaction, common in various scenarios like KYC (Know Your Customer) in banking industry and insurance identification, demonstrates the typical flow in an SSI framework (Farao et al., 2023; Schlatt et al., 2021).

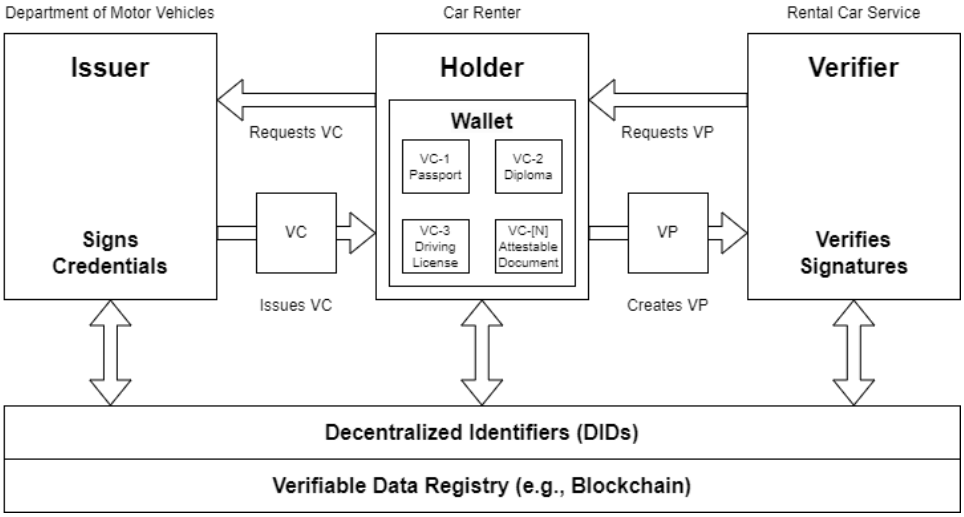

Figure 1.1 Illustration of a Self Sovereign Identity scenario, adapted from Preukschat (2021)

This study posits that SSI could provide benefits to HDE, particularly in empowering individual users with control over their data. SSI gives individuals the power to decide what they will do with their own data, leveraging their position against bigger institutions such as hospitals and the government. This sense of ownership and control might increase the willingness of individuals to participate in the HDE, subsequently increasing the number of data points available for the improvement of a country's healthcare quality. As LMIC are mostly still in the early adoption stage of health data ecosystem (Beane et al., 2019; Mahmood et al., 2023), SSI could strengthen the individuals' data sovereignty from early on and avoid the pitfalls present in countries that are more advanced (Balsari et al., 2018).

It is essential for stakeholders within a healthcare ecosystem to understand how integrated data and technology can improve the quality of health services, and how SSI could encourage the increase of participation from individuals. Emphasis is being put on the concept of personal data sovereignty, a perspective of data sovereignty that focuses on the autonomy of citizens and their roles as individual users of digital technology, as opposed to the national level of data sovereignty that focuses on the state's authority in protecting digital infrastructure and data of citizens and businesses within its territories (Tan et al., 2019) . This study will explore how individuals in LMIC interact with SSI and how it influences their personal data sovereignty.

1.2. Research context: Healthcare data ecosystem in Indonesia as an LMIC

Indonesia is faced with the problem of fragmented health data, driven by numerous health applications that lack standardization and data exchange. Central and local governments have developed more than 400 health applications, resulting in health policies built not based on comprehensive data and inefficient health services. Almost 80% of healthcare facilities in Indonesia are still untouched by digital technology, millions of prescriptions are being given in paper form, and patient data are managed separately in multiple healthcare facilities (Ministry of Health Indonesia, 2021). In 2021, the Ministry of Health launched the Blueprint for Digital Health Transformation Strategy 2024, aiming to build the Indonesia Health Services (IHS) platform where all actors of the health industry can collaborate. One of the main principles of IHS is integrated information that can be exchanged by all its members.

In 2022, Ministry of Health launched SATUSEHAT, an integration platform for all health information technology in Indonesia. This platform connects the entire ecosystem of health industry players (government and private hospitals, health centers, laboratories, clinics, and pharmacies) to create one reliable national health data repository. SATUSEHAT will also be integrated with the PeduliLindungi application, a COVID-19 app that has been accessed by more than 140 million users – or 73% of Indonesia's total productive population. PeduliLindungi was used to track user's vaccination status, COVID-19 test results, also check-in app mandatory for entering public spaces and taking shared transportation modes, intended for tracing purposes. SATUSEHAT provides a promising

starting point for the adoption of Self Sovereign Identity in Indonesia. The UI of the app can be seen on Figure 1.2

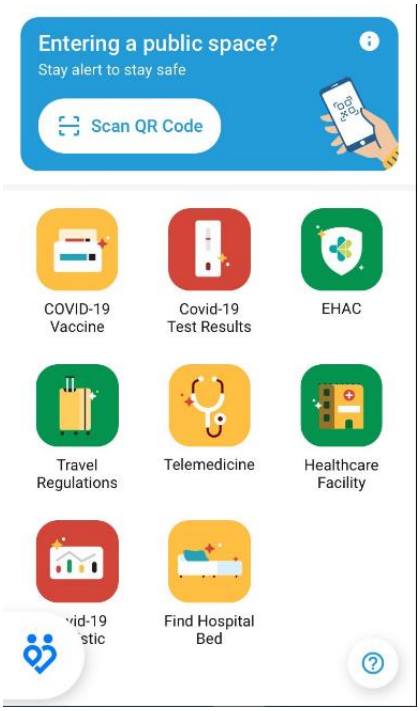

Figure 1.2 User interface of PeduliLindungi (now SATUSEHAT)

In terms of establishing healthcare data ecosystem, Indonesia faces similar challenges as other LMIC. There are inadequate regulations on data protection, data standardization, and patient rights and privacy. The lack of digital infrastructure in Indonesian healthcare facilities poses challenging logistical problem, considering Indonesia is the largest archipelagic country consisting of more than 17,000 islands that extends over 5,000 km from east to west and over 1,700km from north to south. Cybersecurity awareness and capability is still very low, as displayed by multiple data breach that happened to various government apps and databases, including a 3.2 billion data entries breach from PeduliLindungi in late 2022 (Janti, 2022).

1.3. Knowledge Gap and Problem Statement

Topics related to Health Data Ecosystem (HDE) in LMIC, particularly Self-sovereign identity (SSI), are a nascent area of research. A study by Mahmood et al. (2023) highlighted opportunities and barriers needed to be addressed in developing a health data ecosystem in Pakistan, which includes the creation of appropriate governance, regulatory framework, and strategic collaboration between actors. In Kenya, a study implemented SSI in a smartphone-based design artifact system to carry out the initial steps of birth registration and linkage of mothers-baby pairs, obtaining end-user feedback related to feasibility and acceptability of an SSI approach (Freytsis et al., 2021). Other studies highlighted the challenges shared by LMIC in adopting technology to enhance health data ecosystem, including lack of infrastructure and data literacy skills (Jayatilleke, 2020; Kemkes, 2021; Khan et al., 2023; Mahmood et al., 2023).

Research topics on SSI in non-LMIC context focus on the technological enablers of SSI such as blockchain and its emerging best practices (McMullen et al., 2019; Lee et al., 2021; Ahmed et al., 2022), implications for practice around SSI implementation regarding policy, management, and design (Chango, 2021; Weigl et al., 2023). In terms of implementation of SSI in non-LMIC healthcare sector, Lacity & Carmel (2022) assessed the implementation of SSI in UK's National Health Service (NHS), where the NHS developed a digital staff passport used to verify health professional's qualifications and credentials. There is still limited research on real-life SSI implementation, particularly on how such systems should be designed and how they can effectively support business processes (Guggenberger et al., 2023).

Lockwood (2021) addressed this gap by enhancing the topic of SSI functionalities implementation within an interface layer, in which he argued that significant design-focused work is needed to achieve sustainable adoption of SSI. This study will be built based on Lockwood's findings – domains of interaction and the minimum required objects for a full-scale SSI engagement – and addresses the listed knowledge gaps by developing functionalities of an SSI design artifacts in Indonesia's healthcare context and exploring the influence of SSI towards the user's data sovereignty. Therefore, the problem statement for this study is stated as follows:

"This study will investigate the implementation of Self-sovereign Identity (SSI) in Indonesia's healthcare sector, focusing on designing SSI artifacts and assessing their impact on user data sovereignty within a Low- and Middle-Income Country (LMIC) context."

1.4. Research Objectives

To address the problem statement, this study seeks to accomplish the following research objective:

"*Develop SSI functionalities to retain personal data sovereignty for users in Low- and Middle-Income Countries (LMICs) within the health data ecosystem.*"

1.5. Research Questions

The main research question (RQ) of this study is as follows:

RQ: *"How should we **design functionalities in SSI artifacts** for a Low- and Middle-Income Country (LMIC) health data ecosystem that **retains user's personal data sovereignty**?"*

To answer the main research question, the following sub-research questions (SRQs) will be explored:

1. **SRQ1:** *"What are the **requirements** in implementing SSI functionalities in the health data ecosystem to achieve personal data sovereignty for LMIC users?"*
   This sub-research question seeks to investigate what functionalities are needed so that self-sovereign identity can be implemented in the health data ecosystem. This question also aims to understand what is required by users to retain their personal data sovereignty.

2. **SRQ2:** *"What could be the **possible design artifact** that follows the functionality requirements of self-sovereign identity in health data ecosystem to achieve personal data sovereignty for LMIC users?"*
   Answers from SRQ 1 will be used to develop a design artifact. In addition, existing SSI apps are explored to study user flow and compared with design artifacts found in studies focusing on identity management system. The insights are synthesized to build a design artifact that will be demonstrated and evaluated by the users.

3. **SRQ3:** *"**How can SSI functionalities help** LMIC users achieve data sovereignty in the health data ecosystem?"*
   This sub-research question will be answered by conducting user testing between selected respondents and the design artifacts. Scenarios are developed according to real life use cases to observe how they interact with the designed SSI functionalities, and interview is conducted to explore their experience in using the design artifact, particularly to learn how SSI functionalities impact their personal data sovereignty.

1.6. Relevance with MSc program

TU Delft's Management of Technology (MoT) MSc program aims to produce graduates who are well-versed in analyzing technologies in both internal and external contexts in relation to business partners. This master's thesis is relevant to the MOT MSc program as it focuses on SSI as a novel approach enabled by blockchain technology and its implementation in the healthcare sector by considering how different stakeholders deal with the technology, with a particular focus on the individual users and how the concept impacts their personal data sovereignty. The research findings can provide stakeholders from healthcare facilities, businesses, and governments with preliminary insights to explore a more quantifiable research and guide the implementation of SSI into their business processes.

1.7. Report Structure

This report will be divided into eight chapters. **Chapter 1** is the introduction to research background, research context, knowledge gap and problem statement, as well as the research objectives, main- and sub-research questions, and a brief explanation about this study's relevance with MOT MSc program. **Chapter 2** covers literature review on health data ecosystem, personal data sovereignty, self-sovereign identity, and the conceptual framework used to guide the research. **Chapter 3** consists of explanation of design science research as the selected methodology, how the sub-research questions correspond to DSR steps, research methods user to answer sub-research questions, and ends with data management and ethics approval. **Chapter 4** discusses environment analysis and requirements specification. **Chapter 5** presents the design and development of SSI artifact. **Chapter 6** covers the design artifact demonstration and evaluation. **Chapter 7** discusses the linkage of research findings to literature review, discusses methodology, and the study's contribution in both practical and academic perspectives. In **Chapter 8**, recommendations and conclusions of this study are presented.

2. Literature Review

The purpose of this chapter is to discuss existing body of research that are relevant to this study. The literature will be reviewed thematically, starting with the discussion of Health Data Ecosystem (HDE), followed by topic of Personal Data Sovereignty (PDS) and the values essential in achieving such sovereignty, how Self Sovereign Identity (SSI) has emerged as a model that can ensure an individual's PDS, discussion on research that explored the real-world implementation of SSI both in LMIC and non-LMIC context, and introduction to the Indonesian healthcare context. This study considers multiple sources such as peer-reviewed journal articles, books, conference papers, dissertations and thesis, reviews and meta-analyses, government and institutional reports, and relevant grey literature. By synthesizing these themes, this chapter is set to narrow down the scope of this research and provide the concepts that will be used to answer the research questions.

2.1. Health Data Ecosystem

Health Data Ecosystems are socio-technical networks where various actors, including public and private organizations, researchers, and data holders, collaborate in data management, publication, and utilization to foster innovation and support the healthcare sector (Grossman, 2019; Marcelo et al., 2019). Unlike traditional resources, data within these ecosystems does not deplete but grows in availability and utility, as it can be repurposed and reused in new contexts (Aaen et al., 2022). In HDEs, entities like enterprises, institutions, and individuals play diverse roles, typically categorized as data consumers and data providers. Data consumers consume data directly or indirectly, while data providers supply data (Marcelo et al., 2019).

Marjanovic et al. (2018) highlighted challenges in realizing the value in European HDE; a simultaneous focus on technological and structural conditions, collaboration and coordination to transform working culture, and efforts to ensure that policy, industry, and research communities can respond to public concerns. In the context of an LMIC, challenges faced by an HDE in Pakistan include the effective utilization of health data, and how to utilize openness and enthusiasm in data sharing despite limited capacity in human capital and infrastructure (Mahmood et al., 2023). Studies also attempted to offer a technical approach to the operationalization of HDE such as blockchain (Shae & Tsai, 2021), the use of decentralized semantics (Knowles et al., 2023), to API-enabled mobile application (Balsari et al., 2018). Research has highlighted the potential of data ecosystems to create new value for organizations and institutions (Möller et al., 2020). However, challenges arise when repurposing and reusing data, particularly with personal health data. The disparity in data access and control among different actors can lead to an unequal distribution of benefits and responsibilities (Boyd & Crawford, 2012).

Purtova (2017) highlighted two significant dilemmas surface in this context. The first is the provision dilemma, where individuals hesitate to provide their data due to concerns over sensitivity and security that leads to a lack of control over their health information. The second is the appropriation dilemma, which involves ensuring that shared data is used responsibly and ethically, maintaining data ownership. Addressing these dilemmas is crucial for a functional health data ecosystem. Implementing technologies that empower data owners with a sense of ownership and control over their data is a way to improve participation and build trust between individuals and other stakeholders within the HDE.

2.2. Personal Data Sovereignty (PDS)

Data sovereignty is a principle concerned with protecting sensitive, private data and ensuring it remains under the control of its owner within the specified country (Tan et al., 2022). In his study, Tan et al. (2022) highlighted the idea of individual data sovereignty. It is a departure from a state-centered understanding of sovereignty, focusing on the ability of individuals to take actions and decisions in a conscious, deliberate and independent manner of the access and handling of their data.

A larger body of work refers to individual data sovereignty as personal data sovereignty (PDS), which is the term adopted in this study to maintain consistency with existing research. Studies on personal data sovereignty take place in multiple industries such as the public sector (Carvalho et al., 2023), banking (Otieno, 2022), smart city (Sheombar & Sheombar, 2023; Topham et al., 2023). Topics addressed include the technical and non-technical implementation of data sovereignty (Hellmeier, 2023), reference architecture (Scheider et al., 2023; Falcao et al., 2023), model for personal data sovereignty (Giese and Anderl, 2022), and usability (Appenzeller et al., 2023;

Lockwood, 2021). Literature review highlighted the importance of control embedded to data owners and offered solutions in multiple layers – from concept, framework, workflow, system architecture, to prototype development and user feedback. It shows the complexity of developing a system that can guard personal data sovereignty.

This study departs from the work of Hummel et al. (2021) that mapped the values related to the concept of data sovereignty as discussed in 341 research publications. The value 'control and power' has the highest co-occurrences with data sovereignty, followed by 'security and non-maleficence', 'deliberation, representation, inclusion', 'privacy', and 'ownership'. From the top five values, there are three values that are embedded to individual as the main subject of PDS: 'control and power', 'privacy', and 'ownership'. Borrowing the arguments of Austin (2014), privacy is not a self-standing value but is a by-product of one's power. Privacy results from one's ownership over something and can be attained by control and power the owner is entitled to, as guaranteed by law. In addition, the Cambridge Dictionary defines control as 'the ability or power to decide or strongly influence the particular way in which something will happen, or someone will behave', indicating that control *is* power. Therefore, to maintain conciseness only two values related to personal data sovereignty will be explored in this study: 'control' and 'ownership'.

2.2.1. Control and Ownership

Hummel, Braun, & Dabrock (2021) explained that in data sovereignty, individuals must be able to have the capability to steer the data flows and govern the informational resources of their data. Data sovereignty involves the ability to manage and control data flows and information resources. Schar (2010) emphasizes that data sovereignty grants individuals' extensive control over their health data, requiring explicit consent for its use. König (2017) discusses the concept's ambivalence, noting that it promotes consumer and citizen autonomy but also shifts responsibility to individuals. This implies the need to build competencies for personal data control in the context of a data-driven economy. Hummel, Braun, & Dabrock (2021) also explain that in data sovereignty, some data, even though it was created by other actors, still belongs to someone else. For example, a medical data might be generated by doctors and stored in a healthcare facility, but the ownership of such data still belongs to the patient, entitling them to the right to control their data (Plateaux et al., 2013). Ownership is a right embedded to the individual; control is the ability of the individual to exert his/her right.

2.3. Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) is a blockchain-based approach to identity management, integrating a distributed ledger system that empowers individuals' sovereignty to fully own and control their digital identity. This concept introduced by Mühle (2018), decentralizes identity management, shifting the paradigm from traditional centralized authorities to the individual. SSI comprises three crucial actors: the verifier, the holder, and the issuer. Mühle (2018) emphasizes the distinct roles of these actors based on how they interact with Verifiable Credentials (VCs). VCs are digital representations of identity and other personal data issued by the issuer (Naik and Jenkins, 2020). These credentials can be presented to verifiers as a Verifiable Presentation (VP) where information can be selectively disclosed, enabling a secure and decentralized form of digital identity verification.

The issuer plays a pivotal role in issuing and revoking verifiable credentials (VCs) about data associated to identity, storing this information on the distributed ledger. The holder, who is the owner of these verifiable credentials, retains them within their personal system. The verifier acts as a relying party that requires authentication to grant users access to their resources (Schmidt, 2022). Notably, verifiers can authenticate the identity of a holder without direct contact with the issuer, utilizing the data available on the distributed ledger.

SSI is a novel concept that garners a lot of attention in ICT research. Schardong and Custódio (2022) conducted a systematic review of SSI literature and systematic mapping of both theoretical and practical advances in this field. Practical problems that have been addressed include management (governance of credentials and claims presentation in SSI), operational (functional aspects of VCs and VPs), system design, and trust. Conceptually, the study discussed aspects that are relevant in SSI research – such as compatibility with legacy systems and protocols, recoverability of data in the event of personal device loss, usability of users, scalability of SSI system, and regulatory compliance. In essence, developing an SSI system that can ensure users data sovereignty is a challenging task that takes place in multiple layers from conceptual to technical.

2.3.1 Self-sovereign Identity Studies on the Interface Layer

Based on the review paper by Schardong and Custodio (2022), there are six sources on SSI design and architecture, and five references on Human-Computer Interaction (HCI) which focused on usability and human perception issues in SSI systems. Selected studies on SSI design and architecture discussed about data model (Sporny et al., 2022), blockchain and structure designs for SSI (Stokkink & Pouwelse, 2018; Liu et al., 2020), privacy preference recommender system for data sharing control (Barclay et al., 2020; Wohlgemuth, 2020), and the development of design pattern modules that can be implemented as APIs in SSI (Liu et al., 2020). Design pattern can be defined as a general repeatable solution to a commonly occurring problem in software design. Studies on HCI in SSI is more case-specific, from discussing recovery scheme using security algorithm (Singh et al., 2017), authentication method (Mustafa, 2021), managing user privacy (Toth et al., 2020), managing VPs and automated data sharing (Shanmugarasa, 2021). On the other hand, HCI-themed work by Lockwood (2021) offers an extensive study on SSI usability, identifying the domains of interaction and the minimum required objects for a full-scale SSI engagement.

Another relevant study on interface layer is written by Cucko et al. (2023), where eleven SSI-based digital wallets were analyzed to identify and compare design patterns. Digital wallets are an essential element of SSI as it provides users with the platform to interact with other entities in the ecosystems while giving them control of their data. It is argued that by using good practices and design patterns, the reusability of implemented interfaces can be greatly improved. According to Cucko et al. (2023), the basic functionalities of an SSI-based digital wallets are (1) allowing users to establish connections, (2) obtain and store VCs, and (3) share requested data. A key limitation present in most of the wallets is the inability of user intervention, where they have no choice but to accept or reject the data sharing.

There is still a limited amount of research on SSI interface layer, which poses as a gap that needs to be addressed as SSI is a user-centric model. To achieve a sustainable adoption, there is a need to conduct significant design-focused work at the interface layer (Lockwood, 2020), especially when considering the risk of non-technically competent users not maximizing the functionalities in SSI (Shanmugarasa, 2021). Developing interactive SSI design artifacts would enable this study to gain a deeper understanding of how users interact with SSI and study how such technology influences their data sovereignty.

2.3.2 Studies related to self-sovereign identity for personal data sovereignty on health data ecosystem

The current research on SSI in healthcare mostly focuses on identity management-related topics, such as Know Your Customer in banking (Schlatt et al., 2021), Patient Health Record (Houtan et al., 2020), and insurance identification (Farao et al., 2023). Data sovereignty is a recurring concept in SSI research, although most just focus on establishing the importance of SSI in achieving users' data sovereignty but do not delve into how SSI influences their data sovereignty. Studies are mostly focused on technical implementation of SSI in achieving data sovereignty, such as proposing the use of OpenDSU as a modular, extensible and flexible architecture that allows integration of different blockchain technologies in pharmaceutical industry (Balan et al., 2023) and the use of distributed ledger technology for digital transformation in healthcare sector (Jackson & Taiuru, 2023). Geographically, most studies on SSI takes place in the developed world such as European Union and the US, which is reasonable as they are technologically more advanced and have a more established regulations such as EU's General Data Protection Regulation (GDPR) and US's Health Insurance Portability and Accountability Act (HIPAA).

One notable study on SSI in an LMIC context is written by Freytsis et al. (2021). Taking place in Kenya, the study developed a smartphone-based prototype system that allows interaction between families and health workers to carry out the initial steps of birth registration and linkage of mothers-baby pairs. The prototype design and development were preceded by a research phase to understand current birth registration process, development of assumptions, and most importantly understanding the participants of the system in the real world. Users are required to verify and authenticate their identities before registering mother-baby connection. The study also highlighted the importance of interoperability and open-source development for a scalable health technology for LMICs.

2.4. Conceptual framework

A conceptual framework is developed based on the concepts discussed above. It is used to guide this research and focus on the linkage between PDS values (specifically ownership and control) and SSI on the interface layer. According to its functionalities, SSI would allow users to control and manage their personal identifiable information, particularly during interaction with external entities. This study proposes that SSI functionalities are necessary in achieving user's personal data sovereignty. The upcoming chapters will explore the SSI functionalities needed on the interface layer to achieve user's personal data sovereignty, and how they should be designed.

The proposed conceptual framework is presented in Figure 2.1.

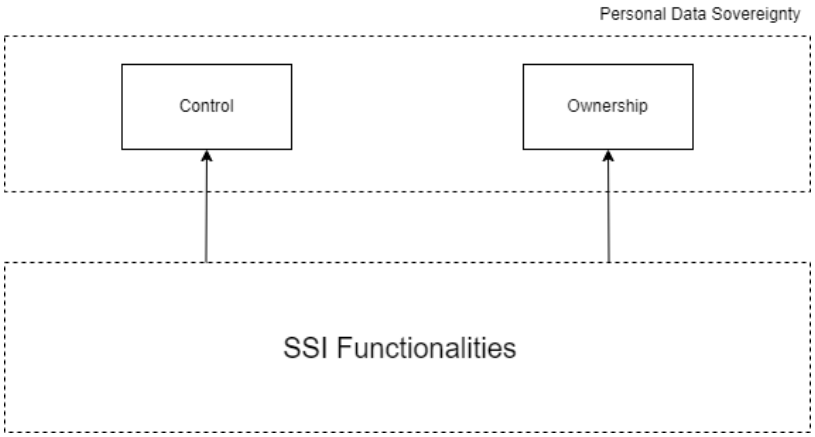

Figure 2.1 Proposed conceptual framework

2.5. Summary on Chapter 2

This chapter discussed relevant literature review on health data ecosystem, personal data sovereignty, SSI, and related research in the LMIC context. SSI research garners a lot of interest, but mostly are focused on technical aspects, and only a limited number of studies took a more user-centric approach in the interface layer. The link between SSI and personal data sovereignty is a recurring idea in studies but has not been delved deeper. Geographically, most research takes place in more advanced countries with established technology and regulations. This study proposes to address a research gap by connecting SSI with personal data sovereignty, taking a user-centric approach on developing SSI functionalities on the interface layer, in the context of Indonesia as an LMIC.

3. Research Methodology

This section will elaborate on how this study will answer the main research question: *"How should we **design functionalities in SSI artifacts** for a Low- and Middle-Income Country (LMIC) health data ecosystem that **retains user's personal data sovereignty**?"*. In section 3.1, an explanation of the selection research methodology will be presented. Section 3.2 will link the selected methodology to the sub-research questions imposed from previous chapters. Section 3.3 will explain the selection of research methods to answer the sub-research questions. Lastly, in Section 3.4, the data management plan will be explained.

3.1. Selection of methodology

The main research question requires a methodology that can test a technological concept and its requirements for solving a practical problem. This study will explore how to design SSI artifacts while retaining a user's personal data sovereignty in the context of a health data ecosystem in Indonesia as an LMIC. Design Science Research (DSR) methodology is suitable for this study as Hevner et al. (2004) developed it specifically to implement design science in the field of Information System (IS). DSR can be used to test user behavior that can be reflected in the design artifact and obtain understanding of the user.

3.1.1. Design Science Research (DSR)

Design Science Research is a widely utilized research approach in the field of information system (Hevner et al., 2004; Peffers et al., 2007). Research on information system is complex because it involves many factors such as people, structure, technologies, work systems (Hevner et al., 2004). Hevner et al. (2004) developed Design Science Research, an approach to conducting research that focuses on creating and evaluating artifacts to advance knowledge and understanding in a particular domain, often within the context of Information Systems. In 2007, Hevner expanded his earlier 2004 work by offering a more detailed view of how DSR operates through three distinct but interconnected cycles: the Relevance Cycle, the Design Cycle, and the Rigor Cycle, as depicted in Figure 3.1.

Hevner (2007) and Peffers et al. (2007) provided complementary perspectives that emphasize the importance of integrating theory and practice, with Hevner (2007) establishing the broad framework for understanding the interaction of different cycles within DSR, and Peffers et al. (2007) providing a detailed, step-by-step methodology for the operationalization of DSR, while guiding the iterative process of design and evaluation of artifacts.

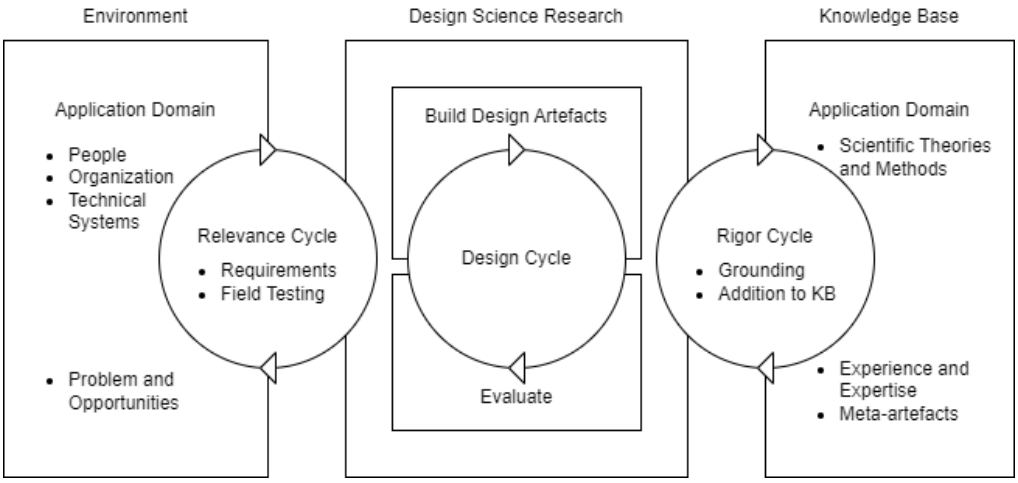

Figure 3.1 DSR approach of Hevner et al. (2007)

Components of DSR:

1. The first cycle is the **relevance cycle** which bridges environmental factors and design science. This cycle is used as a starting point to find out what problems and opportunities can be used to introduce an innovation from IS applications. Apart from the problem that needs to be determined, design criteria and requirements are also determined in this cycle.

2. The second cycle is the design cycle, in which the design and evaluation process of the artifact is carried out. Evaluation is carried out based on criteria obtained from the knowledge base and environment. The focus in this cycle is the design artifact evaluation process which will later enrich knowledge in the knowledge base and reveal new problems or opportunities in the environment.
3. The third cycle is the **rigor cycle** which connects the knowledge base to the design cycle. In this cycle, known methods and theories will be involved as a basis for developing artifact designs. The results obtained through the design cycle will later be communicated again to enrich the knowledge base of the technology or problems discussed, as well as providing criteria for SSI artifacts, which will be used as the basis for artifact design for later evaluation.

Hevner (2007) elaborated how these cycles interact and how they contribute to the development of design science knowledge and artifacts. Peffers et al. (2007) introduced a formalized methodology for conducting DSR in IS, aiming to provide a structured approach to develop and evaluate IT artifacts. The proposed methodology includes six stages:

1. **Problem identification and motivation**: defining the specific research problem and justifying its importance for a solution
2. **Define the objectives for a solution:** establishing what the solution should be able to achieve that based on the problem that has been introduced before.
3. **Design and development**: creating the designed artifact by aligning the desired functionality to achieve the desired solution
4. **Demonstration**: using the artifact to solve the problem in a real or simulated environment
5. **Evaluation**: observing the designed artifact and analyzing whether the designed artifact solves the problem
6. And **communication**: sharing the problem, designing artifacts, and effectiveness with researchers and practitioners

3.2. Sub-research questions and DSR linkage

After understanding the three cycles of DSR and the operationalization of DSR methodology, the next step is to link sub-research questions (SRQs) to the six steps as established by Peffers et al. (2007):

1. **SRQ1:** *"What are the **requirements** in implementing SSI functionalities in the health data ecosystem to achieve personal data sovereignty for LMIC users?"*
    a. In *problem identification,* the problem is defined as individual users' risk of disempowerment due to data processing, as they often lose control of their data once it becomes a part of the data ecosystem. The environment analysis in next chapter will delve deeper into the context of HDE in Indonesia, where problems are further defined
    b. In *defining objectives for a solution*, the next thing is to find out the requirements that need to be considered in developing SSI as a health data sharing medium. This will be done by implementing the requirements engineering approach, researching literature regarding design artifacts, functionalities components of SSI, and criteria so that PDS can be achieved

2. **SRQ2:** *"What could be the **possible design artifact** that follows the functionality requirements of self-sovereign identity in health data ecosystem to achieve personal data sovereignty for LMIC users?"*
    a. The third step of DSRM is the *design and development* of the SSI design artifact. In this step, the collected requirements will be used as a reference as a design choice in forming the SSI artifact design and answering SRQ2

3. **SRQ3:** *"**How can SSI functionalities help** LMIC users achieve data sovereignty in the health data ecosystem?"*
    a. The next stage is *demonstration*. In the demonstration step, the artifact design will be tested by conducting user testing with respondents who are concerned about sharing their health data. This aims to ensure that the design artifact can show the potential to solve problems (Peffers et al., 2007)

b. Next, an *evaluation* will be carried out, which will result in qualitative observations whether the design of the artifact is sufficient for practical use (Johannesson & Perjons, 2021), followed by a semi-structured interview to gain user's insight on how the SSI design artifact might influence their data sovereignty. In this evaluation process, observations are made regarding how SSI can impact PDS and the interplay between underlying concepts

c. The last thing is to *communicate*. In this activity, the findings obtained during the SSI artifact design process will be used to answer the research questions presented in the writer's master thesis and distributed to the respondents. The study will elaborate on the impact of SSI on PDS

The sub research questions and Peffer's six stages of DSR are mapped within Hevner's three DSR cycles, as summarized in Figure 3.2.

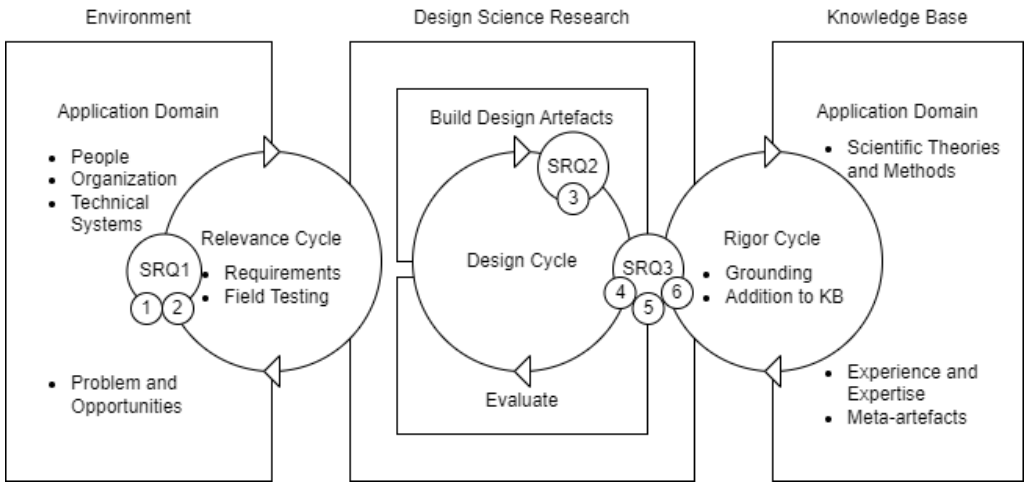

Figure 3.2 DSR approach of Hevner et al. (2007) with mapping of activities and sub-research questions

3.3. Research Methods on Sub-Research Questions

This section will explain the DSR step, goal, and activities done to answer the sub-research questions, as summarized in Table 3.1.

Table 3.1 Summary of research methods

SRQ	DSR step	Goal	Activities	Chapter
1	1. Problem identification	Understand problems experienced by user when sharing their health data through SSI platform	Desk research	Chapter 4
	2. Defining objectives	Find structure of the requirements of an SSI in the context of health data sharing	Literature review, benchmark with existing SSI applications	
2	3. Design and development	Develop SSI design artifact	Scenario development Develop a clickable design artifact using UIzard	Chapter 5
3	4. Demonstration	User testing, allow user to interact with SSI design artifact	Scenario-based user testing	Chapter 6
	5. Evaluation	Assess Design	Semi-structured interview, coding, analysis	
	6. Communicate	Answer all research questions	Discussion, report writing	- Chapter 7 - Chapter 8

DSR Step 1 and Step 2, problem identification and defining objectives, will be written in **Chapter 4,** titled Environment Analysis & Requirements Engineering. This chapter will answer **SRQ1**: *"What are the **requirements** in implementing SSI functionalities on the health data ecosystem to achieve personal data sovereignty for LMIC users?".* The chapter starts with the Environment Analysis section that highlights the problems faced by individuals within health data ecosystems: disempowerment and risk of losing control over data. SSI is positioned as a solution to this problem – giving back control and ownership to the users and allowing them to retain their personal data sovereignty. It is followed by the Requirements Engineering section, a process introduced by Boulanger (2016). The methodology consists of the following steps:

1. **Requirement elicitation.** Gathering and identifying requirements from stakeholders, users, and other sources to understand what the system should do
2. **Requirement analysis.** Examining and refining gathered requirements, involves prioritizing requirements and resolving conflicts or ambiguities
3. **Requirements specification.** Documenting requirements in a structured format that serves as a basis for design and development
4. **Requirements validation.** Reviewing the documented requirements with stakeholders to ensure they accurately represent their needs and expectations
5. **Requirements management.** Tracking changes, ensuring traceability between requirements and other artifacts, and maintaining consistency

In this study, the requirements engineering omits the validation step, as the questions to validate requirements will be asked directly to the end users during the evaluation step (DSR step 5). Requirements management will also be omitted as the step is more suitable in a more advanced step of development. The purpose of requirements engineering is to understand the requirements in the SSI interface layer that can retain user's PDS when carrying out data sharing in the health data ecosystem. In addition, a literature review is also carried out to determine differences in consumer health data sharing preferences in LMIC and non-LMIC. This difference will later be used as a scenario for artifact design when evaluated. After knowing the general SSI requirements and requirements for LMIC, a requirements specification is developed. This aims to formalize the requirements needed to be translated into an SSI design artifact.

DSR Step 3, design and development, will be written in **Chapter 5**, titled Design and Development of SSI Artifact. This chapter will answer SRQ2: *"What could be the **possible design artifact** that follows the functionality requirements of self-sovereign identity in health data ecosystem to achieve personal data sovereignty for LMIC users?".* To answer this research question, the requirements determined in Chapter 4 are translated into an SSI design artifact adapted to the predetermined scenario that covers real-life implementation of such application (i.e., health data sharing between patient and third party). Design artifacts were developed using UIZard, a user-friendly rapid prototyping tool. It resulted in clickable design artifacts shown in the interface layers, adjusted to the determined flow diagram functionalities. Users can click through the interfaces and experience the application. The design and development process includes benchmarking existing SSI digital ID wallet apps available in the market.

DSR Step 4 and **Step 5,** demonstration and evaluation, will be written in **Chapter 6,** titled Design Artifact Demonstration & Evaluation. This chapter will answer SRQ3: *"**How can SSI functionalities help** LMIC users achieve data sovereignty in the health data ecosystem?".* To answer research question 3, semi-structured interviews were conducted while observing users using the designed artifacts. Semi-structured interviews will be conducted to obtain other contextual factors relevant to users when maintaining PDS through SSI. The questions asked during the interview revolved around user concerns when sharing health data, what users feel when using the design artifacts, and how they interact with the features of the artifacts. Validation of features also takes place in this chapter.

To fulfil the research context of LMIC, interviews were conducted with 15 respondents from Indonesia. Five of whom were Indonesian students who are pursuing a master's degree at TU Delft, while ten of them are Indonesians residing in Indonesia who have socially stigmatized diseases such as HIV/AIDS and TB. Respondents with socially stigmatized diseases are included to ensure the inclusivity of this study, as they are more sensitive and aware of their own data compared to the general population. The recruitment process for student

respondents used the author's personal network, while recruiting respondents with socially stigmatized disease was carried out by contacting two representatives from support groups in Indonesia and asking them to find people who were interested to participate in the study. Next, the interview results are transcribed and analyzed qualitatively. Interview transcripts undergone axial coding process in Atlas.ti using thematic analysis and middle-ground approach to answer research questions and provide insights on how SSI design artifact could retain users' personal data sovereignty in the context of health data ecosystem in LMIC.

DSR Step 6, communication, will be written in **Chapter 7 and 8,** Discussion & Contribution and Recommendations & Conclusions, respectively. These chapters will revisit all research questions and synthesized the research process, providing readers with insights to how DSR could be implemented to develop SSI design artifacts in the interface layer that can retain users' personal data sovereignty in the context of LMIC.

3.4. Data Management and Ethics Approval

When collecting data, it is important to ensure that the respondent is not influenced by any external factors that could impact the quality of the research. We prioritize voluntary participation and the freedom of the respondent in our research. For this study, participants are selected based on their accessibility and willingness to participate, and they are required to provide informed consent, which is included in the appendix. This approach helps us to establish trust, respect the participants, and ensure the protection of their data throughout the research period.

This study has been reviewed and approved by the Human Research and Ethics Committee (HREC) of TU Delft, ensuring that ethical considerations are in place. All participants in the evaluation session have provided their informed consent to participate in the research, either in writing or recorded during the interview. Various types of data were gathered for this study, including voice recordings and interview transcriptions, anonymized interview summaries, and coding of the interview results. Throughout the data collection and research processes, measures for research ethics mitigation are implemented, as outlined in Table 3. Interview respondents can only take part in the study after filling out and understanding the attached informed consent form.

Table 3.2 Data Management Plan

Research Activity	Data Type	Goals	Personal Identifiable Information	Data Management Mitigation
Data Gathering	Semi Structured Interview Transcript, Voice recording of Interview	Collecting views and perspective from data holder when using SSI to do health data sharing	Mentioned Name, Gender, Location, Disease	All personal identifiable information will be redacted from the transcription. The transcription and the recording of interview will be stored safely on TU Delft OneDrive. Only author and committee members could access it

4. Environment Analysis & Requirements Engineering

This chapter implements the first and second step of DSR (Peffers et al., 2007)—problem identification and defining objectives for a solution—and provides answer to **SRQ1**: *"What are the **requirements in implementing SSI functionalities** on the health data ecosystem to achieve personal data sovereignty for LMIC users?"*. This chapter has two sections: (1) Environment Analysis and (2) Requirements Engineering, where the output of environment analysis will act as input and context for requirements engineering. Hevner's Relevance cycle will also be discussed. Environment analysis summarizes the context of Indonesian healthcare system and present the identified problem of this study through stakeholder analysis and desk research. The Environment Analysis section starts with stakeholder analysis to identify stakeholders within Indonesian healthcare system, alongside their interests and influences. An analysis on stakeholders' interaction and the general patient data flow is also discussed, followed by a discussion on a particular problem within the Indonesian healthcare ecosystem. The Requirements Engineering section implements the requirements engineering approach adapted from Boulanger (2016) that comprises of two sections: (1) Requirement elicitation and analysis, and (2) Requirement specification.

4.1. Environment analysis

4.1.1. Stakeholder analysis

Kannampallil et al. (2011) described a healthcare system as a network of interconnected elements or participants focused on delivering healthcare services to individuals or communities. It highlights the role of stakeholders actively involved in providing medical care to patients. From a broader perspective, the healthcare system includes three main components: healthcare facilities or providers, healthcare professionals or workers, and financial institutions supporting them. The patient is the user of healthcare services offered within the healthcare system. The other two stakeholder categories are government and healthcare support. The summary of stakeholder analysis is presented in Table 4.1.

Table 4.1 Stakeholder analysis summary

No	Stakeholder category	Stakeholder name	Role	Interests	Influences
1	Patient	Patient	User of healthcare services	Get the best healthcare services at low cost	Demand affordable healthcare services
					Advocacy for needs
					Provide feedback to healthcare providers
2	Healthcare facilities	Hospital	Provide wide-range healthcare services	Provide quality healthcare services and generate revenue	Discussion with government officials
					Participate in policy development
					Negotiate with financing institutions
		Clinical laboratory	Process specimens to support diagnostics of healthcare professionals		Facilitate evidence in policy making
3	Healthcare professionals	Doctor	Provide healthcare services	Deliver healthcare services and be compensated fairly	Participate in policymaking through professional organizations
					Advocacy for quality improvement
					Demand government support for R&D and public health research
					Educate patients

No	Stakeholder category	Stakeholder name	Role	Interests	Influences
		Nurse	Provide support for doctors		Advocacy for patients and quality improvement
					Educate patient
4	Healthcare financing	Social Security Agency of Health (BPJS-JKN)	Finance healthcare expenses of insured citizens	Provide healthcare coverage at low cost	Financial influence
					Negotiate with healthcare facilities
					Discuss with all healthcare stakeholders
					Coordinate with Ministry of Health
		Private insurance	Finance healthcare expenses of policy holders	Provide healthcare coverage and generate revenue for business performance	Financial influence
					Coverage and benefit design
					Advocacy and policy influence
5	Healthcare support	Pharmaceuticals company	Provide supplies and medications for healthcare facilities and healthcare workers	Increase market share amongst healthcare players and generate profitable business	Develop innovation
					Negotiate with government to source foreign supplies that are not available locally
					Partner with healthcare facilities and workers
		Research institution	Conducts research in the healthcare field	Produce impactful research that can improve quality of healthcare	Support government policy-making
					Educate public
6	Government	Ministry of health	Regulate and enforce nationwide healthcare policies	Improve quality and access of healthcare for citizens	Develop policy and regulation
					Impose policy and regulation
					Manage healthcare facilities, workers, financing institution, and healthcare support
					Educate citizens
		Local government	Implement national policy and regulate local healthcare system	Deliver healthcare services and carry out central government policies	Impose policy and regulation
					Coordinate with local healthcare facilities
					Educate local citizens

Patients are the central stakeholder within the healthcare ecosystem, as they are the users of healthcare services provided by healthcare facilities and healthcare workers. Their key interest is to get the best healthcare services at low cost. Since the Indonesian government launched Social Security Agency of Health (BPJS-JKN) as a universal health insurance for citizens, almost 95% of the population is registered under this program. Access to healthcare financing also improved access to healthcare services, improving the quality of life. As a customer, patients have the influence and rights to provide feedback on healthcare providers, workers, financing, support, and the government.

The key interest of healthcare facilities is to provide quality healthcare and generate revenue. Healthcare facilities can be categorized in numerous ways, such as by the types of patients that can be catered, level of care provided, or who owns them. For instance, in Indonesia, individuals can initially seek care at community health centers, which offer integrated healthcare services and are easily accessible to the public (Suryanto et al., 2017). Hospitals in Indonesia can be differentiated by the services they offer or their management style (Suryanto et al., 2017). General hospitals provide a wide range of services for various conditions, whereas specialty hospitals focus on specific diseases or areas of medicine. Additionally, hospitals can be either public- or private-owned. Private hospitals are often reluctant to partner with BPJS-JKN mostly due to financial reasons: slow reimbursement process and low rates set by the government (Heriyanto, 2018). Clinical laboratories are also crucial in processing specimens from patients (e.g., blood, urine, stool, biopsies) and support healthcare workers in providing diagnostic and treatment. Clinical laboratories can also be separated into government-operated and private laboratories, which differ in pricing and range of test they provide. Both laboratories can accept BPJS-JKN if the patient receives a referral from a first level healthcare facility. Healthcare facilities can influence both patients and financing institutions.

The healthcare workforce in Indonesia includes a diverse range of professionals that includes doctors, nurses, midwives, pharmacists, public health officers, and traditional healthcare providers. Their key interest is to provide quality healthcare while being compensated fairly. They provide healthcare services to patients, from diagnostics to treatment. Doctors can work in up to three healthcare facilities per government regulation. As a key healthcare provider, doctors can exert influence through professional organizations such as Indonesian Medical Association (IDI), and specific organization for specialists such as Indonesian Society of Obstetrics and Gynaecology (POGI) and Indonesian Society of Paediatricians (IDAI). Pharmaceuticals companies and consumer brands also often target partnerships with doctors as they hold a key role in influencing patients through consultation, education, prescription of treatments, and endorsement of products.

In terms of financing, Indonesia has a national health agency called Social Security Health Agency (BPJS-JKN). Their key interest is providing cost-efficient healthcare coverage and improve overall country healthcare system. This system covers a wide range of services without extra charges for medicines and supplies, following specific procedures. As a key financier, BPJS-JKN has power over healthcare facilities by setting rates for healthcare services. The key differentiator between BPJS-JKN as a government insurance and private insurance is in the tiered referrals a patient must go through to receive treatment. All patients must start at level 1 healthcare facility (local clinics with limited facilities) and meet a general practitioner, before receiving a referral to see specialist in a hospital. Hospitals are also graded from A to C, C being the lowest in the hierarchy. Level 1 healthcare facility must follow the hierarchy, referring the patient to C-grade hospital if the intended specialist is available. Only if the hospital cannot provide the service, then the patient can be referred to a higher-grade hospital. This system does not apply to private insurance holders. Financing institutions can influence healthcare facilities, healthcare workers, and government.

Healthcare support such as pharmaceutical companies play a vital role in Indonesia's healthcare ecosystem by developing and providing essential drugs, supporting public health initiatives, and conducting clinical trials. Their key interest is in gaining market share and run profitable business. These activities do not only contribute to medical advancements but also support the healthcare infrastructure economically, marking pharmaceutical companies as crucial players in enhancing the health of the Indonesian population. They must maintain close relationship with government to maintain compliance and influence policy making, including in sourcing foreign supplies that are not available locally. Healthcare support businesses are crucial in technology transfer and innovation, thus entitling them to influence the ecosystem. Another relevant healthcare support entity is research institution that conducts research on healthcare, producing research output that can support government policymaking and educate the public at large.

Lastly, the Indonesian government has a significant influence on the evolution of healthcare system. Following decentralization in 2001, local governments gained more control over healthcare, allowing for tailored services and improvements in healthcare infrastructure and services (Suryanto et al., 2017). The Ministry of Health sets national standards, supported by a universal health insurance scheme and regulatory frameworks to ensure

accessible and effective healthcare across Indonesia. The government's key interest is to improve the quality of Indonesian healthcare system by engaging all stakeholders.

4.1.2. Stakeholders interaction and data flow in the healthcare ecosystem

Healthcare ecosystem requires interaction between the stakeholders. The interaction is important because each stakeholder provided substantial effect for patient medical treatment, regardless in the terms of financial, treatment, or policy, which makes them dependent on each other to provide healthcare services especially to information. Therefore, data is essential for this interaction as it will provide all the stakeholder of the information that is circulating within their healthcare system. A data flow analysis between the stakeholders is conducted to provide a general picture on how the data is generated and used from one stakeholder to another. By integrating patient health data from multiple sources, stakeholders will be able to gain a more holistic view of Indonesian healthcare landscape. Patient data flow is presented in Figure 4.1.

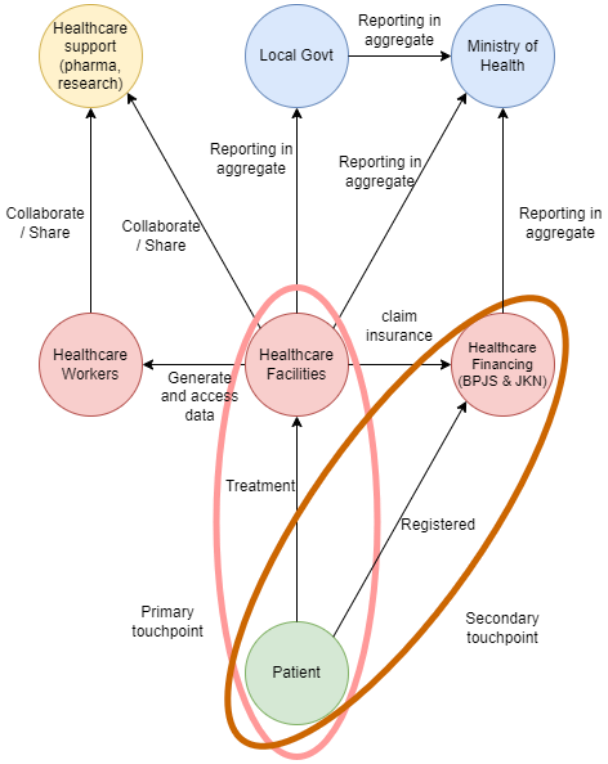

Figure 4.1 Patient's Data Flow in Indonesian Healthcare System

As detailed in the stakeholder analysis, the patient is the primary source of data for the healthcare system. The data flow begins with patients visiting healthcare facilities for treatment, where their medical records, diagnostics, and treatment plans are documented. This information, stored in the healthcare facility's systems, is the primary point of contact for patient data, where sensitive medical information is first recorded. Another layer of data is generated when patients register with BPJS-JKN, providing personal details like national identity number and family registration numbers. This serves as a secondary data touchpoint, adding context for data consumers such as doctors and government officials.

Healthcare professionals can access patient data through medical record systems at their facilities and update records. While healthcare support institutions, like pharmaceutical companies, receive summarized data from healthcare facilities to evaluate drug effectiveness or market demand, supported by data from their supply chain management. Research institutions can also access healthcare data through the ecosystem. These stakeholders can also gather insights on drug performance from physician reviews and patient medical records. Finally, both local and national government (i.e., Ministry of Health) collect aggregated data from various sources, including healthcare facilities, BPJS, and local governments, to inform national health policies, oversee healthcare system performance, and guide resource allocation.

There is a risk that patient data could be accessed and used without consent, leading to privacy breaches and unauthorized use of sensitive health information (Belfrage et al., 2022). This could impact patient trust in the healthcare system. On the other hand, if patients have excessive control over their health data it might cause fragmentation of data in healthcare ecosystem, where healthcare providers might not be able to access critical information needed for optimal care delivery. For example, if a patient restricts access to previous diagnoses or treatments, it could hinder continuity of care and lead to redundant testing or treatment delays (Blumenthal & Squires, 2015). In both scenarios, it is crucial to find balance. Tapuria et al. (2021) showed that if there is a balance between patient and medical workers in accessing patient health data, not only it will increase the relationship between patient and medical workers, but also the health output will improve since patient will be more aware and involved in the healthcare system.

Based on the analysis on stakeholders, stakeholder interaction, and data flow, it is found that data sharing is a key activity in this ecosystem, with patient data being the key resource needed by other healthcare stakeholders. From Figure 4.1., it can be seen that most data sharing utilizes healthcare facilities as an intermediary. SSI has the potential to bypass the need for intermediary and allows third parties to connect directly with patient, providing patient with more authority over their data. Therefore, to ensure relevance of SSI implementation in this study, there are three SSI roles that will be assigned to illustrate real-world interaction, as presented in Table 4.2

Table 4.2 Selected stakeholders in this study

SSI role	Stakeholder
Issuer	Hospital
Holder	Patient
Verifier	Research Institution

Hospital will act as the issuer of health credentials, patient as the holder, and research institution as a verifier. The selection of research institution as a verifier is based on the consideration that they have a much higher interest in accessing patient data, instead of patient's interest in allowing data access. This is different when compared to a new hospital/clinic requesting patient's old medical records to continue their treatment, where patient's interest in receiving treatment outweighs their preference to protect their data. This arrangement allows respondents to freely decide whether to take part in the data sharing request.

4.1.3. Implementable context scenario: Underreporting of socially stigmatized diseases in Indonesia

One contextual problem that might benefit from data sharing between patient and a research institution is studying the coinfection disease within a population, which is hindered by insufficient data. The more data points are available within a health data ecosystem, the better the quality and accuracy of analysis conducted by stakeholders, and the better healthcare programs can be designed in a country. The first step for a patient to participate in the health data ecosystem is by taking a diagnostics test, whether based on doctor recommendation or personal will. Problem arises when patients are reluctant to even take the tests, ignore their symptoms, and pretend that they are not sick. However, by not taking the test and not knowing their real condition, they put other people at risk of contagion and epidemics. A recent example for this situation is the COVID-19 pandemic, where people avoid getting tested because they do not want to be put under the government tracking system. This is an experience relevant to individuals with socially stigmatized diseases, such as those with HIV/AIDS or TB.

Indonesia has an estimated HIV prevalence of approximately 0.3% (~800,000 individuals), the majority of People Living with HIV (PLWH) belongs to the 25-49 years age group, and youth below the age of 19 account for 5.8% of them (WHO, 2017). In 2020, only 64% of PLWH knew their status; only 34% of those positive were on ARV, and 17% of those on ARV were virally suppressed (Jocelyn et al., 2024). Indonesia is still far from UNAIDS 95-95-95 target, meaning that 95% of PLWH know their HIV status, 95% of people who knows their status are on antiretroviral (ARV) drugs, and 95% of those on ARV have suppressed viral loads. PLWH are also at risk of co-

infection, particularly TB-HIV (WHO, 2017). This situation presents a challenging public health problem to Indonesian government, particularly considering the risk of underreporting of HIV/AIDS and TB (Ministry of Health Indonesia, 2022). Significant implications of underreported cases include mismatch between real condition and resource allocation, ineffective epidemiological surveillance in monitoring the spread of disease, and delayed treatment.

The Indonesian government has launched initiatives such as free voluntary HIV testing in primary health centers, providing ARV free of charge under the BPJS-JKN scheme, and engaging communities in reaching out to vulnerable population. However, most people are still reluctant to take the test due to fear of being stigmatized. Having an HIV-positive label puts people at a disadvantage, from difficulties in finding jobs, applying for school, or even in traveling. Therefore, most PLWH prefer to keep their status as a secret, prompting the stakeholders within health data ecosystem to take extra measures in dealing with their data. It is important to incorporate the insights of people with socially stigmatized diseases into the development of the SSI features. Designing for those who are extremely cautious and aware of their data would provide extra measures for population at large. The inclusion of individuals with socially stigmatized disease adds another dimension to a patient's holder role in an SSI system, especially for patients that are extremely concerned about access and usage of their data.

4.1.4. Summary on environment analysis

This section summarizes DSR step 1: problem identification. Multiple stakeholders are identified: patient, healthcare facilities, healthcare professionals, healthcare financing institutions, healthcare support, and the government. Each stakeholder has a different interest and different extent of influence within the ecosystem, but in general all stakeholders would like to improve the quality of healthcare provided by the system while maintaining cost-efficiency and profitability of their operations. Patients first participate in the data ecosystem by taking diagnostic tests and submitting them to healthcare facilities and providers as the primary data touchpoint. Data is stored separately by each facility, but it can be shared between stakeholders for different purposes: for government to develop healthcare policy, for healthcare support companies to guide their R&D efforts, and for healthcare financing institutions to design their policy coverage and premiums.

From desk research, it is found that there is problem of underreporting among individuals with socially stigmatized diseases, particularly those with HIV/AIDS and TB in Indonesia. Their reluctance to take voluntary testing and disclosing their status put the population at risk and preventing the government to intervene optimally in the spread of the disease. This signifies a need for the development of a technology that could provide individuals with control over their data and allowing them to retain their personal data sovereignty, which might increase their willingness to participate in the health data ecosystem. This study proposes SSI as the solution to the problem, as it hands back the control of data into the hands of the user.

4.2. Requirements engineering

The environmental analysis has identified the importance of data sharing in HDE and its context, providing input to the requirements engineering step. This study will focus on requirements on the interface layer of an SSI that can accommodate data sharing between stakeholders. This section covers two stages of requirements engineering approach: requirement elicitation and requirement analysis. Requirement elicitation includes gathering and identifying requirements from stakeholders, users, and other sources to understand what the system should do (Boulanger, 2016). The result of environment analysis is discussed and being taken into consideration, where the context of LMIC will be included to elicit requirements. Elicitation process is then followed by analysis, where the gathered requirements are examined and refined. This process involves prioritizing requirements and resolving conflicts or ambiguities.

Figure 4.2 depicted the focus of requirements engineering process, which is the interface layer of an SSI, specifically from the perspective of an individual user as a holder. As a holder, a user receives a Verifiable Credential (VC) issued by an issuer, and when dealing with verifier, the holder can adjust the information within a VC and create a Verifiable Presentation (VP). There are two key activities that can be done by the holder: (1) requesting VC to issuer, and (2) creating VP from a VC. For each interaction between issuer, holder, and verifier, they will interact with the verifiable data registry to issue, update, and check the validity and authenticity of the VC/VP.

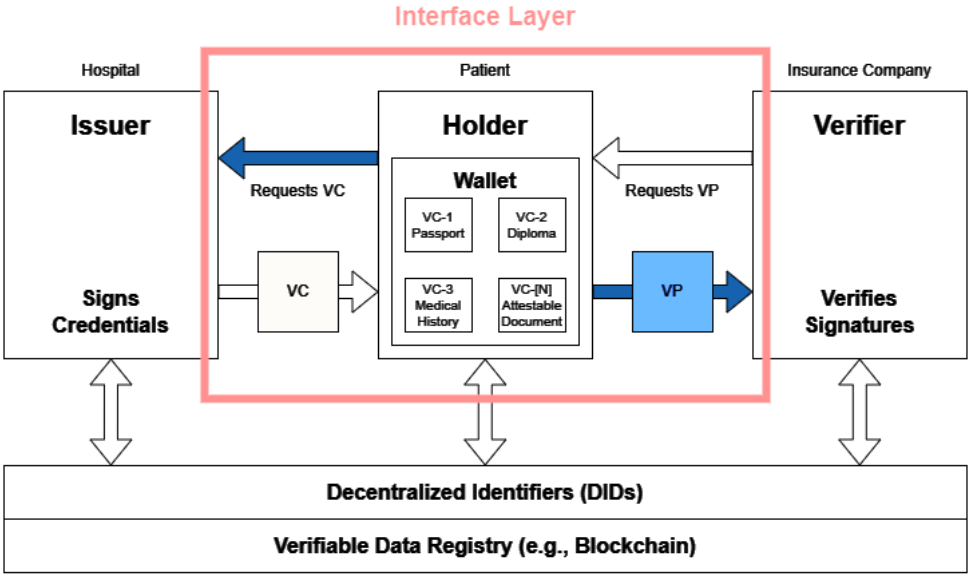

Figure 4.2 Interface layer as focus of requirements engineering process

4.2.1 Requirement elicitation and analysis

Requirement elicitation process is divided into three: (1) a systematic literature review to identify requirements associated with SSI and personal data sovereignty (PDS), (2) analyzing existing ID e-wallets, and (3) identifying and analyzing possible SSI scenarios. Before proceeding to the literature search, main keywords for SSI and PDS are identified to generate a more focused search result. The steps for literature search are as follows:

- Identification of main keywords and synonyms of requirements for the following themes: personal data sovereignty, self-sovereign identity, and data sharing in LMIC. To generate studies relevant for the interface layer, the following terms are used: design pattern OR user interface OR components OR functionalities
- Input search strings into research repositories, such as Google Scholar, IEEE, and Scopus, to find a list of potential journals as requirement references
- Forward and backward snowballing are also implemented, which covers finding other works that reference the document (forward snowballing), and reviewing references in a document (backward snowballing)

Results are filtered using the inclusion and exclusion criteria summarized in Table 4.3.

Table 4.3 Inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Paper Publication Date	Papers published after 2018. The term for self-sovereign identity was coined first by Christopher Allen (2016), but the traction of research began by Muhle (2018)	Papers published before the year 2018 (except for the formal definition stated in the original research that might date back to earlier years)
Language	English	Languages other than English
Type of Publication	- Scientific articles with published results with relevance of study - International standard on technical specification or documentation of SSI	Websites, news articles, blogs
Setting / Study Design	Papers with implementation cases on the interface layer and functionalities, design science	Papers with a focus on technical requirements, system/IT architecture, and implementation

	research, or specifically discuss requirements	

After sources for requirement elicitation are identified, the results will be analyzed, examined, and refined. Afterwards, a table of requirements specification is constructed.

4.2.1.1 Identification of Personal Data Sovereignty (PDS) values

As discussed in the sections 2.2 and 2.2.1, the two key PDS values that will be used as main keywords in the literature search are 'control' and 'ownership'.

Table 4.4. summarizes the search results on PDS requirements.

Table 4.4 Search terms used for requirement search on PDS

Search Term	Synonym	Relevance	Search String	Result
Data Sovereignty Control	Information control, Data stewardship	Putting the requirements of data control in the context of data sovereignty	("concern" OR "requirement" OR "conceptualization") AND "data sovereignty" AND ("control" OR "power") AND ("information system" OR "software") Or using ("design pattern" OR "user interface" OR "user requirement" OR "functional requirement" OR "design requirement" OR "visualization") AND ("data control" OR "information control") AND ("data sovereignty")	6.150
Data Sovereignty Ownership	Data proprietorship, Information Ownership	Putting the requirements of data ownership in the context of data sovereignty	"property" AND "Data ownership" AND "recognition" AND "rights" Or using ("design pattern" OR "user interface" OR "user requirement" OR "functional requirement" OR "design requirement" OR "visualization") AND ("data control" OR "information control") AND ("data sovereignty")	7.210

The search results were filtered according to the exclusion and inclusion criteria, and after a review of the sources, the final references for PDS requirements are summarized in Table 4.5.

Table 4.5 Final references for PDS requirements

Search Term	Inclusion and exclusion result	Key literatures
Data Sovereignty Control	9	1. Von Scherenberg, F., Hellmeier, M., & Otto, B. (n.d.). Data Sovereignty in Information Systems. *EM*, *34*(1). https://doi.org/10.1007/s12525-024-00693-4 2. Jarke, M., Otto, B., & Ram, S. (2019). Data Sovereignty and Data Space Ecosystems. Business & Information Systems Engineering, 61(5), 549–550. https://doi.org/10.1007/s12599-019-00614-2 3. Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532 4. Gelhaar, J., Groß, T., & Otto, B. (2021). A Taxonomy for Data Ecosystems. https://doi.org/10.24251/HICSS.2021.739

Search Term	Inclusion and exclusion result	Key literatures
		5. Munoz-Arcentales, A., López-Pernas, S., Pozo, A., Alonso, Á., Salvachúa, J., & Huecas, G. (2019). An Architecture for Providing Data Usage and Access Control in Data Sharing Ecosystems. Procedia Computer Science, 160, 590–597. https://doi.org/10.1016/j.procs.2019.11.042 6. Gil, G., Arnaiz, A., Diez, F. J., & Higuero, M. V. (2020). Evaluation Methodology for Distributed Data Usage Control Solutions. 2020 Global Internet of Things Summit (GIoTS), 1–6. https://doi.org/10.1109/GIOTS49054.2020.9119565 7. Zrenner, J., Möller, F. O., Jung, C., Eitel, A., & Otto, B. (2019). Usage control architecture options for data sovereignty in business ecosystems. Journal of Enterprise Information Management, 32(3), 477–495. https://doi.org/10.1108/JEIM-03-2018-0058 8. Rahul, K., & Banyal, R. K. (2020). Data Life Cycle Management in Big Data Analytics. Procedia Computer Science, 173, 364–371. https://doi.org/10.1016/j.procs.2020.06.042 9. Yang, R., Liu, N., Pang, Z., Wang, Y., Jia, Q., Lu, W., Li, Z., Li, M., & Wu, L. (2021). The next generation identity platform for digital era based on blockchain. Lecture Notes in Electrical Engineering, 677, 1035–1044. https://doi.org/10.1007/978-981-33-4102-9_124
Data Sovereignty Ownership	4	1. Hummel, P., Braun, M., & Dabrock, P. (2021). Own Data? Ethical Reflections on Data Ownership. Philosophy and Technology, 34(3), 545–572. https://doi.org/10.1007/s13347-020-00404-9 2. Loshin, D. (2001). Enterprise Knowledge Management: The Data Quality Approach. Morgan Kaufmann. 3. Fadler, M., & Legner, C. (2022). Data ownership revisited: clarifying data accountabilities in times of big data and analytics. Journal of Business Analytics, 5(1), 123–139. https://doi.org/10.1080/2573234X.2021.1945961 4. Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big Data and Society, 8(1). https://doi.org/10.1177/2053951720982012

4.2.1.1.1 Requirements on Personal Data Sovereignty

Von Scherenberg et al. (2024) developed a conceptual model on how data sovereignty can be achieved based on several information system literature, which can be seen in the Figure 4.3 The model is derived from several definitions from multiple research domains, such as Polatin-Reuben and Wright (2014), which stated that data sovereignty refers to range of approach that is adopted in many states in controlling data generating or passing through national internet infrastructures, or from German Ethics Council (2017) that defined data sovereignty as responsibility to shape the informational freedom in the perspective of opportunity and challenges presented by big data.

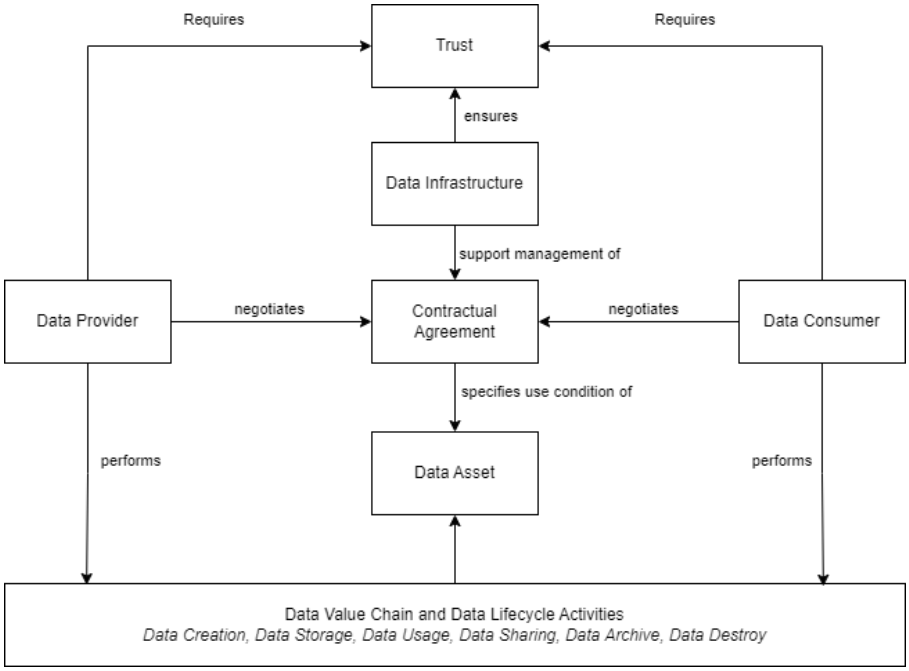

Figure 4.3 Data sovereignty model (von Scherenberg et al., 2024)

Figure 4.3 shows several concepts that are essential in attaining data sovereignty (von Scherenberg et al., 2024). A data asset is the object of data sovereignty in which required control or retention is retained. It may consist of files, databases, data batches, a data warehouse, or an intangible object that can be reproduced repeatedly (Cappiello et al., 2020; Munoz-Arcentales et al., 2019). Data provider, data consumer, and their relation should also be defined in this study. The data provider is an entity, which can be individuals or organizations, that can decide to keep their data private or share it with the public, or even decide to set restricted parties to have access. On the contrary, a data consumer, which also can be an individual or organization, is an entity that is interested in using, creating, deleting, or sharing data assets owned or controlled by the data providers (Gil et al., 2020; Zrenner et al., 2019).

Data value chain and lifecycle activities consist of several processes: creation, storage, usage, sharing, archiving, and destruction. In the implementation of data sovereignty, every individual or organization should be able to control every aspect of the data lifecycle, and it must be listed in the contractual agreement (Banse, 2021). A contractual agreement is a mechanism enforced between the data provider and data consumer so that the data-sharing condition can be monitored and negotiated semi-automatically with the help of data infrastructures, allowing data providers to give or revoke consent if there is a misuse (Jarke et al., 2019). The data infrastructure component enforces the terms and conditions applied to the contractual agreement (Munoz-Arcentales et al., 2019), which acts as a core in the model that bridges the need between the data provider and consumer by validating end execute terms and conditions that have been defined in the contractual agreement. The specification of the contractual agreement should enable the data provider to grant access control (AC) and usage control (UC). Access control is defined as whether a particular entity would be able to access or see specific credentials, while usage control is the extension of control over data before and after it is processed by other actors, explicitly stating the extent of data access and usage. Lastly, while this study does not focus on trust, the conceptual model of data sovereignty requires trust both for the data provider and the data consumer (Peterson et al., 2011).

4.2.1.1.2 Data control requirements

Besides the model that has been introduced, von Scherenberg et al. (2024) also defined how the control should be addressed within the data sovereignty model. At first, a data asset in the object of data sovereignty in which required control or retention is defined (Munoz-Arcentales et al., 2019)). In this study, the data asset will be a VC. The second one is the relation between data provider and data consumer also needs to be defined (Otto et al., 2019), since data provider and data consumer might have different goals then the control should facilitate

for both ends. For example, data provider should be able keep their data or being able to implement strict access for data consumer. Third, ensuring that data providers should be able to control the entire life cycle of the data value chain (Rahul & Banyal, 2020), which include data creation, data storage, data usage, data share, data archive, and data destroy. Fourth, including Access Control (AC) and Usage Control (UC), the extent of the control should be reflected in the contractual agreement, where AC is defined as whether a particular entity would be able to access or see specific credentials, while UC is the extension of control over data after it is accessed by other actors (Gil et al., 2020). Lastly, there is a need to have a contractual agreement between data provider and data consumer to retain and enforce control (Banse, 2021; Zrenner et al., 2019), as the core problem when data sharing between data provider and data consumer is the lack of trust within digital world. The idea of contractual agreement is to establish trust in a data ecosystem (Yang et al., 2021).

4.2.1.1.3 Data Ownership Requirements

Understanding the requirement for data ownership can be seen in multiple dimensions (Fadler & Legner, 2022). Since data are contextual, ownership is hard to define as data cannot be classified as private or public goods (Jentzsch, 2018). However, Hummel, Braun, & Dabrock (2021) have positioned data ownership in four poles: property versus quasi-property, marketability versus inalienability, protection versus participation, and individual versus collective claims and interests. Each dimension has its perspective and expectations. Property versus quasi-property concerns enabling owners to control data flows and impact the outcomes of data processing. This view is aligned with Fadler & Legner (2022), who stated data ownership is a control issue which affects the flow of data, the cost of data, and the value of data. In information system governance, data ownership is controlling rights rather than property. The second dimension - marketability, and inalienability - is more concerned with whether one should be entitled to the benefit of marketing one's data. For example, profiling in targeting advertisements due to the exploitation of one's behaviour data, while at the same time, some people can feel alienated if they do not share their behaviour. Third is the protection versus participation in which data owner could maintain secrecy or privacy while embedding informational terms at their discretion. The last is individual versus collective claims and interests that consider aligning individual needs and common goods. The summary of these dimensions can be seen in Table 4.6

Table 4.6 Perspectives of data ownership (Hummel, Braun, & Dabrock, 2021)

No	Poles	Main Perspective	Claims	Expectations
1	Property—quasi-property	Interplay between individual, rights, and resource	Incidents of (quasi-) property	Control data flows and outcomes of data processing
2	Marketability—inalienability	From the individual to the resource	Freedom whether to market what is mine	Benefit from resource, avoidance of harm from selling core aspects of my self
3	Protection—participation	From the resource to individual constitution, flourishing, and integrity	Protection, participation, inclusion	Maintaining a sphere of secrecy, weaving informational ties at one's own direction
4	Individual—collective	Interplay between individual, others, and resource	Consideration of interest, needs, and preferences	Harmonization between individual and common good

This study believes that ownership requirements do not solely rely on one dimension, but all dimensions should be reflected on the design artifact. The first dimension indicates that to establish one's ownership, the functionalities of design artifact should exhibit control over data flows and the outcomes of data processing. The second dimension of data ownership is out of this study's research scope; since the context of this research is

more on the data sharing nuance, then this study would not provide any insight into how the data owner should be incentivized while sharing their data. The third and fourth dimensions can also be considered in the requirement of data ownership in self-sovereign identity through contractual agreements during the data sharing initiation between the data owner and data consumer.

4.2.1.2 Identification of SSI functionalities in literature

SSI functionalities in the design artifact will correspond to the identified PDS values: control and ownership. The key literature for this section is Schardong and Custodio (2022) that developed a taxonomy on SSI research based on a systematic review of 82 selected works. A simplified version of the taxonomy is presented in Figure 4.5. Based on the taxonomy, this study focuses on the practical aspect of SSI, particularly the operational aspect of an SSI credential that consists of two parts: Verifiable Credential (VC) and Verifiable Presentation (VP). These two components are key to an SSI model and is presented on the interface layer. As this study takes a user-centric approach, the perspective of a patient as a holder will be taken, which leads to focus on the functionalities included under the category of VP: revocation, verifier authorization, data minimization, and reuse prevention. This study does not explore the functionalities under VC category as they belong to the role of issuer.

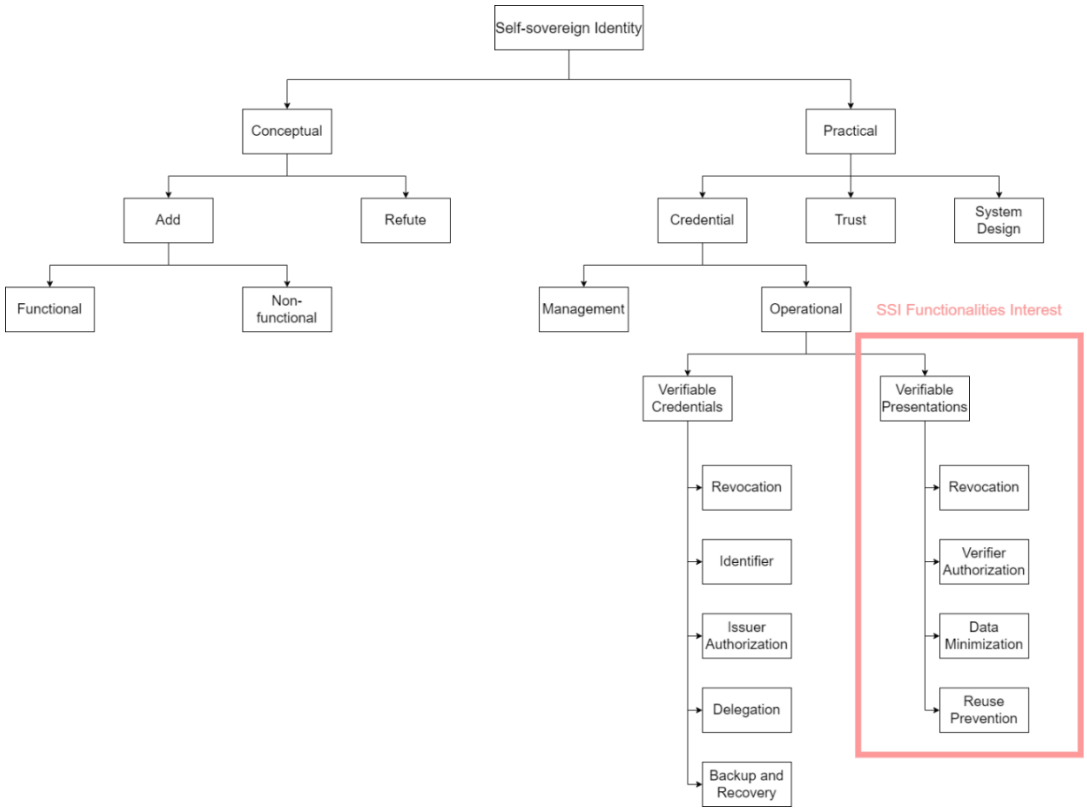

Figure 4.4 Simplified taxonomy model, adapted from Schardong (2022)

Before proceeding to literature search, the definition of each concept is explored and presented in Table 4.5. to check for relevance. Based on relevance of functionalities, only revocation, data minimization, and reuse prevention are used in the search strings.

Table 4.7 Review on VP-related functionalities

Functionality	Description	Relevance to study
Revocation	Process allowing holder to cancel VP access of verifier	**Relevant.** Applicable in the interaction between holder and verifier
Verifier authorization	Provide issuers some control over the credentials they issue by establishing rules	**Not relevant.** Functionality is intended to affect the interaction

	that verifiers must follow to access holders' VPs	between issuer and verifier – not holder
Data minimization	Enable individuals to limit information in their VCs while creating VPs	**Relevant.** Applicable in the interaction between holder and verifier
Reuse prevention	Allow holders to charge relying partners to access their attributes while preventing reuse	**Relevant.** Applicable in the interaction between holder and verifier

Table 4.6. summarizes the search results on SSI requirements.

Table 4.8 Search term used for requirement search on SSI functionalities

Search Term	Synonym	Relevance	Search String	Result
Self-Sovereign Identity	Self-Sovereign Identity properties, components, design pattern	Gathering insight what is the functionality needed in Self-sovereign identity application	("design pattern" OR "user interface" OR "user requirement" OR "functional requirement" OR "design requirement") AND "self sovereign identity"	897
Revocation	Redaction, data cancellation	Collect design principle of how the revocation should work on the interface level	("data retraction" OR "data revocation" OR "data cancellation") AND "Self sovereign identity"	5
Data Minimization	Selective Disclosure, Data Reduction, Data Retention Limitation	To understand the behaviour of data reduction in data sharing	("design pattern" OR "user interface" OR "user requirement" OR "functional requirement" OR "design requirement" OR "visualization") AND ("data minimization" OR "selective disclosure") AND ("self sovereign identity")	258
Reuse prevention	Single-use restriction, usage prevention	Understand the behaviour of reuse prevention interface	("design pattern" OR "user interface" OR "user requirement" OR "functional requirement" OR "design requirement" OR "visualization") AND ("reuse prevention" OR "single use restriction" OR "usage prevention") AND ("self sovereign identity")	1

The search results were filtered according to the exclusion and inclusion criteria, and after a review of the sources, the final references for SSI requirements are summarized in Table 4.7.

Table 4.9 Final references for SSI requirements

Search Term	Inclusion and exclusion result	Key literatures
Self-Sovereign Identity	11	1. Cucko, S., Becirovic, S., Kamisalic, A., Mrdovic, S., & Turkanovic, M. (2022). Towards the Classification of Self-Sovereign Identity Properties. IEEE Access, 10, 88306–88329. https://doi.org/10.1109/ACCESS.2022.3199414 2. Čučko, Š., Šumak, B., & Turkanović, M. (2023). Identification and Analysis of Self-Sovereign Identity User Interface and User Experience Design Patterns. *Proceedings - 2023 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2023*, 166–173. https://doi.org/10.1109/DAPPS57946.2023.00030 3. Design Patterns for Blockchain-based Self-Sovereign Identity 4. Liu, Y., Lu, Q., Paik, H. Y., Xu, X., Chen, S., & Zhu, L. (2020). Design Pattern as a Service for Blockchain-Based Self-Sovereign Identity. *IEEE Software*, *37*(5), 30–36. https://doi.org/10.1109/MS.2020.2992783 5. Lockwood, M. (2021). Exploring value propositions to drive Self-Sovereign Identity adoption. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.611945 6. Lockwood, M. (2021). An Accessible Interface Layer for Self-Sovereign Identity. *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.609101 7. Preukschat, A., & Reed, D. (2021). Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Simon and Schuster. 8. Stokkink, Q., & Pouwelse, J. (2018). Deployment of a Blockchain-Based Self-Sovereign Identity. IEEE. https://doi.org/10.1109/cybermatics_2018.2018.00230 9. *Verifiable Credentials Data Model V1.1*. (2022, March 3). https://www.w3.org/TR/vc-data-model/ 10. Verifiable Credentials Implementation Guidelines 1.0. (2019, September 24). https://www.w3.org/TR/vc-imp-guide/ 11. Guggenberger, T., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). Accept me as I am or see me go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications - Appendix [Dataset]. In *Zenodo (CERN European Organization for Nuclear Research)*. https://doi.org/10.5281/zenodo.7044145
Revocation	5	1. Vidal, F. R., Ivaki, N., & Laranjeiro, N. (2021). Revocation Mechanisms for Blockchain Applications: A Review. *2021 10th Latin-American Symposium on Dependable Computing, LADC 2021 - Proceedings*. https://doi.org/10.1109/LADC53747.2021.9672577 2. Vidal, F. R., Gouveia, F., & Soares, C. (2022). Analysis of revocation mechanisms for blockchain applications and a proposed model based in Self-Sovereign Identity. *DOAJ (DOAJ: Directory of Open Access Journals)*. https://doi.org/10.22059/jitm.2022.87848 3. Lee, Y., Liu, Z., Tso, R., & Tseng, Y. (2022). Blockchain-Based Self-Sovereign Identity System with Attribute-Based Issuance. In Lecture notes in computer science (pp. 21–38). https://doi.org/10.1007/978-3-031-21280-2_2 4. Xu, J., Xue, K., Tian, H., Hong, J., Wei, D. S. L., & Hong, P. (2020). An identity management and authentication scheme based on redactable blockchain for mobile networks. IEEE Transactions on Vehicular Technology, 69(6), 6688–6698. https://doi.org/10.1109/tvt.2020.2986041 5. Čučko, Š., Šumak, B., & Turkanović, M. (2023). Identification and Analysis of Self-Sovereign Identity User Interface and User Experience Design

Search Term	Inclusion and exclusion result	Key literatures
		Patterns. *Proceedings - 2023 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2023*, 166–173. https://doi.org/10.1109/DAPPS57946.2023.00030
Data Minimization	5	1. Teuschel, M., Pöhn, D., Grabatin, M., Dietz, F., Hommel, W., & Alt, F. (2023). 'Don't annoy me with privacy decisions!' — Designing Privacy-Preserving user interfaces for SSI wallets on smartphones. *IEEE Access*, *11*, 131814–131835. https://doi.org/10.1109/access.2023.3334908 2. Mukta, R., Martens, J., Paik, H., Lu, Q., & Kanhere, S. S. (2020). Blockchain-Based Verifiable Credential Sharing with Selective Disclosure. *IEEE*. https://doi.org/10.1109/trustcom50675.2020.00128 3. Ramić, Š. B., Cogo, E., Prazina, I., Cogo, E., Turkanović, M., Mulahasanović, R. T., & Mrdović, S. (2024). Selective disclosure in digital credentials: A review. *ICT Express*. https://doi.org/10.1016/j.icte.2024.05.011 4. Sedlmeir, Johannes; Barbereau, Tom; Huber, Jasmin; Weigl, Linda; and Roth, Tamara, "Transition Pathways towards Design Principles of Self-Sovereign Identity" (2022). *ICIS 2022 Proceedings*. 4. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4 5. Lockwood, M. (2021). Exploring value propositions to drive Self-Sovereign Identity adoption. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.611945
Reuse prevention	1	1. Čučko, Š., Šumak, B., & Turkanović, M. (2023). Identification and Analysis of Self-Sovereign Identity User Interface and User Experience Design Patterns. *Proceedings - 2023 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2023*, 166–173. https://doi.org/10.1109/DAPPS57946.2023.00030

Based on search results, it is found that the functionality 'reuse prevention' has the least number of sources to explore, and all existing works are focused on the technical layer or architecture of the functionality. Therefore, this step excludes 'reuse prevention' from the study. In the upcoming section on SSI requirements, the two functionalities of focus are data minimization and revocation.

4.2.1.2.1 Requirements on Self-Sovereign Identity

There are four key components critical in SSI implementation (Cucko et al., 2022; Teuschel et al., 2023):

- **Decentralized Identifiers (DIDs)** are global, unique, and verifiable digital identifiers that can be generated and used in different digital interactions and are separated from any centralized identity providers
- **Verifiable Credentials (VCs)** act as a medium to show physical credentials or identity in digital format, along with any relevant data or metadata that can be used as proof of tempering and authorship of a credential
- Users can use VCs to create **Verifiable Presentations (VPs)** that can be shared with multiple verifiers by selecting a particular identity or information attributes
- A **digital wallet** is a means for digital identification, authentication, and authorization that enables users to control and manage their digital identities. With this digital wallet, users can request and issue VCs, store and manage DIDs, and distribute VPs

Digital wallet belongs in the interface layer and acts as the platform of interaction between user and their digital credentials. The requirements gathered in this chapter will be translated into the design artifact of a digital ID wallet. The work by Lockwood (2021) highlighted the high-level functionalities that needs to be present in an SSI's interface layer, whereas the works by Čučko et al. (2023) and Liu et al. (2020) which gathered the design

patterns of commercial self-sovereign identity applications in the market. The summary of SSI requirements from the three key literature is presented in Table 4.8.

Table 4.10 Summary of SSI requirements in the interface layer

Title of article	**An accessible interface layer for Self-Sovereign Identity**	**Identification and analysis of Self-Sovereign Identity User Interface and User Experience Design Patterns**	**Design Pattern as a Service for blockchain-based Self-Sovereign Identity**
Author	Lockwood, 2021	Cucko et al, 2022	Liu et al, 2020
Summary of study	Design science research that identifies the domains of interaction and the minimum required objects for SSI engagement	Analyzed 11 digital wallets and extrapolated what features in digital wallets that help users manage and control their personal information	Identification of design patterns deemed critical to SSI application development
Requirements	High-level SSI functionalities: - Manage digital ID or credentials - Support trust network - Manage connection - Facilitate credential exchange and management - Transact with minimal disclosure - Establish boundary control	Design patterns: - VC archive - Extended VC views - Revocation - Notification - Contractual agreement - Review connection - Interaction authentication - Selective disclosure/Data minimization - Transaction duration	Design patterns: DID services: - Update - Revocation Credential services: - Selective content generation - Time-constrained access - Verification

The study also used technical report provided by World Wide Web Consortium (W3C) as a reference, especially on the VC data model and implementation. W3C (2022) have made typical use cases and data model of VP, stating that the VP can be presented by either a holder or a verifier, which might consist of multiple of credentials and have its information selectively disclosed. Other characteristics that need to be considered from Preukschat et al. (2021) are the standard functionalities in the holder digital wallet within SSI system. In general, there are notification for making holder to be fully informed of the with their VC, establishing trusted connection with other roles through secure channel, then receiving, offering, and presenting credentials, which is aligned with Lockwood (2021) high-level requirement of the characteristic from SSI.

4.2.1.2.2 Data Minimization Requirements

Data minimization is one of the SSI functionalities that will be used in this study's design artifact. This functionality allows holder to selectively disclose a subset of information in their VC when sharing (Mukta et al., 2020), resulting in a VP. An example of data minimization can be seen in Figure 4.5, where a holder can share a different set of attributes in their VC with multiple verifiers.

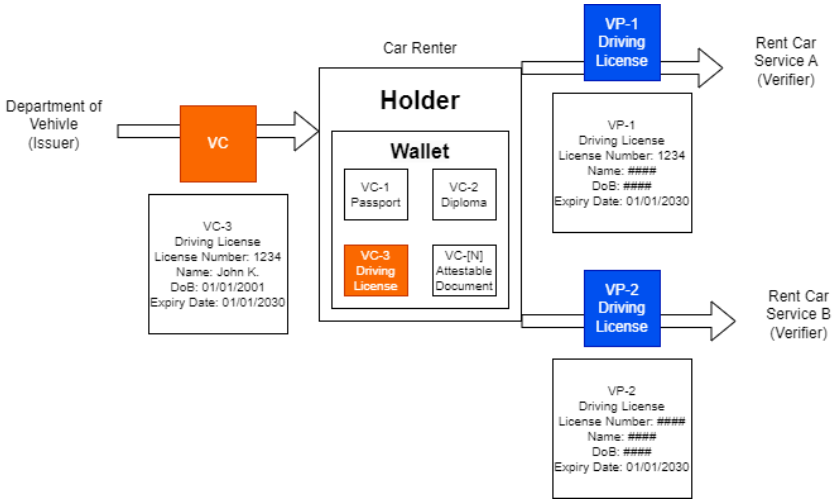

Figure 4.5 Illustration for selective disclosure scheme

There are three techniques to create data minimization in SSI (Mukta et al., 2020). The first one is atomic credentials, which allow holder to create multiple credentials, and each credential will contain only one attribute about the holder. Secondly, hash values, allow the holder to generate general credentials that consist of multiple attributes. However, this attribute is hashed with a different number of once usages. Lastly is the selective disclosure signature, a technique when a generic credential is issued with several attributes on them, the holder can choose to show only specific part that is necessary to the verifier, while the verifier can see the required information and check that the credential is valid (Bauer et al., 2008; Johnson et al., 2002).

Teuschel et al. (2023) conducted design research on SSI wallets for privacy-preserving when sharing identity. The design of Teuschel's research showed three versions; the first one is a no-detail design, where the holder was only presented with the VC that they wanted to share by request of a verifier. However, they could not see which attribute is needed by the verifier. Second is the detailed design, in which holders can see which attribute that the verifier would want to get from the VC. Lastly is the selectable design version where holders can select additional attributes to send to the verifier, while the mandatory attribute cannot be discarded. The screenshot of these designs can be seen on Figure 4.6. This study will utilize selective disclosure signature approach in the creation of design artifact, which allows holder to create numerous VPs with limited information before sharing it with verifier.

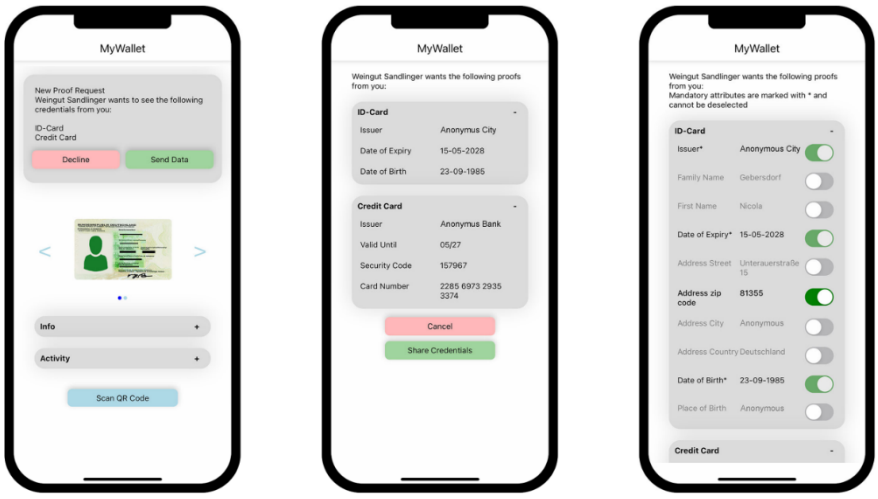

Figure 4.6 Example of interface layer for selective disclosure (data minimization) from Teuschel et al. (2023)

4.2.1.2.3 Revocation Requirements

Vidal et al., (2021) described that revocation in the blockchain is a process where the users are allowed to cancel an ongoing transaction due to many reasons, such as business requests, legislation, or the existence of bugs. Based on such a definition, then this feature would allow holder to cancel their VP to the assigned verifier. Therefore, this section will explore the functionality of how the cancellation should have been implemented in an SSI design artifact.

While conducting desk research for revocation requirements, most of the results lead to the algorithm and methodology of the revocation in various blockchain architectures, leaving minimum results on the user interface of the revocation itself. However, from this search, the study managed to grasp several understandings that can be implemented on the interface level for the SSI digital wallet. Vidal et al., (2022) explained that revocation in a self-sovereign identity model should allow the holder to create control over multiple connections from various data assets, which can also imply the holder should be able to revoke a VP over a particular connection with a specific verifier. The effect of revocation is also aligned with the definition requirement from Hossain et al., (2021) that designed revocation in blockchain to be an admin should be able to grant or revoke access from one to multiple credentials. Based on this definition, the revocation features on this study will be implemented by putting revocation button on every accepted connection between holder and verifier.

4.2.1.2.4 Updated conceptual framework based on SSI requirements

Through data minimization and revocation, SSI promised users that they could have full control over their data and personally identifiable information, that is by limiting the information when shared and retracting the data. All these functionalities are present in the digital wallet where users can interact with the incoming data sharing request from verifier through the usage of VC and VP. Subsequently, based on the selection functionalities, the initial conceptual model introduced in Chapter 2 is updated, presented in Figure 4.7. This research intends to explore how data minimization and data revocation as SSI functionalities influences the values of control and ownership in a user's PDS.

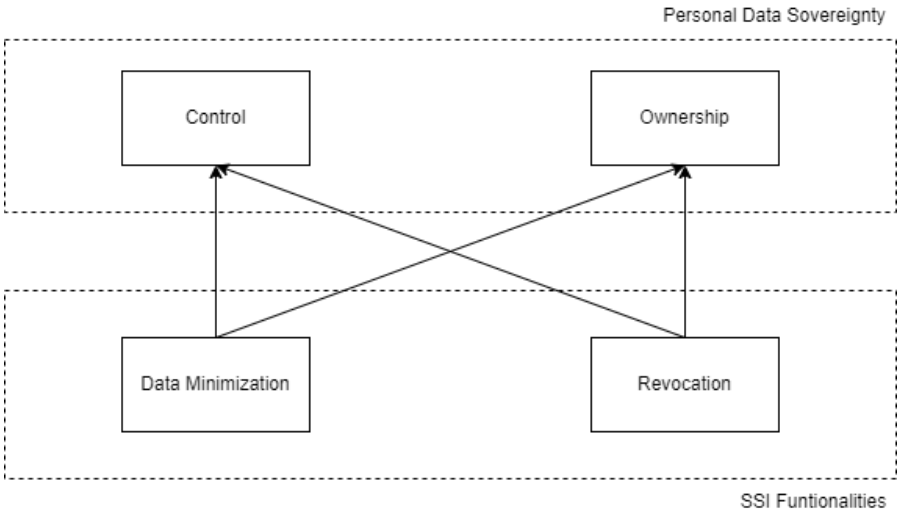

Figure 4.7 Updated conceptual framework

4.2.1.3 Requirements of data sharing in Low- and Middle- Income Countries

SSI is a novel concept that is still in its early adaptation phase, and there is still a limited number of works focusing on SSI in the context of LMIC. This study raises the possibility that holders in LMIC might have a different perspective or requirements when they are faced with data sharing situations, particularly health data. This is also amplified by the fact that the socio-demographic profile in LMIC is different to one in the High-Income Countries (HIC). Some challenges identified in LMIC include low data literacy and limited resources in human capital and infrastructure (Mahmood et al., 2023), which puts more emphasis to the user-friendliness and relevance of an interface layer of a technology. Through literature search, similarities and differences between

people in LMIC and HIC in the context of data sharing are identified and discussed. Table 4.9. summarizes the search terms used for requirement search on data sharing in LMIC.

Table 4.11 Search terms used for requirement search on data sharing in LMIC

Search Term	Synonym	Relevance	Search String	Result
Data sharing in LMIC preferences	Data sharing willingness, preferences, health data sharing, in low middle income countries, in low resource countries	To understand the data sharing practice that would fit with the context of people in low middle income countries	("concern" OR "requirements" OR "consumer preferences") AND "data sharing" AND "low middle income countries" AND "health"	860

The search results were filtered according to the exclusion and inclusion criteria, and after a review of the sources, the final references for SSI requirements are summarized in Table 4.10.

Table 4.12 Final references for LMIC requirements

Search Term	Inclusion and exclusion result	Key literatures
Data sharing in LMIC preferences	7	1. Dhopeshwarkar, R. V., Kern, L. M., O'Donnell, H. C., Edwards, A. M., & Kaushal, R. (n.d.). Health Care Consumers' Preferences Around Health Information Exchange. *The Annals of Family Medicine*, *10*(5), 428–434. https://doi.org/10.1370/afm.1396 2. Howe, analN., Giles, E., Newbury-Birch, D., & McColl, E. (2018). Systematic review of participants' attitudes towards data sharing: A thematic synthesis. In Journal of Health Services Research and Policy (Vol. 23, Issue 2, pp. 123–133). SAGE Publications Ltd. https://doi.org/10.1177/1355819617751555 3. Tiffin, N., George, A., & Lefevre, A. E. (2019). How to use relevant data for maximal benefit with minimal risk: Digital health data governance to protect vulnerable populations in low-income and middle-income countries. BMJ Global Health, 4(2). https://doi.org/10.1136/bmjgh-2019-001395 4. Hussein, R., Griffin, A. C., Pichon, A., & Oldenburg, J. (2023). A guiding framework for creating a comprehensive strategy for mHealth data sharing, privacy, and governance in low- and middle-income countries (LMICs). In Journal of the American Medical Informatics Association (Vol. 30, Issue 4, pp. 787–794). Oxford University Press. https://doi.org/10.1093/jamia/ocac198 5. Kalkman, S., Van Delden, J., Banerjee, A., Tyl, B., Mostert, M., & Van Thiel, G. (2022). Patients' and public views and attitudes towards the sharing of health data for research: A narrative review of the empirical evidence. Journal of Medical Ethics, 48(1), 3–13. https://doi.org/10.1136/medethics-2019-105651 6. Moon, L. A. (2017). Factors influencing health data sharing preferences of consumers: A critical review. In

		Health Policy and Technology (Vol. 6, Issue 2, pp. 169–187). Elsevier B.V. https://doi.org/10.1016/j.hlpt.2017.01.001 Bull, S., Cheah, P. Y., Denny, S., Jao, I., Marsh, V., Merson, L., Shah More, N., Nhan, L. N. T., Osrin, D., Tangseefa, D., Wassenaar, D., & Parker, M. (2015). Best Practices for Ethical Sharing of Individual-Level Health Research Data from Low- and Middle-Income Settings. Journal of Empirical Research on Human Research Ethics, 10(3), 302–313. https://doi.org/10.1177/1556264615594606

The similarities between LMIC and HIC populations in dealing with data sharing include: (1) requirement of trust and security, (2) legitimate agreement process, (3) provision of control over data, and (4) transparency. In terms of trust and security, both LMIC and HIC population requires trust to the entity that will receive their data and demands for protection of their data from unauthorized access or usage (Howe et al., 2018). In terms of agreement process, both LMIC and HIC population emphasized the need to agree to data sharing and ensuring that the agreement process is ethical (Tiffin et al., 2019). In terms of control over data, both groups stressed the need to be able to control the data. In LMIC, most users require a clear guidance on what aspects they could control their data, whereas in HIC they prefer to have control over data access and options of boundaries that can be implemented (Dhopeshwarkar et al., 2012). In terms of transparency, both groups emphasized the need for transparency, including in data sharing for secondary purposes, and the provision of historical data access and audit traces (Hussein et al., 2023).

The differences between LMIC and HIC populations in dealing with data sharing include: (1) motivation to share data and expected benefit, (2) comfort with different types of Health Information Exchange (HIE) models, (3) fear and concern, and (4) legal framework and policy. In terms of motivation to share data and the expected benefit, stakeholders in LMIC emphasized the need for data sharing to improve equality, with a strong focus on practical benefits for community. In HIC, users are motivated by altruism, with a strong emphasis on clinical research results and improved healthcare outcomes (Kalkman et al., 2022). In terms of comfort with different types of HIE models, HIC population are comfortable with various models of HIE including portable devices and prefer this to a centralized database. In LMIC, there is no specific preference on HIE models (Moon, 2017). In terms of fear and concern, LMIC population emphasized the need to minimize harm and ensure that data sharing practices do not lead to exploitation or stigma. HIC population has a broader set of concerns that include fear of data privacy, privacy breach, data misuse, and implication of authorized access such as discrimination and denial of services. In terms of legal framework and policy, LMIC still lags behind HIC, which still discusses the codification of data-related rights and ensuring fair benefit from data sharing. In HIC, legal frameworks have combined mature legal structure and policies such as Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), with ongoing refinements that keep up with technological advancements (Bull et al., 2015).

Based on the discussion, it is found that there is an insignificant difference to the implementation of SSI as both populations in LMIC and HIC requires transparency, consent, control over data, and trust. This study will also focus on the aspect of fear and concern of users, as it is found that LMIC population is more concerned with data misuse and stigma that might result from their health data. This will be included in the consideration of design artifacts through scenario building in Chapter 5.

4.2.1.4 SSI functionalities in existing digital ID wallets

This study also uses existing identity wallets in the market as references for the design artifact. The study used list of existing wallets from Čučko et al (2023), which consist of 11 available digital identity wallets, which can be seen in the appendix A as references. The list also includes 29 identified functionalities out of all the wallets. From that list, scoring system that measure which wallet with the most complete functionalities is shown. Sorting the highest score, the wallet with the most complete functionalities are Esatus wallet (esatus.com) and Trinsic wallet (lissi.id) which has 69% score, followed by Connect.me wallet with 59% score, and Lissli wallet with 55%

score. However, Connect.me wallet sources are unavailable during this study, thus prompting the selection of another reference. Besides the completeness of the functionalities, the study also wants to select wallets with similar identified functionalities, such as selective disclosure. The list pointed out that there are several other wallets that has such functionalities such as Jolocom smart wallet, with 41% completeness, Indisi wallet, 45% completeness, and Talao wallet, with 41% completeness. However, Jolocom smart wallet and Indisi wallet resources also unavailable for access which only allow the study to look at Talao wallet. This leads to the final list of references: Esatus wallet, Lissi wallet, Trinsic wallet, and Talao wallet.

The general flow or phase from using the application during data sharing can be seen in Figure 4.8.

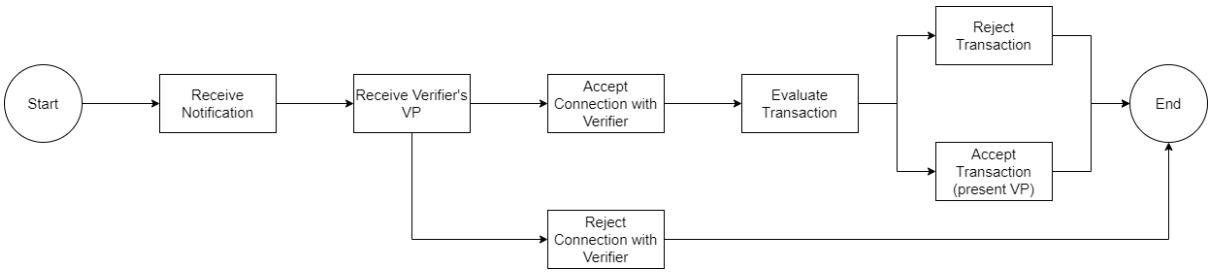

Figure 4.8 General SSI wallet flow from the references (source: Preukschat et al., 2021)

Initially, SSI wallet will give notification for the holder regarding the income event that relates to a particular VC, either receiving or presenting a credential. Then the holder will proceed to receive a VP from verifier regarding their identity, where a holder can assess whether such verifier is trustworthy before they can get an access to their one of the credentials. If the holder rejects data sharing connection request, then the interaction ends. While if a holder accepts, then the holder will have to consider the data sharing transaction. At this point, the data holder will be shown the list of requested credentials along with the data that the verifier asks for, then data holder can decide whether to accept the request or not.

Looking for data minimization references from the existing SSI wallets, the study is using Trinsic wallet and Talao wallet for the overall functionalities in the interface layer. Both applications follow the same function as mentioned by Mukta et al. (2020), where data holder will be shown a list of attributes from a credential, and they can select or deselect attribute that will be shared to the verifier. Illustration of the data minimization can be seen on Figure 4.9 when the selecting or deselecting activity can be represented with a checklist interface or toggle switch during the request review.

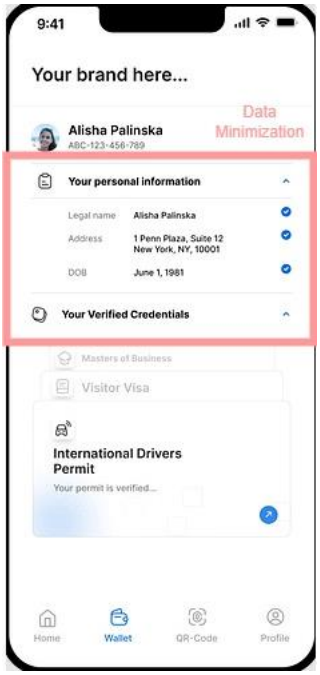

Figure 4.9 Screenshot of data minimization functionality in Trinsic wallet

With regard to data revocation, this study has not found any references or existing wallets in the market with functionality to revoke a credential. However, the study will follow with the literature review where a revocation credential, especially for VPs, can be done in a blockchain-based technology such as SSI that incorporates smart contracts (Lee et al., 2022). This approach is designed because the process of revocation should be tamper-proof in maintaining its validity to the blockchain network. The requirement of data revocation functionality that requires a smart contract is aligned with the data sovereignty model from von Scherenberg et al. (2024), which requires data provider (holder in SSI) to negotiate the contractual agreement for the usage of their data with data consumer (verifier in SSI).

Based on this benchmarking process, the additional requirements that will be added to the design artifact are:

1. Overall artifact functionality flow, which is depicted in Figure 4.8
2. A data minimization functionality interface that uses checklist or toggle switch for selecting data to be shared, and
3. A contractual agreement that accompanied the revocation request

4.2.1.5 Role-changing scenarios for stakeholders within SSI in healthcare

The key proposition of SSI is that users as data holder holds full control over their data, allowing them to grant access and retract access from third parties. In general, there are three types of interaction within SSI (also considering their roles in data ecosystem): (1) between Issuer and Data Provider (Holder), (2) between Issuer and Data Consumer (Holder), (3) between Data Consumer (Holder) and Data Provider (Verifier), (4) between Data Provider (Verifier) and Issuer, (5) between Data Provider (Holder) and Data Consumer (Verifier), and (6) between Data Consumer (Verifier) and Issuer. This implies that user could experience multiple roles during interaction within an SSI, as illustrated in Figure 4.10.

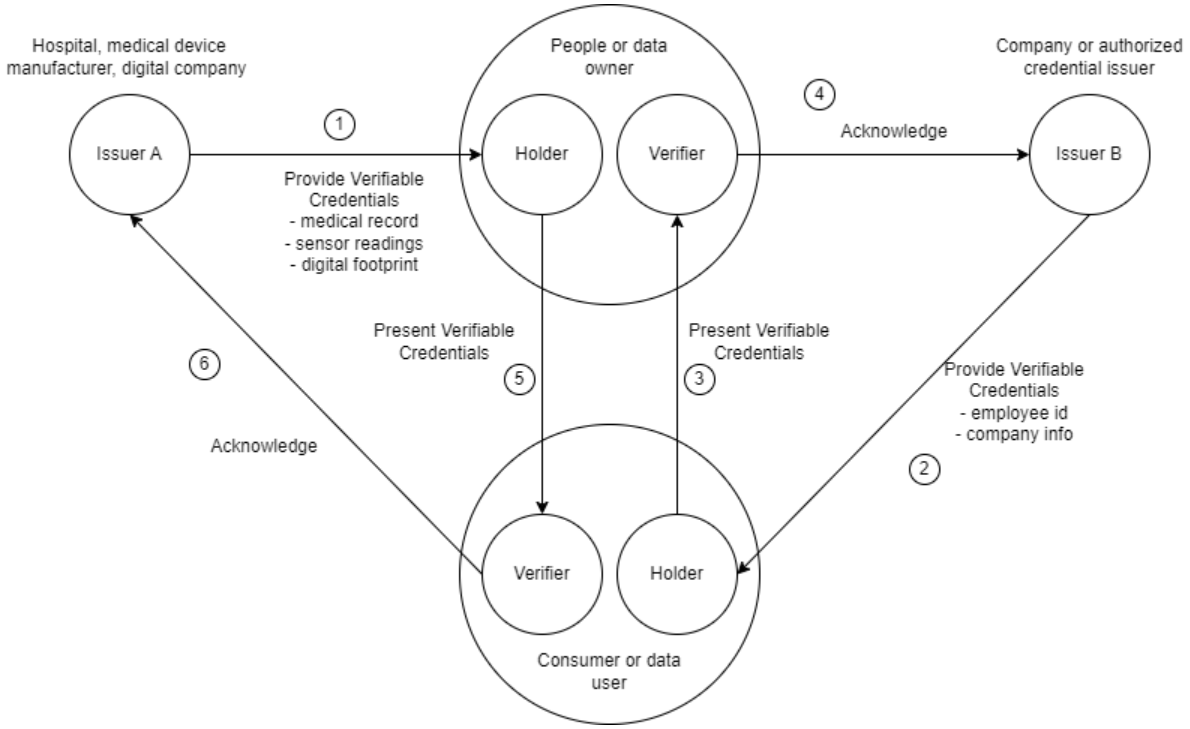

Figure 4.10 Dynamic self-sovereign identity Interaction in health data ecosystem.

In a siloed health data ecosystem, there can be multiple Verifiable Credentials (VCs) associated with the identity data of individuals, generated by organizations or hospitals (Step 1). In this situation, a patient's role in SSI is a holder of the VC, and a data owner from the HDE perspective. In Step 2, another issuer might grant a VC to a different entity, allowing them to participate in the data ecosystem, for example a company that issues VC of a research institution, which will act as a data consumer. When the research institution seeks access to personal data, such as medical records or digital footprints, they adopt the VC holder role within the SSI framework by presenting their VC to a patient, which now acts as a verifier (Step 3). Upon recognizing the data consumer's VC (Step 4), the data owner grants access (Step 5), inverting their roles—the data consumer becomes the verifier, scrutinizing the data's legitimacy as issued by a specific hospital or company (Step 6).

Table 4.13 summarizes all possible SSI roles for the identified stakeholders in the healthcare ecosystem, based on scenarios.

Table 4.13 Possible SSI roles for stakeholders in healthcare system

No	Stakeholder category	Stakeholder name	Possible Roles in SSI	Scenario
1	Patient	Patient	Verifier	When a patient receives a VC from other stakeholders for data sharing request
			Issuer	Not Applicable
			Holder	When a patient receives a VC of medical record or other health data from hospital
2	Healthcare facilities	Hospital	Verifier	When they need to check VC of insurance validity
			Issuer	When they make a VC of medical record or health data
			Holder	When they receive a VC about accreditation
		Clinical laboratory	Verifier	When they need to check VC of insurance claim
			Issuer	When they make a VC of medical record or health data
			Holder	When they receive a VC about accreditation

No	Stakeholder category	Stakeholder name	Possible Roles in SSI	Scenario
3	Healthcare professionals	Doctor	Verifier	When they receive a VC from other stakeholder for data sharing / medical treatment
			Issuer	Not Applicable
			Holder	When a doctor receives a VC of the medical practice in hospital
		Nurse	Verifier	When they receive a VC from other stakeholder for data sharing / medical treatment
			Issuer	Not Applicable
			Holder	When a nurse receives a VC of the medical practice in hospital
4	Healthcare financing	Social Security Agency of Health (BPJS-JKN)	Verifier	When they need to check VC of insurance claim
			Issuer	When they create a VC of insurance card
			Holder	When they receive audit status from the Audit board of Indonesia
		Private insurance	Verifier	When they need to check VC of insurance claim
			Issuer	When they create a VC of insurance card
			Holder	When they receive accreditation VC from financial authority
5	Healthcare support	Pharmaceuticals company	Verifier	When they need to check patient's VC of eligibility to participate in clinical trials
			Issuer	When they issue employment certificates to their salespeople
			Holder	When they receive a VC of accreditation of their drug safety
6	Government	Ministry of health	Verifier	When they need to check a VC from individuals for public health programs
			Issuer	When they issue accreditation VC for healthcare facilities
			Holder	When they receive mandates from President
		Local government	Verifier	When they need to check a VC from individuals for public health programs
			Issuer	When they issue accreditation VC for local community health centers
			Holder	When they receive accreditation from central government

From the table, it is found that individuals such as patient, doctors, and nurses, are not able to uphold the role of issuer as VC issuance can only be done by an entity that has an established credibility and authority, with a well-equipped technical infrastructure that is secure. Individuals generally lack formal authority and institutional backing to authenticate information that others would accept as reliable. The value of a VC relies heavily on the trustworthiness of the issuer, which is recognized to accurately verify and maintain information. Therefore, the requirements of the design artifact will consider an individual user's two possible SSI roles: holder and verifier.

4.3. Requirements specification

This step presents the documentation of requirements in a structured format that serves as a basis for design and development. Table 4.14. summarizes the requirements specification for the next design cycle.

Table 4.14 Summary of requirements specification

No	Elicitation components	Description	Analysis Link	Reference source
1	Key stakeholder	Design artifact needs to accommodate patient as an individual user	Used for scenario development in 5.1	Section 4.1.1
2	Key context	Data sharing in health data ecosystem	Used for scenario development in 5.1	Section 4.1.2
3	Role-shifting scenario	Design artifact needs to consider the role-shifting possibilities	Used for scenario development in 5.1	Section 4.2.1.5
		Roles in data ecosystem:		
		- Data provider		
		- Data consumer		
		Roles in SSI:		
		- Holder		
		- Verifier		
4	Highlighted healthcare issue in Indonesia	Design artifact needs to accommodate users with socially stigmatized diseases	Used for scenario development in 5.1	Section 4.1.3
5	PDS values	Design artifact should uphold ownership and control	Used for conceptual framework development in 4.2.1.2.4	Section 2.2.1
6	Data control requirements	Design artifact should consider the following aspects:		Section 4.2.1.1.2
		1. Identification of data asset as object of data sovereignty	Used in specification 8, in high level functionality 1 and 4, and design pattern 1 and 2	
		2. Identification of data provider and data customer, alongside their relation	Used in specification 8, in high level functionality 2 and design pattern 4 and 6	
		3. Ensuring data provider can control the entire life cycle of data value chain	Used in specification 8, in high level functionality 2, 3 and 6, and design pattern 3 and 8	
		4. Ensuring data provider and data consumer can negotiate	Used in specification 8, in high level functionality 3 and 5, and design pattern 5 and 7 and 9	
		5. Contractual agreement	Used in specification 8, in high level functionality 3 and 5, and design pattern 5 and 7 and 9	
7	Data ownership requirements	Design artifact should consider the following aspects:		Section 4.2.1.1.3
		Can reflect the following poles of data ownership:		
		1. Exhibiting control over data flows and outcomes of data processing	Used in specification 8, in high level functionality 3 and 5, and design pattern 5 and 7 and 9	

No	Elicitation components	Description	Analysis Link	Reference source
		2. Allowing the maintenance of a sphere of secrecy and protect one's information	Used in specification 8, in high level functionality 3 and 5, and design pattern 5 and 7 and 9	
		3. Enabling the harmonization between data as individual and common good	Used in specification 8, in high level functionality 3 and 5, and design pattern 5 and 7 and 9	
8	Requirement of SSI	Design artifact is presented in the form of a digital ID wallet	Used in 5.1	Section 4.2.1.2.1
		Design artifact incorporates **high-level SSI functionalities**:		
		1. Manage digital identities or credentials	Used in design pattern 1,2 and 3	
		2. Manage connection	Used in design pattern 6, 7, 10, and 3	
		3. Establish boundary control	Used in design pattern 5 and 9	
		4. Support trust network	Used in design pattern 4 and 5	
		5. Facilitate credential exchange and management	Used in design pattern 11 and 3	
		6. Transact data with minimal disclosure	Used in design pattern 8	
		Design artifact incorporates the following **design patterns**:		
		1. VC archive	Used for home screen in 5.3.2	
		2. Extended VC views	Used for credential details screen in 5.3.3	
		3. Revocation	Used for credential details screen in 5.3.3, review request screen in 5.3.6	
		4. Notification	Used for notification and notification menu detail screen in 5.3.1	
		5. Contractual agreement	Used for review request screen in 5.3.6, and renegotiate screen in 5.3.7, and notification menu detail screen in 5.3.1	
		6. Review connection	Used for connection details screen in 5.3.4	
		7. Interaction authentication	Used for connection details screen in 5.3.4, and review request screen in 5.3.6	
		8. Data minimization/Selective disclosure	Used for review request screen in 5.3.6	
		9. Transaction duration	Used for renegotiate screen in 5.3.7	
		10. Connection list	Used for home screen in 5.3.2	

No	Elicitation components	Description	Analysis Link	Reference source
		11. Review presentation	Used for review request screen in Interface layer 6: Review request5.3.6	
9	SSI functionalities	Design artifact focuses on the corresponding SSI functionalities:		Section 4.2.1.2
		Data minimization	Used for conceptual framework development in 4.2.1.2.4	
		Revocation	Used for conceptual framework development in 4.2.1.2.4	
9	Data minimization requirement	Design artifact implements selective disclosure approach	Used in specification 8, in high level functionality 6, and in design pattern 8	Section 4.2.1.2.2
10	Revocation requirement	Design artifact implements revocation button on every accepted connection between holder and verifier	Used in specification 8, in high level functionality 3, and in design pattern 3	Section 4.2.1.2.3
11	Data sharing in LMIC	Design artifact considers the aspects of fear and concern of LMIC users	Used for scenario development in 5.1	Section 4.2.1.3

Table 4.13. maps the components of Requirements of SSI: high-level requirements and design patterns, to be incorporated into the design artifact (highlighted yellow in Table 4.10 no.8).

Table 4.15 High-level requirements for SSI functionalities

High Level Requirement	Design patterns
Manage Digital Identities or Credentials	VC Archive
	Extended VC Views
	Revocation
Support trust network	Notification
	Contractual Agreement
Manage Connection	Review Connection
	Interaction Authentication
	Connection list
	Revocation
Facilitate credential exchange and management	Review Presentation
	Revocation
Transact with minimal disclosure	Selective Disclosure/Data Minimization
Establish Boundary Control	Contractual Agreement
	Transaction Duration

4.4. Summary on Chapter 4 and discussion on Hevner's Relevance Cycle

Chapter 4 summarizes the operationalization of Hevner's relevance cycle, which acts as a starting point to find out the problems and opportunities that can be used to introduce an innovation from Information System application, in this case an implementation of SSI in data-sharing context of an LMIC healthcare ecosystem that can help users to retain their personal data sovereignty. This chapter provides answer to **SRQ1:** *"What are the **requirements** in implementing SSI functionalities on the health data ecosystem to achieve personal data sovereignty for LMIC users?".* Contextual insights were generated in the environment analysis step, followed by requirements engineering approach that sources requirements from various sources, resulting in a list of contextual factors, high-level functionalities, and design patterns that will be translated into a design artifact of a digital ID wallet. The design artifact will accommodate patient as an individual user in the key context of data sharing in health data ecosystem. The design will consider the role-shifting possibilities of user's role within data ecosystem: data provider/data consumer, and roles within SSI: holder/verifier. The highlighted healthcare issue in Indonesia is the presence of individuals with socially stigmatized diseases that needs to be accommodated by SSI. The design artifact will be designed to uphold ownership and control as components of a user's PDS, by focusing on two SSI functionalities: data minimization and revocation.

The functionalities that will be added based on the discovered design pattern are 1) verifiable credential archive, 2) extended verifiable credential views, 3) review credentials, 4) notifications, 5) review connection, 6) review presentation, 7) interaction authentication, 8) data minimization, 9) and revocation. To retain data sovereignty, the data provider should be able to control the data life cycle and value chain; that is, the data provider should be able to control data access and data usage in all phases, such as creation, transformation, and deletion. On the ownership part, the data owner should be able to exercise control of their data and negotiate the usage of the data, implying the need for a contractual agreement during the request or connection initiation between the data provider and the data consumer.

5. Design and Development of SSI Artifact

This chapter implements DSR Step 3, design and development, and provides answer to **SRQ2**: *"What could be the **possible design artifact** that follows the functionality requirements of self-sovereign identity on health data ecosystem to achieve personal data sovereignty for LMIC users?".* Hevner's Design Cycle will also be discussed. The requirements specification developed in Chapter 4 will be used as the starting point for design and development of an SSI design artifact, which prompted the design artifact to be presented in the form of a digital ID wallet. Considering the role-changing scenarios experienced by holder, a scenario will also be developed to reason about design and evaluate the design artifact (Sutcliffe, 2003). The design artifact will be developed using Uizard, a drag-and-drop rapid prototyping tool for interface visualization. The output is a clickable design artifact that will be tested by selected respondents, covered in DSR Step 4 and Step 5 in Chapter 6.

5.1. Scenario development for artifact design

Scenario can be understood as an example of real-world experiences that can illustrate possible sequences of user behavior (Suttcliffe, 2003). In this study, scenarios will be used for reasoning about design and to test design artifact in the evaluation step. The key advantage of scenarios is the focus on reality that forces us to address the 'devil in the detail', which in this study covers the role-shifting condition experienced by a holder within an SSI digital ID wallet.

This study posits that data sharing can be beneficial in the context of co-infection research, which aims to understand how one disease affects another and vice versa. For instance, researching the co-infection of HIV and TB, which prompted WHO's creation of a framework in 2012 to address this issue in the Pacific region. By providing patients with TB and HIV diagnoses for surveillance and monitoring of disease activity in a particular region, we can reduce the number of cases of both diseases. However, sharing sensitive information about HIV test results can cause stigma for the holder, who may not want others to know their situation and affect their willingness to share information.

From such elaboration, the scenario will be described in Table 5.1.

Table 5.1 Scenario elaboration

Overall Scenario	Sharing health data for a health study on co-infection or comorbidities
Entity involved	1. Patient/Data provider/Holder 2. Research institution/Data consumer/Verifier
Location	Indonesia
Story	Research institution based in Indonesia aims to conduct a comprehensive study on the comorbidity patterns among patients with HIV/AIDS and tuberculosis (TB). They hypothesize that the interaction of these two diseases could worsen the health outcomes of affected individuals. Recognizing that the interaction between these diseases may exacerbate health outcomes, the researchers are reaching out to end users—patients who tested positive for either or both diseases.
Request for data access	Birth date Gender Latest TB test result Latest HIV test result

The scenario identified the involvement of two entities: a Patient that has both the role of a data provider and as a VC/VP holder in the SSI context (Patient/Data Provider/Holder), and a Research Institution that has both the role of a data consumer and as a VC/VP verifier. In the design artifact, holder will be able to minimize and revoke

access to data that includes birth date, gender, latest TB test result, and latest HIV test result. To maintain clarity, the roles will be mentioned as Patient and Research Institute in the following sections.

5.2. Task sequences of digital ID wallet usage for data sharing

Figure 5.1 summarizes the task sequences of how a user uses a digital ID wallet when completing the data sharing scenario. The Patient will **(1) Receive a notification** from the Research institute requesting access to their health information contained in VC. The Patient can **(2) Review own VCs** to see their data. Next, (3) a secure **connection will be established** between the two parties to allow for review. After that, the Patient will (4) **Receive and review a request** for specific credentials, where the Patient can view the credentials the Research Institution wants to access, perform data minimization or selective disclosure, and review the contractual agreement of the requested data

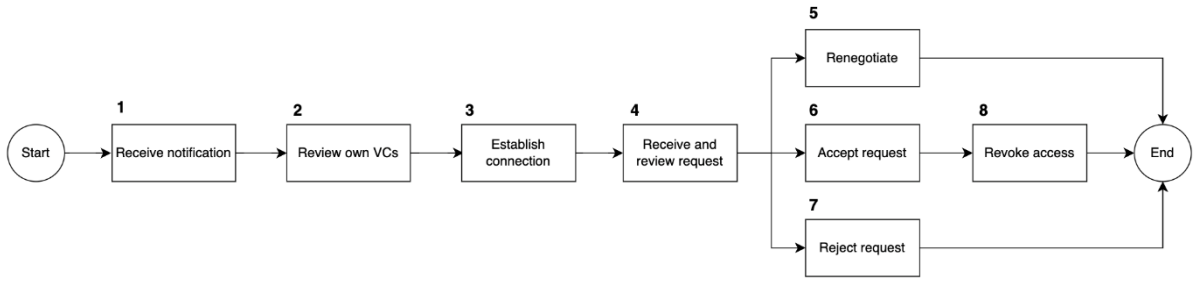

Figure 5.1 Task sequences of user behavior for data sharing

Reviewing a request can results in three outcomes:

> **(5) Renegotiation**—The Patient can renegotiate the contractual agreement by creating new terms and conditions and sending them to the Research Institution. During this renegotiation period, no data-sharing activity will occur, and the credentials will remain unaffected until the Patient or researcher accepts the terms. In this task, the study does not include scenario of a second round of review request, which leads to the end of the design artifact demonstration. This is done to reduce the complexity of the design phase
>
> **(6) Accepting request**—The Patient accepts the terms and conditions provided by the Research Institution and shares the data after performing data minimization. The data sharing will be completed during this process, and the request and credentials in their VP will be updated
>
> **(7) Reject request**—The Patient can reject or decline the request, making the credential unavailable to the Research Institution

After a request is accepted, the Patient can **(8) Revoke the access.** To develop a more detailed design artifact, each task will be broken down into sub-tasks for the Patient. After finishing a task, they can move to the next one.

5.2.1 Receive Notification

In this task, the Patient will receive a notification containing the VP of a Research Institution that requests their health information and the purpose of the request. This notification allows the Patient to decide whether to act or postpone it. This task is critical when handling personally identifiable information because the Patient should be aware of and concerned about their information and interactions with other entities (Čučko & Turkanović, 2021). Additionally, the notification can serve as a status update for the Patient's interactions with other entities, such as for revocation or negotiation of contractual agreements. This task also allows the Patient to exercise their consent and autonomy in protecting themselves from harm, giving them control from the outset (Čučko & Turkanović, 2021). Appendix C-1. summarizes the detail of Receive Notification task.

5.2.2 Review Credentials

After receiving a notification and deciding to take follow-up actions, the Patient will be redirected to the home screen, which will show all their VCs. The Patient can also select a particular VC and see the list of attributes from

that VC. They can also see data-sharing activity from that VC and with whom the data is shared. This is included to enable the Patient to check information contained in their credentials. The details of the Review Credential task can be seen in Appendix C-2.

5.2.3 Establish Connection

This task addresses the role-changing condition experienced by the Patient, where they temporarily assume the role of verifier when reviewing connection requests from Research Institution. This is depicted by sub-task 3-EC-2. From the same home screen, the Patient can see their connection with the Research Institution and the Institution can securely send data sharing requests to the Patient. In this phase, the Patient can manage their connections, such as adding new connections and deleting established connections, while also seeing the details of the connection. When evaluating a new incoming connection request, the Patient will see who the entity is and the purpose of their data-sharing request, allowing the Patient to evaluate their credentials and decide whether they would like to connect with the requester. The detail of this task is presented in Appendix C-3.

5.2.4 Receive and review request

Once a successful connection has been established, a secure channel is created to facilitate the safe sharing of health information between the Patient and the Research Institution. The Research Institution can request the Patient's information and inform the purpose of data sharing and how it will be used. Upon receiving the request, the Patient will receive a comprehensive list of mandatory and optional data request from the Research Institution, along with any pre-established contractual agreements. The Patient can then review the request and choose to either accept it, renegotiate the terms, or decline it altogether. This evaluation process provides an additional layer of protection for the Patient, who can confidently give their consent when sharing data through an established connection. In this task they can also employ selective disclosure on their data before sharing. Appendix C-4. summarizes the Receive and review request task.

5.2.5 Renegotiation

In the process of reviewing a request, one possible outcome is that the Patient may choose to renegotiate the terms of the agreement that governs their access to and use of their health information. This renegotiation process should allow the Patient and Research Institution to reach a mutually agreeable arrangement while also ensuring that the Patient retains control over their health information. The agreement should receive mutual consent from both parties and allow the Patient to revoke data access if necessary.

This study limits the scope of the contractual agreement to the duration of the transaction, which is the length of time that the Research Institution can access the Patient's health information. The agreement also outlines the specific types of usage that are allowed throughout the data life cycle, such as storing, sharing, and deleting. This limitation was included because a contractual agreement could potentially be used in other contexts where additional factors, such as benefits or penalties for breaching the contract, could come into play. As a result, the renegotiation will focus on the general access and usage of the data, as outlined in Appendix C-5.

5.2.6 Accept and revoke request

When evaluating a request, there are two outcomes: rejection or acceptance. Rejection occurs when the Patient chooses not to allow the Research Institution to access their health information. Acceptance means that the Patient has consented the access of Research Institution's to their health information.

Once the request is accepted, the Patient consents to establish a connection with the Research Institution and allows access to their health information. Despite granting access, the Patient maintains control over their data. During this task, they can monitor who has access to their data and revoke access to their credentials, as outlined in Appendix C-6.

If the Patient chooses to withdraw access, they can review the details and click "revoke access," which immediately restricts the Research Institution's access to the health information. Refer to Appendix C-7 for more information on this process.

After analyzing the scenario, tasks, sub-tasks, and design patterns, the interface layer of SSI design artifact is structured and presented on Table 5.9.

Table 5.2 Summary of SSI design artifact interface layer

Interface layer	Design patterns
1. Notification and notification menu detail	Notification Contractual agreement
2. Home screen	VC archive Extended verifiable credential archive Connection list
3. Credential details	Extended verifiable credentials view History Revocation
4. Connection details	Review connection Interaction authentication
5. Request archive	Interaction history
6. Review request	Interaction authentication Review presentation Interaction history Selective disclosure Revocation
7. Renegotiation	Contractual agreement Transaction duration

5.3. SSI design artifact of digital ID wallet

This section covers the process of designing SSI artifact, which is done using UIzard web-based software. UIZard allows users to select a template from the UIzard library and make minor adjustments to meet the interface requirements for the given scenario. The output of UIZard is a clickable design artifact that enable users to move between different screens depending on objects they interact with. Figure 5.2. presents the interface of UIZard. The software consists of elements that can be dragged and dropped into the canvas to develop a design artifact. The flow between screens can also be designed (presented in the figure with blue arrows inside the green box). After the artifact is finished, it can be deployed to the user by clicking the 'Preview' button in the top right corner of the screen (red box).

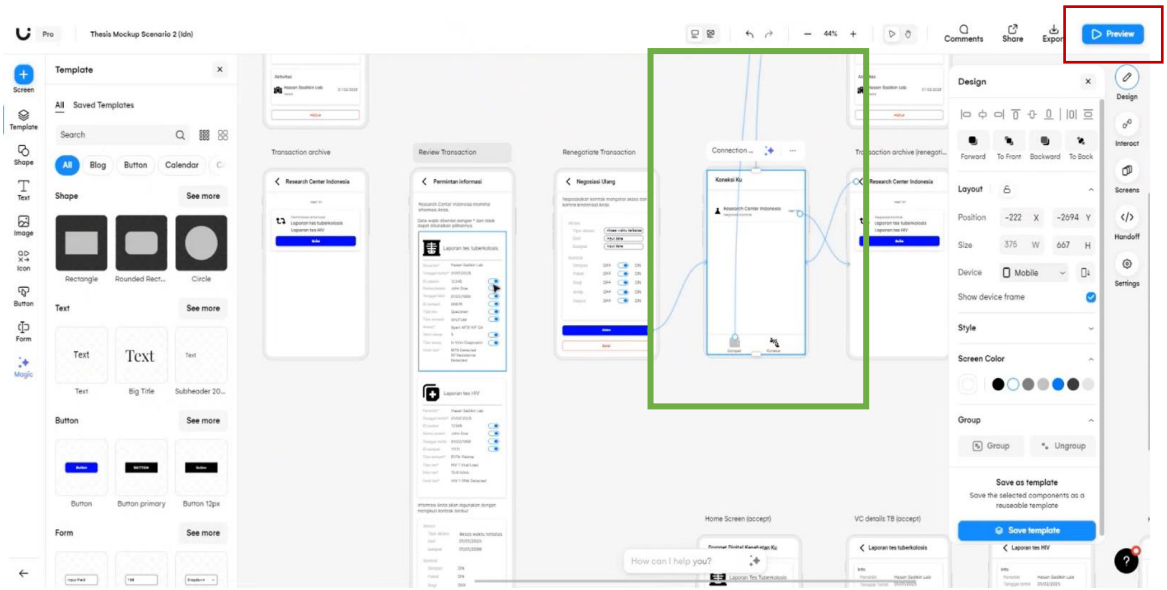

Figure 5.2 UIZard interface

The design process includes referencing existing SSI mobile applications available in Google Play Store, such as Lissi and Esatus Wallet. These wallets use the same task sequences as the designed scenario, where the Patient will receive credentials from the Research Institution before deciding to conduct any interaction, presented in Figures 5.3 and 5.4. The development process includes referencing to lab result formats that are available online, ensuring that the presentation of information on the TB and HIV VCs match the real world's.

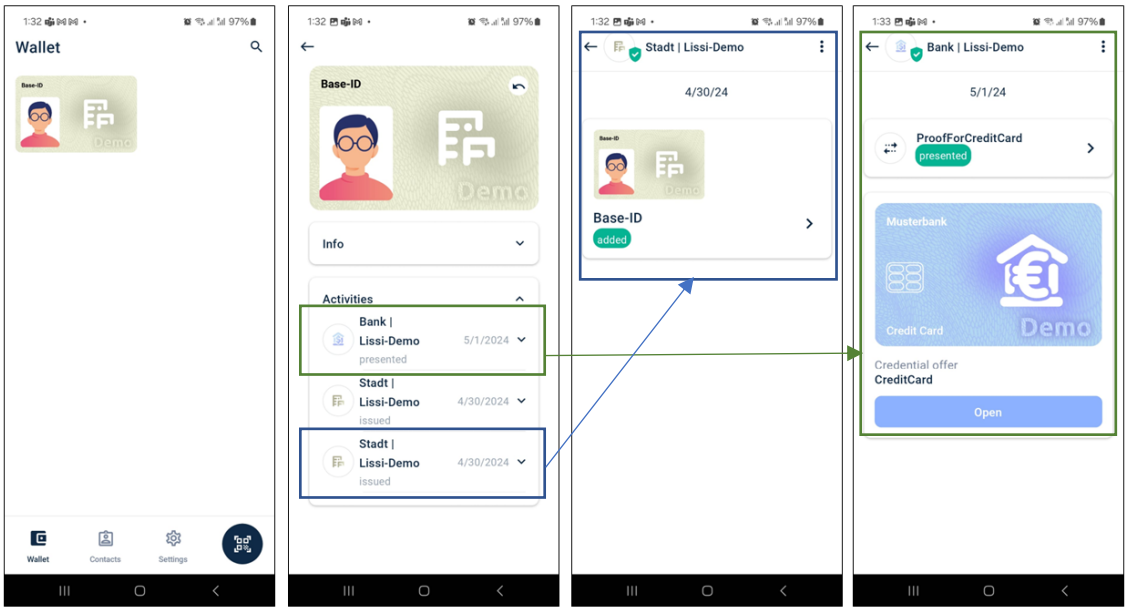

Figure 5.3 User interface reference from Lissi Wallet

Figure 5.3. summarizes a task sequence of how the Patient might use the wallet. First, when the Patient first logs into Lissi Wallet, he is presented with all available VCs. Second, when the Patient opens the VC, he can see activity history related to the VC. The third screen and fourth screen show the detailed VC view.

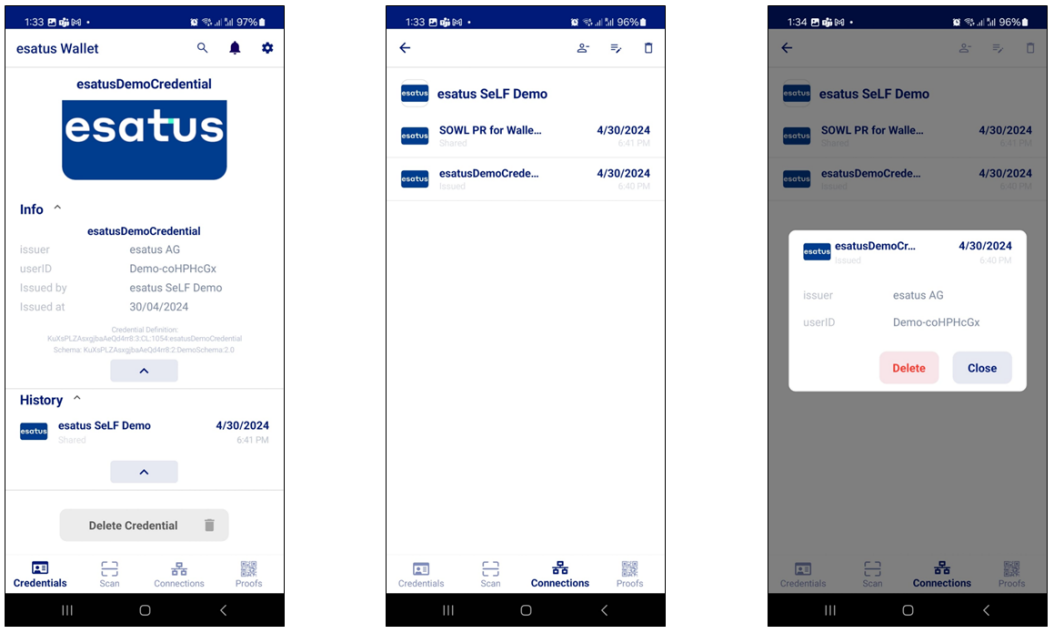

Figure 5.4 User interface from Esatus Wallet

Figure 5.4. presents a screenshot of multiple interface screen. The first screen presents a detailed VC view. The second screen presents detailed activities that have taken place between a holder and a verifier. The third screen shows the option to revoke the VC. In the following sections, each interface screen will be developed according to task sequences and functional specifications presented in Section 5.3, highlighting all corresponding design patterns.

5.3.1 Interface layer 1: Notification and notification menu detail

The notification for this design artifact will be a pop-up, designed to capture the Patient's attention and inform them of requests made by other entities. As a result, on this screen, the data sharing scenario will commence with a pop-up notification that serves as an alert for the Patient (Figure 5.4). The information presented in the notification detail includes who requests for the connection, purpose of data access, type of data access (e.g., limited time, permanent), and duration of data access.

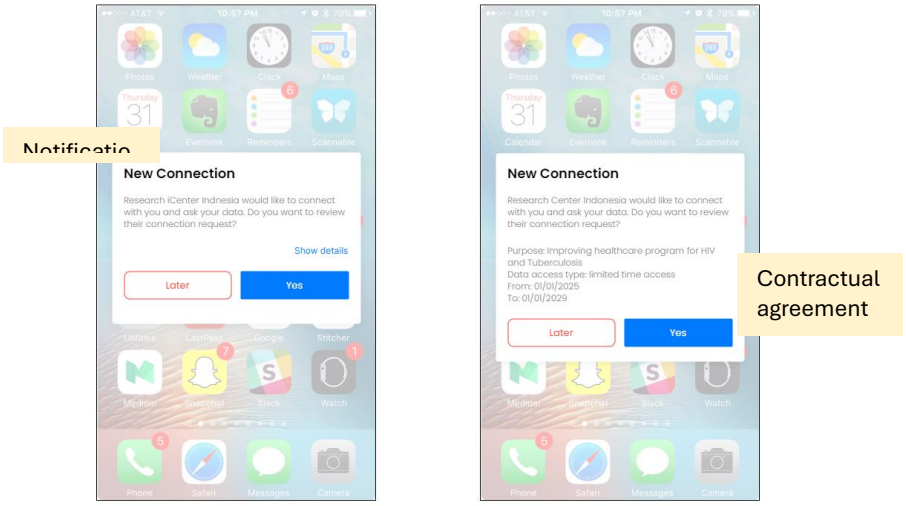

Figure 5.5 Notification and notification menu detail design artifact

5.3.2 Interface layer 2: Home screen

The home screen acts as a comprehensive platform for the Patient to effectively manage their credentials and connections. In the event of a new connection request, a notification mark will appear on the Connection tab, keeping the Patient informed. Separate pages for credentials and connections were developed, providing the Patient with an easier navigation experience when making decisions. Should the Patient wish to manage their credentials, they can simply navigate to the Wallet tab. If they want to handle institutional requests, they can go to the Connection tab. The home screen provides a clear view of each tab, which can be seen in Figure 5.6.

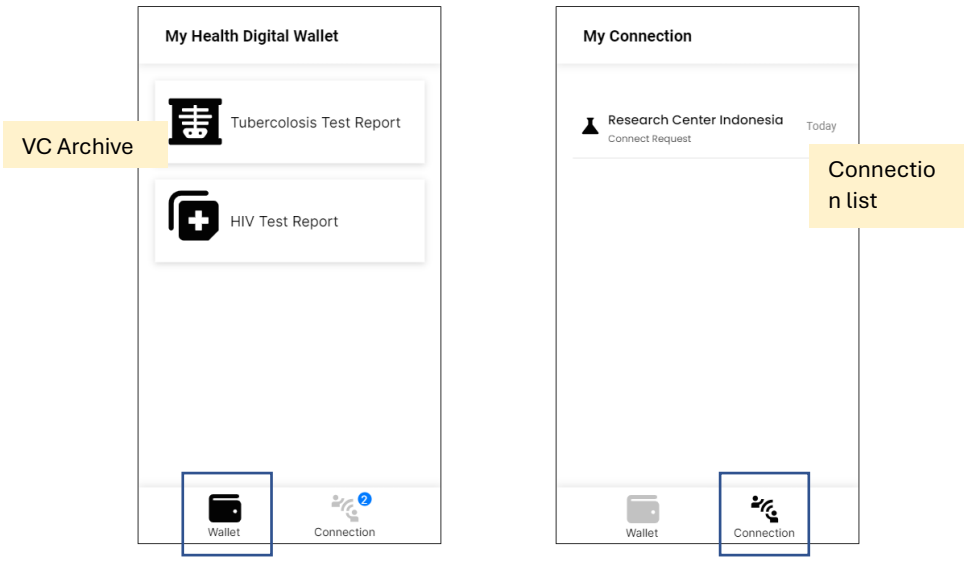

Figure 5.6 Home screen design artifact, left to right: Wallet tab, Connection tab

5.3.3 Interface layer 3: Credential details

The Credential Details interface allows the Patient to get an in-depth view of their VCs, as depicted in Figure 5.7. This page offers a wealth of information about a specific VC, including several health data attributes. From the day of issuance, the Patient can also track the interaction history of a particular VC. Furthermore, the Patient can delete their credential much like they could discard a physical one from their wallet. The attribute granularity displayed within a VC is the primary feature of this page. This level of detail is critical for the selective disclosure or data minimization process demonstrated in the request review page. By using the exact same attributes in the request review page, the Patient can easily reference the familiar VC details from the beginning.

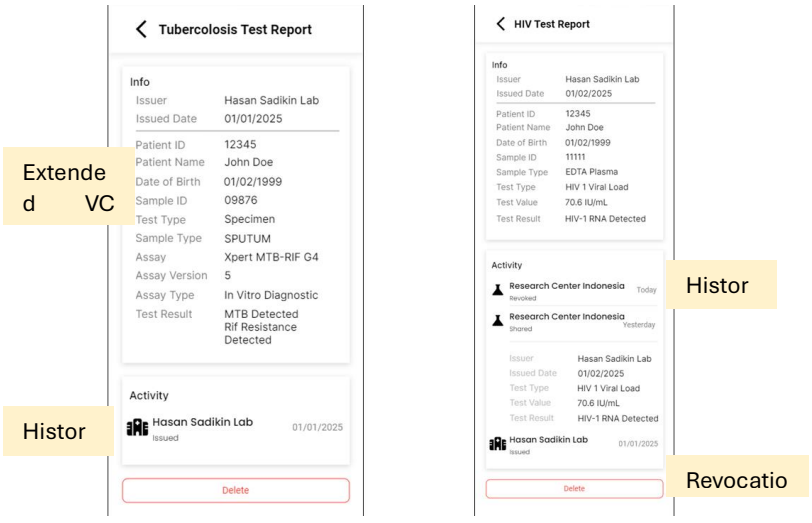

Figure 5.7 Refined design artifact on credential details

5.3.4 Interface layer 4: Connection details

The purpose of the connection details interface is to present the credentials of Research Institution and their reasons for requesting health information from the Patient. This step is crucial in the process as it empowers the Patient to make an informed decision. It is important that the Patient can identify the Research Institution as it establishes a sense of trust between both parties, which is an indispensable aspect of any data ecosystem (von Scherenberg et al., 2024). The verification process happens automatically when the Patient opens the Review

Connection page where they can see the latest version of the Research Institution's credentials saved in the data registry. Being acquainted with the identity of the Research Institution also serves to validate the contractual agreement and expedite the request process (Nagel & Lycklama, 2020). In essence, the connection details feature plays a pivotal role in facilitating a secure and trustworthy data exchange between the Patient and the Research Institution, leading to the creation of a screen in Figure 5.8.

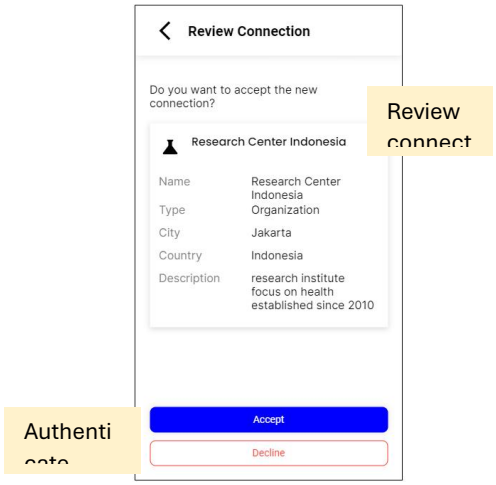

Figure 5.8 Refined design artifact on connection details

5.3.5 Interface layer 5: Request archive

In Figure 5.9, the displayed screens serve the purpose of recording the previous engagements between the Patient and the Research Institution. These interactions may comprise of requesting or transmitting data, bargaining of a contract, or receiving a credential from an issuer. The rationale behind maintaining these historical records is to assist the Patient in prioritizing interactions that need immediate attention. Moreover, these records act as a chronological record of these engagements, which can be referred to by the Patient to grant or withhold their consent.

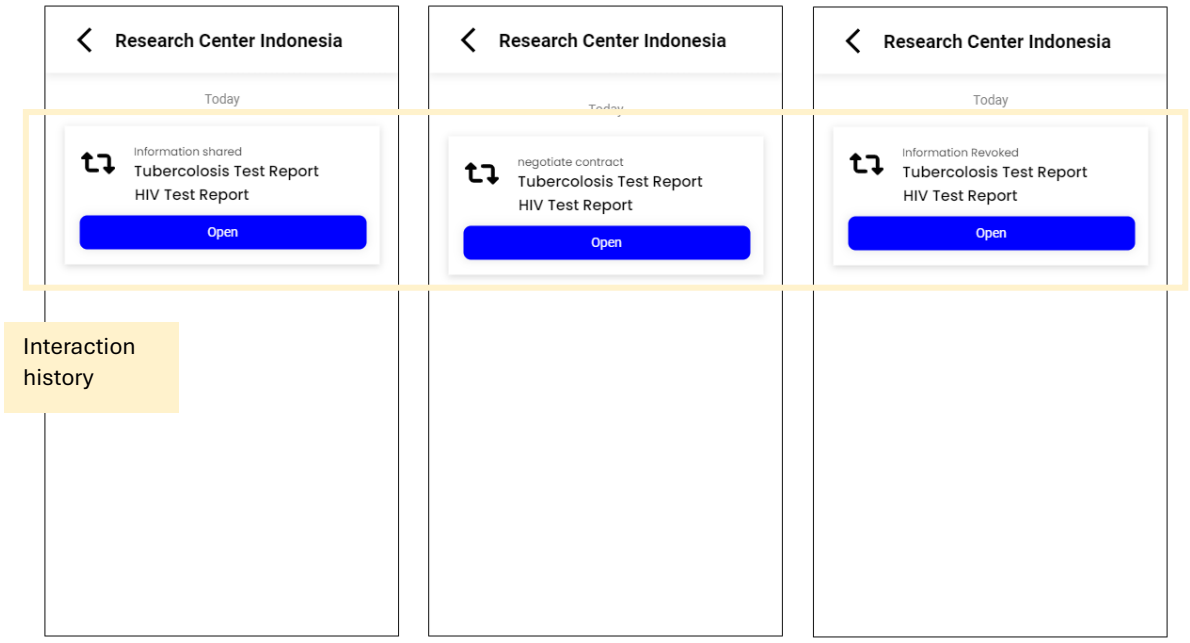

Figure 5.9 Request archive design artifact

5.3.6 Interface layer 6: Review request

The review request interface is a pivotal component in the data-sharing context of the project scenario, as illustrated in Figure 5.10. The Patient is required to provide their consent at three levels, namely data sharing, contractual agreement, and transaction. The consent process begins with the Patient agreeing to the data attributes that will be shared from the requested VC, based on their discretion. In addition, the Patient can choose to include more data attributes in the transaction, beyond the ones requested by the Research Institution. Secondly, the Patient must agree to the contractual agreement, which outlines the duration of data access, and the usage type requested by the Research Institution. If the Patient has any concern regarding the handling of their data, they can negotiate the agreement and wait for the Research Institution's response. Finally, the Patient must provide consent for the request itself. Even if there are no issues with the requested data or the contractual agreement, the Patient can decline the transaction if they do not trust the requesting connection with sensitive data. Upon approval of the request, the consent form changes, and the Patient can no longer limit the data selection. If the Patient decides to withdraw shared data, they can revoke access by accessing the details of the approved request. This revocation prevents the Research Institution from accessing and utilizing the previously requested credentials.

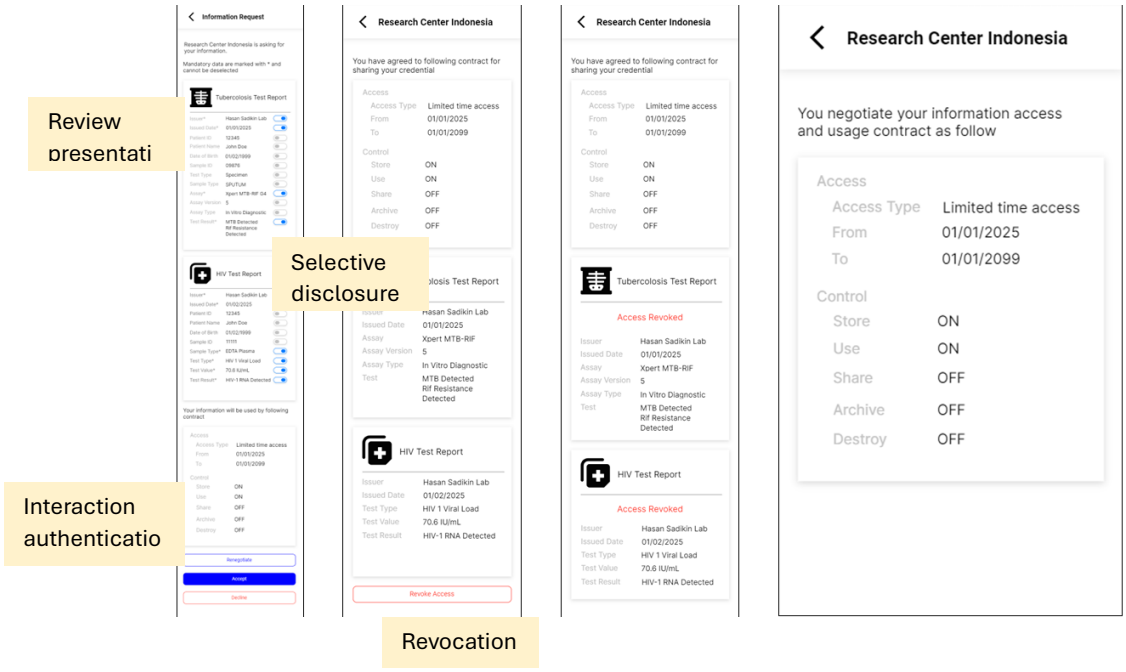

Figure 5.10 Review request design artifact

5.3.7 Interface layer 7: Renegotiate

The Renegotiate interface positions the Patient as an authority over their own data, providing them with power in defining the terms of their data access. As displayed in Figure 5.11, the Patient can regulate the anticipated usage and access of their health information. This approach allows to exert quasi-property rights over their data flows (Hummel, Braun, & Dabrock, 2021). The selective disclosure requirement enacted in the review transaction screen can address the secrecy requirement in the protection-participation view. In the individual-collective view, the contractual agreement can facilitate consent for participation in specific research or withdrawal at any stage.

Figure 5.11 Renegotiate design artifact

5.4. Summary on Chapter 5 and discussion on Hevner's Design Cycle

Chapter 5 summarizes the operationalization of Hevner's design cycle, which covers DSR step 3 of Design and Development. In this step, artifact is designed by aligning desired functionalities to achieve the desired solution. This chapter provides answer to **SRQ2**: *"What could be the **possible design artifact** that follows the functionality requirements of self-sovereign identity on health data ecosystem to achieve personal data sovereignty for LMIC users?".* The design and development step starts by summarizing SSI functionalities resulting from the Requirements Engineering step, which requires the design artifact to be presented in the form of a digital ID wallet. Next, scenarios were developed to provide reasoning for the design and focus on detailed usage task sequence. The scenario embeds elicitation components which include: Patient as an individual user of the app, data-sharing context, the presence of users with socially stigmatized diseases, and the corresponding SSI functionalities translated into design patterns. This study highlights the role-shifting condition experienced by a holder within an SSI digital ID wallet. The scenario is further broken down into tasks and sub-tasks that were matched with the interface layer and design patterns as the basis for the design artifact. A benchmark of existing SSI ID wallets was also conducted to refine usage task sequences and interface design.

The design artifact is developed using UIZard, a web-based software that allows for rapid prototyping for interface visualization. The software resulted in a clickable design artifact with flows that were designed according to the defined task sequences. The Design and Development step resulted in seven interface layers: (1) Notification and notification menu detail, (2) Home screen, (3) Credential details, (4) Connection details, (5) Request archive, (6) Request review, and (7) Renegotiate. The role-changing situation is addressed in the Establish Connection task. The objective of this task is to allow Patient to decide whether to allow Research Institution to connect and access their data. The interface screen consists of two layers: Home Screen and Connection Details. In the Connection Details layer, the Patient can review connection and authenticate the interaction. In the Review Connection page, the verification process happens automatically, and the credentials are updated according to the Research Institution's latest information saved in the data registry. The scenario will also be used in Chapter 6 to guide artifact demonstration and evaluate its functionalities.

6. Design Artifact Demonstration & Evaluation

This chapter implements the fourth and fifth step of DSR—demonstration and evaluation—and provides answer to SRQ3: "***How can SSI functionalities help*** *LMIC users achieve data sovereignty in the health data ecosystem?".* This chapter has three sections: (1) Design Artifact Demonstration, (2) Design Artifact Evaluation, and (3) Summary of Chapter 6 and Discussion on Hevner's Rigor Cycle. The first section, Design Artifact Demonstration, will start by describing the user-testing approach that includes respondent identification and selection, development of user-testing scenario, and demonstration of scenarios. Utilizing qualitative methods such as interviews will enable a thorough exploration of the artifact's utility and gather insights and perspectives from end users in relevant scenarios (Sutcliffe, 2003). The second section, Design Artifact Evaluation, starts by defining a list of questions to guide the semi-structured interviews that accompany the observation of artifact evaluation, followed by explanation of coding process to extract insights from interview transcripts into codebook. Evaluation findings are analyzed by themes, and this chapter ends with a summary.

The demonstration and evaluation step engage selected respondents in a 30–40-minute interview session where the author introduced the research, obtained consent for the recording, and asked whether anonymization is desired. The demonstration and evaluation step are divided into two parts; the first part consists of semi-structured interview that addresses their experiences and concerns in health data sharing, while the second part starts with the presentation of the clickable design artifact, scenario introduction, and instructions for the respondents to accomplish tasks laid out in the scenario. This step is guided by Interview protocol and questions presented in Appendix A. Questions about the artifact are asked after respondents completed the tasks in the scenario. When the respondents perform the scenario tasks, author stood by to clarify the questions that might be raised by respondents. Sessions can take place either online or offline based on respondent's preference. The interview will be recorded; if it is online, then the interview will be using Microsoft Teams. For online session, phone audio recorder is used. All interviews were conducted in Indonesian to avoid misunderstanding. All the recordings will be transcribed using the Google speech-to-text feature in Google Docs, and they will be saved to the author's personal TU Delft OneDrive for manual adjustments.

6.1. Design artifact demonstration

The demonstration step in this study takes a broader perspective of using an artifact in a specific case to prove its feasibility, which includes interviews and observations of people using the artifacts (Perjons, 2021). The design artifact developed in Chapter 5 will be directly demonstrated by respondents through clickable links, exploring whether it can provide individuals with control and ownership over their personal data when sharing it with other entities. This assessment will specifically focus on data minimization and revocation functionalities. The design artifact is hosted in UIZard website, which can be accessed through a link. The respondent can use the clickable artifact either through laptop/PC or a phone. They will be faced with the interface presented in Figure 6.1.

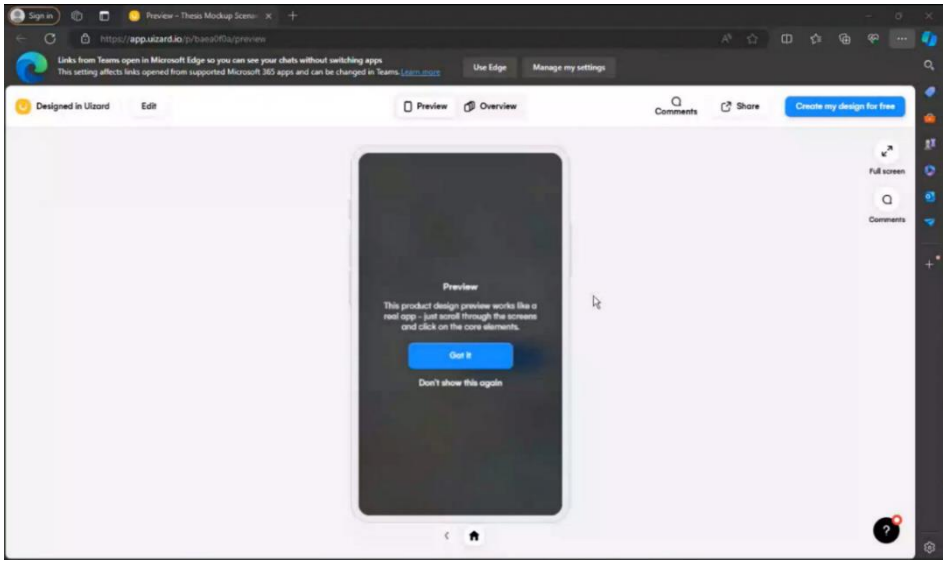

Figure 6.1 UIZard artifact preview

6.1.1. Respondent identification and selection

The demonstration is intended to see if the design artifact can address the problem it intends to solve, which is the issue of retaining user's personal data sovereignty when engaging in data sharing activities within a health data ecosystem. Therefore, respondents are identified and selected to represent the population of intended users that include the following characteristics: (1) adult above the age of 18, (2) resident or citizen of Indonesia as an LMIC, (3) individuals with socially stigmatized diseases that include HIV and TB, and (4) individuals with no socially stigmatized diseases that are currently finishing a graduate study. The inclusion of both individuals with and without socially stigmatized disease is intended to provide different perspectives to how they might perceive sensitive personal data in a data sharing ecosystem.

The author reached out to a healthcare officer working for a HIV center, which has more than 20,000 following on Twitter and spends his time advocating about the importance of HIV testing and consuming ARV. From that connection, the author was referred to his supervisor who is also a leader of an HIV support group. After an introduction meeting to explain the research, the author sent over a short introduction message to be blasted in the community, alongside with a pre-approved informed consent form to be filled by those who are interested to participate. Respondents then voluntarily reached out to author through WhatsApp and email. In the end, this study managed to gather 15 respondents, of whom 8 are HIV-positive, 2 are TB-positive, and 5 are disease-free. Six out of fifteen respondents are pursuing a master's degree in international setting. Three of the respondents are female, and twelve of them are male. Privacy measures for TB/HIV positive respondents include minimization of personal data exposure, all interviews were anonymized, and no information on full name, location, job, or health history were disclosed. Data is stored in TU Delft storage system, where it can only be accessed by author and committee members.

6.1.2. Development of evaluation scenarios

There are two evaluation scenarios that will be given to the respondents, which is the same as the scenario elaborated in Section 5.2. In essence, there are two main scenarios that needs to be done by the respondents: (1) **Evaluate and approve issued credentials**, and (2) **Evaluate and approve data sharing request**. In the first scenario, the respondent will act as a holder in the SSI system. The respondent will act as a holder that receives a medical result VC issued by an issuer. In the second scenario, when the respondent receives data sharing request from a Research Institution, the respondents will briefly experience the role of a verifier when they receive the Research Institution's credential, which showed the shifting role that has been discussed in 4.2.1.5. The objective of the two scenarios is to check whether the functionalities presented in the interface layer affect their perception about their personal data sovereignty. The highlighted functionalities are data minimization and revocation. In the evaluation step, questions will be asked to explore each of the concepts from user perspective.

Figure 6.2. presents the artifacts that will be demonstrated by the respondents for the first scenario.

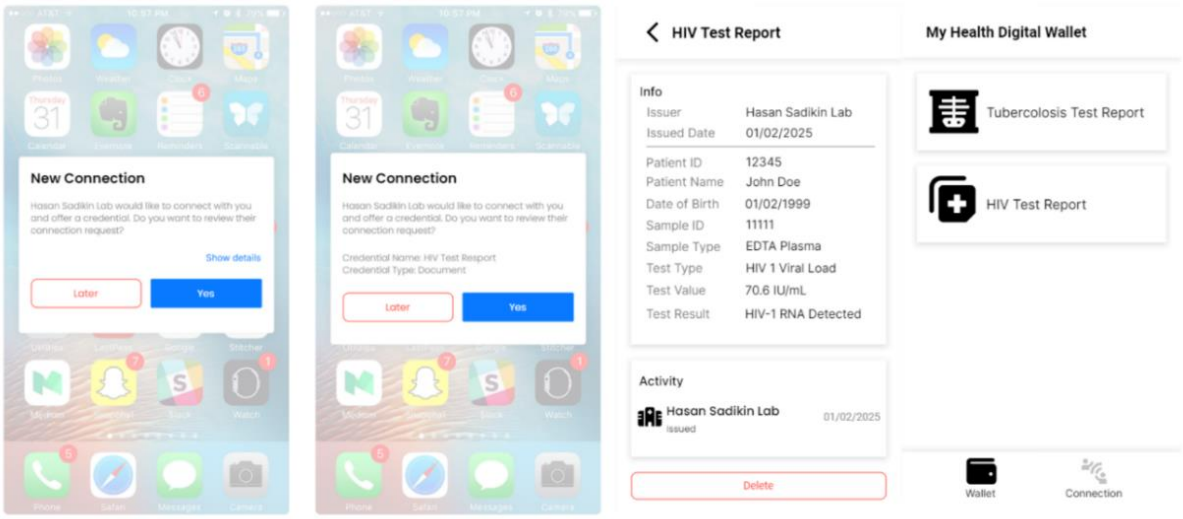

Figure 6.2 Artifacts for evaluate and approve credentials

Figure 6.3. presents the artifacts that will be demonstrated by the respondents for the second scenario.

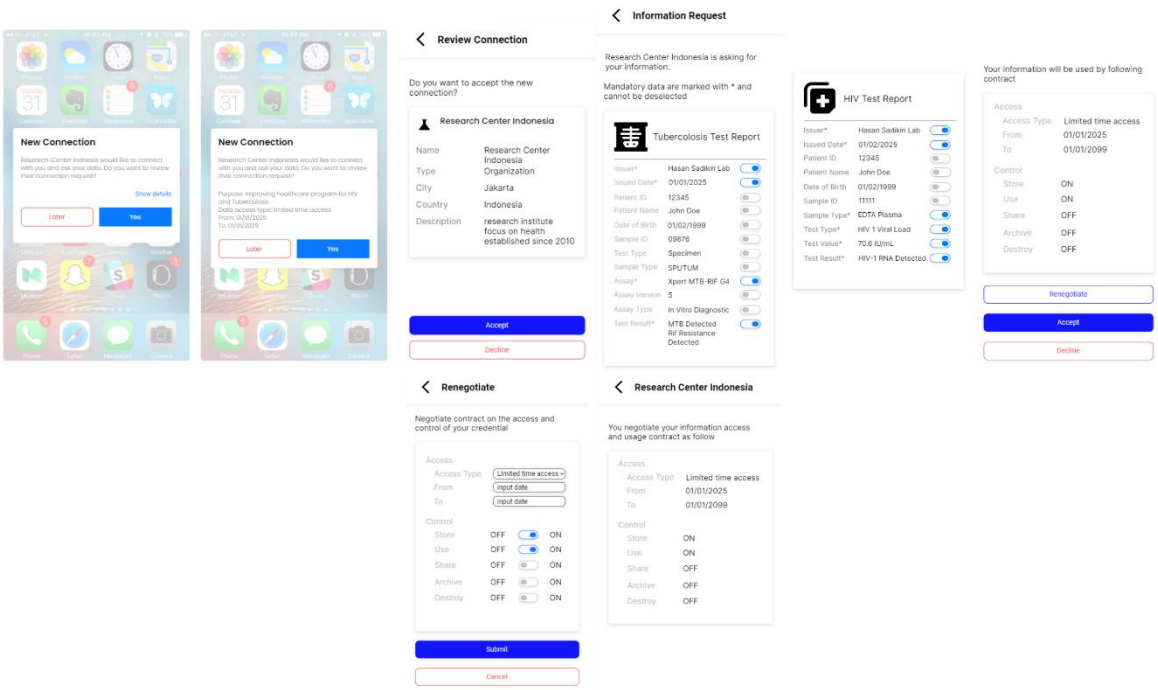

Figure 6.3 Artifacts for evaluate and approve data sharing request

When respondents first access the link, they are allowed to explore the artifact, switch between the different screens, and try to use the functionalities. When respondents are testing the artifacts, author will assist them with any questions and explain the available functionalities when necessary.

6.1.3. Demonstration of scenarios

Each scenario and the corresponding design artifact are presented in the following sub-sections, where respondents will be referred to as user to maintain clarity of scenario. Author will only explain the scenario and let the users to complete the task while navigating the artifact. No verbal explanation of the artifact is provided so users can judge the usability and user-friendliness of the artifact objectively.

6.1.3.1. Scenario 1: Evaluate and approve credentials

The interface sequence is presented in Figure 6.4, with numbers signifying the objects selected by user. Only two tasks are present in this scenario: (1) Receive Notification (Section 5.3.1) and (2) Review Credentials (Section 5.3.2). The first scenario starts with the user receiving a pop-up notification from Hasan Sadikin Lab as an issuer, notifying the user that they have just issued a credential. The initial pop-up design provides minimal information that maintains user privacy, in which the detailed information on the credential can only be read if user clicks the *Show details* menu (1). Afterwards, user can either click the 'Later' or 'Yes' button – the 'Later' button prompting closure of the notification and 'Yes' (2) button brings user to the test report page that shows the result of the test, as well as the issuer. In this page, user can click the 'Delete' button to revoke the credential from their wallet (3). The credential will only be removed from user's wallet but remain in the public data registry. In the home screen, all available credentials of the user are presented (4).

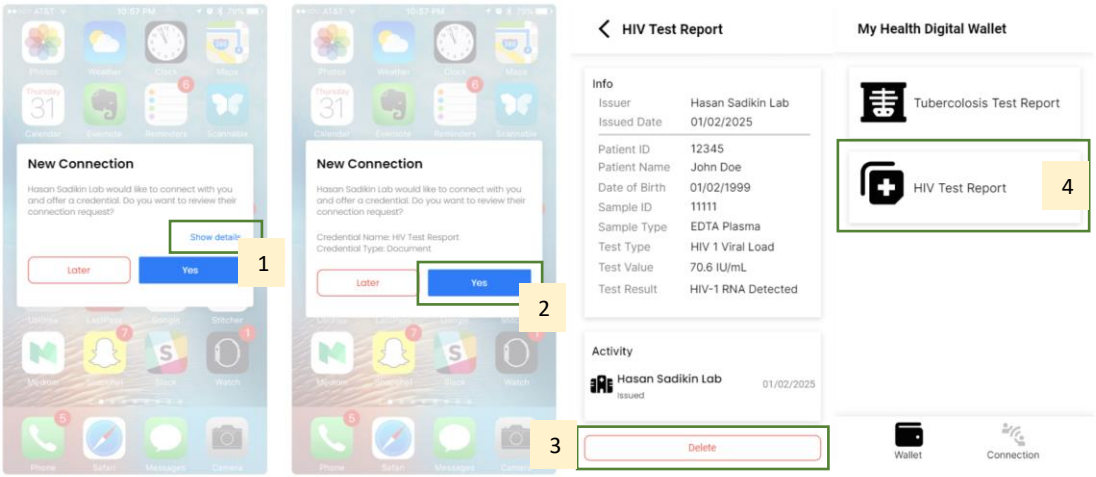

Figure 6.4 Receive notification and review credentials

6.1.3.2. Scenario 2: Evaluate and approve data sharing request

This scenario consists of three tasks: (1) Establish connection (Section 5.3.3), (2) Receive and review request (Section 5.3.4), and (3) Renegotiation (Section 5.3.5). Figure 6.5. presents the interface sequence for Establish connection, with numbers signifying the objects selected by user. First, user will receive a pop-up notification that consists of minimum information for new connection request, where details can be read when *Show details* button is clicked (1). After pop-up notification shows detailed connection request, user can either select 'Later' or 'Yes' (2), which will trigger the VC verification process. The system will briefly position user as a verifier and the most recent credentials of the requester will be shown in the Review Connection page. In the Review Connection page, the user can either decide to accept or decline the request based on the credentials of the requester (3).

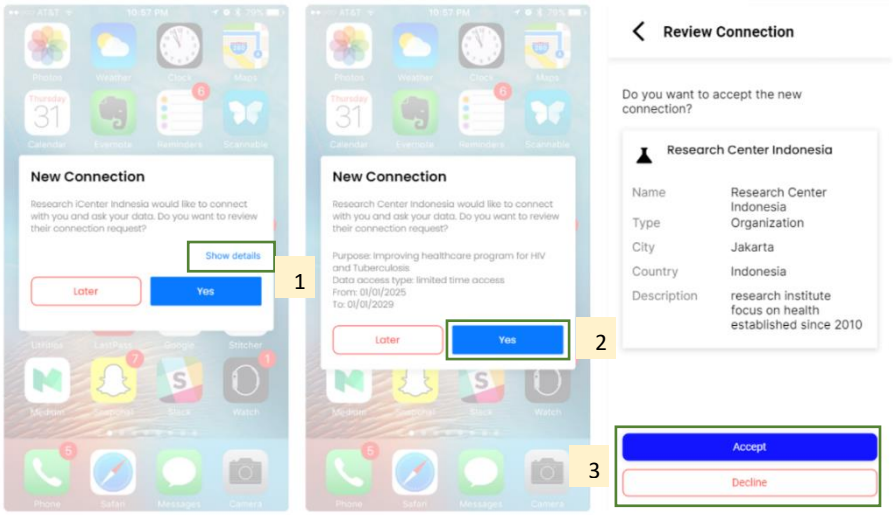

Figure 6.5 Establish connection

For the receive and review request task, user can see the list of requested data from the requester, presented in Figure 6.6. In this page, user can perform data minimization by using the toggle switch to selectively disclose which data they are willing and not willing to share (1). User can also disclose more data than what is requested. When the user scrolls down to the bottom of the page, the contractual agreement on data usage is presented. If the user is unsatisfied with the terms, they can click the 'Renegotiate' button (2). The other available options are (3) Accept or Decline the request.

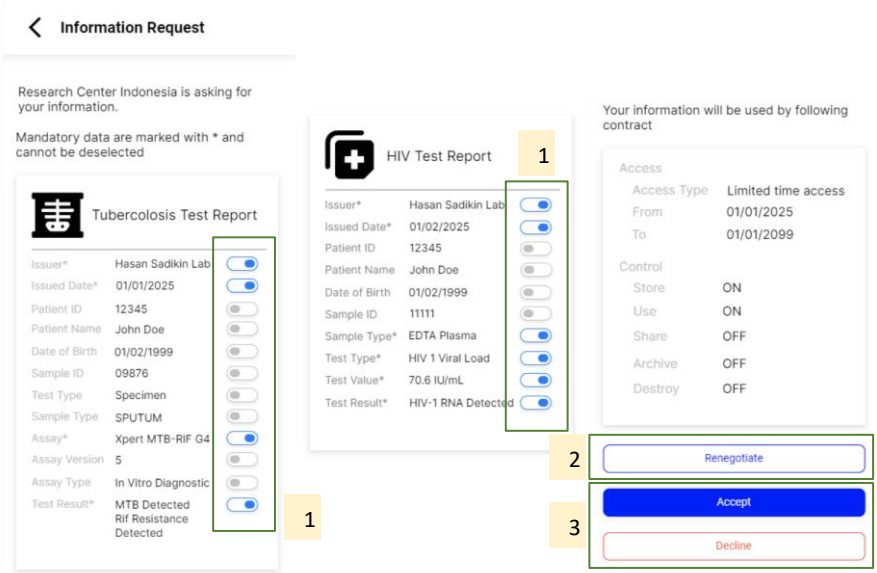

Figure 6.6 Receive and review request

If the user decides to renegotiate the terms, the artifact will take the user to the Renegotiate page and show the components of the contractual agreement they can adjust, which can be seen in Figure 6.7. They can (1) adjust the start and end date of their data sharing, (2) adjust the control that can be done by the data requester, then either (3) Submit or Cancel the Renegotiation. If the user decides to submit the renegotiation request, the artifact will take the user to a summary of the renegotiated contractual terms.

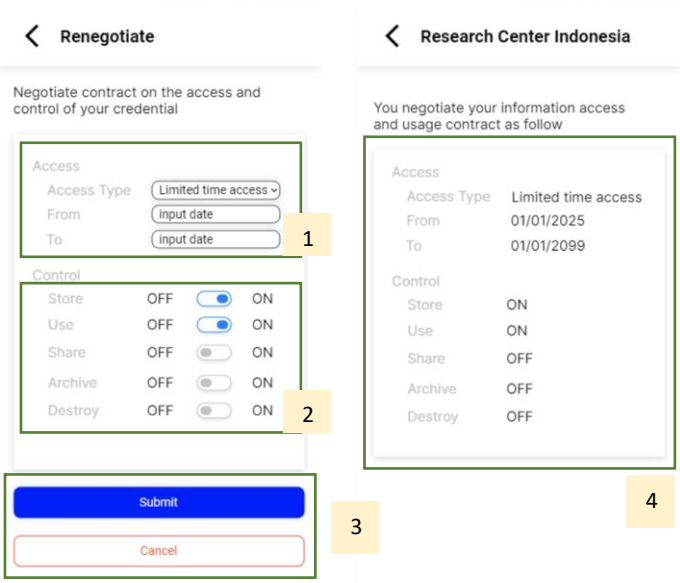

Figure 6.7 Renegotiation

6.2. Design artifact evaluation

Evaluation on design artifact is divided into two: (1) respondents' general evaluation on design artifact and their remarks on how the SSI functionalities address their data sovereignty, and (2) high-level evaluation on the underlying concepts, i.e., how revocation and data minimization affect user's PDS values of ownership and control. The second part of evaluation is conducted by coding the interview transcripts where the insights are extracted and structured by themes.

6.2.1. Respondents' evaluation on SSI design artifact

In general, all of the respondents were able to complete the two scenarios with minimal assistance from the author, such as pointing it to what button that they need to click since the prototype can provide highlighted of clickable button, indicating that the design artifact is intuitive enough. Table 6.1. summarizes the evaluation from respondents, grouped by scenario and the corresponding task and design patterns.

Table 6.1 Summary of respondents' evaluation

Scenario	Task	Design pattern	Respondents' evaluation
Evaluate and approve credentials	Receive notification	Notification	Six respondents mentioned that they need more context provided for the new credential notification – e.g., 'Hospital A wants to issue result for **the test you took on 12/7/2024)**'
Evaluate and approve credentials	Review credentials	VC archive	Clear enough, no feedback
		Extended VC view	Clear enough, no feedback
		Revocation	Two respondents expect that when they delete credentials from their digital health wallet, the main data source is also deleted
Evaluate and approve data sharing request	Establish connection	Review connection	Seven respondents expect a more detailed data usage because providing credential of the data requester is not enough to convince respondents to share data
		Interaction authentication	Five respondents expect a double confirmation before any decision is made to add an additional barrier to sharing private data

	Receive and review request	Interaction authentication	Five respondents expect a double confirmation before any decision is made to add an additional barrier to sharing private data
		Review presentation	Clear enough, no feedback
		Selective disclosure/Data minimization	Five respondents felt that the selective disclosure functionality provides them with control over their data, but they expect a double confirmation before sharing their data as an additional barrier to sharing private data
		Revocation	Four respondents raise concern about the possibility of having second thoughts – wanting to revoke access whenever they want. They felt that if it is possible, they have a higher level of ownership over their data
	Renegotiation	Contractual agreement	Five respondents demand a more detailed usage of their data and the implications – e.g., what does it mean when they allow data sharing
		Transaction duration	Clear enough, no feedback
		Authenticate interaction	Two respondents expect a double confirmation before any decision is made to add an additional barrier to sharing private data

Revocation and data minimization (highlighted in blue and green in Table 6.1.), the two main SSI functionalities explored in this study, were able to provide respondents with the feeling of control in the platform. However, they expressed the need for a double confirmation in the form of a pop-up notification to add additional barrier to sharing private data, indicating that each decision they made regarding their data has a great implication. They also expressed their concerns about the lack of control they have after they shared their data – there is no way of ensuring that the data requester would not reshare the data in other forms even after a contract is agreed by both sides. In addition, some respondents expected that when they delete a data, the main data source will also be deleted, stating that they would feel more ownership if it were possible. However, that expectation is against the value proposition of blockchain as its underlying technology: inherent resistance to the modification of data. In terms of ownership, respondents mentioned that seeing the Page Title 'My Health Digital Wallet' and all their available VCs on the home screen (Figure 6.8.) provides them with the feeling of ownership. They likened it to seeing a physical wallet with their ID cards in it.

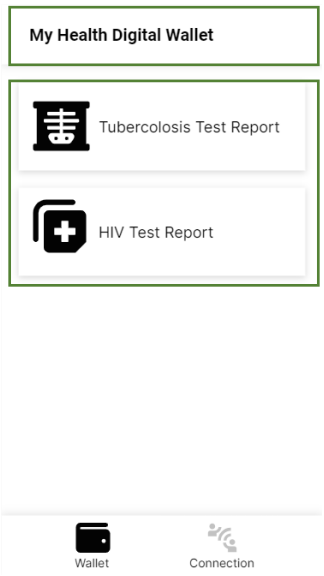

Figure 6.8 Design artifact components providing respondents with the feeling of ownership

When the respondents establish a connection with a new data requester, the verification process takes place automatically in the system. There is no feedback on the artifact regarding the verification process, but the respondents said that the information provided (credential of data requester) is insufficient for them to decide whether to share their data. The respondents said that they need the detailed data usage, i.e., what kind of research will be performed, what are the research output, and how the data will be processed. Another feedback from the respondents includes the need to add more context to the notification, especially for the new VC issuance. Instead of only stating that an issuer wants to issue new credentials, the notification should also refer to the data generation process (e.g., a TB test taken on July 12).

6.2.2. Coding methodology

Having evaluated the design artifact, this section now serves to provide the starting point for high-level concept evaluation through qualitative analysis. The interviews were transcribed and analyzed using the coding methodology. This research uses middle-ground approach to analyzing the gathered interview transcripts, with an initial list of codes developed based on the literature review and requirement engineering process. The initial codes are presented in Appendix B.

The initial code list will be expanded through open coding process by creating subcategories based on the quotations using grounded approach. After iterative analysis, the final code list ends up with 120 codes, in which 10 thematic analysis were identified. The relation from one code to another is identified using code co-occurrence analysis and through the quotes from respondent to understand whether a particular code has significantly come up with another code. The categorization method will use two approaches, content analysis and analytic induction methodology. In the content analysis method, the categorization is based on the symbolic content of various respondents (Kolbe, 1991). This method will help to define ideas or factors that might affect the evaluation of the design artifact on achieving personal data sovereignty. From this analysis, this study will establish the concept of factor through the frequency of such ideas across different respondents and then create a relational analysis through the model that is introduced in Chapter 2, which will show how the factors will help or negate personal data sovereignty. On the analytic induction methodology, this approach will focus on the hypothesis that self-sovereign identity features, data minimization, and data revocation will provide a feeling of control and ownership to the holder until it is found that the hypothesis is not proven. This will allow the research to modify the theoretical model of self-sovereign identity and whether it will achieve personal data sovereignty for LMIC users. Appendix C shows the final code list.

6.2.3. Interrelation between Control and Ownership

Based on the literature review, we learned that control and ownership are separate values. However, this study's empirical findings show that in practice, the pattern between control and ownership are interrelated. Two main

categories are used in this analysis: “Feel control" and "Feel ownership", to group codes that indicate factors influencing a respondent’s sense of control and ownership over their data. Figure 6.1. presents the relation diagram between codes related to ownership and control.

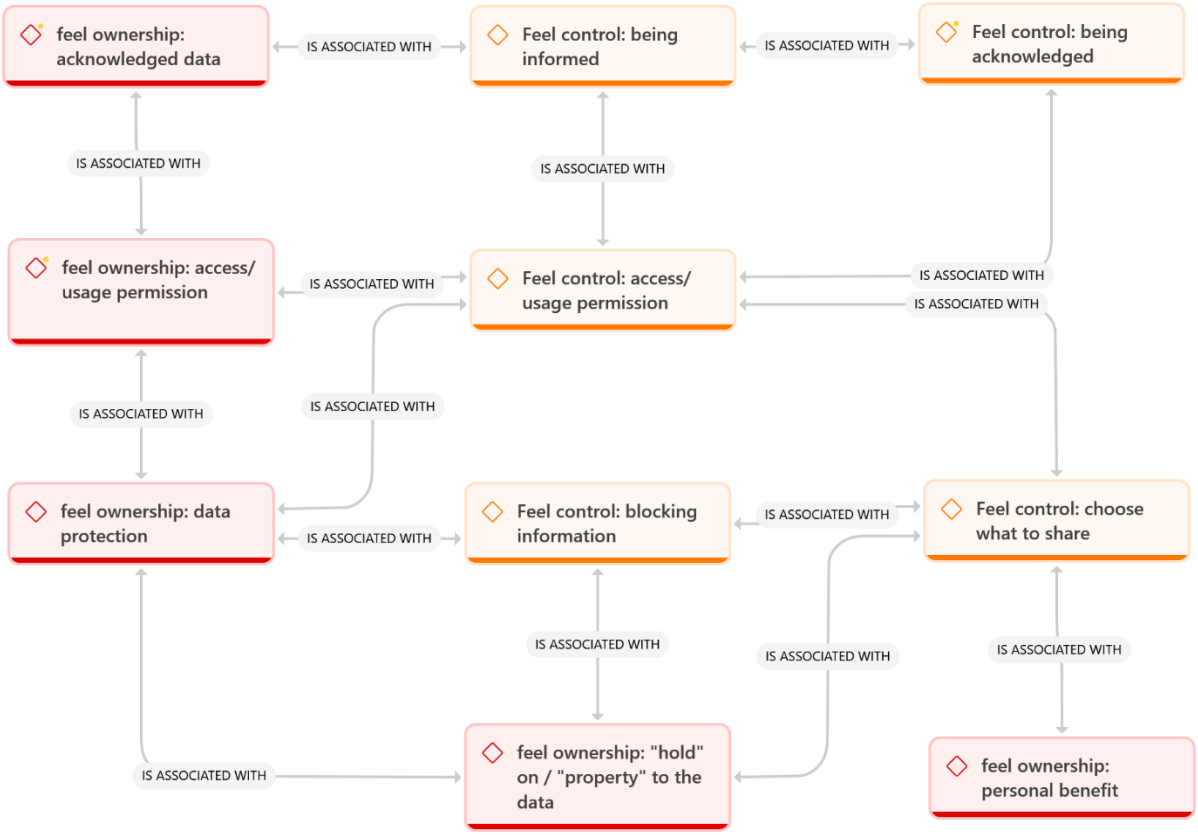

Figure 6.9 Feel control and feel ownership interrelation

We start by finding interrelation where respondents feel control and ownership in the context of this research, which showed that the facets from each value have reinforced each other.

At the beginning of the interrelation, there is a code “feel ownership: acknowledged data”, which is a condition when a data is acknowledged by other stakeholders and the respondent’s claim to that data is recognized, causing the respondent to feel ownership. On the other side, there is a similar code named “feel control: being acknowledged”, meaning that respondent will feel control if they experience recognition and validation from other stakeholders that lets them make decisions on their data (Respondent 09, Respondent 10). The acknowledgments can be informed through data governance or through contractual agreement. This pattern showed there is importance for some respondents because it will highlight their capability when facing a data sharing situation (Respondent 3), another quote that supports such pattern can be seen as follow:

> ***Quote 6.1.*** *“[...] other sharing is allowed, meaning through this application, data from various sources, as long as the dataset that we can share. This means that* ***our data is acknowledged****, without us having to ask back to the agency that issued the report, for example, that recognition is like a country, without recognition from other countries, you don't have sovereignty. It doesn't exist with them, like that.* ***So when the data is given to us, it is acknowledged when we share it again, and we can choose which to share, which not to share, access can be revoked, yes, it feels like, oh yeah, I have the data****.” – Respondent 09*

After respondents are made aware of their ownership through data governance and contractual agreement, they will know their right of access and usage of the data. Knowing the rights to their data cause respondents to feel ownership, highlighted with the code “feel ownership: access/usage permission”. A respondent expressed that being acknowledged over their data ownership causes them to feel more responsible over their data, such as in

granting access or usage permission (Respondent 10). A respondent stated that data ownership is not tied to where the data is stored (e.g., hospital) but to whom the data serves a purpose, such as for a patient's treatment. Therefore, the patient should still have the final say of what happen to their data, as expressed in the following quote:

> ***Quote 6.2.*** *"Our health data should only belong to us and to health services, but health services, in this case, are related to treatment, right? That means no,* ***it's not that the data belongs to them because we are their patients,*** *but because the purpose is for treatment and so on and for tracking recovery and other values,* ***I think the data goes back to its original owner,*** *meaning the certainty, so whether the data will then be used or not or to what extent the user, I think it must have the permission of the data owner, but it's a little because if it's already in the hospital, the data seems to belong to them, right? Well, there are limitations on what they can identify, what they can use, what they can't or what* ***they have to have our permission to use the data,*** *I think that's also a concession." – Respondent 04*

Having control over granting access/usage permission enables respondent to choose which parts of data they are willing to share (Respondent 06). This is important as each respondent will be more aware of the consequences of sharing their data, such as getting stigmatized or being reidentified through associated data (Respondent 05). Such risk showed patterns where respondents to be more cautious in sharing data, particularly common/historical medical data or personally identifiable information. This is aligned with respondent's preference to protect data from public exposure (Respondent 01). The capability to protect data and choose what to share makes some respondents think that they own the data. The analogy is like having land that can be accessed or used by someone else to gain benefit, such as illegal land use, the owner can take measures to restrict such violation. In this study, users also expect that owning the data means that they have control over the data (Respondent 04, Respondent 05).

In addition to exploring the factors causing respondents to feel ownership and control over data, the interview also identified patterns on users not to feel ownership and control over their data, as summarized in Figure 6.10.

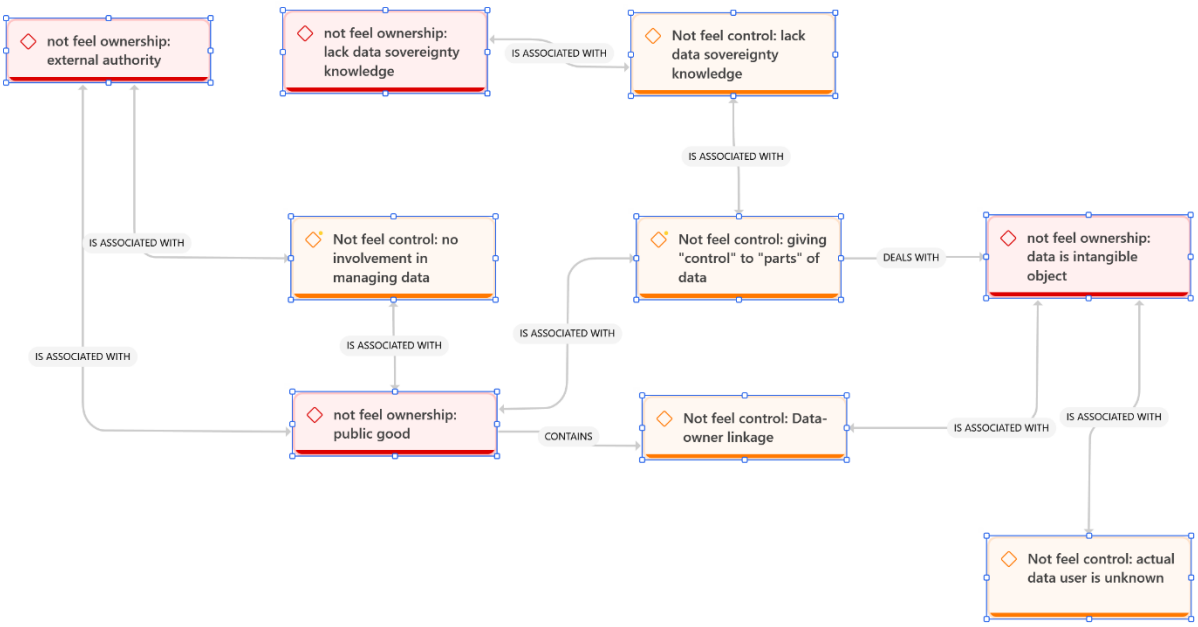

Figure 6.10 Interrelation between not feel control and not feel ownership

The beginning of the interrelation pattern between not feeling control and ownership starts with the code "not feel ownership: external authority", indicating that as data are produced, stored, and used by other stakeholders within the system, respondents cannot fully own the data. For instance, when a test result is issued by a hospital lab and used for diagnostic purposes in a healthcare facility, the respondent must give up a certain level of ownership and control (Respondent 10). Some respondents highlighted that the usage of centralized storage

may put their data at risk of being associated with other sensitive health data, such as linkage to common/historical data enabled by personally identifiable information and harming their privacy (Respondent 14). Another factor that causes respondents to not feel control or ownership is due to the lack of knowledge on data sovereignty. Some respondents mentioned that they do not really understand the concept of sovereignty, making them wonder how personal data sovereignty should be reflected in daily activities (Respondent 02). Having knowledge about data sovereignty is important because it gives respondents a benchmark on how they should feel control and ownership over their data.

The presence of external authority and lack of knowledge of data sovereignty caused respondents to not feel control as they realize that they are not being involved in managing their data. Some interviews indicated that even when they go to a healthcare facility and they receive a medical form to get consent of their health data usage, they do not feel control as the form often only provides two options - opt-in and opt-out – instead of a detailed data usage term (Respondent 07). When an individual is not being involved in managing data and the data is under the governance of an external authority, they feel that the status of their data turned into a public good, causing them to no longer feel ownership over their data. Another factor found is that respondents do not feel control when they must give up parts of their data to a stakeholder, e.g., when a medical officer asks about their most recent blood result. They are aware that they could not control what would happen once the data is shared, which might lead to potential risk such as data misuse and data recreation.

Notably, one respondent said that when data is made and shared within an ecosystem, they feel like they do not own or cannot control the data anymore, and therefore they need to prepare for preventative and mitigation measures to address the impacts of data leaks/spread:

> ***Quote 6.3.*** *"Yes, we definitely can't control the spread (of data), but we can at least know what data is already there, so we can be preemptive. For example, when data a is spread, then* ***we can provide preventive measures so we can handle problems when they arise.*** *But what we deal with is not whether the data will be spread or not, but what the impact of the data is and what we mitigate is the impact of the data.* ***So we don't really have control or ownership****, well, because it's already data." – Respondent 05*

Since respondents cannot control data that is already shared, then they also cannot control the possibility of the data usage, which puts them at risk of data-owner linkage. This is important because respondents see data as something that is not fragmented or modular. Data such as credential is a document with several attributes that is interconnected. If some part of the data is shared, it is possible to create a link back to the owner (Respondent 05). This is also supported by the fact that since data is an intangible object, it is hard for respondent to exert control as data can be replicated easily without trace (Respondent 02, Respondent 05). Lastly, because of the public good status of data, respondents might not know the user of their health data. This is important for respondents because they want to have usage transparency and know how their data is spread.

6.2.4. Effects of SSI functionalities on Personal Data Sovereignty

Based on the findings from previous section, this section will explore and explain how SSI functionalities (specifically data minimization and data revocation) would help individuals in retaining personal data sovereignty (PDS). The findings start with an explanation of data minimization effect on personal data sovereignty in Section 6.2.4.1, followed by an explanation of data revocation effect on personal data sovereignty in Section 6.2.4.2.

6.2.4.1. Data minimization effect on personal data sovereignty

During the interviews, data minimization is identified by two levels of codes: "selective disclosure" and "on-off data attributes". "Selective disclosure" signifies respondent's ability in selecting which VC data will be included in a VP, whereas "on-off data attributes" is the toggle switch designed to select which data attributes from credentials they would like to share. Most of the respondents find "on-off data attributes" as a simple and straightforward operationalization of selective disclosure (Respondent 01). Selective disclosure enables respondents to be more protective over their data for particular reasons, such as privacy (Respondent 06, Respondent 09). The pattern found between data minimization and personal data sovereignty is presented in Figure 6.11, which is derived from the co-occurrence analysis and quotes from the interview transcription.

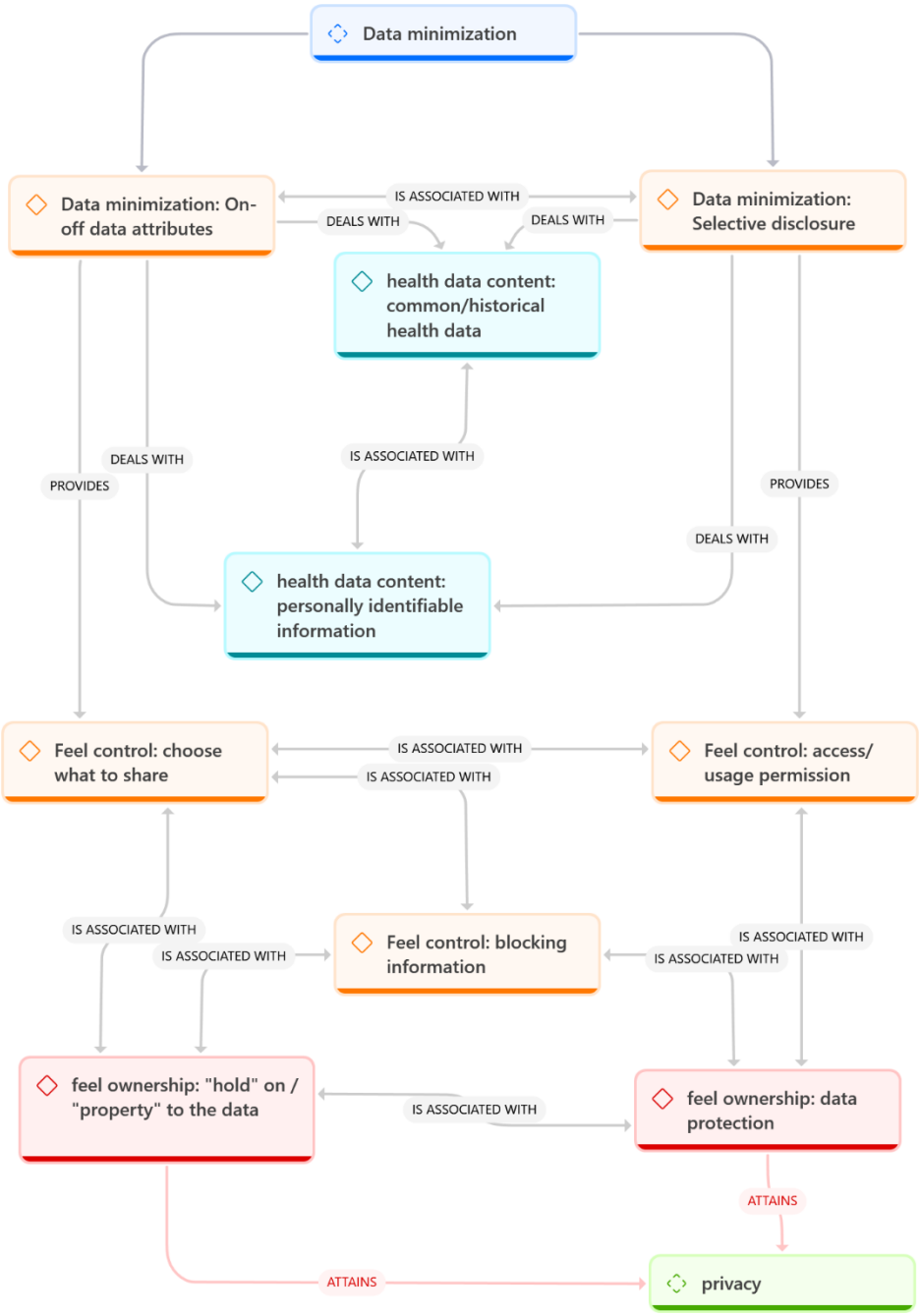

Figure 6.11 Data minimization positive effect on personal data sovereignty

The following quotes highlight the value of data minimization in providing individuals with control:

> ***Quote 6.4.*** *"Data minimization gives me control. Because sometimes, there is a situation where I have to share data whether I like it or not. I will feel like I have ownership over the data because* ***I feel more flexible with my own data. I have the option to share all or selected data****. Even though I share some of it, it's still my data. There are still some that* ***I'm still holding back****." – Respondent 06*

> ***Quote 6.5.*** *"The feature(data minimization) is influential because if it is not there, it seems to raise some concerns, such as the name* ***does not want to be shown****, then the address does not want to be shown, then there is a medical record or national register number, there is a national register number for*

*treatment because the medicine is free. It can be accessed if you use that number. That's **why I want to turn that on and off. It's good if we can control everything without being restricted**." – Respondent 01*

Respondents think that on-off attributes and selective disclosure should be used when controlling a particular VC before sharing it (Respondent 06, Respondent 09). From the interviews, respondents mentioned that they can use both functionalities for two types of health data content, one of them is personally identifiable information, such as name, location, gender, and age, and the other one is common or historical health data, such as medical intervention and medical results, both associated with personally identifiable information. (Respondent 04, Respondent 14). Selective disclosure would allow respondents to choose what VC to include in the VP, whereas using on-off data attributes, respondents can choose what to share from VC attributes to the VP. Several respondents also mentioned that by being able to turn off not only the data attribute but also the VC, they can feel control from blocking the information. This supports data protection and feeling hold of an identity credential (Respondent 03, Respondent 04), helping respondents to have privacy.

Despite the positive effect of PDS, data minimization still has limitations in addressing PDS, which can be seen in Figure 6.12.

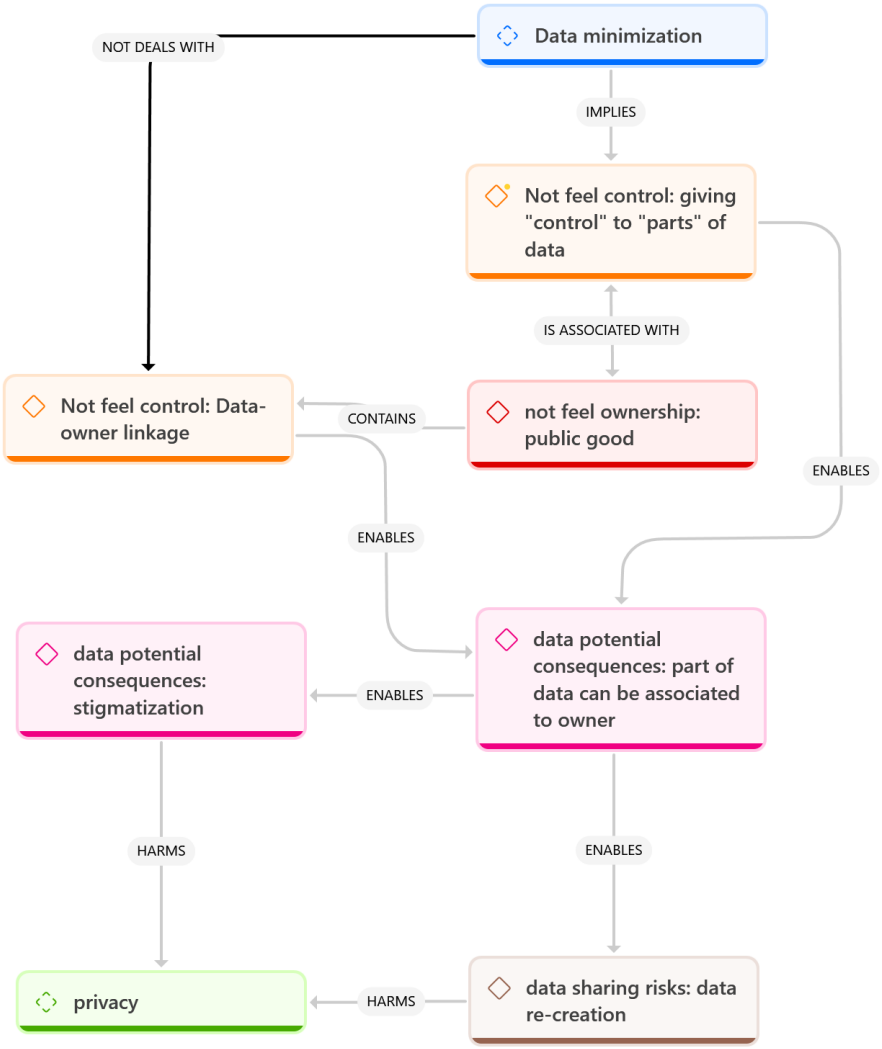

Figure 6.12 No effect to personal data sovereignty from data minimization

As elaborated in the previous findings, data minimization allowed some parts of the data in VC to be accessed by the data consumer, which individuals mentioned to have less control over the shared data. There is a risk of the data becoming a public good as it can be accessed by other parties and might be used by third parties. Additionally, data minimization does not deal with the existing linkage between data and the owner, such as

limiting access to data that is in another database that can be associated back to the owner, risking stigmatization, and harm their privacy. By not being able to control the linkage, respondents mentioned that they can still be unknowingly associated to the data, as mentioned in the following quote:

> ***Quote 6.6.*** *"I don't feel like I have control (from data minimization). Can I control the data that will be shared? yes, but can we fully control the data that we shared, and do I feel like we own it? Not really. Because the problem is that we have different ownership and a sense of control. If control is that there is a part that is shared, we can control what is shared, I agree.* ***But because data is abstract, even if we share part of it, part of the data is still one whole data, even if people say it is only for diseases or other information, but if the person who receives it can connect the information to other information, the data will come back.*** *So the first control I can do is only at the beginning, but the data association is still there." - Respondent 05*

From these findings, the effect of data minimization can be seen that it has a direct impact towards feeling control. However, it does not have any direct impact on ownership, but the pattern of the feeling of control invoked from data minimization has a relation with individuals feeling more ownership. The findings that some people mentioned that data minimization does not lead them to have any control implies that there is still some concern. Even though data is shared and minimized, some people do not feel control and requires additional measures.

6.2.4.2. Revocation effect on personal data sovereignty

Most of the respondents thought that revocation functionality helped them to regain full control over what has been shared. Respondent thinks that data revocation can be used in 4 conditions; (1) retract data when they think it is necessary, such as pulling the VP from circulation when it has exceeded a certain duration (Respondent 04). Another point of view is that (2) data revocation should be available when respondent has a second thought or doubts over the shared data. Since data sharing requires respondents to be careful, they need to be fully informed on the context of their data usage. Some respondents thought that it is important that they can retract data when they realize how the data could potentially harm their privacy (Respondent 03). For the respondents, this will be beneficial for them only if the revocation is simple and straightforward (Respondent 03). Next, (3) data retraction in times of problems such as a data leak and (4) revocation based on contract.

Contractual agreement provides respondents with acknowledgment and guarantee that breaches will be legally prosecuted the terms of the contract will be honored and executed (Respondent 13, Respondent 04). The contract needs to be acknowledged by the stakeholders within the healthcare ecosystem, such as healthcare financing institutions and healthcare facilities that utilize healthcare digital infrastructure (Respondent 09, Respondent 14). Being able to revoke access is a translation of granting access/usage permission, thus providing the respondents with control and ownership.

However, the study does not find whether data revocation has connection to the negative aspect that did not help individuals to reach PDS. Some remarks from interviewee only mentioned that transparency of their data usage can support their decision, such as following quote:

> ***Quote 6.7.*** *"The control is only in our part, we can give or sometimes just revoke, but if for example the use of the data, we do not know, do they really use the data for that. [...]* ***if there's a (usage) history, okay, that can help****" - Respondent 13*

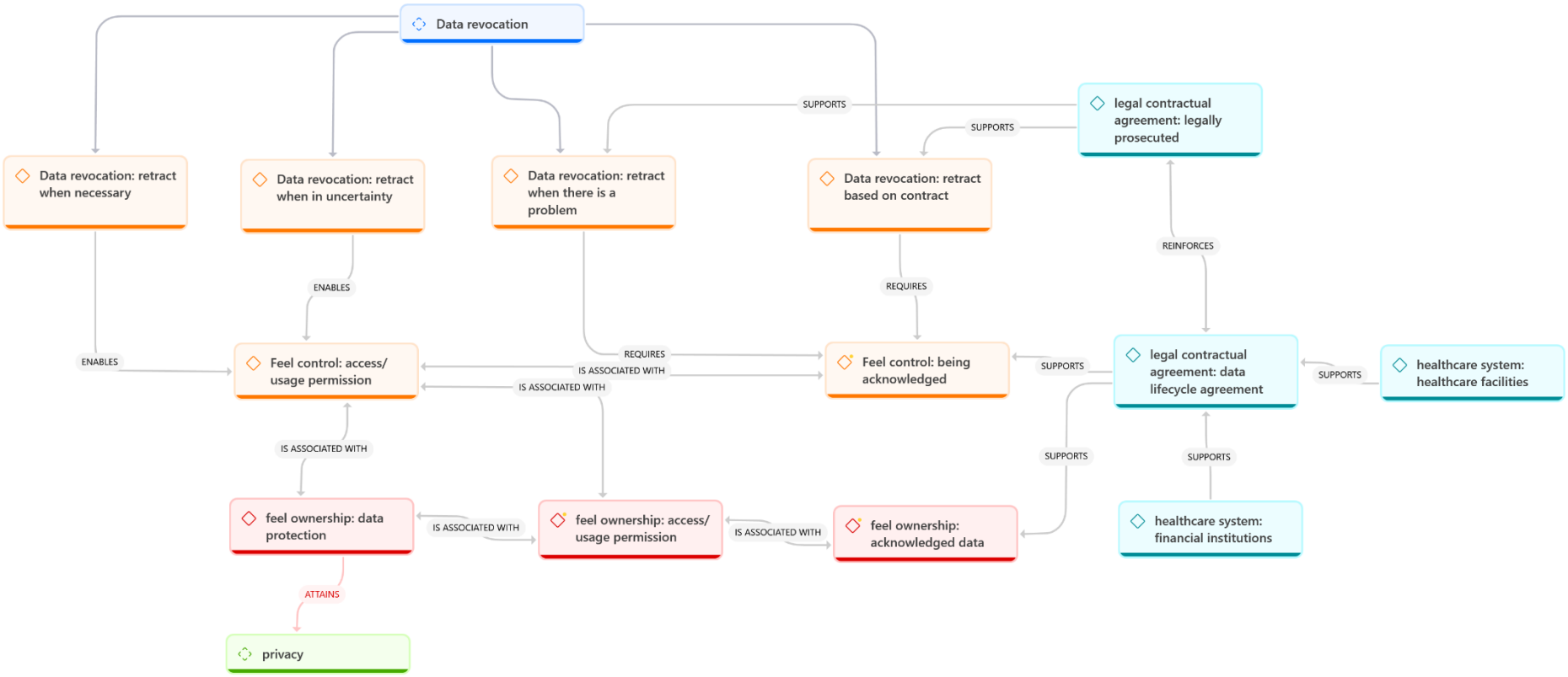

Figure 6.13 Data revocation effect to control and ownership

6.2.5. Other relevant findings

6.2.5.1. Influence of data-sharing experience on the effectiveness of SSI functionality

During the interview, some of the respondents mentioned the experience when they interact with the design artifact. Several respondents had familiarity with data sharing gained through education or experience. For example, Respondents 03 and 05 were exposed to the conduct of data sharing and gathering in Netherlands and the risk of personal data, another example is Respondent 09 having experience to share personal health data for applying house credit. This experience made respondents realize the risk when sharing their health data (Respondent 03, Respondent 05, Respondent 09), leading them to be more critical over the data. This is reflected in how they perceive the effectiveness of data minimization in providing them with control, as experience is found to be associated with their perception of the interface. For people with experience in data sharing, a more complex interface that includes a warning pop-up pattern is preferred as it provides them with more barriers to sharing data and allows them to be more critical of its use. On the other hand, for respondents who did not mention any experience or awareness towards data sharing except during health treatment, the pattern of accepting a simple interface was found. This led our finding to build a hypothesis where experience in data sharing influences the perception of interface, which subsequently acts as a moderating factor between the data minimization functionality and the feeling of control, as shown in Figure 6.14.

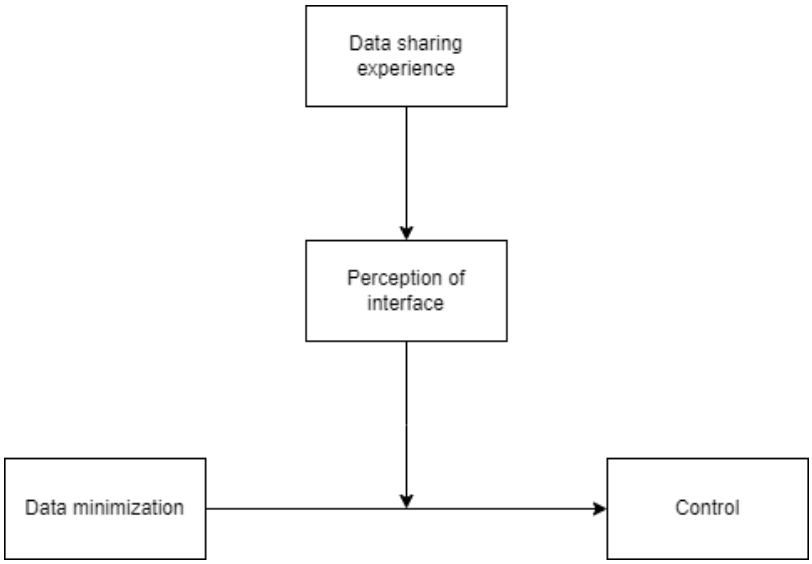

Figure 6.14 Moderating effect of data sharing experience

Their concern can be addressed by the SSI design artifact such as adding warning sign for every action taken and implementing legal components such as contractual agreements. Some respondents also indicated that there should be more barrier before agreeing to share such data, as presented in the following quote:

> ***Quote 6.8.*** *"**The usage details should not be that easy to accept**, if earlier you could accept the request with one click, it seems extremely easy to accept the contract, **it should be more difficult.** [...] apart from the interface, for example information about the purpose of sharing data, it should not be in the form of a notification. Then other descriptions that can be presented in a PDF can also be better. **The interface is interesting because it shows that people can have more control because the interface can condition people to be more concerned about their data**." - Respondent 05*

> ***Quote 6.9.*** *"I also feel that (design artifact) is quite good, especially the feature to revoke access directly, without it being too difficult to do, **in my opinion it is better to make it difficult to provide access** (through data minimization) and then easier to revoke access [...] I personally have the experience of often regretting it after filling out a survey or using it, I feel like oh yeah, it seems like this can be tracked, it turns out it goes here or something, oh it turns out this is quite sensitive for me, I realized it after this, after filling it out. [...] I need to be more careful" - Respondent 03*

From the comments, the pattern between data sharing experience and the perception of the interface was found in Figure 6.15, where respondents with experience in data sharing showed a pattern of a need to be in control by being informed of what their situation is. Such needs are associated with the SSI design artifact to provide a more complex interface that shows them the information on the data sharing, such as from contractual agreement of warning sign. By having more information at hand, respondents feel that they are well-informed and can be more cautious in selecting what data needs to be shared, influencing their perspective on the effectiveness of SSI functionalities. From these findings, it showed that data sharing experience affects the effectiveness of SSI functionalities through the perceived interface usability.

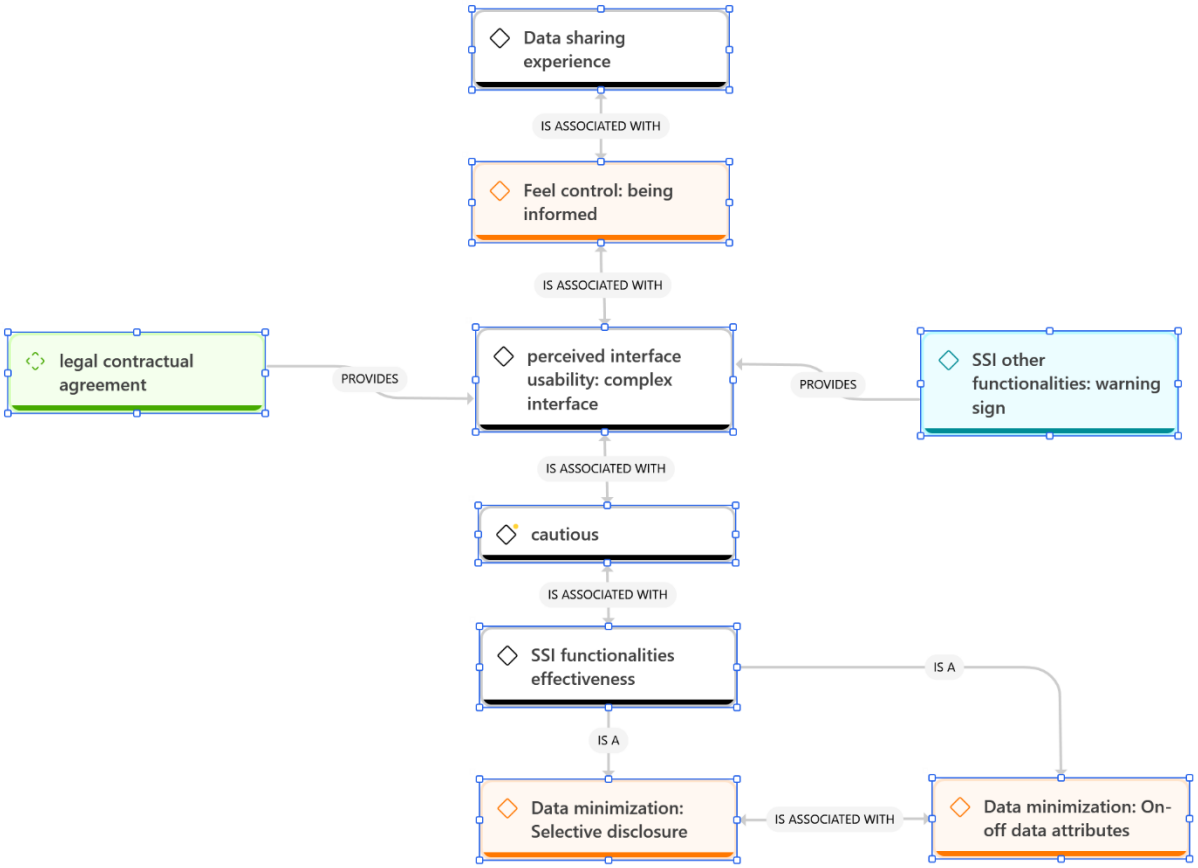

Figure 6.15 Functionalities effectiveness factors

6.2.5.2. Trust and contractual agreement as the foundation of user's willingness to share data

The study asked several respondents about their decision on why they are willing to share their health information to strangers, which mostly depends on the verifier's trustworthiness. To assess their trustworthiness, there are several patterns found from SSI that could bridge user assessment for the risk which can be seen in Figure 6.16. Most of the respondents mentioned that they need to receive formal notification such as email from the data consumer (Respondent 01, Respondent 15). The need for formal notification is said to help them interact with the data consumer so they can ask several questions about the data that they need and the terms and conditions, enabling them to measure data consumer trustworthiness (Respondent 01, Respondent 15). Another way to convey the formalities of the notification can be supported by informed consent and contractual agreement in SSI. Respondents mentioned that from the informed consent and contractual agreement, they need to know who they are interacting with, such as the name of individuals or organization, which is important for them so they can do background check and mitigation measure when there is a trouble (Respondent 11, Respondent 13).

One notable finding from the respondents is that they still do not have enough trust in the digital wallet, saying that verifiable credential provided by the data requester is insufficient to convince them for data sharing. They

still demand a formal letter with official letterhead and stamp to indicate their credibility, as mentioned in the following quotes:

> ***Quote 6.10.*** *"If the request does not look official and convincing, it seems questionable. It seems like it is not enough to just provide information that the data will be used from such and such date to such and such date. But, how is the letter structured, is it true that* ***we can cross-check it, in the letter we definitely have a telephone number, address, oh the address is here****, so, if for example the worst case my data is used to slander me or to ruin my career, I can go to that person, go to that place. If it's summarized like that, I will not share anything." - Respondent 13*

> ***Quote 6.11.*** *"**If the (verifier) has an official letter, there is a signature, there is a letterhead like that, yes, I will definitely give it,** but if it's just a blue tick or something like that, I have a bit of a trust issue, but if for example it is indeed an official letter, there is a letterhead like that, There's a signature like that, which is more convincing to me that the data will not be misused." - Respondent 13*

Other components that need to be mentioned are the list of verifier affiliations in which they will reshare individual's data and verifier request's purpose. Some respondents realized that when they shared the data, the data can be reshared to third parties that might also can gain benefit from their data. However, respondents mentioned that the design artifact only provides information of the requester, but not the affiliated parties who also can have access to the requester's data. They mentioned that they also need to be able to know who they are going to share the data with and select which affiliation they will allow for data-reshare (Respondent 06, Respondent 10). Related to the purpose of the data sharing, respondents mentioned if the request is about improving research or related to their health benefit, they are willing to share it (Respondent 04, Respondent 09, Respondent 13). However, they also need to know why they need to provide certain data, especially those with sensitive information (Respondent 04, Respondent 06). Respondents think that the more sensitive information, the higher the risk and the consequence when it is shared, as mentioned in the following quote:

> ***Quote 6.12.*** *"For me, it depends on what is requested, meaning if the data is ordinary data, ordinary health data, then for example, if it is related to that, for me it is also okay to share it, it will not cause any unpleasant effects, maybe,* ***but if it is related to some data that we want to keep, such as *Disease* status, sexually transmitted infection data that we have to talk about carefully, well, that might be very important for who we can share this with,*** *but for other data, in my opinion, it depends on the interests (of holders) whether the data needs to be protected or not. " - Respondent 4*

> ***Quote 6.13.*** *"If I want to use the prototype**, I still have to meet (the requester) first**. Or there must be something like chatting. Basically, there **is evidence that the (requester) is trustworthy**. Whether the evidence is online or offline, like a meeting. If it's online, it can be from chat, it can be from phone calls, it can be from digital footprints, there are many of them. [...] (meeting) can be trusted and there is a plus point. [...] if I don't meet, I won't give the data**, unless there is already something like a purpose**, well it goes back to... it goes back to what the purpose is, is there any benefit for me or not, for both of us, so both of us benefit... benefit doesn't mean in the form of money or anything like that. For me,* ***the purpose is as long as the purpose is right, and I understand the purpose, as long as the purpose is good, then it's okay.****" – Respondent 15*

This finding showed a pattern that before individuals use SSI to share data, they need to be willing to share the data first, which requires information that helps them decide whether to participate. Such information needs to be formalized and comprehensive, so individuals are confident that the data is safe when it is shared. Such findings give this study insight that the willingness to share data is a prerequisite for individuals to use the SSI functionalities.

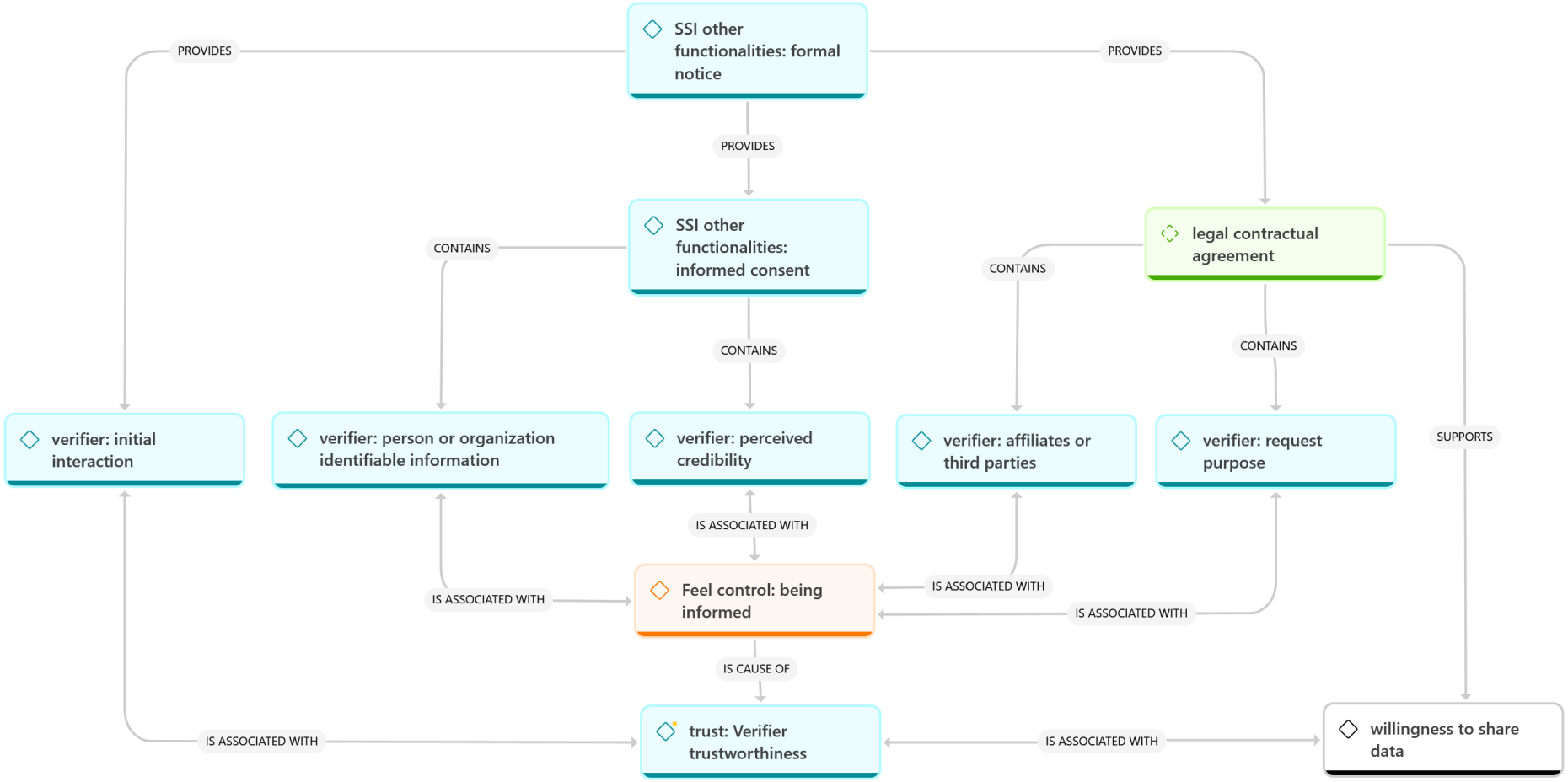

Figure 6.16 Willingness to share factors

6.2.6. Final conceptual framework

This section generalizes the previous findings and elaborates on how SSI functionalities will affect the PDS which can be seen in Figure 6.17. From the first findings, we learn that there is an interrelation between control and ownership, which shows that the more control they have, the more ownership they can feel. If they can select data, then respondents can decide on data access or usage and protect the data. Then, most of the control can be attained using the SSI functionalities. However, none of the functionalities can directly provide the feeling of ownership. This is reflected in how each functionality enables users to feel control first before invoking the feeling of ownership.

Extending the conceptual framework, the study learns that both control and ownership are needed because there are privacy-related goals that individuals would like to achieve, such as maintaining reputation or medical needs that require the sharing of sensitive information. Such privacy reasons come from the sensitivity of health data, which can include personally identifiable information or common/historical health data. The potential problem when sharing health data is that the data can be associated back to the owner, and if such data has sensitive information, it can create stigmatization for the owner and harm their privacy.

In terms of the contextual factors that support the SSI functionalities, two factors were identified. The first factor is the effectiveness of SSI functionalities, which is connected to how individuals perceive utility from the SSI interface. This can be affected by the level of individuals' data sharing affinity. This study showed that people with exposure to data-sharing activity with health data have a pattern to be more critical. They demand more information to be included in the interface so they can make better judgments. The second contextual factor is the willingness to share, which is defined as how the individual would like to let go of parts of their data to be controlled by other parties. On these contextual factors, the willingness of the individuals to share data showed by pattern from verifier trustworthiness before interacting with SSI functionalities, which can be affected by the presence of legal and contractual agreements and provide rules such as responsibilities and rights for the individuals and data consumers over the shared data.

Lastly, there is trust, which is defined as the level of confidence of individuals in taking risks and sharing the data with the data consumer. To develop trust, individuals need information describing the credibility of the verifier, which also extends to the verifier’s affiliation and the purpose of the data-sharing request. Some of the respondents were adamant that they need such information in formal notice so they can be sure that the data is not going to be misused. Figure 6.17 summarizes the final conceptual framework of this study.

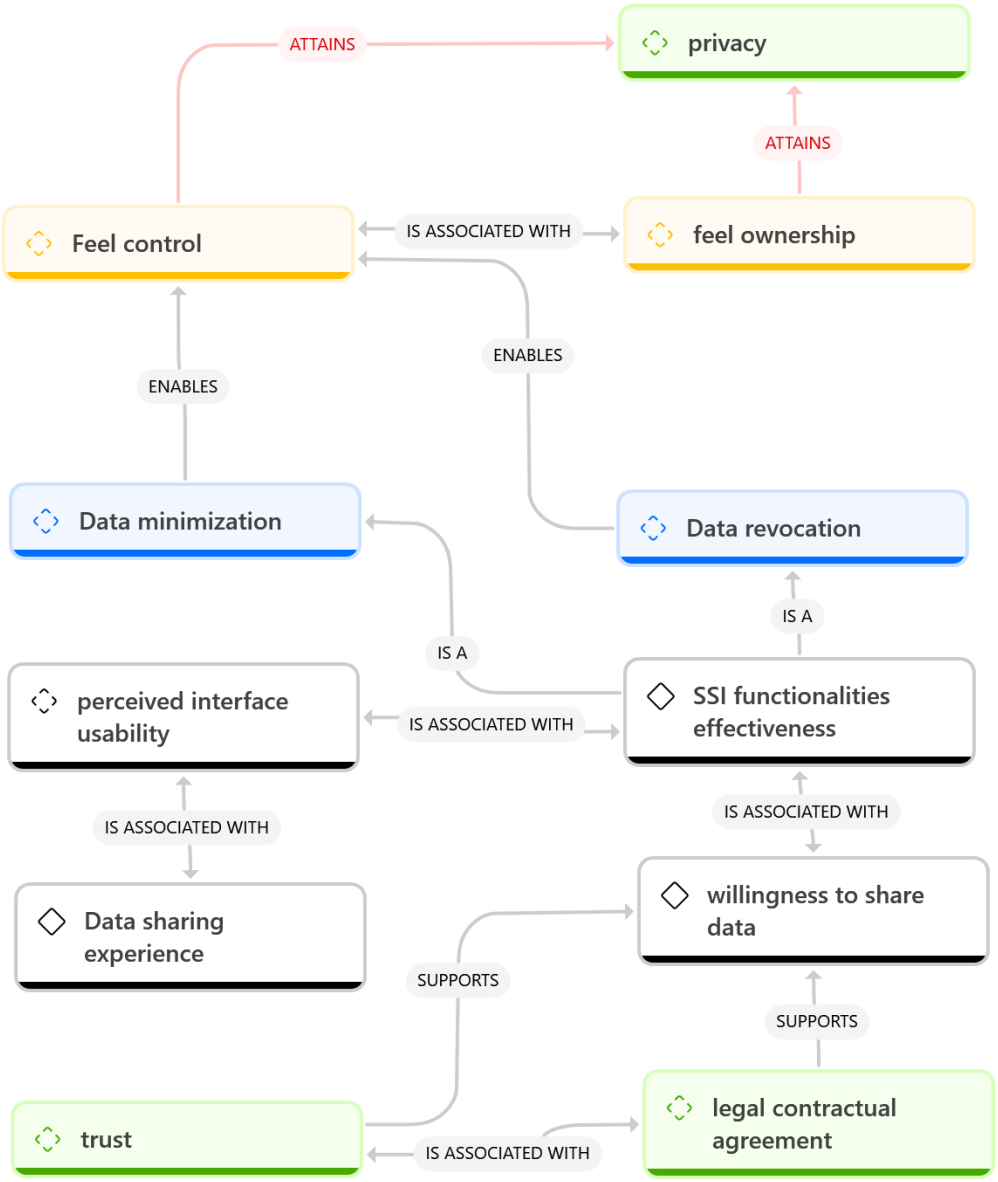

Figure 6.17 Final conceptual framework

6.3. Summary on Chapter 6 and Discussion on Hevner's Rigor Cycle

Chapter 6 provides answer to SRQ3: "***How can SSI functionalities help*** *LMIC users achieve data sovereignty in the health data ecosystem?",* through the demonstration and evaluation of design artifact developed in Chapter 5. In this chapter, design artifact is demonstrated and evaluated by selected respondents by completing two scenarios: (1) Evaluate and approve issued credentials, and (2) Evaluate and approve data sharing request. The scenarios take place in the context of health data sharing requested by an external research institution for research purposes, in which the respondent would have the opportunity to experience both the role of a holder and a verifier in the SSI context. The scenario developed for artifact design has proven to be useful in guiding the demonstration and evaluation step, in which respondents can provide specific feedback for specific functionalities (in this case, data minimization and revocation). The development of a clickable design artifact in the form of a digital ID wallet has also gained positive feedback and demonstrates the user-friendliness of the artifact, as indicated by the lack of need for author's assistance during the demonstration and evaluation session.

As a part of the Rigor Cycle, this step highlighted user feedback that can be used as the basis for artifact design in later evaluation, including adding pop-up window that warns users before agreeing to share data, and

providing more context in the notification of new credential, such as mentioning the type of test and when the test was taken. In terms of the connection with knowledge base, the demonstration and evaluation step has exhibited the usability of design patterns found from literature review, and adaptation from existing digital wallet has proven to provide a well-functioning design artifact.

The demonstration and evaluation sessions were guided by semi-structured interview protocol and questions, in which each interview was recorded and transcribed to be analyzed using the coding methodology. Patterns found that SSI functionalities, particularly data minimization and revocation, can help LMIC users in achieving data sovereignty, particularly in retaining the ownership and control values through coding and content analysis. It is found that empirically, ownership and control are interrelated. Answers from respondents indicated that to feel ownership, they need to be acknowledged over their rights and must be able to exert control over their data. Data minimization allows respondents to selectively disclose parts of personal information that they are willing to share, whereas revocation allows respondents to “take back” the data from third parties whom they have granted access too. Both functionalities provide respondents with control, which in turn also enhances their feeling of ownership over their data. The more rights, responsibilities, and decisions they can make over their data, the more sovereign they feel. However, the respondents also expressed their concerns about risks in sharing data, such as the change of status of data into public good when data are partially available through multiple sources, causing individuals to lose control over their data, and the risk of deanonymization where siloed data can be brought together and traced back into an individual. This pattern showed more within the population of respondents with socially stigmatized disease, which 7 out of 10 respondents. Additionally, all respondents mentioned the importance of detailed contractual agreement between users and a credible third-party, which related to the verifier trustworthiness when asking their health data, which showed pattern of an important concern for respondents before they are participating in data sharing activity.

7. Discussion & Contribution

After all of the DSR steps are implemented in this study to answer SRQ 1-3, this chapter will discuss the findings by reflecting them to the components brought up in the study, including literature review and methodology. This chapter will be divided into several parts following the structure of this report. The first part is the discussion on the literature review (Section 7.1), which points out how the research could fit into the study of HDE, PDS, and SSI, which can be seen in the Section 7.1.1., 7.1.2., and 7.1.3. respectively. Then the reflection continues in Section 7.2. to discuss the methodology that has been implemented. The discussion will arrive to the implementation aspect of SSI in LMIC in Section 7.3. Lastly the contribution for practical and academic perspectives are elaborated in Section 7.4 and 7.5.

7.1. Linking to the literature review

7.1.1 Implementation of self-sovereign identity in HDE

From this study's Environment Analysis (Section 4.1), we can see the components of a health data ecosystem that include actors, roles, relationships, and resources (Grossman, 2019; Marcelo et al., 2019). This study identified stakeholders within a HDE, their interests, and influences, and positions patients as the central stakeholder as they are the users of healthcare services provided by healthcare facilities and healthcare workers. The implementation of SSI in HDE exhibits how SSI can accommodate the actors and roles within the HDE, specifically in the context of data sharing. SSI covers identity management system and credentialing, which is a small part of health data ecosystem, but provides an essential first step of convincing individuals to participate in the data ecosystem.

Additionally, there is a gap of understanding between the roles in SSI and HDE. Knowing that roles in SSI consist of 3 categories, compared to the roles in HDE, there are more than 10 roles with sub-roles that can interact with other stakeholders. This makes the stakeholder analysis in the healthcare system too small for simulating the stakeholder analysis in HDE. Another concern with the differences in roles between SSI and HDE is the possibility of interaction that is required to accommodate the stakeholders. The current research only covers the interaction of data sharing that has a direct approach from data providers and data consumers. However, there are others who may be involved in HDE, such as data aggregators that collect particular data as a whole before sharing it with other actors (Immonen, 2014), or data brokers that promote and match data owner and data consumer (Immonen, 2014), then the interaction may not only covers the shifting roles only between holder and verifier, then probably might also require how issuers can be included as well. On the other hand, there is a possibility that SSI itself may not be able to facilitate interaction.

When testing the design artifact, there are two problems that kept coming up – provision and appropriation dilemma (Purtova, 2017). When being asked about data sharing concern, most respondents expressed the need to understand their data usage, which must not harm their privacy. This is reflected in the provision dilemma as they are afraid the data will be used to affect their daily lives. The second one, appropriation dilemma, surfaced when most of the respondents mentioned that there should be an ethical approach when data sharing can affect the interest of individuals. During the evaluation, most of the interviewees mentioned that they require verifier's credentials and the purpose of using their data so the respondents can be confident in sharing data. In the context of the individuals, SSI can help solve the two dilemmas. Moreover, as shared data in the ecosystem can be considered as public good, there will always be a possibility of data misuse without the consent of data providers. SSI can address the dilemmas that occur before personal data is shared; however, when the data is already shared, there will always be concerns of ethical usage and security risk about their data.

7.1.2 Interrelation of values in PDS

Personal data sovereignty involves the ability of an individual to manage and control data flows and information resources. This study focuses on ownership and control as two key values of PDS, and from the findings, we learn that even though existing studies identified ownership and control as two separate values, in practice they are highly interrelated. This is aligned with the fact that ownership is a *right* embedded to an individual, whereas control is the *ability* of the individual to exert his/her right. Ownership causes an individual to feel entitlement to control over their data, and exerting control over data reflects their ownership. During the interviews, some respondents also showed difficulties in differentiating between ownership and control, indicating that the two

values often got intertwined in user's understanding. For instance, when being asked if the design artifact was able to provide them with the feeling of ownership, they said "Yes, because I feel control over my data". Answers provided by respondents also indicated that the more control they can exert over their data, the more they feel like they own the data. For instance, when they decide to revoke access to data, they also expect the data to be deleted from the data repository, and they want to be able to retract data access halfway before the end of contract if they change their mind.

The analysis of this study identifies 'privacy' as one of the codes. According to Austin (2014), privacy is a result from one's ownership over something and can be attained by control and power the owner is entitled to, as guaranteed by law. This definition aligns with the findings of this study, where ownership and control need to be supported by legality in order to create a sense of privacy in individuals. Respondents emphasizes the need for a detailed contractual agreement and terms & conditions that need to be agreed by both sides (data provider and data consumer), in which they expect to be protected by the law should anything bad happens to their data.

7.1.3 The importance of contractual agreement and trust in self-sovereign identity

The findings from this study showed that SSI does affect personal data sovereignty, especially to the extent of feeling control towards individuals' health data. This does align with the data control requirements that has been elicited by von Scherenberg (2024) where the control needs to be able to identify the data asset, the relation between data provider and data consumer, the access and usage to the data asset, transparency, and the needs for negotiating agreement for the access and usage of data. Yet, the findings in this research have shown more nuances for the data sovereignty as the individuals in LMIC have prerequisite before using SSI functionalities.

Some of the individuals thinks that the feel of control and ownership should begin before they are interacting with verifier through SSI functionalities, which they need to know who the verifiers are and how they are going to use the data, meaning they need to know the verifier credibility in formal way. This can be reflected in how the research in this study conducted, where most of the respondents willing to share their data when they know who the researchers are, the researchers' contact, and what kind of data the researchers would want. As the study focuses that having control and ownership would make people to opt-in for data sharing, the findings from quote G.11 and 6.12 showed pattern that the willingness itself might have become a prerequisite for having personal data sovereignty before it can be exercised through SSI. This finding challenges our understanding whether willingness to share data in LMIC is more important compared to personal data sovereignty.

The study also learned from the data sovereignty model in the information system (von Scherenberg, 2024) that sovereignty can be upheld if there is a contractual agreement that discusses the access and usage of shared data. This is aligned with the design patterns identified by Cucko et al. (2022). From the respondents' interviews, the presence of contractual agreements can support the effectiveness of SSI functionalities, especially in data revocation. From the findings, the usage of contractual agreements has given individuals the basis to understand their rights to their own data. The study argues that this is important for individuals because it gives legitimacy to their right to control and protect information that is embedded in health data which affect their willingness to share their data.

The extent of benefit of the contractual agreement also includes other SSI functionalities that help individuals decide the data sharing activity, such as interaction authorization, which is a functionality that allows individuals to accept or reject the verifier's requests, such as permission to connect and permission to ask the data. When establishing the connection, most of the respondent thinks that they need to be sure of the verifier's identity, whether they are trustworthy or not. This leads to most of the respondents demanding clear, informed consent from the beginning that consists not only of the identity and credibility of the verifier but also of the initial contract terms. For example, some of the respondents mentioned that the usage of informed consent, availability of contract covering data processing for this study, and the data management plan would give them sense of trust to share the data. In essence, the respondents are more willing to participate in data sharing activities if a clear contractual agreement is provided.

7.1.4 The unidentified direct effect of SSI functionalities to ownership

When comparing findings to the conceptual model, one difference that this study found is that there is no identified pattern that shows a relation or effect from the selected SSI functionalities to the ownership value.

Refer back to the literature review from Hummel et al (2023), the study learns that the dimensions of ownership that can be implementable in SSI design artifact can be seen either through property–quasi - property, which concerns about controlling data flow, Protection – participation that focus on consent and secrecy, and individual – collective that contributes to the public good. Reflecting to the selected SSI functionalities, both data minimization and data revocation functions allowed individuals to have these three dimensions. However, our findings showed that most of the respondents feel ownership when they see their data asset, which is their VC, in the digital wallet which has been explained in Section 6.2.1. This showed that having a safe and secure space that store all the data that related to the owner can make individuals to feel ownership, which adds a new perspective that ownership can be seen through a simple label that showed data and owner relations.

7.2. Linking to methodology

7.2.1 Suitability of design science research methodology with this study

Chapter 3 stated that this study utilizes a design science research approach that combines the Hevner and Peffer procedures. From the output of this research, this study believes that the methodology is appropriate as the study aims to create a design artifact that will be user-tested to evaluate a particular theory or behavioural research. The methodology has helped the study to build up what behavioural needs to be researched through the problem identification and the connection to the solution objective, which later can be reflected in the design artifact. Benchmark leads the artifact to be presented in the form of a digital ID wallet. In the Hevner's relevance cycle, the environmental analysis provided understanding on how stakeholders interact with health data, presenting how SSI could facilitate health data sharing between the identifiable stakeholders, and it can be used to define the required scenario for demonstration and evaluation purposes. In the design cycle, requirements engineering sourced from literature and app benchmarking were translated into a clickable design artifact. Scenarios were developed to create a detailed use case of the design artifact, which is also beneficial in the demonstration and evaluation step. The scenarios consist of tasks and subtasks that are addressed with design patterns embedded in the interface layer. In the rigor cycle, user feedback was gathered and are included in the findings. The findings provide valuable addition to existing knowledge base, especially in the context of health data sharing using SSI in LMIC.

However, the methodology requires experts to validate the solution's requirements, and finding experts in SSI for the LMIC context is challenging. Although the step is omitted in this study, the gathered requirements have created non-validated functionalities, whether implementable or not, especially in defining the solution's objective. Closing the gap, this study implemented several approaches to validating the requirement; the first one is the literature review that specifically studies the functionalities of SSI. This approach has provided the study with theoretical foundation for constructing the design artifact. However, the problem with this approach lies with the limited amount of literature that discusses the functionalities of self-sovereign identity. To compensate for such limitations, the study also uses different literature, such as books and technical reports, to understand the limitations and what can be built on the interface layer. Another approach that is used to narrow the gap from expert validation is by benchmarking available SSI applications in the market, which has created a clear flow of the functionalities of the SSI design artifact. While data experts can validate requirements, benchmarking with the existing application can also be used to validate the requirements from literature reviews and expanded requirements that are already accepted for actual usage by the user. In the demonstration and evaluation step, the functionalities within the design artifact were validate by the users. It is found that the artifact was intuitive enough, indicated by the lack of assistance required by the users while completing the scenario tasks.

7.2.2 The importance of scenarios in artifact design and development

The scenarios are critical in structuring the design and development step, as well as the demonstration and evaluation step of design science research for this study. Health data sharing is selected as the main scenario to be completed, focusing on an individual user as the data provider, and an external research institution as a data consumer. Both roles have a different interest in this scenario; the research institution needs individual health data to work on their research, whereas the individuals have a lesser interest in the research – the individuals have the freedom either to participate or not participate in the data sharing. This scenario enables us to take a user-centric perspective and understand how individual user interacts with SSI in a real-world context. The

demonstration and evaluation resulted in a detailed analysis of the design artifact, where we can compare real user interaction with the task sequences that were developed. By observing how respondents interact with the design artifact, it is found that the two key functionalities – data minimization and revocation – were able to provide users with ownership and control over their data to a certain extent. This demonstrates that the scenario was able to help author validate the functionalities, as well as providing a sufficient starting point for artifact's further refinement.

This study implements scenario development for artifact design that started with defining an overall scenario (health data sharing), identification of involved entities (patient and research institution), location (Indonesia), story (reasons for data sharing), and details for data access requests. This helps to structure task sequences of a user when using the digital ID wallet. Based on the process of design artifact development, key aspects in scenario development were identified: (1) conducting a stakeholder analysis to understand the interest and influence of selected roles within the scenario, (2) ensuring that scenario reflects real-world activities, (3) creating a breakdown of task and subtasks for each scenario, and (4) develop points of observation. In addition, as scenarios are meant to be a detailed breakdown of user behavior, creating a well-rounded design artifact that can be used by multiple roles demands the development of multiple scenarios. For this activity, the research managed to found patterns whether SSI functionalities will have relation to PDS. However, some of the respondent mentioned that the introduced scenario might not be applicable in medical urgency. For instance, there might be a situation where a user needs to share health data with a new doctor, indicating that the user now has a much higher interest in sharing their data. In such a scenario, the feeling of control and ownership can be diminished since the sense of urgency might require the user to sacrifice their privacy in order to continue their medical treatment or receive health expertise. Most of the respondents, especially those who are sick, raised concerns about how they should be able to share their sensitive health data while maintaining privacy. This also raises a challenge to our understanding of what data-sharing scenario is acceptable in medical settings or how the code of ethics from a particular profession can be aligned to support PDS facets.

7.2.3 Importance of inclusivity in respondent selection

Involving individuals with socially stigmatized disease as respondents of this study has enriched the insights of this study. The demonstration and evaluation steps showed that respondents with socially stigmatized disease were more cautious and critical about their data and has expressed more concern in doing data sharing. Designing for people with higher standards could be considered as including a "safety factor", a concept in engineering which expresses how much stronger a system needs to be for an intended load. However, although this study has succeeded in involving a higher proportion of people with socially stigmatized diseases, the population are overwhelmingly male. This is due to the limitation of finding female respondents, as most of HIV communities that are open to external communications are those with mostly male members. This might result in bias when demonstrating and evaluating the design artifact.

This study found several notable findings on how respondents with socially stigmatized disease behave regarding their health data. Seven out of ten respondents that are sick tend to be reluctant to share their health data if the requester does not have clear credibility or trustworthiness. They are concerned with the requester's affiliates, purposes, and how they would process the data. For people who are not sick and have higher educational degrees, such as a master's degree, while three out of five non-sick respondents mentioned the data requester trustworthiness, they also put stress on the need to be informed of data sharing risk, which should be reflected in the more complex functionality interface in order to feel control. This led us to have a hypothesis about whether people with data-sharing affinity have a moderating effect on SSI functionalities towards control.

7.3. Implementation of SSI in LMIC

The study understands that SSI is still a rather new technology that has not really been implemented in the LMIC settings. While the blockchain-based technology and distributed ledger technology has been around for several years, the implementation of SSI for data sharing in LMIC HDE has not really been explored. This raised several assumptions on this study to design the artifact, such as the assumption that there is a standardized data set that can be interoperable across actors in healthcare systems, an architecture that support the data sharing and storing the VC and VP, and other assumptions that may be required before discussing the interface layer. This

positions the evaluation for SSI in LMIC context as an implementation of a far-future technology that is based on the present problem.

In the case of Indonesia, the study believes that the implementation of SSI has a potential to be implemented for data sharing in HDE. The first reason is that some LMIC have already developed an HDE that integrates healthcare system and other actors to have access to the patient's data, indicating an established environment to implement SSI. Second, individuals in LMIC do not possess substantial differing requirement compared to people in HIC for data sharing, indicating that on the interface layer there should not be a significant difference in design choices. However, the barrier of the implementation may lie on the technical aspect of SSI technology, especially in the infrastructure layer, such as a standardized set data interoperability and architecture that can accommodate different stakeholders.

In addition, we learn that the extent of data sharing experience might also affect people's preferences on data control. If the data has a high sensitivity, then respondent with more experience may require a more detailed interface so they can understand the whole extent of the usage of their data. On the other hand, LMIC respondents indicated that the concept of SSI and verifiable credential is insufficient for them to trust the data requester. Some respondents also need the verifier's credibility in the form of a formal letterhead attached to the notice or a trusted symbol in the interface. This is important for the respondents because it showed that the verifier is genuine to present themselves. This remark indicates that users need to build their data sharing experience and familiarize themselves with new technology.

7.4. Practical Contribution

The practical contribution of this research lies in the design artifact that allowed this research to gather insights from people in LMIC who have concerns about sharing health data, especially for users with sensitive information. From the requirements analysis, we found that data minimization is a well-known functionality in SSI which already being implemented in available digital wallet in the market. However, data revocation remains undeveloped since the revocation only works by issuer and does not include a contractual agreement. As such, practitioner can develop data revocation that can be adjusted based on the extent of data lifecycle which should be reflected on the contractual agreement. Next, the study also provides the overall interface level evaluation on what is the preferences from the user in LMIC when they have to interact with SSI functionalities, for example some respondents mentioned that they requires an in-app functionality between them and verifier for asking the purpose of their request, or another example is some respondents mentioned that they need a clear warning sign on every action that is about to be taken within the design artifact. Another practical contribution from this research is that it provides scenarios where data consumer and data provider can have their role shifted when exchanging data, which can be used not only to the health data ecosystem but also other data ecosystem that allow data sharing can be done with more than two stakeholders within the system.

7.5. Academic Contribution

In regard to academic contribution, Gregor and Hevner (2013) It has created a framework for positioning the contribution of DSR research to the knowledge body, which can be channelled through descriptive and prescriptive knowledge. Since the knowledge contribution from DSR will be based on the previous idea, the framework of knowledge contribution or DSR is based on two dimensions, that are problem maturity and solution maturity, which can be created into a 2 x 2 matrix that can be seen in Figure 7.1, showing 4 categories, improvement, invention, routine design, and exaptation. Based on the findings in this study, the knowledge contribution can be seen in personal data sovereignty (PDS) in the health data ecosystem (HDE) problem through SSI functionalities solutions, particularly in the improvement quadrant.

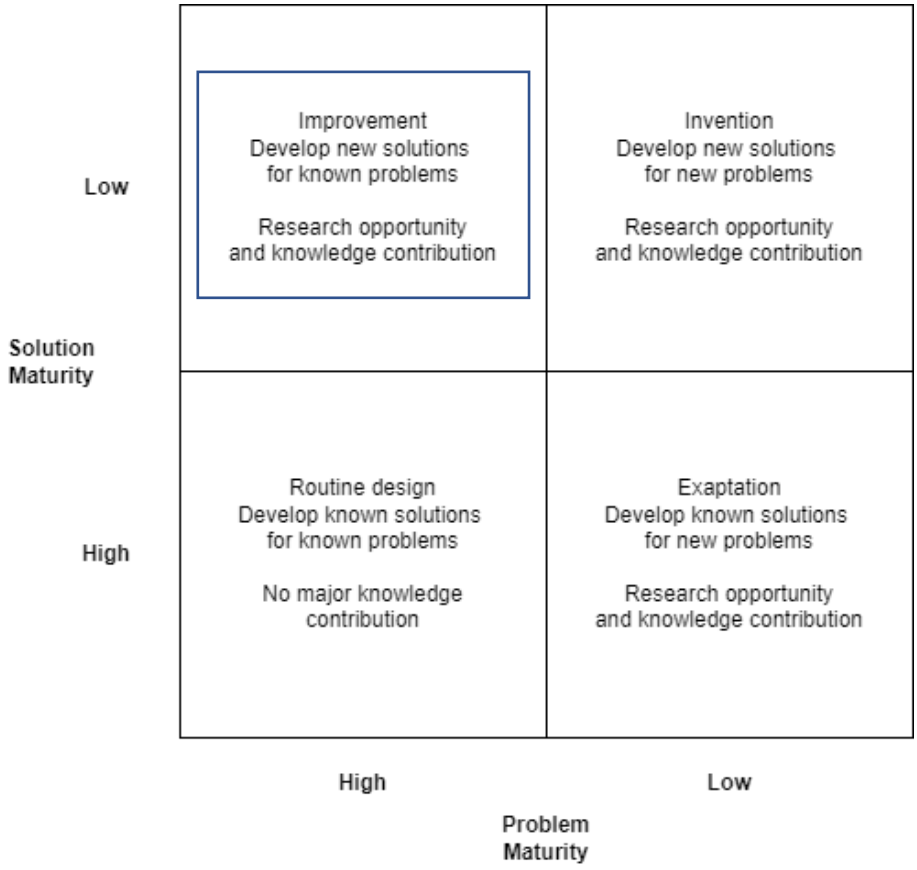

Figure 7.1 DSR knowledge contribution framework (Gregor & Hevner, 2013)

First of all, the problem for PDS in HDE has been reflected through the literature review, such as the lack of data provider involvement due to appropriation and provision problem (Marcelo et al., 2019; Purtova, 2017; Rantanen et al., 2019). However, we also learn how the problem for this provision should be addressed in data space through the data sovereignty model from von Scherenberg (2024), which also highlighted how sovereignty should be reached through the means of control and ownership. From this reference, the problem within the health data ecosystem for personal data sovereignty is a high to medium maturity problem.

Second of all, looking at the literature review, most of the studies regarding SSI functionalities primarily focus on a one-way credential provision such as claim insurance and know-your-customer (Farao et al., 2023; Schlatt et al., 2021). However, the study has not explored SSI functionalities for sharing health data within the health data ecosystem in LMIC, which allowed two-way interaction that has shifting roles within the health data ecosystem, data minimization, and data revocation. Reflecting on the ongoing interest for the research regarding the SSI design artifact, which explores the use cases and technicalities that have been stated in the SSI state of the art, it has put this solution at the low to medium maturity level.

By combining the problem and solution maturity, this research can be placed within the improvement quadrant, where it develops new solutions for known problems, especially by aligning SSI functionalities to the data sovereignty model in information by von Scherenberg (2024), where the data consumer and data provider should have interacted, and they could negotiate the data access and usage through a contractual agreement. The findings showed that merging SSI functionalities (data minimization and revocation) and the data sovereignty model, along with the requirements for control and ownership, does indicate that individuals feel control and ownership in HDE. Respondents showed that they could make sure they interact with a trustworthy requester for some retractable parts of their data based on an agreement, which also suggests that the SSI and data sovereignty model allowed individuals in LMIC to have data sovereignty. Moreover, the findings also showed that on the individual or personal level, feeling control and ownership are interrelated, as shown in the empirical findings. Such findings also suggest that control and ownership have causality or influence towards each other.

8. Recommendations & Conclusions

The final chapter in this research concludes the study by answering the sub research questions and the main research question that has been introduced in Chapter 2 based on the findings from Chapter 4, 5 and 6. This chapter consists of research limitations, conclusions of this study, and recommendations.

8.1. Limitations of this study

There are several limitations of this study. First, in defining the objective for the design artifact solution, the study only relies on the literature review and benchmarking to the existing applications that has been launched for people in HIC. Therefore, it may have created some bias in the requirement analysis. The second limitation is the assigned roles for the scenario in evaluation phase that is limited to patient-hospital-research institution, resulting in a highly specific SSI application. As there are other roles within HDE that can be facilitated through SSI, the flow for SSI functionalities might differ to accommodate PDS for individuals if they interact with different stakeholders. The different scenario might have affected the findings during the evaluation phase differently. In addition, the design artifact in this study does not account for scenarios where incentives may influence a data owner's willingness to share their health information.

Third, the respondents selected in this study have all finished tertiary education, indicating that they are highly educated and thus might influence their ability to navigate the design artifact with minimal assistance. This might not be the case if respondents with limited education background were being included in this study. In practice, the users of digital ID health wallet would have different educational backgrounds, and different insights might be needed to enhance the user-friendliness of the application. Lastly, this study assumes that the prerequisite of an SSI is established in Indonesia, such as infrastructure, blockchain system, and sufficient digital literacy. There are still a lot of technical gaps that needs to be addressed. Therefore, this study still has a limited applicability in the near future.

8.2. Conclusions

In this section, the answers for each sub-research questions are revisited to answer the main research question.

8.2.1 Answering Sub Research Questions

8.2.1.1 Sub-research question 1

*"What are the **requirements** in implementing SSI functionalities in the health data ecosystem to achieve personal data sovereignty for LMIC users?"*

Answer:

After thorough environmental analysis, literature review, application benchmarking for requirement elicitation, and forward research based on relevant references, requirements to implement SSI functionalities in a health data ecosystem were identified and filtered. Based on literature search, it is found that there is no significant difference in needs between LMIC and HIC users, and therefore available SSI apps that were mostly developed for HIC users are assumed to be sufficient for benchmark. These functionalities ensure that LMIC users can achieve personal data sovereignty through effective control and ownership of their data.

The requirements in implementing SSI include design artifact that is developed in the form of a digital ID wallet to allow users interact with the interface layer, SSI functionalities need to uphold PDS values of ownership and control, SSI functionalities need to consider identification of data asset as object of data sovereignty, identification of data provider and data consumer alongside their relation, ensuring data provider can control the entire life cycle of data value chain, ensuring data provider and data consumer can negotiate, and the presence of a contractual agreement. The identified SSI functionalities that need to be present are 1) verifiable credential archive, 2) extended verifiable credential views, 3) review credentials, 4) notifications, 5) review connection, 6) review presentation, 7) interaction authentication, 8) data minimization, 9) and revocation. In particular, the two functionalities of data revocation and data minimization are essential to achieve personal data sovereignty.

8.2.1.2 Sub research questions 2

*"What could be the **possible design artifact** that follows the functionality requirements of self-sovereign identity in health data ecosystem to achieve personal data sovereignty for LMIC users?"*

Answer:

In the design phase, this study has developed a clickable design artifact consisting of seven distinct interface layers that were designed according to the defined task sequence from scenarios, as shown in Figures 5.4 to 5.10. The seven interface layers are: (1) Notification and notification menu detail, (2) Home screen, (3) Credential details, (4) Connection details, (5) Request archive, (6) Request review, and (7) Renegotiate. Each screen is designed to facilitate the interaction of roles in a different context: data provider-data consumer in an HDE, and between holders-verifier in the SSI context. The role-changing situation is addressed in the Establish Connection task, where holder can briefly experience the role of a verifier when checking the credential of data requester. The objective of this task is to allow user to decide whether to allow Research Institution to connect and access their data. The interface screen consists of two layers: Home Screen and Connection Details. In the Connection Details layer, the user can review connection and authenticate the interaction. In the Review Connection page, the verification process happens automatically, and the credentials are updated according to the Research Institution's latest information saved in the data registry.

The Request Review screen incorporates data minimization SSI functionality. This functionality allows user to share only the necessary data, thereby enhancing their control over their personal health information. Additionally, the revocation feature is implemented, enabling user to withdraw from the data-sharing scheme if a particular request is no longer acceptable, thus reinforcing their sovereignty over their data. A notable functionality of the design artifact is the inclusion of a contractual agreement, providing user with a mechanism to exercise control and ownership over their data, establishing clear terms for data access and usage, and ensuring compliance with agreed-upon conditions. By enabling users to maintain control over their data through minimization, revocation, and embed contractual agreements, this design artifact aligns with the core principles of self-sovereign identity, ensuring that data owners are empowered, and their personal data sovereignty is retained.

8.2.1.3 Sub research questions 3

*"**How can SSI functionalities help** LMIC users achieve data sovereignty in the health data ecosystem?"*

Answer:

It is found that SSI functionalities, particularly data minimization and revocation, can help LMIC users in achieving data sovereignty, particularly in retaining the values of ownership and control. It is found that empirically, ownership and control are highly interrelated. Answers from respondents indicated that to feel ownership, they need to be acknowledged over their rights and must be able to exert control over their data. Data minimization allows respondents to selectively disclose parts of personal information that they are willing to share, whereas revocation allows respondents to "take back" the data from third parties whom they have granted access too. Both functionalities provide respondents with control, which in turn also enhances their feeling of ownership over their data.

The more rights, responsibilities, and decisions they can make over their data, the more sovereign they feel. However, the respondents also expressed their concerns about risks in sharing data, such as the change of status of data into public good when data are partially available through multiple sources, causing individuals to lose control over their data, and the risk of deanonymization where siloed, anonymized data can be brought together and traced back into an individual. This concern is particularly prevalent within the population of respondents with socially stigmatized disease. Therefore, although SSI functionalities presented in the design artifact can provide users with personal data sovereignty, a detailed contractual agreement between user and a credible third-party is key in establishing trust and willingness of users to participate in data sharing activity.

8.2.2 Answering Main Research Question

*"How should we **design SSI artifacts** for a Low- and Middle-Income Country (LMIC) health data ecosystem that **retains user's personal data sovereignty**?"*

Answer:

To effectively implement self-sovereign identity (SSI) functionalities in the health data ecosystem for LMIC users, a thoughtful approach in designing SSI artifacts is necessary. This includes the inclusion of potentially vulnerable population that might have a different perspective regarding health data. This study proposes that the design artifact should incorporate data minimization, revocation, trust-building mechanisms, legal clarity, and user-friendly interfaces to facilitate smooth data sharing even as roles change.

Data minimization should be tailored to allow users to share only what is necessary. By specifying the granularity of data attributes within requested credentials, users can understand exactly how their information will be used. This helps them make informed decisions about sharing sensitive data by weighing the risks and benefits, like the quality of medical care. The user interface should clearly explain options and provide detailed control over what data is shared, making users feel more involved and empowered in the process.

Revocation functionality is equally important. The artifact should make it easy for users to withdraw access to their health data whenever needed. This should be supported by a feedback system confirming that access has been revoked, so users know their data is secure. Additionally, conditional revocation should be implemented when there is legal evidence of misuse, with the system keeping detailed records of data usage to support these decisions.

Trust is a key element in health data ecosystem. The system must be transparent about who accesses the data, why it is needed, and how it is used. This transparency, combined with effective revocation mechanisms, helps build trust in the data-sharing infrastructure. A strong legal foundation is also necessary, ensuring that both data provider and consumer are protected. Legally binding agreements should be in place to prevent misuse and provide clear consequences for any breaches.

The interface layer plays a crucial role in this process. While simplicity is generally preferred, some users feel more secure if more complex steps are embedded, creating a barrier in decision-making, and pushing users to rethink their decision. The design should cater to these varying preferences, ensuring that users feel in control and confident. Interactive features like in-app chat, verified labels, and formal notices can facilitate initial interactions and build trust before any data transactions occur. Finally, the system should be flexible enough to accommodate the varying levels of urgency and privacy needs of users. In urgent medical situations, the system should enable broader data sharing to ensure timely and appropriate care. In non-urgent scenarios, it should support more stringent data minimization to maintain privacy.

8.3. Recommendations

8.3.1 Recommendation for users

Even by including people with tertiary education backgrounds, there are still cases where respondents demonstrate their lack of understanding of concepts brought upon this study. For instance, some respondents indicated that to develop trust with data requester, they need a formal letter with an official letterhead and official signature – a function that is actually provided by an issuer-verified VC that is present within the platform. This indicates the need for users in building their data sharing experience and understanding the basics of technology so they can trust the technology and be more inclined to adopting it.

Users also need to be more cautious in participating in a health data ecosystem, from data creation, data sharing, to data usage. Most people are already aware that data is a critical resource that can be misused by criminals and other third parties. Users need to identify ways in which their data can be misused, to avoid being swindled or being further deprived of personal information. For instance, users need to know what things can be done with a national ID number, what information are contained within the ID number, and other personal information like a mother's maiden name. In terms of sensitive health data, they need to identify credible health vendors before using their services.

8.3.2 Recommendation for policy makers and HDE developers

This study provides an insight to how individuals within an HDE perceive their data, alongside their expectations of a data sharing setting. There is a need for the government to develop a thorough data governance policy for health data, to protect the citizens and create a conducive environment that foster trust between stakeholders. The government can benchmark to regions with more established data policy such as the EU or the US. Citizens need to understand their rights and government needs to protect them. Trust is currently what is lacking in the Indonesian data ecosystem – the incompetence of government agents in safeguarding citizen data has caused people to be sceptical in participating within a data sharing ecosystem. Developing a strong cybersecurity capability is key to maintain data sovereignty in the national level. In addition, technical capabilities are essential in the development and implementation of SSI.

HDE developers need to understand stakeholder dynamics and the level of literacy amongst individuals. For LMIC, where educational levels between citizens are uneven, a technological implementation might cause low-educated and low-economic population to be vulnerable to exploitation. This calls for a collaborative approach that involves people with different socioeconomic backgrounds and an extensive educational campaign to build knowledge and capabilities of users.

8.3.3 Recommendations for future studies

There are several recommendations for future studies that can be explored, based on the results of this research. First, future studies could include more diverse respondents since this study found no significant differences between HIC and LMIC. This could be done by specifically including respondents from different age brackets, educational backgrounds, and basic digital literacy levels that represent the general population. Second, this study can be replicated in a different LMIC country, to explore whether the findings of this study would hold in a different setting. Third, implementing a quantitative approach to explore the generalizability of the findings. Fourth, exploring the aspects of a contractual agreement could affect the willingness for individuals to share their data and having more PDS, or research that investigates the rights and responsibility on the access and usage control along with the data lifecycle for every stakeholder when doing data sharing could benefit the connection to PDS. Fifth, a study that develops technological roadmap to the implementation of SSI in the context of LMIC. Lastly, a study that explore the economic feasibility of SSI.

References

Anderson, C., Carvalho, A., Kaul, M., & Merhout, J. W. (2023). Blockchain innovation for consent self-management in health information exchanges. *Decision Support Systems*, *174*. https://doi.org/10.1016/j.dss.2023.114021

Bai, P., Kumar, S., Aggarwal, G., Mahmud, M., Kaiwartya, O., & Lloret, J. (2022). Self-Sovereignty Identity Management Model for Smart Healthcare System. *Sensors*, *22*(13). https://doi.org/10.3390/s22134714

Banse, C. (2021). Data Sovereignty in the Cloud - Wishful Thinking or Reality? *Proceedings of the 2021 on Cloud Computing Security Workshop*, 153–154. https://doi.org/10.1145/3474123.3486792

Beane, A., De Silva, A. P., Athapattu, P. L., Jayasinghe, S., Abayadeera, A. U., Wijerathne, M., Udayanga, I., Rathnayake, S., Dondorp, A. M., & Haniffa, R. (2019). Addressing the information deficit in global health: Lessons from a digital acute care platform in Sri Lanka. *BMJ Global Health*, *4*(1). https://doi.org/10.1136/bmjgh-2018-001134

Belfrage, S., Helgesson, G., & Lynøe, N. (2022). Trust and digital privacy in healthcare: a cross-sectional descriptive study of trust and attitudes towards uses of electronic health data among the general public in Sweden. *BMC Medical Ethics*, *23*(1). https://doi.org/10.1186/s12910-022-00758-z

Blumenthal, D., & Squires, D. (2015). Giving Patients Control of Their EHR Data. *Journal of General Internal Medicine*, *30*(1), 42–43. https://doi.org/10.1007/s11606-014-3071-y

Bull, S., Cheah, P. Y., Denny, S., Jao, I., Marsh, V., Merson, L., Shah More, N., Nhan, L. N. T., Osrin, D., Tangseefa, D., Wassenaar, D., & Parker, M. (2015). Best Practices for Ethical Sharing of Individual-Level Health Research Data from Low- and Middle-Income Settings. *Journal of Empirical Research on Human Research Ethics*, *10*(3), 302–313. https://doi.org/10.1177/1556264615594606

Cappiello, C., Gal, A., Jarke, M., Rehof, J., Aachen, R., & Dortmund, T. U. (2020). Data Ecosystems: Sovereign Data Exchange among Organizations. *Seminar*. https://doi.org/10.4230/DagRep.9.9.66

Chango, M. (2021). Building a Credential Exchange Infrastructure for Digital Identity: A Sociohistorical Perspective and Policy Guidelines. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.629790

Čučko, Š., Šumak, B., & Turkanović, M. (2023). Identification and Analysis of Self-Sovereign Identity User Interface and User Experience Design Patterns. *Proceedings - 2023 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2023*, 166–173. https://doi.org/10.1109/DAPPS57946.2023.00030

Čučko, Š., & Turkanović, M. (2021). Decentralized and Self-Sovereign Identity: Systematic Mapping Study. *IEEE Access*, *9*, 139009–139027. https://doi.org/10.1109/ACCESS.2021.3117588

Dhopeshwarkar, R. V., Kern, L. M., O'Donnell, H. C., Edwards, A. M., & Kaushal, R. (2012). Health care consumers' preferences around health information exchange. *Annals of Family Medicine*, *10*(5), 428–434. https://doi.org/10.1370/afm.1396

Fadler, M., & Legner, C. (2022). Data ownership revisited: clarifying data accountabilities in times of big data and analytics. *Journal of Business Analytics*, *5*(1), 123–139. https://doi.org/10.1080/2573234X.2021.1945961

Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., & Xenakis, C. (2023a). INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00741-8

Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., & Xenakis, C. (2023b). INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00741-8

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access*, *7*, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173

Freytsis, M., Barclay, I., Radha, S. K., Czajka, A., Siwo, G. H., Taylor, I., & Bucher, S. (2021). Development of a Mobile, Self-Sovereign Identity Approach for Facility Birth Registration in Kenya. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.631341

Gil, G., Arnaiz, A., Diez, F. J., & Higuero, M. V. (2020). Evaluation Methodology for Distributed Data Usage Control Solutions. *2020 Global Internet of Things Summit (GIoTS)*, 1–6. https://doi.org/10.1109/GIOTS49054.2020.9119565

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. In *MIS Quarterly: Management Information Systems* (Vol. 37, Issue 2, pp. 337–355). University of Minnesota. https://doi.org/10.25300/MISQ/2013/37.2.01

Grossman, R. L. (2019). Data Lakes, Clouds, and Commons: A Review of Platforms for Analyzing and Sharing Genomic Data. In *Trends in Genetics* (Vol. 35, Issue 3, pp. 223–234). Elsevier Ltd. https://doi.org/10.1016/j.tig.2018.12.006

Guggenberger, T., Kühne, D., Schlatt, V., & Urbach, N. (2023). Designing a cross-organizational identity management system: Utilizing SSI for the certification of retailer attributes. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00620-z

Heriyanto, D. (2018, April 7). Q&A: BPJS Kesehatan, health for all Indonesians. *The Jakarta Post*.

Houtan, B., Hafid, A. S., & Makrakis, D. (2020). A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare. *IEEE Access*, *8*, 90478–90494. https://doi.org/10.1109/ACCESS.2020.2994090

Howe, N., Giles, E., Newbury-Birch, D., & McColl, E. (2018). Systematic review of participants' attitudes towards data sharing: A thematic synthesis. In *Journal of Health Services Research and Policy* (Vol. 23, Issue 2, pp. 123–133). SAGE Publications Ltd. https://doi.org/10.1177/1355819617751555

Hummel, P., Braun, M., & Dabrock, P. (2021). Own Data? Ethical Reflections on Data Ownership. *Philosophy and Technology*, *34*(3), 545–572. https://doi.org/10.1007/s13347-020-00404-9

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data and Society*, *8*(1). https://doi.org/10.1177/2053951720982012

Hussein, R., Griffin, A. C., Pichon, A., & Oldenburg, J. (2023). A guiding framework for creating a comprehensive strategy for mHealth data sharing, privacy, and governance in low- and middle-income countries (LMICs). In *Journal of the American Medical Informatics Association* (Vol. 30, Issue 4, pp. 787–794). Oxford University Press. https://doi.org/10.1093/jamia/ocac198

Janti, N. (2022, November 22). Apparent data breach at govt COVID-19 health app increases privacy concerns. *The Jakarta Post*.

Jarke, M., Otto, B., & Ram, S. (2019). Data Sovereignty and Data Space Ecosystems. *Business & Information Systems Engineering*, *61*(5), 549–550. https://doi.org/10.1007/s12599-019-00614-2

Jentzsch, N. (2018). *Think Tank für die Gesellschaft im technologischen Wandel Dateneigentum-Eine gute Idee für die Datenökonomie?*

Jocelyn, Nasution, F. M., Nasution, N. A., Asshiddiqi, M. H., Kimura, N. H., Siburian, M. H. T., Rusdi, Z. Y. N., Munthe, A. R., Chairenza, I., Ginting Munthe, M. C. F. B., Sianipar, P., Gultom, S. P., Simamora, D., Uswanas, I. R., Salim, E., Khairunnisa, K., & Syahputra, R. A. (2024). HIV/AIDS in Indonesia: current treatment landscape, future therapeutic horizons, and herbal approaches. In *Frontiers in Public Health* (Vol. 12). Frontiers Media SA. https://doi.org/10.3389/fpubh.2024.1298297

Kalkman, S., Van Delden, J., Banerjee, A., Tyl, B., Mostert, M., & Van Thiel, G. (2022). Patients' and public views and attitudes towards the sharing of health data for research: A narrative review of the empirical evidence. *Journal of Medical Ethics*, *48*(1), 3–13. https://doi.org/10.1136/medethics-2019-105651

König, P. D. (2017). The place of conditionality and individual responsibility in a "data-driven economy." *Big Data and Society*, *4*(2). https://doi.org/10.1177/2053951717742419

Lee, Y. H., Liu, Z. Y., Tso, R., & Tseng, Y. F. (2022). Blockchain-Based Self-Sovereign Identity System with Attribute-Based Issuance. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13620 LNCS*, 21–38. https://doi.org/10.1007/978-3-031-21280-2_2

Liu, Y., Lu, Q., Paik, H. Y., Xu, X., Chen, S., & Zhu, L. (2020). Design Pattern as a Service for Blockchain-Based Self-Sovereign Identity. *IEEE Software*, *37*(5), 30–36. https://doi.org/10.1109/MS.2020.2992783

Lockwood, M. (2021). An Accessible Interface Layer for Self-Sovereign Identity. *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.609101

Mahmood, S., Noorali, A. A., Manji, A., Afzal, N., Abbas, S., Qamar, J. B., Siddiqi, S., Hoodbhoy, Z., Virani, S. S., Bhutta, Z. A., & Samad, Z. (2023). Health data ecosystem in Pakistan: A multisectoral qualitative assessment of needs and opportunities. *BMJ Open*, *13*(9). https://doi.org/10.1136/bmjopen-2023-071616

Marcelo, M. I., Barros Lima, G. de F., & Farias Lóscio, B. (2019). Investigations into Data Ecosystems: a systematic mapping study. *Knowledge and Information Systems*, *61*(2), 589–630. https://doi.org/10.1007/s10115-018-1323-6

Ministry of Health Indonesia. (2021). *ENG-Blueprint-for-Digital-Health-Transformation-Strategy-Indonesia 2024*.

Ministry of Health Indonesia. (2022). *Tuberculosis Control in Indonesia 2022*.

Moon, L. A. (2017). Factors influencing health data sharing preferences of consumers: A critical review. In *Health Policy and Technology* (Vol. 6, Issue 2, pp. 169–187). Elsevier B.V. https://doi.org/10.1016/j.hlpt.2017.01.001

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. In *Computer Science Review* (Vol. 30, pp. 80–86). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2018.10.002

Mukta, R., Martens, J., Paik, H.-Y., Lu, Q., & Kanhere, S. S. (2020). *Blockchain-based Verifiable Credential Sharing with Selective Disclosure*. https://doi.org/10.1109/TrustCom50675.2020.00128/20/$31.00

Munoz-Arcentales, A., López-Pernas, S., Pozo, A., Alonso, Á., Salvachúa, J., & Huecas, G. (2019). An Architecture for Providing Data Usage and Access Control in Data Sharing Ecosystems. *Procedia Computer Science*, *160*, 590–597. https://doi.org/10.1016/j.procs.2019.11.042

Nagel, L., & Lycklama, D. (2020). *OPEN DEI Position Paper Design Principles for Data Spaces*. https://doi.org/10.5281/zenodo.5105744

Otto, B., Steinbuss, S., Teuscher, A., & Lohmann, S. (2019). *IDS Reference Architecture Model 3.0*. https://doi.org/10.5281/zenodo.5105529

Peng, C., Goswami, P., & Bai, G. (2020). A literature review of current technologies on health data integration for patient-centered health management. *Health Informatics Journal*, *26*(3), 1926–1951. https://doi.org/10.1177/1460458219892387

Plateaux, A., Lacharme, P., Rosenberger, C., & Murty, K. (2013). A contactless e-health information system with privacy. *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 1660–1665. https://doi.org/10.1109/IWCMC.2013.6583805

Preukschat, A., Reed, D., Allen, C., & Vogelsteller, F. (2021). *Self-Sovereign Identity*.

Purtova, N. (2017). *Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons* (pp. 177–210). https://doi.org/10.1007/978-3-319-48342-9_10

Rahul, K., & Banyal, R. K. (2020). Data Life Cycle Management in Big Data Analytics. *Procedia Computer Science*, *173*, 364–371. https://doi.org/10.1016/j.procs.2020.06.042

Rantanen, M. M., Hyrynsalmi, S., & Hyrynsalmi, S. M. (2019). Towards Ethical Data Ecosystems: A Literature Study. *2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 1–9. https://doi.org/10.1109/ICE.2019.8792599

Sahay, S., Nielsen, P., & Aanestad, M. (2019). Institutionalizing information systems for universal health coverage in primary healthcare and the need for new forms of institutional work. *Communications of the Association for Information Systems*, *44*(1), 62–80. https://doi.org/10.17705/1CAIS.04403

Schaar, P. (2010). Privacy by Design. *Identity in the Information Society*, *3*(2), 267–274. https://doi.org/10.1007/s12394-010-0055-x

Schardong, F., & Custódio, R. (2022). Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. In *Sensors* (Vol. 22, Issue 15). MDPI. https://doi.org/10.3390/s22155641

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021a). Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. *Information and Management*. https://doi.org/10.1016/j.im.2021.103553

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021b). Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. *Information and Management*. https://doi.org/10.1016/j.im.2021.103553

Sporny, M., Longley, D., & Chadwick, D. (2022). *Verifiable Credentials Data Model*.

Sutcliffe, A. (2003). Scenario-based requirements engineering. *Proceedings of the IEEE International Conference on Requirements Engineering*, *2003-January*, 320–329. https://doi.org/10.1109/ICRE.2003.1232776

Tapuria, A., Porat, T., Kalra, D., Dsouza, G., Xiaohui, S., & Curcin, V. (2021). Impact of patient access to their electronic health record: systematic review. *Informatics for Health and Social Care*, *46*(2), 192–204. https://doi.org/10.1080/17538157.2021.1879810

Tiffin, N., George, A., & Lefevre, A. E. (2019). How to use relevant data for maximal benefit with minimal risk: Digital health data governance to protect vulnerable populations in low-income and middle-income countries. *BMJ Global Health*, *4*(2). https://doi.org/10.1136/bmjgh-2019-001395

Vidal, F. R., Gouveia, F., & Soares, C. (2022). Analysis of Revocation Mechanisms for Blockchain Applications and a Proposed Model Based in Self-Sovereign Identity. *Journal of Information Technology Management*, *14*, 192–210. https://doi.org/10.22059/jitm.2022.87848

Vidal, F. R., Ivaki, N., & Laranjeiro, N. (2021). Revocation Mechanisms for Blockchain Applications: A Review. *2021 10th Latin-American Symposium on Dependable Computing, LADC 2021 - Proceedings*. https://doi.org/10.1109/LADC53747.2021.9672577

von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data Sovereignty in Information Systems. *Electronic Markets*, *34*(1). https://doi.org/10.1007/s12525-024-00693-4

Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. *Government Information Quarterly*, *40*(4). https://doi.org/10.1016/j.giq.2023.101873

WHO. (2017). *Review of the national health sector response to HIV in the Republic of Indonesia*.

Yang, R., Liu, N., Pang, Z., Wang, Y., Jia, Q., Lu, W., Li, Z., Li, M., & Wu, L. (2021). The next generation identity platform for digital era based on blockchain. *Lecture Notes in Electrical Engineering*, *677*, 1035–1044. https://doi.org/10.1007/978-981-33-4102-9_124

Zrenner, J., Möller, F. O., Jung, C., Eitel, A., & Otto, B. (2019). Usage control architecture options for data sovereignty in business ecosystems. *Journal of Enterprise Information Management*, *32*(3), 477–495. https://doi.org/10.1108/JEIM-03-2018-0058

Appendices

Appendix A – List of existing SSI applications in the market and its functionalities

No	Design Pattern	Functionality	Connect.me	Esatus	Lissi	Trinsic	Jolocom SmartWallet	Indisi	DIT	Sideos	ProofSpace	Talao	Atala PRISM	%
1	Restricted Wallet Access	User authentication before accessing a wallet	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	73
2	QR Code/Link Presentation	Sending/receiving QR codes and links	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	100
3	QR Code/Link Generation	Generating a connection invitation	No	No	No	Yes	No	No	Yes	No	No	No	No	18
4	Connection Initiation	Establishing a connection by scanning a QR code or clicking on a link	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	100
5	Credentials Request	Requesting issuance of VC by scanning a QR code or clicking on a link	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	100
6	Connection List	Display of established connections	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	73
7	Extended List View	Extended connection view	No	No	No	No	No	No	No	No	No	No	No	0
8	VCs Archive	Display of obtained VCs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	100
9	Extended VC View	Extended connection view	Partially	Partially	Partially	Partially	Partially	Partially	No data	No data	Partially	Partially	Partially	82
10	Auto-Connection	Automated connection acceptance	Yes	No	Yes	No	No	No	No data	No data	No	No	No	18
11	Auto-Credential	Automated VC acceptance	No	Yes	Yes	No	No	No	No data	No data	No	No	No	18
12	Auto-Presentation	Automated VP creation and distribution	No	Yes	No	No	No	No	No data	No data	No	No	No	9
13	Review Connection	Review connection before its acceptance	No	Partially	Partially	Partially	No	Partially	No data	No data	Partially	Partially	Partially	64

No	Design Pattern	Functionality	Connect.me	Esatus	Lissi	Trinsic	Jolocom SmartWallet	Indisi	DIT	Sideos	ProofSpace	Talao	Atala PRISM	%
14	Review Credential	Review VC before its acceptance	Yes	Yes	Partially	Yes	Partially	Yes	No data	No data	Partially	Yes	No	73
15	Review Presentation	Review VP before sending the data	Yes	Yes	Yes	Yes	Yes	Yes	No data	No data	Partially	Yes	No	73
16	Interaction Autentication	User authentication before completion of important interaction	Yes	No	No	No	No	No	No data	No data	No	No	No	9
17	Notifications	Notification of important interactions	Yes	Yes	Yes	Yes	Partially	Yes	Yes	No data	Yes	Yes	Yes	91
18	Chat	Messanger or chat functionality	No	No	No	Yes	No	No	Yes	No	No	No	No	18
19	Selective Disclosure	Selectively disclose VCs information	Yes	Partially	No	Yes	Yes	Yes	No data	Yes	Yes	Yes	Partially	64
20	Self-Attested Attributes	Issuance of self-attested attributes	Yes	No	Yes	No	Yes	Yes	No data	Yes	Yes	Yes	No	64
21	Transaction Duration	Information on trasaction duration	Partially	Yes	No	Partially	No	No	No data	No	No	No	No	27
22	History	History of (all) interaction	Yes	No	No	No	Yes	Yes	No data	No data	No	No	No	27
23	Interaction History	History of interaction according to established connection	Yes	Yes	Yes	Yes	No	No	No data	No data	No	No	No	36
24	Shared Data History	History of shared data from each VC	No	Yes	Yes	No	No	No	No data	No data	No	No	No	18
25	Data Deletion	Request for deletion of data	No	Yes	No	No	No	No	No data	No data	No	No	No	9
26	Backup/Recovery Phrase	Backup and recover a wallet	No	Yes	No	Yes	No	No	Yes	No	No	Yes	No	36
27	Export-Import Phrase	Export and import a wallet	No	Yes	No	Yes	No	No	No	No	No	No	No	18
28	Clipboard	Copy/save (content) to the clipboard	No	No	No	Yes	No	No	No	No	No	No	No	9
29	Phrase Verification	Recovery phrase verification	No	Yes	No	Partially	No	No	Yes	No	No	No	No	27
%			59	69	55	69	41	45	38	17	41	41	34	

Appendix B – Interview Protocol

The interview aims to understand the experiences and concerns of individuals in LMIC about their health data, as well as to evaluate the SSI functionalities embedded in the design artifact and how they address the respondent's data sovereignty, particularly for the control and ownership values. The interview protocol is structured as follows:

1. **Introduction**
    a. Greetings and introduction of the researcher and the research
    b. Obtain consent for the recording and ask whether anonymization is desired.
2. **Introduces interview theme: The current state of health data sharing, control, and ownership for LMIC individuals**
    a. Do you have any experience when you need to share your health data?
        i. [Probe] Could you describe your experience?
    b. Do you have any concerns regarding your health data when sharing it? OR If you have to share your health data for some reason, do you have any concerns about it?
        i. [If no, skip this] Can you please elaborate on those concerns? (note whether they have mentioned any aspect related to control and ownership)
    c. On control
        i. What are your thoughts about control over your health data?
        ii. Why do you feel that way?
    d. On ownership
        i. What are your thoughts about ownership of your health data?
        ii. Why do you feel that way?
3. **Presents design artifact to respondents**
    a. Scenario introduction
    b. A brief explanation of Self-Sovereign Identity and the design artifact
    c. Request them to do Scenario 1: Evaluate and approve issued credentials
    d. Request them to do Scenario 2: Evaluate and approve data sharing requests
4. **Evaluates respondents over design artifact demonstration**
    a. Could you please describe your data sharing experience when using our prototype?
        i. [Probe for] Could you please describe the benefit of using our prototype to share your health data?
        ii. [Probe for] How much control over data did you feel when sharing your data through our prototype?
        iii. [Probe for] Which features of the prototype made you feel you have more or less control of your health data?
        iv. [Probe for] How much ownership did you feel over your data when sharing your data through our prototype?
        v. [Probe for] Which features of the prototype made you feel you have more or less ownership of your health data?
        vi. [Probe for] Could you please describe any challenges you encountered when using our prototype? Could you please describe your data sharing experience when using our prototype?
    b. How would you suggest making an improvement to the prototype

[Back up questions]

- How did data minimization impact your decision to share your health data? (probably requires me to explain what is “data minimization”)
    - Probing questions:
        - If mentioned control: Why do you think data minimization would make you feel more control over your health data?
        - If mentioned ownership: Why do you think data minimization would make you feel more ownership over your health data?
- How did revocation impact your feelings when sharing your health data? (probably requires me to explain what is “revocation”)
    - Probing questions
        - If mentioned control: Why do you think revocation would make you feel more control over your health data?
        - If mentioned ownership: Why do you think revocation would make you feel more ownership over your health data?

Appendix C – Sub tasks lists

C-1. Receive Notification

<table>
<tr><td>Task ID</td><td colspan="4">1-RN</td></tr>
<tr><td>Task Name</td><td colspan="4">Receive Notification</td></tr>
<tr><td>Task Description</td><td colspan="4">Patient will be notified about the incoming health information request from a Research Institution
This task also applies when the Patient receives a notification about incoming VC from an issuer, e.g., hospital issuing a medical test result</td></tr>
<tr><td>High-Level Requirement</td><td colspan="4">Support trust network</td></tr>
<tr><td>Design patterns</td><td colspan="4">Notification
Contractual Agreement</td></tr>
<tr><td rowspan="4">Sub-Task(s)</td><td>Sub-task ID</td><td>Sub-task Name</td><td>Sub-task Description</td><td>Interface Layer</td></tr>
<tr><td>1-RN-1</td><td>See Notification</td><td>Patient will be shown who is requesting access to their health data</td><td>Interface layer: Pop-up Notification
Design patterns: Notification</td></tr>
<tr><td>1-RN-2</td><td>Extend Notification Details</td><td>The Patient can show details of what data is requested and what the purpose is</td><td rowspan="2">Interface layer: Notification Menu Detail
Design patterns: Notification, Contractual Agreement</td></tr>
<tr><td>1-RN-3</td><td>Decide follow-up action</td><td>The Patient can follow up immediately for the request or put it on hold</td></tr>
</table>

C-2. Review Credentials

<table>
<tr><td>Task ID:</td><td colspan="4">2-RC</td></tr>
<tr><td>Task Name:</td><td colspan="4">Review Credentials</td></tr>
<tr><td>Task Description</td><td colspan="4">After checking the notification for data request, the Patient will be redirected to the home screen, where he can see all his VCs
This task also applies when the Patient opens a newly issued VC, e.g., medical test result from a hospital lab</td></tr>
<tr><td>High-Level Requirements</td><td colspan="4">Manage Digital Identities and Credentials</td></tr>
<tr><td>Design patterns</td><td colspan="4">Verifiable Credential Archive
Extended verifiable credential view
History
Revocation (delete report)</td></tr>
<tr><td rowspan="3">Sub-Task(s)</td><td>Sub-task ID</td><td>Sub-task Name</td><td>Sub-task Description</td><td>Interface Screen</td></tr>
<tr><td>2-RC-1</td><td>Check available credentials</td><td>Patient sees the list of available verifiable credentials they own.</td><td>Interface layer: Home screen
Design patterns: Verifiable Credential Archive</td></tr>
<tr><td>2-RC-2</td><td>Go to TB medical report detail</td><td>The Patient can select the TB medical report and see the detailed information attribute on the TB medical</td><td>Interface layer: Credential Details</td></tr>
</table>

			report credentials. The Patient can return to the list or delete the report.	**Design patterns:** Extended verifiable credential view, History, Revocation
	2-RC-3	Go to HIV medical report details	The Patient can select the HIV medical report and see the detailed information attribute on the tuberculosis medical report credentials. The Patient can return to the list or delete the report from here.	

C-3. Review Credentials

Task ID:	3-EC			
Task Name:	Establish connection			
Task Description	The Patient decides whether to allow Research Institution to connect and access their data.			
High-Level Requirements	Manage Connection			
Design pattern	Connection List Review Connection Authenticate Interaction			
Sub-Task(s)	**Sub-task ID**	**Sub-task Name**	**Sub-task Description**	**Interface Screen**
	3-EC-1	Check incoming connection request	The Patient can see a list of their connections or the incoming request for connection from a Research Institution in the data ecosystem.	**Interface layer:** Home Screen **Design patterns:** Connection List
	3-EC-2	Review Connection Requests from Research Institution	The Patient can select incoming connection requests to evaluate the requester based on the data on their credentials.	**Interface layer:** Connection details **Design patterns:** Review Connection, Interaction authentication
	3-EC-3	Decide connection request	The Patient can decide either to accept or reject connection requests from Research Institution.	

C-4. Receive and review request

Task ID:	4-ET
Task Name:	Receive and review request
Task Description	The Patient decide whether they would allow connections to be made to share their health information
High-Level Requirements	1. Facilitate credential exchange and management 2. Transact with minimal disclosure 3. Establish boundary control

Design patterns	Interaction history Interaction authentication Review presentation Selective disclosure/data minimization Contractual agreement Revocation			
Sub-Task(s)	**Sub-task ID**	**Sub-task Name**	**Sub-task Description**	**Interface Screen**
	4-ET-1	Review the list of requests from a connection	The Patient can see a list of requests from a specific connection and select the details.	**Interface layer:** Request Archive **Design patterns:** Interaction History
	4-ET-2	Review request from Research Institution	The Patient can see the selected request, which consists of the list of requested data	**Interface layer:** Review Request **Design patterns:** Interaction Authentication, Review presentation, Interaction History, Selective disclosure/Data minimization, Revocation
	4-ET-3	Select data that want/do not want to be shared	The Patient can select and deselect information based on the available credentials before sharing it with the Research Institution	
	4-ET-4	Review contract from transaction	Data owners can see contractual agreements from data consumers on how they would access and use their data	
	4-ET-5	Decide on the request	The data owner can decide whether to renegotiate the contract, decline or accept the request	

C-5. Renegotiation

Task ID:	5-RC			
Task Name:	Renegotiation			
Task Description	The Patient can renegotiate the contractual agreement offered by the Research Institution by creating a new contractual agreement and sending it to the Patient.			
High-Level Requirements	Establish boundary control			
Design patterns	Contractual agreement Transaction duration			
Sub-Task(s)	**Sub-task ID**	**Sub-task Name**	**Sub-task Description**	**Interface Screen**
	5-RC-1	Choose to renegotiate contract	The Patient can select the renegotiate button and be redirected to the renegotiation feature.	**Interface layer:** Renegotiate **Design pattern:** Contractual agreement, Transaction duration

	5-RC-2	Create new contract	The Patient can create a new contractual agreement about their health information.	**Interface layer:** Connection details **Design patterns:** Review Connection, Authenticate Interaction
	5-RC-3	Decide action on new contract	The Patient can submit new contracts or cancel by clicking a button.	
	5-RC-4	Check renegotiation	The Patient can check the renegotiation status.	

C-6. Accept request

Task ID:	5-AR			
Task Name:	Accept request			
Task Description	The Patient decides to accept request and have their data shared with the Research Institution			
High-Level Requirements	1. Facilitate credential exchange and management 2. Establish boundary control			
Design patterns	Extended verifiable credential view History Interaction history Interaction Authentication Review Presentation Revocation			
Sub-Task(s)	**Sub-task ID**	**Sub-task Name**	**Sub-task Description**	**Interface Screen**
	5-AR-1	Choose to accept a request	The Patient can decide to accept request by clicking the accept button	**Interface layer:** Review Request **Design patterns:** Interaction Authentication, Review Presentation
	5-AR-2	See the update on the request list	Once accepted, the Patient will be redirected to the request list to see an update on the recent request.	**Interface layer:** Request archive **Design patterns:** Interaction history
	5-AR-3	See the update on the request detail	The Patient can click the latest request to see what data is shared, and they can also opt-out (revoke) the shared data.	**Interface layer:** Review Request **Design patterns:** Review Presentation, Revocation
	5-AR-4	See the update on the credential	The Patient can go to the credentials details and see a historical update on the recent activity of their credentials.	**Interface layer:** Credential details **Design patterns:** Extended verifiable credential views, History, Revocation

C-7. Revoke request

Task ID:	5-RVA			
Task Name:	Revoke request			
Task Description	Once a request is accepted, the Patient can decide to withdraw the shared information			
High-Level Requirements	1. Facilitate credential exchange and management 2. Establish boundary control			
Design Patterns	History Interaction history Interaction Authentication Review Presentation Revocation			
Sub-Task(s)	**Sub-task ID**	**Sub-task Name**	**Sub-task Description**	**Interface Screen**
	5-RVA-1	Choose to revoke access	The Patient can decide to revoke access by clicking the revoke button and be redirected to connection archive	**Interface layer:** Review Request **Design patterns:** Interaction Authentication, Review Presentation, Revocation
	5-RVA-2	Check update on the connection archive	The Patient can see recent update on the revocation to a specific connection and click to see more detail	**Interface layer:** Connection archive **Design patterns:** Interaction History, Revocation
	5-RVA-3	See the update on the request list	The Patient will be redirected to the request list and see an update from the recent revocation.	**Interface layer:** Request archive **Design patterns:** Interaction history
	5-RVA-4	See the update on the request detail	The Patient can click the latest request and see what data is shared with the revocation status	**Interface layer:** Review Request **Design patterns:** Review Presentation
	5-RVA-5	See the update on the credential	The Patient can go to the credentials detail and see the historical update on revocation of the recent activity of their credential.	**Interface layer:** Credential details **Design pattern:** Extended verifiable credential views, history, revocation

Appendix D – Initial code list

No	Definition	Code
1	Individuals right to the health data	Ownership
2	individuals ability to manage and decide health data	control
3	ability to selectively disclose aatributes in health data	Data minimization
4	ability to retract health data that already shared	Data revocation
5	functionalities that allows data provider and data consumer to agree upon data lifecycle	contractual agreement
6	functionalities that allows holder to decide verifier interaction	Interaction authentication
7	functionality that places credential in one storage	Digital wallet
8	person or organization that require to verify holder credential	Verifier
9	Doctor or nurse or medical staff	Healthcare worker
10	Hospital, or health community centers, or clinics	Healthcare facility
11	insurance company or national insurance scheme	Healthcare financing
12	ability to selectively disclose credential for presentation	Selective Disclosure
13	functionality where holder will receive information regarding their credential	Notification

Appendix E – Final code list

Code				Grounded	Density
○ Actors				74	0
	○ Healthcare systems			22	0
		● healthcare system		22	0
			● financial institutions	6	1
			● healthcare digital infratructures	7	0
			● healthcare facilities	5	1
			● healthcare workers	11	0
	○ Verifiers			53	0
		● verifier		53	3
			● affiliates or third parties	3	2
			● initial interaction	10	2
			● perceived credibility	21	2
			● person or organization identifiable information	6	2
			● request purpose	31	2
○ Control				119	0
	● Feel control			97	5
		● access/usage permission		49	10
		● being acknowledged		6	5
		● being informed		9	12
		● blocking information		17	3
		● choose what to share		22	6
	● Not feel control			25	0
		● actual data user is unknown		3	5
		● Data-owner linkage		5	6
		● giving "control" to "parts" of data		9	8
		● lack data sovereignty knowledge		6	1
		● no involvement in managing data		5	4
	● segregated and anonymized data			5	2

Code				Grounded	Density
○ Data minimization				35	0
	● Data minimization			35	5
		● On-off data attributes		21	6
		● Selective disclosure		14	6
○ Data revocation				22	0
	● Data revocation			22	5
		● controlling access		2	0
		● general revocation remarks		4	0
		● retract based on contract		6	2
		● retract when in uncertainty		3	1
		● retract when necessary		5	1
		● retract when there is a problem		2	2
○ Data sovereignty goals				84	0
	● medical needs			26	0
		○ collective good		3	0
		● drug problem prevention		5	0
		● free drugs		2	0
		● health research		2	0
		● personal health target		4	0
		● starting or continuing treatment		16	0
		● Undecided		1	0
	● privacy			69	7

Code				Grounded	Density
		● avoiding misuse		14	0
		● keeping or protecting secret		17	2
		● personal data security		4	0
		● professional impact		9	0
		● reputation		22	0
		● social repercussion		8	0
		● unwanted attention		1	0
○ External Factors				50	0
	● Data governance			14	0
	● data sharing risks			36	2
		● accidental data exposure		6	0
		● data leaks		13	2
		● data re-creation		6	2
		● unauthorized access/usage		23	4
○ Health data				54	0
	● data potential consequences			30	0
		● part of data can be associated to owner		4	5
		● stigmatization		27	3
	● health data content			35	0
		● common/historical health data		25	5
		● personally identifiable information		13	4
○ Ownership				60	0
	● feel ownership			45	2
		● "hold" on / "property" to the data		16	4
		● access/usage permission		13	4

Code				Grounded	Density
		● acknowledged data		10	3
		● data protection		6	5
		● general ownership remarks		2	0
		● personal benefit		4	1
	● not feel ownership			16	0
		● data is intangible object		6	2
		● external authority		3	2
		● lack data sovereignty knowledge		3	1
		● public good		7	8
○ SSI technology				139	0
	○ cautious			7	2
	○ confused			3	0
	○ data safety			31	0
	○ data visibility			4	0
	○ Digital literacy			0	2
	● legal contractual agreement			24	6
		● data lifecycle agreement		16	7
		● data valuation		2	0
		● financial penalty		2	0
		● legally prosecuted		7	3
		● negotiable contract		5	0
	○ not cautious			4	0
	○ perceived interface usability			13	2
		○ complex interface		5	5
		○ simple and straightforward interface		8	1
	○ SSI functionalities effectiveness			2	7
	● SSI other functionalities			68	0
		● digital wallet		8	0
		● formal notice		10	4
		● informed consent		22	5
		● interaction authentication		14	3

Code				Grounded	Density
		● relatable credentials		9	0
		● warning sign		12	1
	● trusting SSI			35	1
		○ data flow		9	2
		● secure database		3	0
		● usage transparency		28	3
○ Trust				36	0
	● trust			33	5
		● confidence (trust)		12	3
		● facilitating trust		6	0
		● perceived trust		15	2
	○ willingness to share data			4	4