Stanislav Mahula

Opportunities and challenges for self-sovereign identity in the public sector: a case of Belgium

Master Thesis

at the Chair for Information Systems and Information Management

Supervisor: Prof. Joep Crompvoets

Presented by: Stanislav Mahula
Verboekhaven 5
1210 Brussels
+32497221606
st.mahula@gmail.com

Date of Submission: 2020-06-02

Acknowledgments

I will not be a pioneer by saying that writing this thesis was a challenging period, given all the circumstances we had. My dear PIONEERs, our class was with no doubt a unique one. We taught and learn from each other, share meals, moments and memories, and I am sure this is just the beginning.

Two years ago, I was finishing my bachelor thesis and at the same time, feeling excited about starting my master programme in September 2018. Becoming a PIONEER student and living this life for two years was the best experience I've ever had. I wholeheartedly thank everyone committed to creating and running this programme, for the efforts to put together the best minds from all over the globe to learn and become the future of our countries. I wrote this in my motivation letter, and now I feel that those words were not empty, so I thank you for believing in them two years ago. I've learned five times more; I've challenged myself ten times more, but I've felt happy hundred times more than before. I am indebted to this programme for making me the person I am today and opening the new page of my life. With the knowledge, experience, passion and stamina I have now, no height shall be unconquered!

During these two years, I also was lucky enough to learn from real experts in my field in Estonia and Belgium. My internship e-Governance Academy in Tallinn gave a valuable experience from the world's digital pioneers. I am grateful to my colleagues and coordinators for sharing it with me. This thesis would also be absolutely impossible without the input from the IAA department at DT Digital Transformation at Belgian FPS BOSA. I am thankful to all the experts, and particularly to my coordinator Noël Peeters for his guidance and enthusiasm about my topic.

I thank my supervisor, professor Joep Crompvoets for his professional guidance and support, which made the process of writing this thesis a comfortable experience for me. I've discovered the magical world of qualitative research, and I am sure I will not stop there.

My dear family and friends from Ukraine, thank you forever for staying connected throughout this journey and feeding my confidence, supporting and believing in me. This paper is yours.

I owe a special place on this page to Ekaterina: a colleague, classmate, mentor, my friend. Thank you for always be there and pushing me when I needed it the most. I am sure our paths will cross.

Last but not least, I want to thank myself for not being afraid to apply for the PIONEER programme and making it till the very end.

Table of contents

Figures

Tables

List of abbreviations

BOSA	Federal Public Service for Policy and Support of Belgium
DG DT	Directorate General for Digital Transformation at BOSA
DID	Decentralised Identifier
DLT	Distributed Ledger Technology
EBP	European Blockchain Partnership
EBSI	European Blockchain Service Infrastructure
eID	Electronic identity card
eIDAS	Electronic Identification, Authentication and Trust Services
ESSIF	European Self Sovereign Identity Framework
EU	European Union
FAS	Federal Authentication Service
FPS	Federal Public Service of Belgium
GDPR	General Data Protection Regulation
IAA	Department of Identification, Authorisation and Authentication at DG DT
IAM	Identity and Access Management
ID	Identity Document
ISO	International Standardisation Organisation
KYC	Know Your Customer
OECD	Organisation for Economic Co-operation and Development
PoC	Proof of Concept
SDG	Sustainable Development Goals
SSI	Self-sovereign identity
UNCHR	United Nations' Charter on Human Rights
VC	Verifiable Credential

1 INTRODUCTION

1.1 Research Motivation

The advanced technological developments and the growing presence of citizens in the digital world allowed the governments offering public services online. What could seem impossible a decade ago is now conventional in everyday life: online tax declaration and social benefits, or even online voting are available for citizens. Many advantages of such service delivery can be mentioned, including reduced cost, better accountability of the government, and increased trust (Carter & Bélanger, 2005). Still, new challenges emerge for authorities concerning security, interoperability, and universality of data (Lyons, Courcelas, & Timsit, 2019).

The public sector is also challenged with managing citizens' identities (Siriwardena, 2017). Apart from having the infrastructure and technology in place, service providers need to guarantee that a person behind the screen is who they claim to be, and they have access to the services they should. Unlike the offline world, no physical verification is possible (Shavers & Bair, 2016). Accessing online services is possible using a diverse set of modern identification methods. Still, the main principle remains the same: the user has only the static view on their identity information and have little to no control over it. Also, protecting citizens from data capitalists constitutes another challenge for governments. Citizens, who take various roles when interacting in the digital world, have their data scattered all over the globe, duplicated in several databases, questionably maintained and shared by different organisations, including the big corporations (Zyskind, Nathan, & Pentland, 2015). One of the risks of such a state of play is numerous data breaches, which are highlighted in the news regularly.

Overall, the current circumstances are that the citizens do not hold exclusive control over their identities, which is why the governments should consider improving the status quo for identity management. These reasons for that are having strong digital identities of their citizens for correctly identifying citizens and distributing benefits, allowing electronic voting, fighting money laundering or terrorist financing, as concluded by the EU Blockchain Observatory and Forum (Lyons et al., 2019).

The concerns on privacy and control over data triggered a social debate on seeking new ways for identity management, where the user is central to the administration of their identity information. However, giving citizens more control is a promising yet difficult-to-implement idea (Lyons et al., 2019). Field experts across the globe started to think about how the status quo for identity can develop towards more independence from third parties managing identities.

In the light of modern technological advancements, it was debated that decentralising is the way to go and that involving a distributed ledger technology (DLT) and its renown application blockchain can enable bringing the control over the identities back to their owners. Admittedly, within the public sector context, despite the cautiousness about DLT and blockchain, their potential is acknowledged. In fact, public sector bodies actively experiment with blockchain technology, especially in the field of identity management (Hileman & Rauchs, 2018). On the one hand, it is expected that blockchain's full impact is to be realised in decades, and its wide adoption can only be a subject of high-level discussions (Iansiti & Lakhani, 2017). A typical issue here, as scholars admit, is that blockchain's use-cases are mostly technology-driven, while instead, they should start from the needs-driven perspective to address particular societal challenges with the technology (Ølnes, Ubacht, & Janssen, 2017). Nevertheless, blockchain has passed the peak of its hype, gradually becoming more mature and surpassing the surrounding challenges (Gartner, 2019b). Experts expect it to demonstrate its best applications coming to life within five to ten years (Gartner, 2019b).

Hence, on the intersection of identity management and decentralised technologies, the embodiment as self-sovereign identity (SSI) paradigm was found. SSI has become a hot topic in the identity circles over the last couple of years after it was first mentioned in the blogpost of Christopher Allen in 2016. In general terms, SSI can be understood as the identity controlled by a user (an individual, object or even an enterprise), putting him or her in the centre to its administration (Allen, 2016).

Many researchers attempted to make sense of this paradigm; various publications define the essential components, features and properties, mathematic models or technological implementations. Several private-sector projects, including Sovrin, Jolocom or uPort, exist, giving the first glance on how the user-controlled world of identity could function. Also, SSI is acknowledged on the European level as well. It is expected to become mainstream over the ten years (European Union, 2018), which is also a focus of the European Self-Sovereign Identity Framework (ESSIF).

1.2 Research problem

Addressing the issue of bringing the control back to the user seems to be a burdensome task because many centralised identity management systems are entrenched into the public sector routine. However, limited research is conducted on the possible application of SSI in the public sector and what benefits and challenges could be expected. Lessons from the past taught that merely introducing a new technology in the public sector will unlikely enjoy much success. Public sector experts learned to take a systematic step-by-step approach for obtaining better experience before deploying large-scale

technologies (Ølnes & Jansen, 2018). Initially starting from the social needs, SSI itself is not a mature technology yet. Still, the problems it seeks to solve are acute in the context of the public sector. Therefore, it is worth discussing whether the SSI can be a good fit for empowering citizens to restore authority over their identities. SSI best applications are yet to come, so it is not rational to look at its concrete benefits and limitation it implies for building specific roadmaps. Instead, following the increasing interest in this new identity management model, the authors wants to explore opportunities SSI can offers, particularly in the context of the public sector.

Literature review in scope the present research revealed that there is no study addressing SSI within the public sector; hence, this thesis paper offers an exploratory view of the self-sovereign identity and how can it impact the identity management of the public sector. Such an analysis will allow staying up to date with the trends while also making more informed decisions about them. For that, the explanatory description of one country will be provided in the scope of this thesis. For this study, Belgium was chosen due to its stable identity system, a high provision of identity documents and the author's familiarity with the context. Moreover, the presence of SSI-related initiatives indicates possible interest of Belgian public sector in exploring SSI.

1.2.1 Research question

Concluding everything from the previous section allows forming the following question to be set as a task of this thesis:

What opportunities and challenges can the Belgian public sector expect from implementing the self-sovereign identity model?

Answering this question is a comprehensive process as it requires prior information and context. For that, the authors posed additional questions to be answered:

1. What are the drivers for implementing a new model of identity management in Belgium?

Although the identity infrastructure of this country is robust, Belgian public administration model known for its complexity. Looking at how the current identity and access management was developed, as well as learning the hurdles with this system in Belgium allows listing the issues which could be addressed by SSI. For that, the benefits and drawbacks of the current identity system of the countries will be studied.

2. How can SSI address the existing problems with identity management?

Knowing that SSI still matures and does not have a firm shape yet, gaining a more in-depth understanding of SSI as an identity paradigm is needed. This study will explore its functionality principles by aggregating the available information.

3. What are the barriers of its deployment in the state-wide context?

It should also be taken into account that no technology is flawless, and the risks and limitations involved with the SSI should be considered to provide a holistic overview of this technology opportunities. Best practices from existing use-cases, as well as the ongoing research on SSI, will be taken into consideration.

1.2.2 Research aims

Seeking clarity in how SSI can be beneficial to the public sector and citizens, the research questions reflect the overall aim of this research. The author intents to investigate the popular concept of self-sovereign identity and provide the ground for assessing its opportunities and challenges within the public sector, where Belgium will serve the example of such research.

This thesis paper does not, however, aim at suggesting concrete implementation steps but instead opens a discourse on the relevance of doing so and could guide future research on SSI in the public sector. Likewise, the expected results of this research are the areas where SSI can contribute within the public sector's identity management domain, as well as the various factors which can facilitate or hamper this process.

1.2.3 Research objectives

Achieving the research aim is possible through setting the primary objectives to guide this thesis study throughout the course:

- define the core concepts within the research domain to use throughout the study;
- inspect the body of literature covering identity management and SSI to gain a better understanding of SSI principles and functionality;
- study the background of ID management in Belgium and understand its drawbacks and opportunities;
- conduct at least 10 interviews with fields experts to gain a more insightful view on the identity management state of play and recent SSI developments;

- carefully assess the benefits and barriers for SSI, using the framework suggested by Ølnes & Jansen (2018);
- write the report of the analysis before the 02.06.2020;
- provide the results of the assessment and propose a revised framework.

1.2.4 Workplace justification

This master thesis's preparation takes places as a part of the internship at the Federal Public Service for Policy and Support of Belgium (BOSA), under the department for Identification, Authorisation and Authentication (IAA). The premise for this research is the workplace of BOSA in Brussels, Belgium, with the coordination from its side provided by the head of the IAA Noël Peeters. This internship will facilitate gaining more knowledge on the subject and get acquainted experts, which will support the background and data collection phases of this study. The aim of the thesis is also aligned with the long-term plans of IAA. They want to look at future identity solutions and anticipate the drivers for the evolution of digital identity.

1.2.5 Structure of the thesis

This thesis paper is structured as follows. In chapter 2, the terms and definitions are provided to ensure the consistency of reading this thesis. Also, the main initiatives within the SSI field are listed. The following chapter presents the overview of academic discussion in the studies subject. It includes the topics of challenges of the current identity management systems, the drivers towards the evolution of these systems, and a more specific view on the SSI, its possibilities within the context of implementing the blockchain technology in the public sector. Based on the literature review, a conceptual framework for this research is presented. The fourth chapter illustrates the research design deployed by this study; the techniques of data collection and analysis were listed there. A description of the studies case, Belgium, is given in chapter 5. It provides general information about the country and its public sector, as well as sheds light on the aspects of identity management. Chapter 6 denotes the main findings from the empirical part, followed by the discussion chapter 7. The paper is closed with the conclusion and future work chapter.

2 BACKGROUND STUDY

Well-defined terms and concepts related to the studied problem are essential not only for the consistency throughout the thesis but also for establishing the ground the future research (Oliver, 2010). Before digging into the self-sovereign identity knowledge area, the author needs clarity regarding what are identity and digital identity in the first place. Thus, this chapter presents the overview of main definitions related to identity, digital identity and identity management. Within the evolution of identity management, the drivers and principles of future identity are also presented. Finally, this chapter also explains what can stand for self-sovereign identity and lists several initiatives and use-cases of this identity model. Acquiring this knowledge is the prerequisite for the next chapter, where the conceptual model for analysing the opportunities and barriers of SSI is presented.

It should be noted, however, that this thesis is conducted in the domain of social sciences and examines the inclusion of SSI in the public sector from a public administration perspective. Consequently, the essential definitions are listed here for the reader's overall understanding and are in no case fully elaborating on all technical aspects presented, leaving this beyond the scope of this work.

2.1 Identity fundamentals

2.1.1 What is identity?

The research on identity takes back many years and can be found in such areas as psychology, philosophy and social sciences. In the latter, depending on the context, it is commonly given two primary meanings: social and personal (Robins & Foster, 1994). Personal identity defines an individual as a unique person in terms of their differences from other people. In contrast, social identity does it with regards to the similarities of one social group in comparison to another (J. C. Turner, Oakes, Haslam, & McGarty, 1992). Some studies argue, however, that this division is unhelpful because definitions of identity are both dependent on the personal definition and socio-cultural context (Vignoles, 2017).

Looking from a more pragmatic perspective, International Standardisation Organisation (ISO) defined identity as a set of attributes related to an entity, where attributes stand for particular characteristics of this entity (ISO/IEC, 2019). In other words, attributes are properties that belong to the entity. They are distinct, properly-named and measurable, which can be used to identify the entity in each context but not always uniquely (Ferdous, Chowdhury, & Alassafi, 2019).

Identifiers, according to Ferdous et al. (2019), are the attributes which alone allows uniquely identifying an entity within each context. These identifiers do not necessarily describe the person but rather allow referring to them (Wang & De Filippi, 2020). The following typology of attributes describes them based on the mean they are collected: inherent, accumulated and assigned attributes (BBVA, 2019). Credential, in turn, is an attribute which is used to attest the authority of the entity (Ferdous et al., 2019). The three types of credentials are typically defined: state-, commercial- and self-issued credentials (Stevens, Elliott, Hoikkanen, Maghiros, & Lusoli, 2010).

However, it is more pertinent for this study to determine the identity in the context of public services and government-citizens relationship because the governments are primary providers of legal identities (The World Bank, 2017). The state-issued credentials, which are the most trusted ones, comprise for passports and other regional or local credentials, and they can be issued on paper, electronically or in a hybrid form (Stevens et al., 2010). Nevertheless, as the study will show further, SSI is not merely comprised of state-issued credentials like name of the date of birth. It can also include attributes issued both by the private sector and by the identity subject themselves and to be used in all sectors.

2.1.2 Identity management

In many daily situations, identity needs to be presented and verified to get access to services. Be it visiting a hospital, proving one's age or logging into the local commune's website. In each of these interactions, presenting proof of one's identity is needed, and it can be both face-to-face or online (Gisolfi, 2018). As mentioned before, attributes allow uniquely identifying an entity. In order to better comprehend what is precisely meant by "uniquely identifying", the definitions of identification, authentication and authorisation need to be broken down (Laurent & Bouzefrane, 2015). These processes are considered forerunners to high-quality service provision and can allow citizen-oriented services (Taylor, Lips, & Organ, 2008).

Substance-wise, identification of a user happens when they provide the information to identify themselves, such as name, user name, and answers the question "who are you?" (Zviran & Erlich, 2006). However, as these authors also suggest, merely providing these data does not verify that the user is who he or she is. Authentication, in turn, is the process of verifying that the provided information is correct, and the person is who he or she is (ISO, 2013). Some means to perform authentication include passwords (either by chosen by the user or generated by the system), tokens or biometrics (Zviran & Erlich, 2006). The processes of identification and authentication are usually merged as one step in many systems (Ferdous et al., 2019). Finally, authorisation is a process of distributing the rights

of an entity to perform specific actions (Ferdous et al., 2019). In essence, ensuring those processes are performed correctly is a task of the identity and access management (IAM), which could appear in different contexts. The Gartner glossary interprets IAM as the "discipline that enables the right individuals to access the right resources at the right times for the right reasons" (Gartner, 2019a).

A commonly accepted way of claiming one's identity in society is by presenting their identity document (ID). In the historical perspective, the widespread use of IDs truly started after the end of the World War II, having in mind reinforcing state authority, better immigration control and combating fraud (European Union, 2018). Nowadays, ID forms and usages differ across the world; they can be compulsory or arbitrary to use, in the form of paper, plastic card or even a mobile application. The main principle remains the same that each ID documents has an identifier and other information, and it is linked to one person in real life. For a smooth flow of the identity management, the two objectives must be fulfilled: only one identifier can be given to a person for each domain, and that no two people can possess the same identifier (Wang & De Filippi, 2020). Additionally, Taylor et al. (2008) investigated to what extent the state identification models are subjects of "surveillance", mentioning the citizens being concerned about their personal data usage beyond the level needed for service provision. For that reason, identity management systems have to be developed so that they contain the variable and complex nature of human identity, by making these systems "sufficiently flexible, resilient, and dynamic" (Wang & De Filippi, 2020, p. 2).

Still, many challenges exist for identity management in the world: nearly one billion people around the globe do not have such a document verifying their identity (The World Bank, 2018b). Not possessing any identification does not allow people claiming who they are and restricts them from benefiting from the services as mentioned earlier. A key player in the building the worldwide peace and prosperity, the United Nations, acknowledged this problem and addressed it in the Sustainable Development Goals (SDG). Precisely, the UN aims at eradicating this obstacle under goal 16, target 9 by providing a legal identity document for all (United Nations, n.d.). Also, "Identity for Development" programme of the World Bank aims at contributing to solving global identity crisis via researching, advocating, financially and technically supporting countries in need (The World Bank, 2019). Another global effort for providing ID is the OECD-featured project called "ID2020", which aims to reinforce the global efforts to provide robust, secure and inclusive identity schemes worldwide, most importantly to those who do not have the ID yet (ID2020, 2019). For that, as the project's manifesto suggests, a sustained collaboration of all stakeholders is needed to create the shared principles and regulatory framework to ensure sustainable identity development (ID2020, 2019). Overall, although the majority

of people without identity come from Sub-Saharan Africa and South Asia (The World Bank, 2018b), global solidarity and cooperation can be of significant help in solving this problem.

2.1.3 Digital identity

Along with the identity document crisis, the digital world is growing tremendously fast, with the access to the internet of nearly 60% of the world's population, according to the latest data (Statista, 2020). Although the numbers vary across the countries and continents, the overall penetration grows all over. As a result, the digital transformation made a revolutionary shift of many public services online.

As was highlighted in the previous chapter, having robust identity management in the digital world is crucial for providing public services. In this study, it is essential to break down the essence of digital identity first. The primary challenge with digital identity is to understand what it is (Goode, 2019). The author of well-known "7 laws of identity" Kim Cameron refers to digital identity as "a set of claims made by one digital subject about itself or about another digital subject" (Cameron, 2005, p. 4). Similar to the identity in the physical world, digital identity can be twofold. It is both a set of attributes to identify a person uniquely or their self-projection in the digital world, different roles they take in the digital society, their set of its beliefs and activities (Laurent & Bouzefrane, 2015). The latter term is also commonly used as "online identity" (Kennedy, 2006). However, considering the psychological and socio-cultural relations goes beyond the scope of this thesis.

Lyons et al. (2019) also suggest that digital identity is twofold in another sense: its nature is both atomic, meaning it is based on the distinct pieces of information about a user. However, as Lyons et al. (2019) argue, it is also cumulative, representing the collection of other attributes. Needless to say that digital identity is not a full digital copy of a human being, and therefore cannot be considered a "property" and cannot be owned (Allen, 2016). To prevent ambiguity, by "digital identity" the author of this research implies a set of attributes allowing to uniquely identify a person in the digital environment. This definition is more suitable because it excludes the "self-projection" component.

2.2 Evolution of identity

Throughout the evolution of identity management models, several milestones can be distinguished: siloed, federated and user-centric (Ferdous et al., 2019). Self-sovereign identity is believed to the next step in the sequence, which is illustrated in the figure below:

Figure 1. Evolution of identity

Learning from the previous models and defining the challenges of the current identity models is vital before proceeding with the SSI features. The following paragraphs give a summary of various identity models and provide the context for the evolution of identity.

2.2.1 Identity models

Siloed model

The siloed identity model, also referred to as isolated, is the oldest identity model and is the most used one. Siloed identity is created and used exclusively for one particular purpose or organisation, with the shared trust being established between the user and the identity provider (Ruff, 2018). In this case, the personal information provided by the user is stored in the organisational database, i.e. a silo, hence, forcing the user to create these relations for every interaction with the different entity (Ruff, 2018). This model became cumbersome with the growth of online services, resulting in users having to remember numerous passwords for every resource (Jøsang & Pope, 2005). Notably that the central registries are also in place in many countries, storing lots of personal information about the citizens. As such, centralisation of identities' increases the risk of data misuse and abuse (ID2020, 2019)

Federated

An identity federation is composed of "agreements, standards and technologies", which allow several service providers accept the identifiers of users from a limited number of other providers (Jøsang & Pope, 2005, p. 4). In such systems, the user's identity data is created via one provider and can be reused in another one (Dunphy & Petitcolas, 2018). The Thales Group, a French electronic systems developer, believes that these federation are most commonly pushed by banks, due to the trust and broader outreach (Thales, 2019). Single sign-on is the authentication subset of the federated identity scheme, which can provide access to various platforms after logging in via one provider (Abraham, 2017).

Federated platforms are criticised for not being vulnerable to passwords proliferation and having privacy risks, identity theft and impersonation associated with that (Toth & Anderson-Priddy, 2019). Although the federated identities offer easy logging in experience, they provide little credibility in terms of security instead (Syed, 2019)

This identity model is prevalent within the public sector. The report on the identity solution in the EU showcases several renown federated identity solutions, namely the Italian SPID, Swedish BankID, British Gov.uk Verify and the Belgian itsme (European Union, 2018).

User-centric

User-centric identity management systems move the federations away and put the user in administration and control of identity information (Dunphy & Petitcolas, 2018). These systems were created with the idea that federated models are complicated. Consequently, more automation and system support on the user's side is indispensable (Jøsang & Pope, 2005). In this identity management scheme, the information about the user is stored by the user's side, in the way of a secure token, such as a smart card (Abraham, 2017). Hence, sharing an individual's identity information can only happen with their explicit consent (Abraham, 2017). User's consent and interoperability were at the focus of user-centric methodologies (Allen, 2016). This approach is believed to make the user experience better by "strengthening the mutual authentication between users and service providers" (Jøsang & Pope, 2005, p. 7). However, as Allen (2016) argues, powerful institutions possess the final ownership over user-centric identities.

2.3 The future of identity management

Self-sovereign identity is believed to replace the current identity models and become the next stage in their evolution. Many features of SSI are being discussed, but before that, there needs to be a clear problem statement of why current identity management is wicked and, therefore, needs this evolution.

Several studies were conducted to shed light on the evolution of identity management to outline these drivers to change but also to anticipate the future of identity schemes. In the context of global identity development, ID2020 project argues that the emerging technologies, especially decentralised identity systems, hold a potential to improve the privacy of user's data and allow portability and verifiability of identities. Still, a commonly agreed semantic and technical standards are needed to make that happen (ID2020, 2019).

2.3.1 Drivers for the identity evolution

Research by European Commission

European Commission undertook a challenge on mapping the current technological developments in the identity management landscape and published the report of the study

conducted by Deloitte. This report highlights the importance for governments to stay up to date with the eID landscape evolution to guarantee the relevance of the state-issued documents. Following the recent trends in the electronic identification discussed in the report, several factors driving the evolution of identity were presented. Those factors grouped under four categories: social, economic, technological and political and are shown in the following figure.

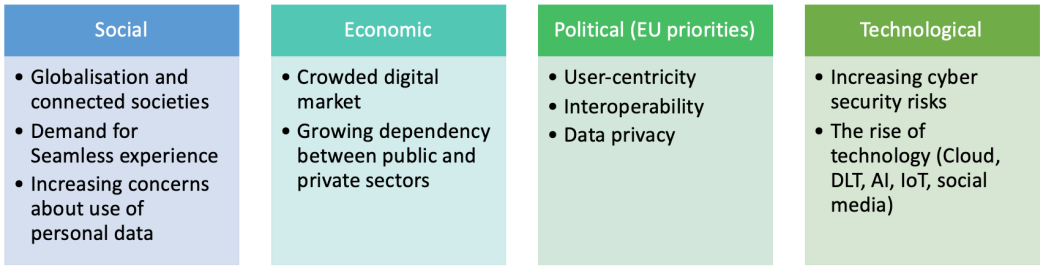

Figure 2. Drivers to identity evolution by European Union (2018)

Based on these drivers, experts foresee the following trends in the identity realm: increasing usage of mobile identity systems, deploying behavioural biometrics and most importantly, giving citizens more control over their data (European Union, 2018). In that sense, the authors also foresee SSI to be a mainstreaming model in ten years. The report concludes that the roles of different actors and the value division in future identity ecosystems will be entirely different (European Union, 2018).

Research by BBVA

Another study conducted by a Spanish financial company looks at identity as the fundamental development enabler, both in political and economic dimension (BBVA, 2019). The authors believe that financial institutions could act as relying parties within the federated identity systems because of their experiences with managing their customers' identities and established trust in banks as institutions. Also, the researchers identified the drivers to lead the transformation of identity solutions:

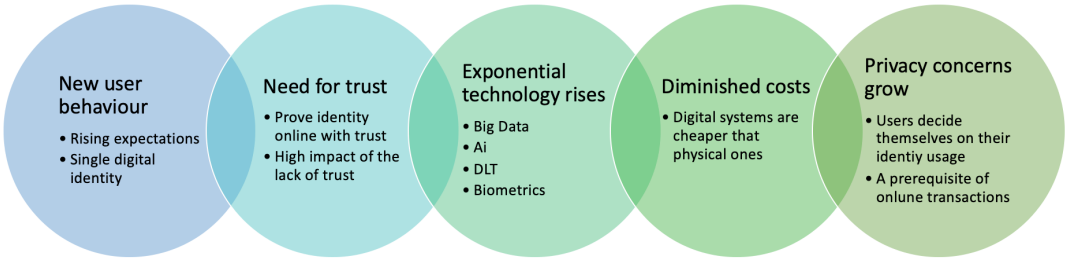

Figure 3. Evolution of identity drivers by BBVA (2019)

Legally enabled interoperability is a key to ensuring that future identity system benefits to their best ability, along with a strong focus for data protection (BBVA, 2019). Hence, it will be essential for governments to set up trust frameworks to regulate the components of those identity systems (BBVA, 2019). Also, the authors of this study highlight that both security and comfortable user experience are essential components of the future identity solution. In the discussion on users demanding more control over their identities and increasing usage of mobile devices, self-sovereign identity is viewed as the following evolutionary step of the identity, specifically mentioned banks being identity authenticators with a possibility of employing blockchain (BBVA, 2019).

2.3.2 Principles of future identity

ID2020 project believes that the identities of the future should be private, portable and persistent, and their subjects must hold full authority over its sharing and usage (ID2020, 2019). For a more thorough analysis of what the identity could look like, The World Bank took the initiative and conducted the respective study on the principles of future identity. These principles serve as a guide for global cooperation towards building sustainable identity models under the "Identification for Development" programme. They are endorsed by a large number of organisations worldwide from development, academic, and private sectors (The World Bank, 2019). Although the main target is developing countries without streamlined identity systems, the principles are universal and comprise best practices and knowledge from all over the globe.

The total of ten principles was grouped into three sub-categories, being inclusion, design and governance (The World Bank, 2017). In essence, the core idea is to ensure that identity systems are universal and globally covered; robust, secure and long-lasting but also trustworthy and well-governed. A summary of these principles can be found in the figure below.

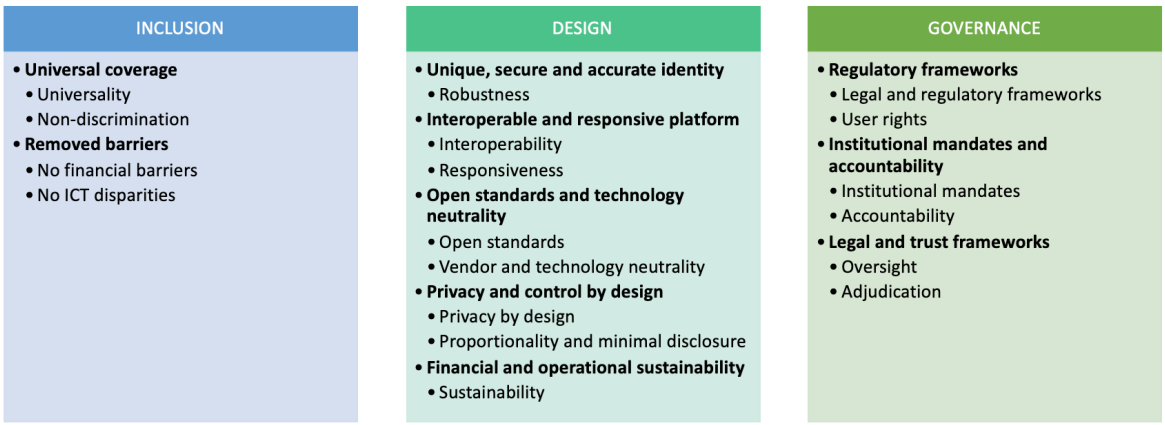

Figure 4. World Bank's Identity principles by The World Bank (2019)

The latest report on the project implementation suggests the trends of shifting towards decentralised identity solutions, which are believed to increase data security, give people more choice and generate better solutions via increased competition (The World Bank, 2019). However, it argues that shifting towards these identity paradigms requires the ability of public and private sectors to leverage the foundational identity systems in order to boost the integrity of data or onboard new users (The World Bank, 2019).

2.4 Self-sovereign identity

Decentralised identity management implies that as much as possible control over issuing and administrating identity is given to its subject, or a user, which can be achieved using the cryptographic algorithms and mathematical models (Lyons et al., 2019). As the next generation in the identity evolution, SSI emerged as a genuinely new identity paradigm. Originally coming from the technical community, SSI has now reached a state of increased interest from its enthusiasts. An active community of SSI enthusiast and practitioners uses the GitHub platform for exchanging the ideas and working on the improved terminology and concepts of self-sovereign identity. The following chapter will present the overview of concepts related to SSI as one of the forms of decentralised identity.

In essence, sovereignty refers to having the highest power or being entirely independent (Cambridge Dictionary, n.d.). In simple words, self-sovereign identity is a form of a decentralised identity where users can create their own identity and collect the credentials from verified sources and store them securely in their "identity wallet". It thus excludes control from the third party and enables a two-party relationship (Ruff, 2018). Notably, the key difference between the SSI and the previous identity models is that with SSI users exist independently from any service provider (Mühle, Grüner, Gayvoronskaya, & Meinel, 2018).

2.4.1 Principles of SSI

Despite its ongoing formation and missing a commonly accepted definition, SSI can be described with ten core principles outlined by Christopher Allen in 2016. He opened a discussion on SSI with his publication "The Path to Self-Sovereign Identity". Inspired by the "7 laws of identity", written by Cameron (2005) and the United Nations' chapter on human rights (UNCHR), Allen proposed his ten principles that allow describing the full spectre of features for the self-sovereign identity. A more comprehensive academic debate on these principles can be found in section 3.6. The overview of the overview and brief explanation of these principles is illustrated in the figure below.

SSI PRINCIPLES
• an independent **existence** of a user; • **control** of user's identities; • **access** to user's own data; • **transparency of** systems and algorithms must be; • **persistency** of identity; • **portability** of information and services about identity; • **interoperability** of identity; • explicit **consent** to use the identity; • **minimised disclosure** of claims; • **protection** of the rights of users

Table 1. Ten principles of SSI by Allen (2016)

2.4.2 Essential components of SSI

Within the SSI ecosystem, commonly there are four main actors, depending on their relation to the identity. These are an issuer, a subject, a holder and a verifier of identity. Identity issuer is the entity that creates, or issues identity attributes, which characterise the identity subject. Identity holder, in turn, is an entity, which is held accountable for interacting on behalf of this identity. A difference between the identity subject and the identity holder should be drawn because although in most cases both terms refer to the same person, in the event of an individual having a legal guardian, who is the identity holder but not the subject (Mühle et al., 2018). A verifier is a party that verifies or relies upon a piece of presented identity information (Wagner et al., 2018). In other words, this presented identity information is referred to as verifiable credentials (VC), which are digital credentials that come with such cryptographic proofs (Lyons et al., 2019). Ensuring its authenticity and integrity can be achieved by distributing it as a cryptographic token (Ferdous et al., 2019)

As denoted earlier, the identifier allows uniquely identifier the person without necessarily disclosing any other information about it. In the SSI system, this minimum data is represented by a URL-type identifier and is referred to as a decentralised identifier (DID) (W3C, 2020). According to the World Wide Web Consortium, DID works globally and does not require a centralised registration entity. It is registered with a decentralised network, such as DLT, and is entirely under the user's control (W3C, 2020). DID has two parts: the public and the associated secret one. The latter is used to prove the ownership of that identifier and serves a strong link between the DID and the data (Lyons et al., 2019). A schematic relationship of the actors and the underlying SSI ecosystem is illustrated in the following figure, suggested by Preukschat & Reed (2019):

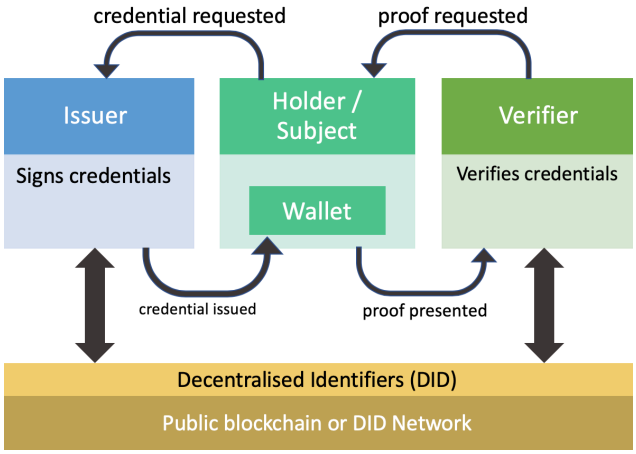

Figure 5. SSI roles by Preukschat & Reed (2019)

It should be noted that although the idea of decentralised identity is to put the user in control, it cannot exist entirely independently and it relies on the data provides by the third parties (Lyons et al., 2019). As such, SSI can have the credentials issued by the identity subject but also contain elements issued by other parties, including the government (Wang & De Filippi, 2020). Similarly to the physical world, the government remains the possibility the revoke credentials (Lyons et al., 2019).

2.5 National SSI projects

Amidst the global SSI development, several initiatives took a further step and developed working solutions, that tackle the technical part of self-sovereign identity and explore its implementation. Among those are solutions designed by uPort, Jolocom, Sovrin, Evernym and IBM, which vary in their core principles and the technology involved. European Blockchain Partnership, along with the European Commission, initiated the creation of a European Blockchain Service Infrastructure (EBSI) in order to facilitate creating efficient digital cross-border services (European Commission, 2018a). It is believed that EBSI will boost the development of the Digital Single Market and enhance service provision by public and private sectors. Under this initiative, the European self-sovereign identity framework (ESSIF) was created to embrace the knowledge about self-sovereign identity and to coordinate the activities around Europe regarding it (Du Seuil, 2019).

ESSIF's primary goal is to coordinate efforts to ensure the interoperability in the cross-border interactions. Among other things, ESSIF looks at how SSI can be aligned with the once-only principle, the EU Regulation №910/2014 (eIDAS) and hence build the identity layer for the EBSI (Du Seuil, 2019). The first phase of the project had the goal to define the necessary components of the SSI ecosystem. It was finished in 2019, followed by

framework research and the pilots' phase, with the mass implementation scheduled for 2021-2022 (Du Seuil, 2019)

Also, since the governments are more actively catching up with emerging technologies, SSI is no exception. At the moment, these initiatives are in the exploration stage, meaning that no specific takeaways can be derived from them for this study. The following section presents the overview of SSI-related activities happening in the public sector in different countries.

Belgium

Belgium has also expressed its interest in leveraging the blockchain technology for providing identity solutions for its citizens. The "Blockchain on the move" project was created as a collaboration of the Flemish Government, the city of Antwerp, Antwerp's IT company Digipolis and the Flemish ICT organisation Victor under the Innovative Public Procurement Program (Flemish Government, 2019). It was anticipated that citizens would get more freedom of choice in terms of sharing their data and having full control over it via having their digital vaults (Flemish Government, 2019). The first phase of the project involved the technical partner Jolocom and has the aim to develop building blocks, and it was completed in 2019 (PIO, 2019). The result of this phase was the developed PoC to illustrate the possibilities of SSI, upon which the use-cases can be built (Flemish Government, 2019). The scope of the project was modified, making the next step the investigation of the added value and the feasibility of the processes in Antwerp, such refugees' identities, digital key for civil services and the relocation in the city (PIO, 2019).

Canada

While setting a goal of digitalising all public services by 2025 (Canadian Digital Service, 2019), Canadian public sector also seeks to explore the opportunities of the self-sovereign identity. The country has also set the principles for the future of digital identity, where decentralisation is mentioned among the key priorities (Wolfond, 2017). While the country used both federated and centralised identity management systems, the Pan-Canadian Trust Framework was created to explore the opportunities of SSI in the context of Canadian public sector (Bouma, 2020). It aims at facilitating the transition towards a digital ecosystem for Canadians, which will increase the efficiency and secure interoperability among the current processes (Canada.ca, n.d.). Additionally, evaluating the possibilities of shifting from centralised digital identities towards VC is on the Canadian public sector's agenda (Bouma, 2020).

Becoming the world leader in terms of SSI implementation both an ambitious goal and also a part of the reality: many initiatives in Canada already explore the opportunities of SSI (Digital Canada, 2020). One of these projects was launched in the province of Alberta, where the local efforts were put together to launch the "Alberta Credentials Ecosystem". Inspired by the SSI, the project intends to increase the understanding of the self-sovereign identity and focus of specific use-cases for SSI inside the province (Digital Canada, 2019b). Another application can be found in the province of British Columbia, where a decentralised registry was created to combat the excessive red tape under the "OrgBook" project (Digital Canada, 2020). Following the example of the "Once-only" principle of the European Union, the OrgBook project created a publicly available repository, where the credentials of the organisations are stored, so they can share the data

Overall, Bouma (2020) believes that it is too early to make predictions on the outcome of the efforts happening in the field. It is also mentioned that a legal framework is required to fully support the implementation of the new technology (Digital Canada, 2019a). If addressed in the right manner, SSI is believed to create a better digital ecosystem for Canada (Bouma, 2020).

Germany

Apart from having an active community working on blockchain-related projects, Germany also has an initiative for SSI coming from the public sector as well. German authorities, in cooperation with business and academia, started exploring the opportunities for SSI on the national scope. The project named "Self-Sovereign Identity für Deutschland" (Self-Sovereign Identity for Germany) aims at developing the entire ecosystem for decentralised identity. It also aims at allowing secure digital identities, which are also compatible with other international networks, in Europe in particular (Bundesministerium für Wirtschaft und Energie, 2020). According to the Federal Ministry for economy and energy, this project will attract businesses, public administrations and citizens for creating user-friendly, trustworthy and cost-efficient solutions. Users will have a chance to store their data at their end, at the phone or other device, for instance. The data can be shared with other institutions' open request via the DLT network (Bundesministerium für Wirtschaft und Energie, 2020). As the ministry reports, the technology behind the system is the Hyperledger Indy and Hyperledger Arias by Linux.

The Netherlands

The blockchain is a significant part of the technological agenda in the Netherlands, with Dutch Blockchain Coalition being the key body. Also, the Delft University of Technology

is involved in the research on DLT for more than ten years, with Dutch Digital Passport being of their renown projects (TU Delft, 2018). As the Ministry of Interior supported this initiative, the developed application was meant to facilitate many identity checks procedures, having the SSI principle at the backbone (Delta, 2019). Notably, the previous initiatives with a similar scope from Utrecht and Eindhoven were cancelled due to immaturity of technology at that stage. At the same time, the TU Delft employs the brand new TrustChain technology (Delta, 2019).

Also, a mentorship initiative was started in the Netherlands. In November 2019, a new 3-years project named "NGI eSSIF Lab", initiated by the consortium of companies, was launched under the EU Horizon 2020 research programme (TNO, 2019). This project is aimed at exploring the self-sovereign identity and will allocate the 5.6 million euros for 62 business- and infrastructure-oriented projects (eSSIF-Lab, n.d.). (TNO, 2019)Therefore, the top priority of the eSSIF-Lab to create scalable and mutually interoperable solutions to be used throughout all domains (TNO, 2019).

Sierra Leone

The West-African country of Sierra Leone decided to launch national decentralised identity system using the Hyperledger layer. San Francisco-based company Kiva developed the protocol for this decentralised system, which uses the DID and VC models, having public bodies as VC issuers (Wang & De Filippi, 2020). Because the design of the system is private and permissioned, the approval of credentials issuers is done with the approval from the government and presently, these trust anchors comprise governmental and microfinance institutions (Wang & De Filippi, 2020). Hence, every citizen of Sierra Leone will be able to obtain credentials guaranteed by trusted sources and the possibility to make claims about themselves. Additionally, the pan-African coalition is working on Vibranium-ID decentralised identity to consolidate the initiatives and bring the SSI to African citizens. However, as Wang & De Filippi (2020) conclude, the high connectivity and smartphone penetration are necessary to enable the benefits of SSI, while Sierra Leona is a low-income country with significant economic barriers yet to overcome.

Spain

A national blockchain system named Alastria is being built in Spain by a non-profit consortium of 70 companies from various sectors (Wagner et al., 2018). This network had the aim to boost the creation of digital ecosystems by allowing stakeholders, both private and individual, to create the digital representations of their assets (InnoCells, 2019). As such, this new system will enable control over the personal data to Spanish citizens, following all European Regulations (Wagner et al., 2018).

In addition to that, a province of Catalunya has started another DLT-initiative of providing SSI to its residents (Government of Catalunya, 2019). The eIDAS-aligned project named "IdentiCAT" aims to benefit Catalonians by giving them the sole control over their data, making it one of the first use-cases in the world, where SSI is supported by the public sector (Government of Catalunya, 2019). Although the Catalan government will remain as the identity validator, the citizens are foreseen to have sole control of their identities (Government of Catalunya, 2019)

2.6 Summary of chapter 2

The notion of "identity", in the physical and digital dimensions, cannot be looked at in isolation because of its dependence on other factors. This chapter presented the main concepts related to identity and digital identity, as well as underpinned the drivers and principles of future identity systems. Based on the existing discourse, SSI conceptually fits this narrative by bringing more control to the citizens and allowing transportability, interoperability and higher security of identities.

Also, the public sector has already demonstrated its interest in this identity model. Presently, many SSI-related initiatives can be found around the globe. As the aim of this study is to assess the possible benefits and challenges that SSI can bring to the public sector, the following section elaborates on the conceptual framework for this analysis.

3 LITERATURE REVIEW & CONCEPTUAL FRAMEWORK

The analysis of the SSI implications in Belgium will be guided by the conceptual framework proposed in the literature and tailored for the needs of this research by the mapped academic debate on SSI opportunities and challenges. Using the conceptual framework, according to Miles and Huberman (1994), allows researchers presenting what is included in the scope of the research and establishing the relationships between the constructs of the study (as cited in Baxter & Jack, 2008).

Hence, it is vital to outline the key achievements in academic research to put this thesis in perspective to understand how the opportunities and challenges can be assessed. The selection of papers was made by the following keywords: "self-sovereign identity", "decentralised identity", "blockchain identity" with the combination of "framework", "benefits", "challenges" and "principles". The illustrated matrix of the selection of papers is presented in the following figure:

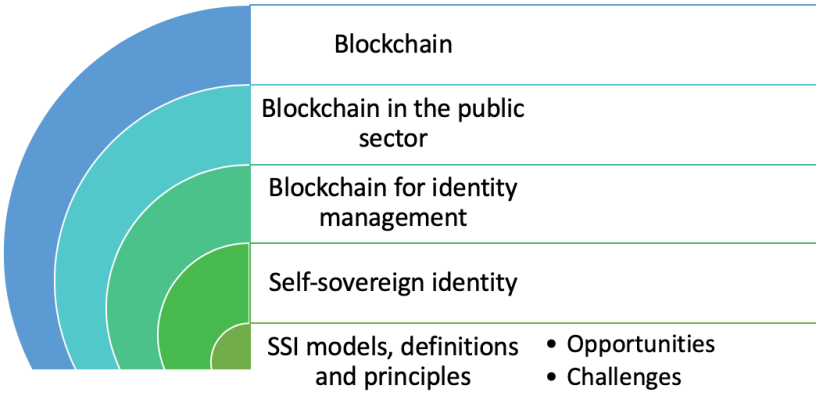

Figure 6. Themes of the literature review

3.1 Blockchain

Blockchain unconditionally is a buzzword: as a technology behind the acclaimed cryptocurrency bitcoin in 2008, blockchain invoked many uncertainties in the society. Scholars and practitioners argue that blockchain is a disruptive innovation with the economy-changing capability (Mattila, 2016; Trautman, 2016; Yuan & Wang, 2018), or even calling it a fundamental technology (Iansiti & Lakhani, 2017).

A white paper on SSI, prepared by Sovrin Foundation, gathered experts from various fields and suggested that SSI does not depend on a certain kind of DLT, meaning it is not necessarily blockchain-based (Wagner et al., 2018). It is important to draw a line between the blockchain, and a distributed ledger should be drawn. A distributed ledger refers to an architectural constitution of nodes spread across the network with no governing or

central body, and the consensus on its current state is reached by the participants of this network (Maull, Godsiff, Mulligan, Brown, & Kewell, 2017). DLT can be best described as copied, shared, and synchronised data spread across different locations (Yu, Liu, He, Si, & Zhang, 2018). Notably, that although every blockchain is a distributed ledger, it does not work vice versa (Yu et al., 2018).

In essence, blockchain is a public ledger, that can be used throughout the globe for storing records in a decentralised fashion (Swan, 2015). It means that blockchain is a distributed database, maintaining a continually growing list of records, which are called blocks, each of those blocks storing transactions (Ølnes & Jansen, 2018). These transactions could be anything from financial data to votes, software or even ideas (Swan, 2015). Hence, the immutability of such way of storing the data is created, as the blocks are linked with a cryptographic function called a hash. Hash is a cryptographic function to return a value of a fixed length, no matter the size of the input.

Speaking of DLT is impossible without mentioning its essential elements. Yu et al. (2018) systematised the overall composition of DLT into several layers: application, contract, privacy, incentive, ledger technology, consensus, network and data layers (Yu et al., 2018). For blockchain, in a universal explanation, the following figure presents the five main components of blockchain:

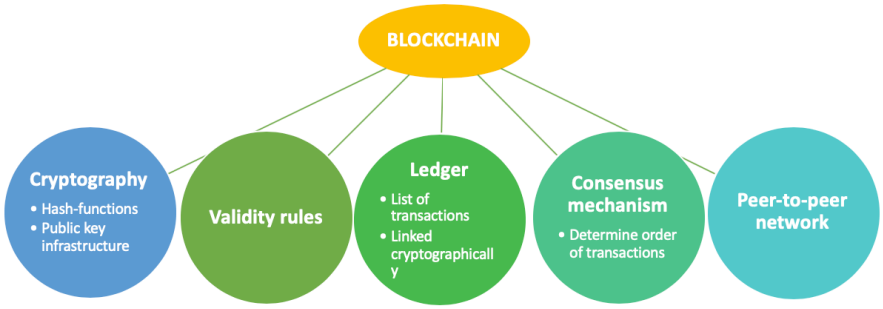

Figure 7. Blockchain's main elements by Hileman & Rauchs (2018)

The typology of blockchain illustrates how can this technology be used for different purposes. Commonly, blockchains can be public or private, based on the possibility for any user to join the network, and permissioned or permissionless, based on what parties are entitled to make contributions to the state of the ledger (Hileman & Rauchs, 2018).

3.2 Blockchain in the public sector

The application of distributed ledger technologies, blockchain, in particular, has got attention from scholars. Apart from the financial and business sectors, it is more of interest for this thesis work to consider how blockchain found its place in the public

sector. Levering the industry-disrupting technology within the government with the potential to solve transparency and security problems seemed promising both for the public administrations and the scholars working in this field. Researchers explore what the opportunities for employing blockchain with social impact are. Kuo, Kim, & Ohno-Machado (2017), for instance, explored the prospects of implementing this technology in healthcare. Despite the expected challenges, the authors gave a positive forecast for blockchain's application for improving biomedical and health care domains (Kuo et al., 2017). Researchers also highlight that what can be expected from blockchain is transparency, equality and autonomy in the realms of "online identity, human trafficking, corruption, fraud, democratic participation and freedom of expression" (Al-Saqaf & Seidler, 2017, p. 12).

The paper of Ølnes, Ubacht, & Janssen (2017) presents an in-depth analysis of academic work. It sets the ground for a future scientific debate on blockchain implementation in the public sector, specifically for e-government. The authors acknowledge that modern research tends to ignore factors such as "implementation, trade-offs, limitations, materiality and governance aspects" when discussing blockchain's possibilities (Ølnes et al., 2017, p. 355). In case of the government, a thorough analysis of its processes is needed before any expectation should be made because many benefits lying behind the blockchain are not exclusively attributed to the blockchain (Ølnes et al., 2017). In that way, before any concrete implementation plans are developed, it is crucial to map what benefits are blockchain-specific and for which situation blockchain could be the best fit to achieve the desired benefits (Ølnes et al., 2017). A crucial issue of blockchain governance was raised, specifically its two roles: "governance by blockchain" and "governance of the blockchain" (Ølnes et al., 2017). While the former stands for using blockchain for organising the governmental processes, the latter means that the process of blockchain implementation and maintenance has to be guided by both technology experts and policymakers (Ølnes et al., 2017). From a more technical perspective, an information stewardship issue was raised because the ledger equipment is owned and has to be maintained by some party (Ølnes et al., 2017). The authors also suggest that government can act as a trusted administrator, and will initiates and maintain the ledger, "determine the transaction rules and audit applications" in order to guarantee stable functioning (Ølnes et al., 2017, p. 363).

On the international scene, a notable contribution to mapping blockchain's possible implications in the public sector was made by the Organisation for Economic Co-operation and Development (OECD) (Berryhill, Bourgery, & Hanson, 2018). Its report has aggregated the existing knowledge, interviewing field experts, among other things. Despite the expected benefits of increased effectiveness, knowledge sharing and

automation, as well as the decreased bureaucracy and friction between agencies, they concluded, that blockchain technology is not universal and cannot be used to solve all existing challenges of the public sector (Berryhill et al., 2018). They suggested that the public administrations, along with the partners from all industries, should experiment with this technology, test use-cases and accumulate the knowledge on blockchain's application. As Ølnes et al. (2017) suggest, along experiments goes the adaptivity for the changing circumstances. In order to make that happen, public administrations need to be agile and open to digital transformation, as bringing blockchain-based identity ecosystems will likely change many entrenched processes and governance framework (Wolfond, 2017).

The same suggestion regarding the future experiments was made by the World Food programme, where Blockchain was used to provide the financial aid to refugees and managed to eliminate 98% of the related transaction bank fees, compared to standard transfers via the local bank (Zambrano, Young, & Verhulst, 2018).

3.3 Blockchain for digital identity

An even more specific application of blockchain in the public sector, for digital identity, in particular, can also be found in the literature. Zyskind, Nathan, & Pentlad (2015), inspired by the success of the bitcoin in reducing surveillance, argued that a similar approach could be used to build decentralised personal data schemes. They attempted to leverage blockchain technology to create a decentralised platform for securely sharing personal data.

HBR researchers also concluded that the domain of identity management will benefit from blockchain the last but can deliver the highest value (Iansiti & Lakhani, 2017). Also, the EU report on the blockchain on digital identity states that although this technology might not be required for achieving decentralised identity, it can still be a powerful tool for many facets of its framework (Lyons et al., 2019). These authors also suggested that those aspects could be, for instance, issuing and registering decentralised identifiers, notarising user's credentials, as well as providing decentralized infrastructure for access control (Lyons et al., 2019).

Dunphy & Petitcolas (2018) were interested in looking at the opportunities for the distributed ledger technologies used for solving the centralisation problem of identity management. They defined two categories of DLT-enabled identity schemes: SSI and decentralised trusted identity". Despite mentioning SSI, the paper does not address this particular paradigm as its core objective and is instead looking at the overall opportunities for the distributed ledger technology. The authors analysed the existing DLT identity

solutions against the "laws" of identity by Cameron (2005). Yet, this assessment cannot be considered relevant as of today as Cameron's laws are dated 2005, leaving many recent developments behind.

Nevertheless, based on the evaluation of those DLT solutions, authors concluded that although they aim at eradicating the middleman and hence removing the centralisation, it is not possible to be done entirely due to the nature of identity management, where there is a "profound need for trust" (Dunphy & Petitcolas, 2018). They suggest that the task for the future research is to find the balance between centralisation and decentralisation in the DLT-based identity management systems, underscoring that the blockchain is not a "silver bullet solution" for this (Dunphy & Petitcolas, 2018)

Driven by the social demand of having more control over the personal data in the Netherlands, Baars (2016) conducted a study on exploring the opportunities of using blockchain for achieving self-sovereign identity. At that time of the study, the available decentralised identity solutions were analysed, and the majority of them did not allow the user storing their personal data, or the solution did not gain a wide adoption yet (Baars, 2016). Hence, novel at that time, the decentralised identity management solution proposed by the author encompasses ten principles offered by Allen (2016). Based on the developed proof of concept, the author acknowledged the opportunities for blockchain to be used as the underpinning technology on the infrastructure level to achieve self-sovereign identity. No information should be stored on a blockchain, and claims should be used instead (Baars, 2016). Overall, the author concludes the blockchain can be used to solve the trust problem, instead of guiding the development of the artefact.

3.4 Theoretical development

3.4.1 Definitions of SSI

Self-sovereign identity research emerged as a separate stream relatively recently, though circulating discussion on brining control over the personal data was there for a long time. Interestingly, the paper published in 2010 argues that the initiatives on creating a citizen-controlled decentralised vault were abandoned due to privacy and security concerns at that time (Dumortier & Robben, 2010). Also, despite the earlier attempts to resolve the decentralised identity puzzle, the official name of "self-sovereign identity" the topic of this thesis received only in 2016.

Many scholars refer to the article at the "Life with Alacrity" blog as a turning point specifically for self-sovereign identity. However, due to its dynamic development, there is no commonly-accepted definition for SSI, and the ones found on the internet can also

vary (Mühle et al., 2018). It is also argued that the present definition may not only vary but also contradict to each other (Ferdous et al., 2019).

Christopher Allen is considered to be a pioneer in the SSI discourse and defines self-sovereign identity as an identity paradigm where a user is central to its administration (Allen, 2016). He argues that this identity has to be interoperable and autonomous, as well as transportable. Another definition of SSI can be denoted, which was elaborated by the collective efforts of researchers and private sector companies. According to them, SSI is a "model of digital identity where individuals and entities alike are in full control over central aspects of their digital identity, including their underlying encryption keys" (Wagner et al., 2018, p. 27).

3.4.2 Principles of SSI

The nature of SSI can be described via its core principles, which were the first outlined in the blog post by Allen (2016). These principles, in essence, give a full spectre of requirements for the identity to be called self-sovereign, covering the perspective that human rights, which, according to the UNCHR, are universal and should be conveyed in the digital world too (Allen, 2016). Not long after their publication, some criticism from the experts' side was published in the SSI directory on the GitHub platform (Schutte, 2016). In one of the webinars on SSI, Christopher Allen also mentioned that the principles would be revised in 2020 (Allen, 2020).

For an unambiguous understanding, those principles were divided into the following categories: controllability, portability and security (Tobin & Reed, 2017). Scholars also argue for breaking down the security category for two sub-categories, stating that protecting personal data and limiting its exposure to a minimum can describe SSI more explicitly (Mühle et al., 2018). While some studies refer to the SSI principles just as Allen wrote them, others argue that those are incomplete or misguiding. The new principles were suggested by Stokkink & Pouwelse (2018), namely, provability, stating that "claims are not worth anything if they cannot be shown to hold true" (p. 1337). Also, Satybaldy, Nowostawski, & Ellingsen (2020) propose including usability to emphasise the importance of comfortable user experience. The following section illustrates some works elaborating on their vision of SSI core principles.

Principles of SSI by Toth & Anderson-Priddy (2019)

Toth & Anderson-Priddy (2019) followed discourse that the principles of SSI are still commonly defined. Seeking possible standardisation of the SSI properties, authors considered the previous efforts to propose a unified framework to describe a self-sovereign identity. While existence, transparency, and protection from Allen (2016)

require further debate, the remaining ones were regrouped and enriched by Cameron's laws and W3C's identity standards. These authors also conclude that new principles are needed to make the definition of SSI more explicit: usability, counterfeit prevention, identity verification and assurance, as well as secure transactions (Toth & Anderson-Priddy, 2019). The summary of these 14 SSI principles can be found in the following figure:

Identity data model	Interoperability
• Persistence • Portability • Control • Access • Consent • Disclosure	• Usability • Counterfeit prevention • Identity assurance • Identity verification • Secure identity transfer • Secure transactions

Table 2. SSI principles by Toth & Anderson-Priddy (2019)

The authors acknowledge the possible disagreements among the colleagues and indicate their openness for the future debate. The authors used SSI architecture, which they developed to validate these principles. Toth & Anderson-Priddy (2019) concluded that further research is needed to incorporate user's consent into that architecture.

Principles of SSI by Ferdous et al. (2019)

Seeking a shared understanding of what self-sovereign identity semantically is, Ferdous and colleagues (2019) critically assessed the existing knowledge. Their goal was to pose a unified definition of this concept, as well as the properties that SSI should have. They argue that most of the definitions of what SSI is are based on the textual properties and usually neglect the real implementation. Also, Ferdous et al. (2019) mentioned that identity and identity management systems are different concepts, and often the properties listed to SSI are more related to the identity management system.

As their contribution, Ferdous et al. (2019) proposed a mathematical model to illustrate SSI functionality, based on its features, which were derived from the existing discussion in academia and practice. These authors believe that although there are some market solutions labelled as SSI, they do not meet the full list of requirements and hence, more rigorous work in needed to achieve SSI fully. Initiating a debate on a more stringent way of looking at SSI, the authors proposed the typology of SSI properties, which are illustrated in the figure below:

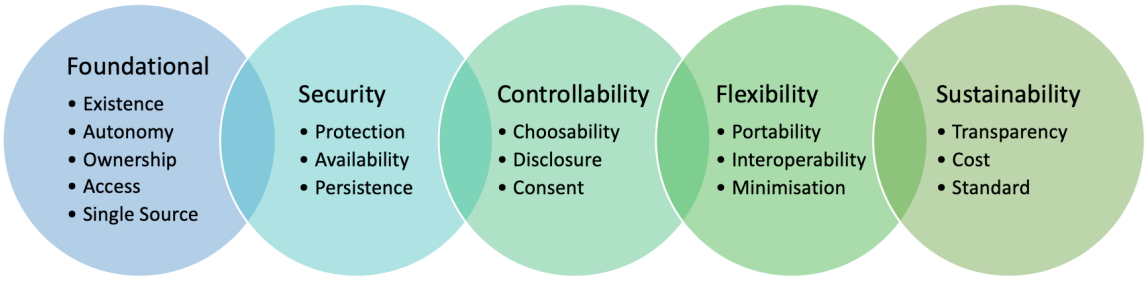

Figure 8. Principles of SSI by Ferdous et al. (2019)

Notably, the authors distinguish which principles are SSI-inherent and which correspond to the identity management systems: they believe that the first group of principles, namely the foundational, are the ones without what the SSI cannot exist. Regarding the technological implementation for the proposed model, smart-contract supported blockchain systems are believed to be the core solution due to its compliance with the principle SSI features (Ferdous et al., 2019).

3.4.3 Models of SSI

Focusing on a more practical side of self-sovereign identity has posed difficulties on researchers as it is difficult to foresee the best use-case for an immature technology. Although the standardisation and interoperability are essential for ensuring the development of the SSI, there is no universal identity model for each use case, and it should be hence tailored for each application (Wang & De Filippi, 2020).

Requirements for SSI information system by Van Wingerde (2017)

A study by Van Wingerde (2017) aimed at uncovering the requirements for a regulatory compliant SSI information system. Also, the author wanted to determine how can blockchain technology contributes to that and whether it is a must component of this model. The ten principles of SSI by Allen (2016) guided the processes of building these requirements, as well as the trans-European regulations such as GDPR, eIDAS and 2nd Payment Service Directive. Additionally, functional and non-functional requirements for six use-cases of SSI were identified, including establishing a digital identity, issuing verified claims, asserting a verified claim, revoking a claim, authenticating an entity and providing access to personal data to another entity (Van Wingerde, 2017).

The author then validated to what extent does the blockchain technology help achieving these requirements for the SSI (based on the 1 to 3 satisfaction), resulting in 79% of the criteria being satisfied (Van Wingerde, 2017). This researcher concluded that although blockchain can significantly contribute to achieving SSI in practice, additional technology is needed to meet all the requirements entirely. It was explained that

blockchain has several drawbacks such as loose scalability, privacy is not entirely achieved, and the cost of transactions is still high (Van Wingerde, 2017). The Dutch government used the result of this study in the SSI policy

Model by Stokkink & Pouwelse (2018)

Stokkink & Pouwelse (2018) suggested an academically pure model for self-sovereign identity. This model takes the existing solutions (Sovrin and uPort) and, using the results of the Van Wingerde (2017) research, authors create a standard SSI model, in cooperation with the Dutch Ministry of the Interior and Kingdom Relations (Stokkink & Pouwelse, 2018). The process of developing this model was also guided by the ten principles by Allen (2016), mentioning that the blockchain technology itself intrinsically fulfils some of those principles. However, the authors also suggest that another principle should be added, namely the provability, as without being provable, the claims are not worth anything (Stokkink & Pouwelse, 2018).

The developed solution contains a model for the claim and its metadata, integrated on the blockchain, including fields such as "name, timestamp, validity term, proof format and proof link" (Stokkink & Pouwelse, 2018, p. 1338). Several solutions were hence evaluated using the model, and one of the main takeaways was the ease-of-use of this model, resulting from a low duration of claims verification, which was one of the authors' aims in the first place (Stokkink & Pouwelse, 2018). The results of this study were used as blueprints for the Dutch blockchain-based passport, being not only SSI principles-compliant but also cheat-proof.

Van Bokkem et al. (2019)

Van Bokkem, Hageman, Koning, Nguyen, & Zarin (2019) looked at the problem from the opposite direction, exploring whether blockchain is a compulsory component of SSI or not. For that, they assessed 12 various SSI-labelled implementations against multiple criteria intending to verify this assumption. These criteria comprised the ten principles of Allen (2016) plus the provability principle, added by Stokkink & Pouwelse (2018). These researchers proposed the framework for evaluating the existing SSI solutions and concluded that although the blockchain-bases solution fulfilled more criteria, the DLT is not necessarily underpinning self-sovereign identity (van Bokkem et al., 2019). Nevertheless, blockchain can serve as a solid basis for building up SSI, given its features.

Apart from the works mentioned above, some notable papers also include one of Satybaldy and colleagues (2020), who proposed the framework for evaluating, describing and comparing SSI solutions. They looked that the Sovrin, uPort, ShoCard, Civic and

Blockstack to check how these SSI solutions correspond with the set requirements. The conclusion of the benefits and challenges associated with SSI are presented in sections 3.8 and 3.9, respectively.

Since SSI does not necessarily stand for the identity for individuals, it was also studied in the context of objects, namely, the Internet of Things. Bartolomeu, Vieira, Hosseini, & Ferreira (2019) looked at the existing technological solutions, including the Sovrin, uPort, Veres and Jolocom and compared them against the following criteria: the presence of a distributed ledger, number of supported transactions per second, a transactions delay and transaction cost. Regarding the latter, the authors underscored that the users would not commonly adopt the solution if the transaction fee is too high (Bartolomeu et al., 2019). These researchers also admitted that Sovrin's Hyperledger Indy, being one of the most advanced solutions at the moment, stands out due to its permissioned nature, and hence, no proof-of-work is needed for spam eliminations, which in turn minuses the transactions delays and costs (Bartolomeu et al., 2019).

3.5 Benefits of SSI

Mapping the benefits of the maturing technology is tricky because there are no use cases to validate those, and they can only be a subject of conceptual debate. Speculating of benefits of an emerging technology that still matures must be done with care in order to avoid exaggerating and deceitful statements. In this respect, Ølnes & Jansen (2018) suggest that revealing the full potential of blockchain, not only in the public sectors, lies in exploring the specific areas where this technology can be used effectively.

Nevertheless, many publications mentioned the areas where the SSI could positively contribute. The following section presents the excerpts from the SSI-themed studies trying to make sense of the potential benefits of this identity paradigm. Some of them are blockchain-specific, while others are derived from the conceptual definition of SSI

Ferdous et al. (2019) also argue that mapping concrete use-cases is needed to uncover the usefulness and the applicability of SSI. In that sense, Keil (2019) suggests that industries that benefit the most from the uptake of SSI are the ones where the know-your-customer (KYC) processes play a significant role.

The World Bank believes that decentralised identities can support refugees and grant them absolute authority over identities (The World Bank, 2018a). That is to say that as such, SSI is digital by default, and hence it is also more portable than a standard identity document (The World Bank, 2018a). Not only in case of refugees but overall, SSI holds the potential to bring more freedom to the individual and hence, "counteract the oligopoly

structure of today's Internet" (Der, Jähnichen, & Sürmeli, 2017, p. 3). It will remove the need to trust a single authority and increase the trust in the governments since the processes will become more transparent (Abraham, 2017). Overall, United Nations believe that enhanced privacy and control over personal data impact the way an individual develops, it is early to speculate whether SSI can guarantee that on practice without concrete solutions (Zwitter, Gstrein, & Yap, 2019). Consequently, more democratic societies can also be achieved with SSI, via better utilisation of online voting in particular (Preukschat & Reed, 2019).

Governments can also expect to mitigate the "risk transacting with fraudulent and malicious actors" for all levels of credentials (Syed, 2019, p. 58). Reducing fraud was also mentioned by Toth & Anderson-Priddy (2019), who believe that SSI can contribute to combating identity impersonation and data breaches.

The cross-border transactions can be made simpler and faster (Abraham, 2017). In a broader scope, SSI is believed to remove the trust barriers in the European single market and hence, to bolster it (Der et al., 2017). Also, the issue of reducing costs for an identity management system is discussed as the key tasks for SSI (Abraham, 2017), knowing that the current systems are costly (Doerk, 2020). Wolfond (2017) also argues that using blockchain in a digital identity ecosystem can help cut costs caused by passwords management. The higher standards will also result in increased efficiency in all sectors (Wolfond, 2017). However, a more thorough analysis from the economic point of view is needed because the present papers and publication merely provide a rationale behind the statements on the financial benefits of SSI.

Preukschat & Reed (2019) argue that SSI can be explained neither within a limited array of benefits nor with a primary one. They point out that these features and benefits are diverse and depend on the specific use-case and industry where SSI is applied. The developed scorecard illustrated the expected benefits of SSI, consisting of five major categories, which are depicted in the following figure:

Bottom Line	Business Efficiencies	User Experience & Convenience	Relationship Management	Regulatory Compliance
• Fraud reduction • Reduced customer on-boarding costs • Improved e-commerce sales • Reduced customer service costs • New credential issuer revenue	• Auto-authentication • Auto-authorization • Workflow automation • Delegation & guardianship • Payment and value exchange	• Auto-authentication • Auto-authorization • Workflow automation • Delegation & guardianship • Payment and value exchange	• Mutual authentication • Permanent connections • Premium private channels • Reputation management • Loyalty & rewards programs	• Data security • Data privacy • Data protection • Data portability • Regulation Technology

Table 3. Benefits of SSI by Preukschat & Reed (2019)

All in all, the list of benefits is not exhaustive and depends on the particular context. This section only glances at the possible benefits of SSI. Consequently, more research is needed in this field, and more use cases need to be tested to verify the statements as mentioned earlier.

3.6 Challenges and driving forces

Apart from only seeing SSI as a universal and panacea-like solution, scholars also admit several challenges, which might occur when implementing SSI paradigm. Experts argue that although SSI might seem to solve the issue of trust, implementing this technology is much harder than "selling" it. The World Bank reports that the opportunities for decentralised identities, with many uncertainties associated with their implementation: legal alignment, interoperability, "maturity, ease of adoption, affordability, performance, security and scalability" (The World Bank, 2018a). The following section presents the discourse around the challenges and flaws associated with the SSI and its implementation, as well as the respective driving forces to support the SSI implementation. Many of those challenges are not exclusively SSI-specific, yet it is worth noting them to be able to build a holistic picture of SSI implementation.

3.6.1 User-related factors

Wagner et al. (2018) believe a most critical challenge in SSI wide acceptance is its perceived complexity. As a result, SSI risks being not widely adopted. Most of the modern SSI solutions are very technology-focused, meaning that the interfaces, managing the keys and privacy concerns are "not addressed yet in sufficient depth" (Satybaldy et al., 2020, p. 13). The idea of user-friendliness was also mentioned by Dunphy & Petitcolas (2018). These authors also foresee a risk of having users with little technical background left behind, as well as not being able to recover their keys if those are lost, hence losing the access to their data. These researchers also argued that users are not very concerned about the technology behind the identity management, having its usability as the primary objective.

This behaviour is also mentioned in the study of Der et al. (2017). They pointed that users usually choose to risk their privacy when using, for instance, Facebook or Google log-in services in return with a conformable user-experience. They suggest that using SSI should guarantee not only privacy and control but also a comfortable usage. Baars (2016) indicated that the complexity of the technology can be tackled by creating a user-friendly interface.

Another important issue is social inclusion. Child's identity has to be managed by someone else due to legal constraints, as well as older adults who are not familiar with the technology are at the risk of being left behind (van Dongen, 2019). Hence, the new technological solutions are not likely to enjoy a wide adoption if their implementation is based on the old schemes, as (Dunphy & Petitcolas, 2018) argue, and forget the comfortable user experience in the equation (Satybaldy et al., 2020).

3.6.2 Technology-related factors

The primary challenge of SSI is its low maturity and a small usage, hence, its impact is yet to be seen (Bartolomeu et al., 2019). These researchers also acknowledged that commonly accepted specifications terms of standardisation are lacking, despite the ongoing development. Among the SSI solutions available, a majority has a blockchain infrastructure from its financial implementation at the base, which implies the transaction fee-based and contradicts the principles of SSI that it should be free and available to everyone (Satybaldy et al., 2020). As a way of achieving the standards, being open-source is essential for broader adoption of SSI (Baars, 2016). Moreover, consolidation of best practices with a reflection on the current regulations is needed (Doerk, 2020) However, another blockchain-related challenge was pointed out, as anonymity implies having no possibility to track the data of criminal for the investigation, if needed (Setsaas, 2020).

A foreseen challenge is ensuring the sustainability of SSI-like digital identities. As previously suggested, utilising SSI puts too much responsibility on the user (Setsaas, 2020). Wang & De Filippi (2020) also mentioned the key recovery as one of the most crucial problems with SSI. Technology needs to ensure that there is a backup if it loses their access for various reasons to a physical device containing the identity wallet (Zwitter et al., 2019). For that, they suggest that identity custodians can play a crucial role to ensure the viability of the user's data (Wang & De Filippi, 2020).

Implementing SSI needs a decent infrastructure in place to guarantee the usage, namely high-quality connectivity and high smartphones provision and at an affordable price (Wang & De Filippi, 2020). Additionally, there is also a need for updating of legacy systems, so that they can benefit "from the increased cost efficiency and redistributed liability risk of SSI" (Wagner et al., 2018).

Following the lack of technical understanding as a hurdle, Abraham (2017) also envisioned challenges with the type of blockchain's access permission and the associated difficulties with calculating the proof of work and the data storage issues. However, this author does not provide an elaborated way of dealing with these challenges. The

reasoning is also missing on whether these challenges are caused by a low maturity of SSI and could have been improved in future.

3.6.3 Governance- and government-related factors

Organisational resistance is also mentioned as a possible obstacle for decentralising identity systems (Baars, 2016). Although the nature of SSI implies having no third party, the infrastructure and the architecture has to be developed, maintained and administrated by some entity, and hence, an issue of power balance remains critical (Zwitter et al., 2019). Also, there must be guidance on re-using the VC in a different context, as it is believed that it will define the way companies, including public organisations, will adopt the SSI principles (Wagner et al., 2018)

Intrinsically, having robust governance frameworks in place is needed when implementing SSI, given the issues mentioned above of user competence and the maturing technological provision (Wang & De Filippi, 2020). The frameworks will ensure the "legal liability for fraudulent validators on a network" (Syed, 2019, p. 59). For that, governments have to be educated about this domain and their role as identity issuers (Lyons et al., 2019). Additionally, as the EU Blockchain Observatory and Forum suggest, the pan-European guidance can enhance the usage of decentralised identities.

The governance issue is also partially connected to the economic models behind it, meaning that the consensus of the distributed ledgers like blockchains is used via the consensus mechanisms (Nakamoto, 2009). Because of this incentive mechanism, the SSI has a risk of being expensive due to power and hardware needs. However, as Satybaldy et al. (2020) argue, should the permissioned blockchain be used, it could solve the cost challenge by moving them to the service provider's side. Nevertheless, by doing so, the SSI risks moving towards a more centralised approach again, as these authors also admit.

There are many developing SSI solutions, and they need to be leveraged by governments and the industry for the concrete use-cases, where public institutions currently fail to succeed (Zwitter et al., 2019). Mainly, the success of SSI is entirely dependent on those use cases (Wang & De Filippi, 2020). Governmental support and the alignments with the existing regulations are mentioned as the important success factors. Those cases include cross-sectional usage of credentials, customer-driven workflows, bringing more standardisation and protecting personal data as per the regulations (Doerk, 2020). For instance, smart cities can be an excellent playground for decentralised identifiers, and hence the European Union could support local authorities with funding and expertise with SSI (Lyons et al., 2019).

3.6.4 Legal factors

Being technologically developed does not guarantee the successful implementation of SSI if it is not fully compliant with both national and pan-European regulations. Scholars and practitioners looked at how the current developments of SSI are aligned with the main legal frameworks, namely GDPR and eIDAS, and gave their recommendations towards the future advancements.

eIDAS

Being one of the crucial European regulations, eIDAS dictates the way decentralised identities are built. The eIDAS was adopted in 2014 and set the new path for the digital transaction across the EU (European Commission, 2018b). This regulation aims in the first place at regulating the environment for smooth and secure electronic interactions between citizens and public and private sectors (European Commission, 2018b).

In essence, the trust services, according to the eIDAS, are electronic signatures, seals, timestamps, websites authentication certificated and registered delivery services (European Commission, 2018b). To allow its full functioning, eIDAS obliges EU member states to develop authentication mechanisms, which can be either federated or non-federated (Roelofs, 2019). As Lyons et al. (2019) suggest, one could treat eIDAS as a powerful tool for supporting decentralised identity throughout the EU and strive to have SSI solutions which are eIDAS compliant at the highest level of assurance.

Overall, practitioners of SSI admit that the challenge remains with translating the centralised eIDAS view on trust services in a more decentralisation fashion, staying compliant with the regulations at the same time (Wagner et al., 2018). Some studies argue that eIDAS implies that blockchain records “cannot be denied legal force” due to their electronic nature (Lyons et al., 2019). Nevertheless, the DID, a core of SSI transactions, is not currently recognised at the electronic signature within the SSI ecosystem (Wagner et al., 2018).

One of the EU reports discusses how the development of SSI can be supported by the trust frameworks and related services (European Commission, 2019c). In that paper, the parallel was drawn regarding the electronic document as per eIDAS and the blockchain, which, in fact, can be legally considered an electronic document. The authors also provided the example on the possible linkage between eIDAS and SSI-related concepts of DID and VC, concluding that more discussion is needed in this direction (European Commission, 2019c).

GDPR

GDPR stands for General Data Protection Regulation of the European Union №2016/679, which sets the advanced requirements for the processing of individuals personal data in a rapidly growing digital world, hence strengthening citizens fundamental rights (European Commission, n.d.). It was published on 24 May 2016 and was legally enacted on 25 May 2018 and will affect all entities processing the data of EU residents, no matter of their physical location (GDPR.eu, n.d.). The following seven principles of data processing, which can be found in the article 5.1-2, describe the essence of the GDPR: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability (GDPR.eu, n.d.). The clear and unambiguous consent has to be given by a data subject to permit processing their data, and this consent can be revoked upon a time if the subject wishes so (European Commission, n.d.).

Studies and publications agree that aligning with the leading European regulation should be taken into consideration during the SSI implementation. While some studies mention that conceptually SSI aligns with the GDPR (Der et al., 2017), the practical aspect of it is much more complex and requires comprehensive analysis. Blockchain specific-characteristics like immutability and storing the information on a public ledger might be hazardous (Kondova & Erbguth, 2020). Even though the firm definition of SSI is not there, its concept implies that a user has a right to modify or remove their data via "control" and "consent" principles (Mühle et al., 2018). This right is also supported by GDPR's right to be forgotten (GDPR.eu, n.d.).

The Sovrin Foundation put efforts to look into the compliance of this regulation, of the DLT and SSI in particular. Experts seek for clearance on how SSI-related terms, such as DID, can be made GDPR-compliant (Sovrin Foundation, 2020). Following that further, other researchers also noticed that the legal and technical ground for the DID revocation needs to be foreseen in the SSI model (Kondova & Erbguth, 2020). Also, a clearance on who is considered a data controller and what data is regarded as personal data is needed (Kondova & Erbguth, 2020). Overall, a concrete system with specific use-cases is needed to speculate about the alignments with this regulation.

3.7 Summary and conceptual framework

This chapter presented the overview of academic works regarding self-sovereign identity, its expected opportunities and challenges associated with its implementation. SSI has acquired the same development path as blockchain: experiments take place and curious practitioners expand its capacity of restoring the control of identity to the user.

Present-day self-sovereign identity undeniably matures, attracting more experts and scholars to investigate it. What is known in concrete is that self-sovereign identity promises the revolutionary shift in identity management, no matter with or without blockchain at the backbone. It implies granting the user control over the data flows regarding their identity, hence eliminating the need for the third parties to be involved. With the attempt to map the possible opportunities and challenging of SSI implementation in the public sector, the author will use the conceptual framework.

This framework was developed by Ølnes & Jansen (2018) for analysing the blockchain opportunities, barriers and driving forces in the public sector, mentioning that digital identity is among the most suitable domains to benefit from blockchain within the governmental operations. The framework was validated in the Norwegian public sector context, and it can be hence considered suitable for this study. However, because the SSI is not necessarily the sub-domain of blockchain innovation, the framework was further adjusted, given the input from the literature. Hence, the proposed framework is illustrated in figure 11.

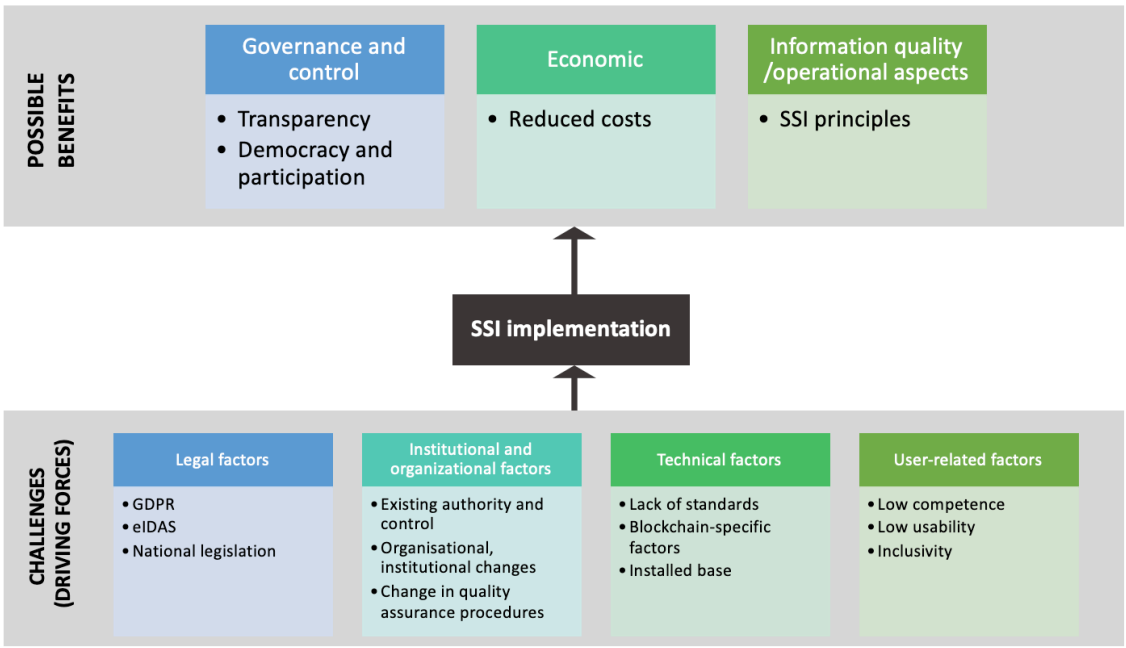

Figure 9. Conceptual framework, inspired by Ølnes & Jansen (2018)

This framework will guide this study on exploring the two pillars of the studies problem: opportunities and challenges for self-sovereign identity. It originally consisted of two dimensions: potential benefits and challenges (or driving forces), which both determine the adoption of the new technology in the public sector.

The academic discussion on the benefits of SSI, specifically in the public sector, is not exhaustive. Although there is an assessment form for denoting SSI benefits, namely the

rigorous scorecard suggested by Preukschat & Reed (2019), it still gives a rather broad overview for those benefits. After aggregating the data from different sources in combination with the original framework, the framework's components remained as follows. The "governance and control" elements within the benefits domain originally contained the "reduced corruption" item. However, it is less relevant for the identity case, given that the identity impersonation and identity theft are resolved via the "transparency" feature. The expected cost savings from using self-sovereign identity were mentioned in the literature, and in the scoreboard, as mentioned above in particular. In this dimension, Ølnes & Jansen (2018) argue that although its benefits can affect many stakeholders, its deployment is still on the central power's shoulders. Whether or not it can be a limitation will be revealed in the upcoming sections. Finally, the original factor of "information quality and operational aspects" was mentioning the principles of data integrity, security, privacy, reliability, persistency and immutability (Ølnes & Jansen, 2018). In such a way, those features were intersecting with the ones from the scoreboard's "regulatory compliance" column of Preukschat & Reed (2019) scoreboard.

Overall, this list was adjusted, as in the case of the studied topic, those features are better represented by the principles of SSI. Based on the papers provided above, the conclusion can be made that the precise and exhaustive list of SSI principles is still to be defined. Scholars vary in their opinions, ranging from 5 to 14 essential principles of SSI, also arguing that other principles are only relevant to the identity system, not to the identity itself, as per Ferdous et al. (2019). The following table presents the comparative summary of SSI principles with the papers, where they were mentioned:

SSI PRINCIPLE	PROPOSED BY
Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimisation (Disclosure), Protection	Allen (2016)
Provability	Stokkink & Pouwelse (2018)
Usability, Counterfeit prevention, Assurance, Verification, Secure transfer, Secure transactions	Toth & Anderson-Priddy (2019)
Autonomy, Single source, Ownership, Choosability, Cost, Standard	Ferdous et al. (2019)

Table 4. SSI principles summarised

Although this paper is not able to rank, merge, split or eliminate these principles for the further normalisation, within the public sector context the author proposes considering

the principles suggested by Allen (2016), with the new principles of "usability" and "cost" for the further usage in this thesis. Usability implies that the SSI solution is easy to use so that the users do not struggle with coping with secure yet difficult-to-understand technology. The cost criteria, in turn, is relevant for the government context as the identity provision cannot be based on the fees. The remaining principles are important as well, yet they describe SSI in the level of technical and conceptual detail that goes beyond the scope of this thesis. Overall, despite the surrounding discussion on being incomplete or misguiding, these principles can provide a holistic overview of the fundamental identity paradigm shift that SSI intents to bring within the public sector context.

Now, the driving forces, or the barriers, dimension illustrates the possible hampers to slow down the SSI implementation. Legal barriers in the original framework were mentioning the national legislation. In the context of SSI, it is vital to indicate the pan-European regulations, such as GDPR and eIDAS, as the literature suggests. Institutional and organisational factors are derived from the fact that every innovation will bring change to the current organisation within the public sector. The possible disruption within the authority is considered as another possible challenge here. In terms of technical factors, those from the original frameworks were grouped under the blockchain-specific sub-group as the dependency of SSI from the blockchain technology is debatable and not all the features of SSI are exclusively the features of blockchain. Another important factor is missing standards and governance frameworks of SSI, which can be both a driver for innovation and a hurdle in adoption, according to the framework's authors. Finally, the installed base refers to the existing infrastructure and solutions in place, which again, according to Ølnes & Jansen (2018), can both a barrier and the facilitator.

Lastly, this framework was adjusted by adding the "user" component in the barriers (or driving forces) dimension because they are crucial adopters of the technology, and the studies argued that the SSI complexity could hamper its implementation and broad adoption. Because this framework is not SSI-specific, for the Belgian context the study will do both validating the existing factors but also uncovering the new, yet unpredictable ones, and hence, revising this framework at the end of this study.

The selected conceptual framework will guide the process of mapping the possible benefits and challenges of SSI. This study will also help mapping additional factors or benefits, which are not included in the framework, hence making it more specific for the context of the studies environment: Belgian public sector.

4 RESEARCH DESIGN

This chapter presents the research design deployed in this study. The structure of this chapter was suggested by Saunders, Lewis, & Thornhill (2009), and will guide the author throughout all stages of this research. This "research onion" approach consists of six steps, and it is illustrated in the figure below.

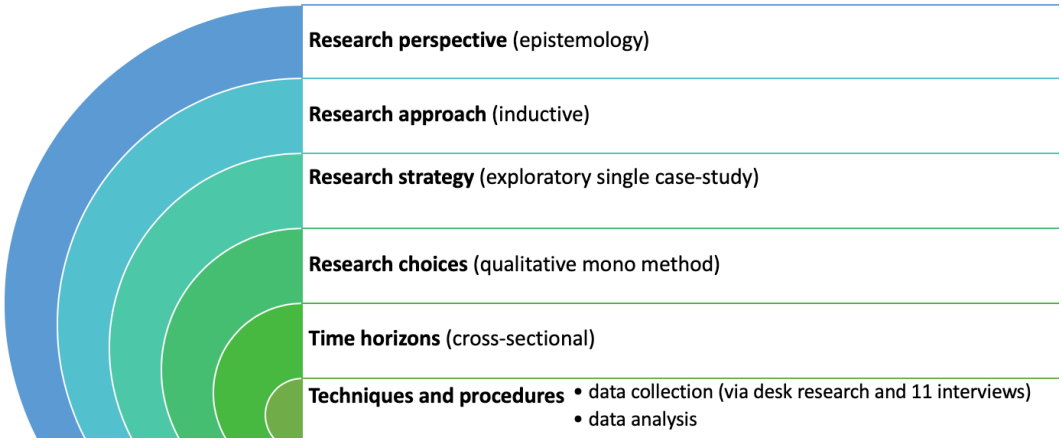

Figure 10. Methodological approach, based on Saunders et al. (2009)

Regardless of the research design, as Walliman (2017) argues, there are questions to be answered by each author of a good research paper. Those are "what", "why", "how" and "when" is the research conducted. The following figure presents the stages taken for achieving the objectives of this study:

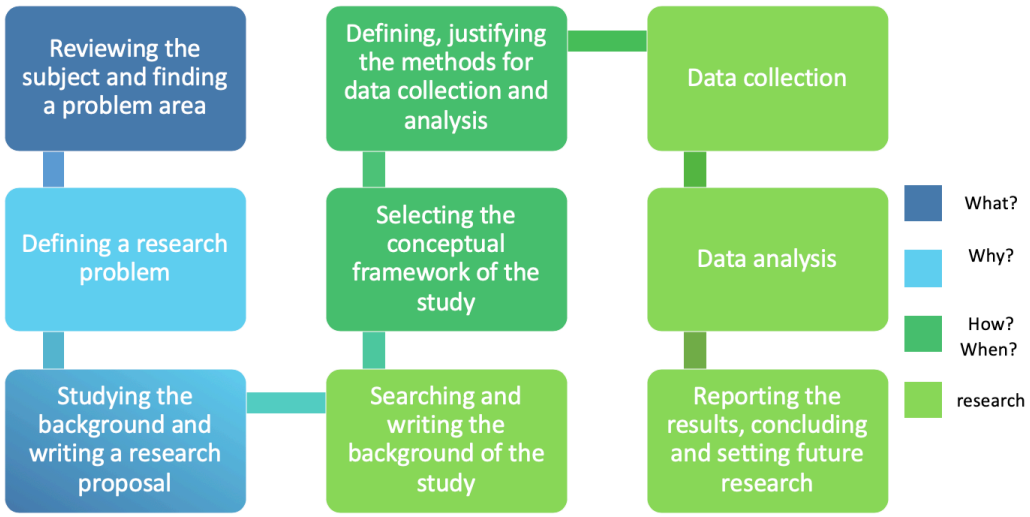

Figure 11. Research process, suggested by Walliman (2017)

4.1 Research perspective

The research perspective sets the scene for the whole research by defining assumptions and beliefs used for conducting research (Saunders et al., 2009). These researchers suggest that a credible, consistent research philosophy sets the ground for choosing the following parts of the research design and ensure coherence between them. Commonly, scholars separate three main types of philosophy: ontology, epistemology and axiology. Epistemological approach concerns the process of knowing things and understanding what is the acceptable knowledge within the research discipline (Walliman, 2017). Because the goal of this study is to develop a piece of new knowledge, the epistemology was chosen as its philosophical stance. Furthermore, the interpretivism was perspective taken because, in an interpretive study, the researchers position themselves as social actors within the research process and derive new knowledge from this positioning (Saunders et al., 2009).

4.2 Research approach

The research approached indicates the relations of the theory and the research: whether a theory is guiding research or is an outcome of it (Neuman, 2011). There are two conventional approaches: deductive and inductive: the former uses the existing theory to test the proposed hypothesis in the study, while the latter develops a new theory (Bryman, 2012).

This study aims to derive conclusions about the possible opportunities and challenges of implementing the SSI in the Belgian public sector. In other words, it aims at suggesting a new knowledge, a theory to be further used, based on the conducted analysis of the obtained data. Hence, the approach chosen for this study is inductive because, as Bryman (2012) indicates, it allows deriving generalisable conclusion from the observations. Also, an interpretive study is typically inductive (Saunders et al., 2009). It worth mentioning that using the conceptual framework poses the risk of limiting the inductive approach by becoming driven by it and becoming, hence, deductive (Baxter & Jack, 2008). To prevent that, this research will use the selected conceptual framework only to guide the direction of this study. Consequently, the final themes and phenomena will be derived based on the empirical part.

4.3 Research strategy

This section elaborates on the means chosen for conducting this research to uncover the studies problem. A case study is the research method that allows an in-depth investigation of a contemporary phenomenon within a real-world context (Yin, 2018).

Several types of case-studies are commonly discerned: explanatory, exploratory, descriptive, intrinsic, instrumental and collective (Baxter & Jack, 2008). The nature of this study falls under the exploratory type as, according to Yin (2003), it seeks to delve into the situations where the "intervention being evaluated has no clear, single set of outcomes" (as cited in Baxter & Jack, 2008, p. 548). This thesis aims to uncover unknown opportunities and challenges of SSI in the Belgian public sector. This premise is also supported by Yin's argument that researchers investigate the phenomenon via exploratory case studies when there is a lack of theoretical ground about a particular subject. Hence, new knowledge is developed (Yin, 2018).

Choosing the case-study method also lies in the availability of data (Yin, 2018), as author's internship at IAA of BOSA provided the opportunity to reach out to people directly involved into the identity management of this country. Yin (2018) also accentuates the importance of clearly defining the scope of the case. In this study, the opportunities and challenges for self-sovereign identity were studies from the public administrative perspective, leaving financial and technical details out of its scope.

4.4 Research choices

This section elaborates on what type of methodology is used in this study. Saunders et al. (2009) indicate that three ways of using qualitative or quantitative approaches exist for data collection and data analysis: mono, mixed and multi-methods. A qualitative approach is used when non-numeric types of data are considered, as well as the interpretive research philosophy is chosen (Bryman, 2012). Correctly applied qualitative research techniques can help develop new theory, evaluate programmes and developed interventions (Baxter & Jack, 2008). Given that this thesis main aim is to create a piece of new knowledge, non-numerical data being collected and analysed, a qualitative mono-methods is used in this research.

4.5 Time horizons

Time horizon defines a time at which research is conducted. Commonly, there are two types of time dimension for studies: cross-sectional studies and longitudinal studies (Babbie, 2010). Given the exploratory nature of this research, the present time constraint for data collection and conducting this master thesis research, cross-section research is selected. This type implies that a study sample is observed at one point in time, unlike the longitudinal study, where several snapshots are taken at several points of time (Babbie, 2010). Hence, a broader picture of a studied subject is created (Levin, 2006), which satisfied the initial research question.

4.6 Techniques and procedures

Data collection

To conduct this research, various sources of data collection were used: desk research and interviews. According to Yin (2018), using several different sources of information is beneficial to the case-study research strategy, resulting in higher quality research. Baxter & Jack (2008) believe that by using several sources prevents studying the issue for a single lens and allow uncovering many facts of the phenomenon and gather more insights into the case. Desk research is a secondary data collection method, and it was used to create the background of the study before commencing with the empirical parts (Walliman, 2017). While there are several advantages of this method, such as the overview of the existing body of knowledge on a particular topic, up-to-date information and facts, it still implies having a biased selection of the sources, as well as the difficulties in getting open access to some of them.

Interviews technique is used because it allows collecting in-depth information regarding participants points of view and experiences (D. W. Turner, 2010). This author also suggested that data obtained via interviews should be combined with other forms of data collection.

Desk research

In this research, the desk research was focused on obtaining data from various publicly available sources, such as, first and foremost, academic research, as well as online publications, collaboration platforms such as meetups and GitHub, dated from 1948 (the UNCHR) to 2020. Searching the academic sources was conducted via the Google Scholar, Web of Science and the Limo search engines, considering the following keywords: “self-sovereign identity”, “blockchain identity”, “decentralised identity”. Given that the concept emerged recently, the range of years that papers were published varied from 2015 to 2020. The retrieved studies include research articles, conference proceedings and dissertation studies conducted by other scholars in this domain. Also, for the case-study description, official government websites and the EU documents were used to receive the latest information about Belgium and its digital development. A total of 147 sources were used in the paper.

Interviews

The participants were selected based on their expertise in the field of identity management and self-sovereign identity but also their relevance for answering the research question. Within the studied topic, research suggests that understanding the benefits (in this case, of blockchain technology) is possible when both organisational and technological

viewpoints are considered (Ølnes et al., 2017). For that reason, this study aimed to interview experts from both organisational and technical fields to map both points. With the cooperation of IAA, the list of potential stakeholders was created. This list included the experts working in the area of identity management, self-sovereign identity, research and technology, both from private and public sectors. In the end, based on the availability of the experts, 11 positive answers were received, and the interviews were scheduled. The summary of interview partners can be found in appendix A.

This study employed two types of interviews, and a total of 11 interviews were conducted: two informal conversational and in nine semi-structured interviews. Informal conversational interviews are unstructured interviews conducted without a fixed list of questions, allowing the interview participant to guide the discussion, hence providing more flexibility (D. W. Turner, 2010). In this study, the unstructured interviews were conducted to establish the context and get a broader picture of the blockchain and innovation landscape of the Belgium public sector. Also, another interview managed to acquire more details on the "Blockchain on the move" project in another case. Semi-structured interviews are used when more structure than a previous type is needed, yet leaving room for flexibility (D. W. Turner, 2010). This type of interviews contains both structured and unstructured sections and open format of questions (Walliman, 2017).

Given that the studied topic is multidisciplinary, it is necessary to follow the respondent's flow and for that, the additional questions were posed as the interviews went. The interview guide was developed to serve a baseline during the interview. One of the most important parts of the interview method is forming the interview questions (D. W. Turner, 2010). For this study, questions were developed following the idea that each question should provide an extensive view of participants knowledge and experience so that as much data is collected possible (D. W. Turner, 2010). According to McManara (2009), the excellent interview consists of the open-ended, neutral, discrete and clear questions (as cited in D. W. Turner, 2010). Creswell (2007) also suggest that to avoid the respondents answering the questions partially or answering the wrong question, the guide should be developed in such a way that a participant keeps focused on the topic discussed (as cited in D. W. Turner, 2010). This author also believed that if needed, the follow-up questions must be asked in order to ensure the full answer is provided (as cited in D. W. Turner, 2010).

Depending on each interviewee's expertise and experience, the topics covered in the interviews were: the experience with SSI, their opinion on the expected opportunities and challenges of SSI in the context of the public sector, suggested by the conceptual framework. Nevertheless, the final list of questions was a tailor for each interview partner.

After the interviews, the email follow-up was used for clarifications and additional questions. The interview guide can be found in appendix B.

The interviews took place between the 1st of March and the 13th of May. Due to the COVID-19 outbreak, 9 out of 11 interviews took place online using Skype for Business, Microsoft Teams and Zoom platforms, while one informal face-to-face interview took place in the premise of BOSA. The interview lasted from 25 to 65 minutes.

Data analysis

In case studies, data collection and data analysis go hand in hand (Baxter & Jack, 2008). A thematic analysis of interviews was conducted following the approach, suggested by Braun & Clarke (2006). Its main steps are depicted in the following figure:

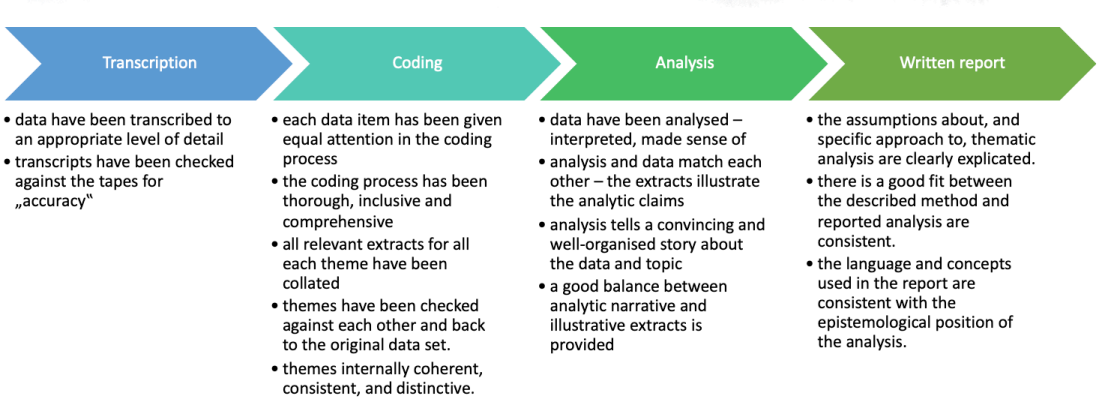

Figure 12. Thematic analysis phases by Braun and Clarke (2006)

The coding part was done via NVivo software, and a summary of the codes table can be found appendix D. Given that the interview questions were developed using the framework suggested by Ølnes & Jansen (2018), the codes were expected to get aligned with the proposed factors impacting SSI development. Nevertheless, since there is no particular framework describing SSI in particular, new themes were also identified and proposed for the revised framework. Based on the coded data, the themes were analysed and compared with the literature review.

4.7 Ethical consideration

Ethical issues need to be considered in various parts of the research (Bryman, 2012). Human interaction lied based on the data collection process, and hence, the checklist suggested by Bryman (2012) was followed.

Most importantly, before starting the interview, participants were introduced its objectives, the topics to be touched upon during the conversation, given the expected

duration. Interview participants were also asked to give consent to record the conversation, and only the relevant information was used for the data analysis part.

4.8 Summary for chapter 4

This chapter presented the methodological approach taken by this study. Seeking the propose the assessment framework for the emerging field, it takes the epistemological position for constructing the new knowledge. Using the explorative case-study approach, the authors aims at gaining more in-depth data about the case (Belgian identity management) and the studies problem (self-sovereign identity), as the available research on SSI in public sector is limited. By means of desk research and interviews, the author will gather the data for the analysis and developing the new theory on how SSI can contribute to the identity management and what challenges can be associated on its way. The limitations of the methodology and of the overall study are presented in the end of the paper under the “Conclusion” chapter.

5 THE CASE

5.1 General information

The Kingdom of Belgium is a country in Western Europe with a population of around 11,4 million people (Statbel, 2019) and the area of 30,528 km^2 (Belgium.be, n.d.-b). Its capital city Brussels is also considered the capital of Europe as it accommodates various institutions of the European Union and NATO. Belgium can be described as an economically developed state, with the gross domestic product per capita being 53.6 thousand US dollars (OECD, 2020).

The three administrative regions of Belgium are Flanders, a Flemish-speaking part, Wallonia, mostly a French-speaking part with a German minority and the bilingual Brussels Capital Region, holding its own administrative unit. The regions are further divided into the communes and municipalities (Belgium.be, n.d.-b). Alongside the regions, Belgium also has three language and culture communities, for Dutch, French and German languages respectively. Both regions and communities hold their responsibilities for various aspects of life, having their own legislative and executive powers (Belgium.be, n.d.-a).

On the federal level, the power is distributed among the King, Federal Parliament, Governments and the formerly-known ministries (Belgium.be, n.d.-d). As a result of the so-called "Copernic" reforms in the 2000s, Belgian executive powers were reorganised, making the "ministries" an obsolete term (Belgium.be, n.d.-c). Having the aim of providing the services to the citizens, the "Federal Public Services" (FPS) and "Federal Public Planning Services" were established.

5.1.1 Digital development

Generally, the Belgian digital strategy is presented in the actions plan named "Digital Belgium". This plan aims at achieving the digital transformation in the country, based on five pillars: infrastructure, confidence and security, government, economy, skills and jobs (Digital Belgium, 2017).

Interestingly, Belgium ranks 6th across the EU in terms of Internet connectivity (DESI, 2019). According to the OECD, 89.7% of household in the country has an internet connection (OECD, 2020), placing it just in the middle among the European Union member states. Nevertheless, the mobile broadband subscription rate in Belgium is rather low (78.3 subscriptions per 100 inhabitants), which makes it third to last in the European Union (OECD, 2020).

Following that further, the overall e-government development in Belgium was described as “expandable”, in the context of the EU benchmark report for 2019 (European Commission, 2019b). The report indicates that Belgium underperforms in terms of adopting e-government services online. Several numbers can illustrate the situation by using public services online, according to the Digital Government Factsheet 2019, 59% of Belgian citizens use online means of interaction with the government (European Commission, 2019a). In Belgium, smartphones have overcome desktop computers regarding internet usage. According to the statistics, 84% of the Belgian population has a smartphone, and its utilisation in various spheres of life grows annually (Deloitte, 2018).

Additionally, Belgium, along with other European countries, has pledged to contribute to creating a European Blockchain Service Infrastructure, having their first EBSI-node launched on the 12th of February 2020 (Belnet, 2020). It was the first step in creating the pan-European decentralised network for creating better public services, the cross-border interactions in particular (Belnet, 2020).

5.2 Identity management in Belgium

5.2.1 Legal framework

Since the 1980s, the National Registry of Belgium was regulated by the law 1983-08-08/36 “On regulating a National Register of natural persons” (FPS Justice, 1983). In this document, the National Registry is defined as an information system responsible for recording, storing and communication the natural person’s identification information (FPS Justice, 1983).

With the shift towards electronic services, the first document to legally enact Belgian eID card was the law 2003-03-25/31, which is the Royal decree “On transition measures on electronic identity cards”, giving the birth to one of Europe’s first electronic identity card schemes. Its full kick-off was in 2004 when the pilot was officially started in all levels of administration under the Royal Decree 2004-09-01/33 (FPS Justice, 2004).

The Royal Decree 2017-10-22/11 defines the conditions and produces for the Federal government to recognise external identification means for online public applications (FPS Justice, 2017). This law allowed private mobile solutions to be recognised by the governments as authentication methods and be available at Federal Authentication Service (FAS). Also, this decree indicates that the DG DT holds the authority to revoke these providers to be the recognised authentication method and exclude them from FAS and eIDAS notification (FPS Justice, 2017).

5.2.2 Authentic sources

Moreover, within the authorisation domain, the notion of the "authentic source" is commonly used (Dumortier & Robben, 2010). The authentic source is the reference database containing the authentic data of the citizens with a high level of quality and security (DG Digital Transformation, n.d.-a). Using the authentic source from various bodies removes the need for the duplication of data, making it hence compliant with the "once-only" principle. All authorities can then use different institutions with the relevant permissions (DG Digital Transformation, n.d.-a). These authentic sources also serve a backbone for the verification of various information provided by citizens. Overall, several groups of these authentic sources can be set out, based on their origin: Federal government, Social Security and the authentic sources from all three administrative regions (DG Digital Transformation, n.d.-a). For instance, the National Registry is the Federal government's authentic source and is managed by the FPS Home Affairs (FPS Home Affairs, 2017).

At the core of the Belgian ID scheme is the Belgian national number (FPS Justice, 1983). All Belgian citizens and residents are uniquely identified by a national number, which is written on the card and is stored on the chip as well (European Commission, 2019a). The Belgian Privacy Commission supported using the only identifier throughout the country, thus eliminating the usage of social security or a taxpayer number (Dumortier & Robben, 2010), which would create information siloes and higher complexity. Ensuring the availability of the data for all the state bodies is the responsibility of the state service integrator. DG DT organised the access to various authentic sources via the Federal Service Bus so that the data is retrieved and transmitted in a fast and secure fashion (DG Digital Transformation, n.d.-b)

5.2.3 Belgian ID card

The main form of identification in Belgium is via the National electronic identity card (eID), which is issued to every citizen of Belgium via the local municipalities (FPS Home Affairs, 2017). Foreign residents are entitled to use the electronic residence permit cards, and the children from age 12 are given the Kids-ID (European Commission, 2019a). In the contrast of a global identity documents crisis, an impressive total of 28 million eID cards has been issued as for 2020 (Thales, 2020). With these cards, citizens can enjoy accessing many online services (FPS Home Affairs, 2017). This smart card contains two certificates, which can be used for authentication and generating digital signatures (European Commission, 2019a). In order to use the card, one must have a card reader and the special software.

Belgian eID scheme passed the peer-review and is now compliant with the highest level of assurance under eIDAS regulation (European Commission, 2019a). The card has also passed the ISO-7816 certification, as DG DT at BOSA reports (BOSA, 2017). Moreover, starting from 2019, the card security for enhanced by adding the fingerprint information on the card (Thales, 2020).

The advantages of this card, as discussed by Dumortier & Robben (2010), are the advanced security via the two-factor authentication, as both the document and the knowledge of a PIN-code are needed. These authors also suggest that several "factual and legal factors" reduce the risk of abuse should the card be lost or stolen. In this event, a card is immediately blocked via a 24/7 available resource DocStop (FPS Home Affairs, 2017).

5.2.4 Online identification

CSAM is a Belgian framework for providing identity and access management within e-government, used both by citizens and private companies for identification, authentication, authorisation and for the mandate management (CSAM, n.d.). Initially, CSAM was created as a result of several governmental bodies, including the FPS Home Affairs and DG DT of BOSA and now is supported by a growing number of online public services (CSAM, n.d.)

This platform offers a unified interface for all public services via a single sign-on option, allowing the citizens only to log in once if they wish to access multiple services. When a citizen desires to log in to the governmental service, they get redirected to the CSAM's FAS (CSAM, n.d.). At FAS, the users are requested to provide the credentials and are further redirected back to the online service.

Presently, not only the ID card but also several other identification options are offered to Belgian citizens, such as itsme, a one-time issued password with the combination of either a certificate, citizen's token, and application or an SMS (IAA, 2019). Foreign residents can also access the services via the eIDAS node if their countries have provided their information. According to the IAA, around 2000 applications are available for online usage, with the majority coming from the local level at 70%, followed by the federal level applications at 14% and the regional level applications at 10% (IAA, 2019). The information on the frequency of each identification method, provided by the IAA (2019), is illustrated in the figure below:

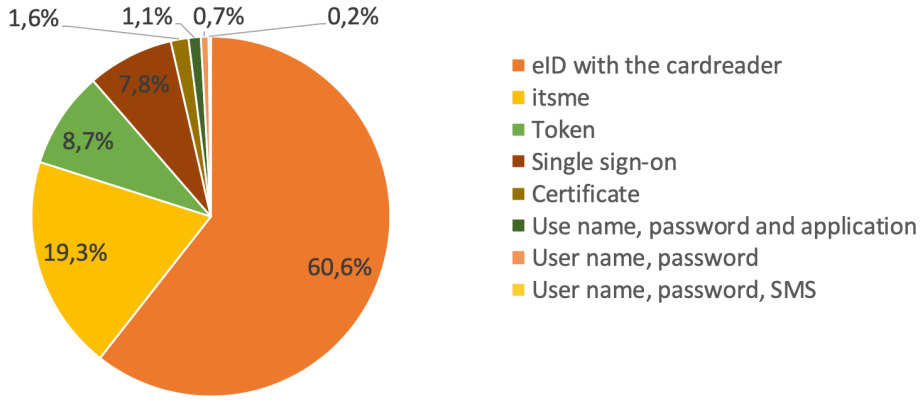

Figure 13. Authentication of Belgian public services in 2019, per key type

However, the authentication to the services is not done via CSAM, and this process is handled by the specialised eID middleware, which is available in open source on the DG DT's GitHub repository (BOSA, 2017).

Itsme

Itsme is the mobile application used for federated identity management. Launching this solution was the initiative by the Belgian Mobile ID consortium, which consist of Belgian banks and cellular connection providers (itsme®, n.d.). It was created in the cooperation with Gemalto company and can be used for single sign-on, log-in and signature process (Gemalto, 2019). One of the drivers for creating the application is the burden of remembering many passwords, risk of cyber-attacks and little control over personal data in the traditional ID schemes (Gemalto, 2019).

Using itsme is possible via the activation made with any of the supporting banks or using the eID and the card reader. After three years of utilisation, itsme offers to log in in numerous platforms, including public and private sector ones to over 1.8 million customers in Belgium (itsme®, n.d.). According to the chart from the previous section, this application's share in online authentication was almost 20% in 2019. Following to the Thales Group recent report, an average itsme customer has used the application six times for commercial and three times for the public sector interactions (Thales, 2020).

The application claims to be a secure, portable and omnipresent mean of identification. As such, it has been officially recognised as the trusted authentication provider by the Royal Decree of 22.10.2017 (FPS Justice, 2017). In December 2019, itsme was also notified by the European Commission, making it compliant with the eIDAS regulation and allowing it to be used in other member states (itsme®, 2020).

6 RESULTS

This chapter presents the main findings from the empirical part, obtain via thematic analysis. The chapter follows the identifies theses and uncovers experts' views on the issues of the identity management in Belgium and the SSI possibilities.

6.1 Belgium status quo

Belgian public administration is not typical and is known for its complexity. Belgium is also known for being dynamic in terms of politics and administrative organisation, as expert J elaborates, "things get migrated from a federal to a local level".

Belgian public administration treats security at a very high level, thus having a lot of data sources at government possession does not allow doing otherwise. Expert J confirms from his experience: "*I have not seen a very loose attitude towards privacy and GDPR, quite the contrary*". Belgium also implemented the once-only principle to prevents citizens from providing the same information to the public administrations twice. However, it also means that although the citizen does not have to provide his or her information twice, the interconnections between different registries still stays behind the scenes.

6.1.1 Attitude towards technology

Stepping away from the centralisation is a burdensome process, which in many ways, referring to the views of expert G, "*is a lot about the cultural aspect of the country*". Expert C describes the overall public administration in Belgium as a conservative: "*it is true that the political culture in Belgium is very conservative. Belgian people are conservative*".

This conservativism, on the one hand, comes out of the significant responsibility lying on the government's shoulders. Unlike major private companies, it cannot spend money on researching every single innovation. Expert H gives a precise clarification: "*it's taxpayers' money, and you cannot just do whatever you want, you have to be responsible with a few resources you have*". However, he also believes that researching and investing in the long-term innovations can be promising, but still "*you have to make choices and cannot embrace everything innovation that comes*". In this sense, expert J says that governmental projects are rolled out to a considerable number of users, and there "*there is little to no room to make mistakes*", so this is where the cautious attitude comes from.

However, as expert H explains, that this attitude depends on different bodies because the government is quite diverse, and those bodies hold certain autonomy level: "*you have governmental institutions which are very innovation-driven and other who are more*

reluctant". Expert D provides an example that, for instance, "*in Flanders, there is more discussion on using more technology*".

Overall, among those different bodies, there are efforts put towards investigating the new technology. However, their capacity for doing that is limited. Regarding the digital transformation, experts reveal their frustration that there is no entity coordinating and working directly in this field, as DG DT is only a small division at BOSA, and it has the limited power. Expert A elaborates that even though DG DT is "a*n e-gov, innovation-minded, our budgets say that we are very much of a legacy organisation*". Running some initiatives within the DG DT is via the innovation labs, which are the sandboxes for new technology and innovations, is surrounded by several challenges as well. Organising innovation labs is a cumbersome process due to the bureaucratic limitations to attract more funds, and with small budgets, a rather small number of projects things can be conducted. A partial explanation could be that there is a special unit at Smals, that works specifically on researching these things for the government, for various public bodies.

One of the reasons for a moderate activity within the innovation domain could be that Belgium finds itself in "*not in the green field, we are in the brownfield"*, according to expert F. The brownfield means that there are already many solutions available. Seeing innovation can also be done via the lens of added complexity. Expert H provides an example: "*it happens that there are enthusiastic employees who propose something with smart contracts, but why would you do it and complicate things?".* Especially when it comes to immature technologies with not many successful use-cases, the legacy technologies that already work smoothly win the battle. Expert J explains that "*we cannot afford to be in a try out stage*". He also believes that some technologies just appear on the way of hype and will not necessarily be seen with the same value in five or ten years. As such, information technology should not be treated as the goal but rather a mean to achieve those goals.

On the other hand, as expert J admits, that "*people in government are not reluctant to new solutions*". The problem is instead with making sure that the new concepts are evident to every non-specialist stakeholder: "*we lack enough of people to translate concepts that are understandable, business-driven use-cases*". Additionally, another challenge lies in not being able to consider all the adverse effects of the new solutions if it comes with uncertainties surrounding their implementation. It can be well illustrated with the following quote: "*I've never had somebody to say no, it's a bad idea. Ever. But it takes time to explain and to make sure that they understand what you explain"*, according to expert J.

Overall, expert H provides an excellent summary that innovating is always hard: "*there is always resistance towards new things, that's not always a bad thing. I mean, sometimes it is. If you just accept everything new without questioning it too much, you risk building something which is very unstable*".

Blockchain

Particular attention can be drawn to the blockchain as it plays an important role within the SSI domain. Overall, expert D believes that "*Belgium was indeed a late player in that new technology and they rapidly withdrew from it*". As such, there was a lesser interest from the government side to the decentralised technologies, compared to other countries. Expert J pointed out that it is difficult to "*see a direct need to change our business model in a decentralized one*". In turn, expert H elaborates that blockchain and DLT is only one way of addressing the centralised approach in the multitude of other technological tools.

The incipience of blockchain in Belgium started along with the rising hype around it. Expert A explains that the initiatives started in 2016, where several round tables with multiple stakeholders were held to look at "*how can it support the life events*" because much paperwork was present in Belgium public services. The Smals was involved in the research on the possible benefits and opportunities of blockchain for the public sector. There were visible questions or even sort of a "*the pressure towards the government institutions to investigate if anything could be done about it*", according to expert F.

The follow up resulted in the development of going in two tracks: the technical and content. In the former, there were difficulties caused by low maturity of technology, particularly in ensuring the interoperability of blockchain systems with other ones. Although there were many experiments, both on the federal and regional levels, regarding the content the conclusion was that blockchain would not add much added value in supporting those life events, "*it didn't help to move further*", according to expert A. Therefore, the government's position was that "*blockchain is an interesting technology, but we do not see a use case for the federal level*", expert A explains.

Consequently, it wasn't possible to go on before working solutions with the real added value can emerge, "*the initiatives on blockchain were postponed*", according to expert D. Mainly because there was a little interest in the governmental side in all the decentralised technologies, "*certainly if you compare it to other countries like Germany, Netherlands, we have a limited field on that*", as expert D explains. Additionally, the dominant technology research centre, Smals, did not receive funding to "*to do things specifically with blockchain*", as expert H explains.

Similar to what experts shared in the previous section, "*you might stumble upon processes where Blockchain could be the ideal solution, but you cannot start from technology*", as expert A argues. In the case of Belgium, the initiatives were mainly technology-driven, following the globally rising interest towards it, while it would be of more use "*to start from the business needs, see what exists, and what is the best technology for our needs*", as expert H mentioned. It was challenging to find projects where the added value brought by blockchain is sufficient to convince people to implement it. Instead, it should be used "*for things, for the need that exists but for which there is not yet a solution*", according to expert H. One of these possible use cases should not be cumbersome but rather start with simple projects, "*like just registering stuff in the immutable way and distributed way".*

6.1.2 SSI experience

Indeed, Smals works on researching on the possible innovations: "*We are looking at what exists, we are scanning for new innovation and see if we can apply it in a useful way in our context*", as expert H shares, mainly with is a focus towards social security and e-health domains. On the other hand, it is also worth seeing what government's experiences with SSI are, either directly or indirectly.

One of those use-cases from the beginning of 2019, which was very relevant, was the project to validate the identity of foreigners who want to access the online federal services and have to do it in person nowadays. As expert A explains, there was the concept of an identity management platform, with several parties: a citizen, who has and manages his or her identity attributes and can prove their identity by offering his attributes. She adds that "*in the middle somewhere there is a thing we call the trust anchors*", in expert's A opinion. These trust anchors could be any party, starting from a bank or one's employer and ending with Facebook, for example. As such, the public bodies would accept the attributes of those pre-defined trust anchors, which would help thousands of people yearly, expert A believes. The conclusion made was that blockchain could be used for it, but it was not necessary as a result could be achieved by the existing building blocks, according to expert A.

Another initiative that features several SSI principles was initiated by IAA department and is called "My Profile". This project has an idea of introducing the "Consent-as-a-Service" and allowing the citizens to see what data the government has on them. In such a way, users would give their active consent to use their data, except for the cases where it is required by law, according to expert B. Because the state authentic sources guarantee some identity attributes, it is presumed that in "My Profile" the citizens will be able to extend those by adding their "self-sovereign" attributes, as per expert C.

Most interestingly, “Blockchain on the move” project is the one that has explicitly stated the goal of achieving SSI. Although the original goal was using blockchain for improving the relocation use-case within the city, the project team realized that “*it was bigger than just the trust layer*”, according to expert D. The first phase of the project the just aimed at developing a PoC to see how things can work, as expert G explains. Later, the project team encountered issues of governance and stakeholder management, which lead the project toward focusing on “*a more functional analysis to see what kind of business opportunities there are*” and finding the cases with the proven added value, according to expert D. Following that, the project faced the power and capacity problem: “*we are not in power to make a wallet, to construct the entire ecosystem”*, as reported by expert D. Further, the scope of the project was reduced “*because of the technical side took too much time, and there is still a maturity problem*”, as expert A informs. As Jolocom was a technical partner of the project, they share that many aspects within the scope of the project were “*not within their legal domain of the city to be implemented*”, according to expert G. Also, expert D explains that the increased complexity was too much to handle for a small project as starting the initiatives with credentials issuance and sharing was way beyond that it could tackle.

The following stage of the project takes place at the moment. Ballisti-X company takes over analysing the “*business processes within the city*” and evaluating “*where the SSI might be a useful technology to improve these processes*”, according to expert L. As the project is still ongoing, the current conclusion is that “*there can be some advantages of using it within the city administration context, mainly in the processes where a lot of information is shared between services or is shared by the citizen*”, as expert L reports. The expert L also informs that in case of the “Blockchain on the move” project, the technology-driven approach was never taken. Instead, the analysis was conducted to reveal the best possible use-cases within the city of Antwerp.

6.1.3 Citizen’s experiences

Being the main stakeholders within the identity ecosystem, citizens should dictate the way these ecosystems operate. Their trust towards the government and technology determines whether or not individual solutions will be adopted and actively used. Belgian citizens, as experts suggest, consider the interactions with the government as the burden and tend to limit their usage to the ones necessary, “*they don’t want to interact with the government unless they have to*”, according to expert B. Although quantitatively the interactions show a high number and are growing annually, there is still a room for improvement, even compared to the neighbouring countries.

Also, the privacy issues are rising, especially with regards the trust to the government, as people tend to feel "watched" and trust to their government less. This paradox in the government-citizens relationship leads to the fact that citizens are prone to giving their data away to private companies like Google or Facebook, but are still sceptical about the government, for example, in the context of embedding the biometrical data on the eID, according to expert B.

There is also a need to explain the nature of a common confusion regarding what identity (or digital identity) is in the first place, what attributes can be considered parts of their identity and what responsibility is held by who. In this respect, expert E argues that "*people realise that they didn't have it because no one gave then name*". Consequently, it could have also been a momentum for the private initiative with a specific identity branding itsme to take off: "*people wanted to have an alternative to the eID card, so our users are quite happy that they can do it with itsme*", according to expert E. And given that it has been endorsed by the government and has passed several certifications, including the eIDAS, bring more trust to this solution, and hence, increases its usage.

6.2 Current ID

Presently, identity management is the responsibility of the FPS for Home Affairs. They "*also determine what is going to be the new functionalities and features on the new eID*", according to expert B.

6.2.1 Itsme

A critical player in the identity market of Belgium today is itsme, a private sector-initiated mobile solution, which has been recognised by the government. The itsme team admits that although there were governance frameworks from the government to specify the level of quality required, it was still enough room for flexibility in terms of what technology to use, as expert E points out. Enjoying a high market penetration with around 25% of identifications, itsme brings advantages of are "*convenience, security, privacy and interoperability*", according to expert E. It means that the application and user's identity are linked to user's phone and can be used across different institutions in both public and private sectors, according to expert F.

The team of "itsme" further explains that the elements of "self-sovereignty" are enacted via the active consent that users give for the transaction, explicitly showing which elements of their identity information are shared with what party. The application has been certified, and there is a clear scope of getting and managing identity information, as expert F suggests. Also, itsme has achieved the recognition of their brand of identity,

meaning that there is a party that users can approach, which created better trust towards the application too, as explained by expert E.

Although some parallels between the itsme and the visions of SSI can be drawn, expert D believes that itsme is "*a very centralised wallet, only limited to one component: the authentication of identity*". Another key difference is that in itsme, every transaction of a citizen can be monitored, even though the active consent for it is requested. Also, the fact that itsme is coming from the private world presumes that it has the earning model behind it, according to expert B. But most importantly, as expert believes, having such a user-friendly solution in a private company *"creates a big dependency for a government on one technology provider"*, as expert L suggests.

Among company's plans are considering the possibility for the user to have "*a wallet where you have your centralised identity and decentralised attributes*", according to expert E. The way it could work is described in the following manner: there could be various sources of attributes sitting in the databases of different entities (banks or healthcare facilities), and "*the DID ledger will point to those authentic sources, and the digital identity will provide the access and the consent management between the parties*", as expert F clarifies. Another option is to issue so-called disposable identities, which are only available to a requesting party for a certain amount of time, according to expert F. Overall, the itsme in many aspects of it features the SSI yet it is difficult to speculate whether it will become a proper SSI wallet.

6.2.2 Benefits of the current identity system

Belgian identity system can be discussed in much detail, given the complexity of the Belgian administrative division. What is important here though is that all the interview partners agree that the main advantage is the entire identity ecosystem with the robust infrastructure and the existence of stable authentic sources, as expert J thinks, especially in the light of identity crisis in the world. "*We have been consistent with the ID since 2003*", as expert B suggests.

Expert C also believes that the fact that there is an authentic source, which verifies and guarantees one's identity, the self-sovereign elements, such as email address or a phone number, can be easily linked to that. The high availability of smartcards, but also their security aspects are also considered as strong sides of the current identity management model in the country. All that infrastructure in place allows building better applications for citizens, expert J believes. Regarding the citizen's digital identity, it comprises a small subset of data, which is aggregated from several sources, including the National Registry and in principle replaces the information printed on the eID card.

6.2.3 Drawbacks of the current identity system

Nevertheless, the stable identity infrastructure does not insure from having various drawbacks. Having a robust system for many years brought the issue of maintaining a legacy system as now "*we have millions of lines of code. It becomes tough to maintain it, people who really know the system might not be around anymore*", as expert B informs. While the previous solutions, including the smartcards, were standardised and adopted by the government, the present-day technologies are mainly offered by companies, sometimes even sitting in other countries, and the auditing of such technology is challenging because their source code is private. And if the new solutions are to be rolled out to the whole population of Belgium, it has to satisfy the security requirements for everyone; however, the smartphone provision in Belgium varies substantially.

Along with that, perhaps the most poignant issue raised was privacy, as the citizens are getting more concerned that the government possess a lot of information of them and can control all their actions, as expert C observes. In some cases, for instance, with fighting against the crime, the government can and should use the data it has, but usually, people are afraid of that kind of surveillance. But in a sense, it can be explained that privacy and security tend to be confused and treated as one, as noted by expert E. While in practice, those are two different things.

It was also highlighted that citizens do not have control over their data. The solutions that the regional governments work on will only allow partial access for citizens to their data by only providing a static view on it, without having a possibility to re-use it, share it take ownership, as stated by expert D. Following that further, digital identity has many more aspects other than those stored in the central databases, as reported by expert K. It is not easy to link those with the person using the existing tools.

Also, despite being an apparent item, a static aspect of the eID card was mentioned as a drawback. In this sense, "*once you have it in your hands, you cannot change it*", as expert J explains. Adaptivity is one of the prerequisites for future identity systems, with the privacy and security respected.

Another factor mentioned is the usability, meaning that many citizens experience issues with using the eID card via card reader and using its software. "*People dislike using the eID if they don't have the infrastructure ready to use them*", expert J said. As such, the trade-off between the security and usability was mentioned because it is difficult to ensure both a secure but at the same time easy to use solution, and in the context of the government the former should prevail.

Regarding using the eID outside of the public sectors, issues also occur, "*if you want to interchange data between the private and public sector, that is also very difficult*", as explained by expert D. The itsme attempts to solve this problem by involving a lot of partners from the private worlds and allow citizens presenting who they are at those platforms. Nevertheless, other experts believe that the interaction between public and private sectors is beyond merely an authentication, "*it is about your identity components, and this is what SSI can really improve"*, as reported by expert D.

Belgium, as highlighted several times, has several administrative divisions, each of them is responsible for different aspects, including education, social welfare or healthcare. Due to a tough process of linking the existing authentic sources, exchanging data between the various administrative divisions is cumbersome as many protocols and levels of administration are needed to arrange that. "*When we need to communicate from the Flemish to the Walloon government, or from the Flemish to the federal government, it takes so much time*", expert K illustrates. Similarly, the cross-border services are performed, as the incoming students, for instance, receive a new temporary ID, which is different from their home ID card, and hence, their diploma is linked to that identifier, not their original one, according to expert D.

6.3 Future steps

Amidst many trends in identity management development, the role of the government is to choose the optimal path to move. DG DT needs a precise positioning regarding the future of identity, as expert A argues. The expert personally believes that it could be a role of "*service integrator"* and that it should "*have access to the authentic source*", so that other stakeholders could collaborate on validating citizens' identities. Indeed, as expert C mentioned, although the future of identity can be self-sovereign, there still must be parties to guarantee citizen's identity, and that the Belgian government foresees the ways of replacing or dematerialising the identity card.

Expert C personally believes: "*we must bring the identity to the citizen and not to the central member state because this is the problem that we have with EIDAS*". This attitude confirms what expert J said about the future perspectives: "*I think there we really have a lot of opportunities, as a federal government, to offer better solutions, […], we can do more tailored services*".

However, it is still too early to speculate about the concrete possibilities for the SSI or blockchain: "*you cannot say that we're throwing away the eID and we will change the technology, does it have an added value?"*, as expert A informs. A comprehensive analysis of possibilities in this direction is needed before any steps can be made.

Primarily, there is a vision of improving the user experience of governmental identification methods and increasing the overall awareness of citizens on how their data is treated. The government already has sufficient data on the citizens to work towards more personalised services, and the focus is on improving the overall experience, in the light of rising private initiatives and total citizens' expectations. As a possible way of achieving it, expert B foresees an active collaboration between private and public entities via an open-source FAS entering the private world. FAS was built a long time ago, and the new functionalities were built on top it, which increases the overall complexity and usability of the system.

Mobile-first

Many factors impact how identity management will develop. One of them is the mobile identity, and as expert J points out, "*the phone is the new hype that everyone wants to go*". He elaborates on that that the phone is the "*ideal interface to show these tailored messages for the person in question at his fingertips*", and that moving towards mobile means moving away from the physical eID card.

Expert C described the goals of one of IAA's initiatives, which consist of 4 to 5 phases and implies having the combination of the vault on one's mobile device and the central database. That expert also believes that this could be another step towards having an SSI in Belgium, or "*the base footprint by ID of a future sovereign identity*". Changing the identity card for a mobile solution or a vault with remote access in a secure way, "*complete it with a hardware token which only you possess, which is linked to your vault: in that case, you have an SSI*", according to expert C. Still, expert B explains that "*there is a lot of reluctance with digital identity on mobile devices because it can be hacked*".

The future of Belgium's mobile ID is seen as the enhanced government-citizen collaboration with very transparent consent mechanisms. Expert J elaborates on that: "*we're going to do the negotiation with the citizen on the phone, at the moment he says yeah, we go. Before that, nothing is ever leaked. We don't know a phone number; we don't know anything*".

Summarising these opportunities up, expert C thinks that the overall movement is towards SSI: "*some people don't even realize that what we're doing is self-sovereign identity*".

6.4 Opportunities for SSI in Belgium

No matter to what extent is the SSI set of rules finalised, it is already possible to discuss which benefits this identity paradigm can bring. In the abundance of data that citizens give to the tech companies, the government's mission is to protect the citizens and empower them to execute their rights for keeping their personal data secure. Looking at the intersection of academic debate, practitioners work and the findings from interviews with the Belgian context, the following sections contains the overview of the opportunities of implementing SSI in the public sector context.

6.4.1 Governance and control

Storing things in a centralised way poses a direct risk of the data breach from a single point of failure. Public administrations put "*citizens in danger by storing all the data in one central place*", according to expert I. Having the government possess all the citizen's data can be a subject of a big debate regarding its supremacy and its ultimate control over everyone's data. Expert D underscores that this is the most important in terms of SSI features: "*if you look at it from the perspective of a citizen, of course, gaining control of this data is the most essential feature*".

In Belgium, the government refuted the common fear of surveillance: "*as government, we're not involved into the location tracking*", according to expert J. The overall issue of state surveillance, especially in the digital world, is acute as was mentioned in the upper section, and this is where SSI seems to come into action because from a technological perspective, SSI prevents this surveillance from happening. In principle, a party can check the validity of the VC, to attest whether it was revoked or not. Nonetheless, the way SSI is designed makes it impossible for the credentials' issuers or any other party to know where it was used and whether it was used at all, according to expert G. This model empowers the citizens to stay in the full control of their data without fear of being watched. The government will then have no chance to track the transactions of the citizen. At the same time, it will remain its power to serve an authentic source of data, due to SSI enabling "*having a privacy-presenting exchange, where the party that issued the credential is not necessarily able to follow it",* as expert G reports.

A direct link between the identity management and risk of dictatorships can be drawn, as having all the data in one hand can empower the state for malicious purposes, should this be a case in the future. A good example was illustrated from the Netherlands and Germany, where having a central database of all citizens records is forbidden by law. These measures are done to prevent the dictatorships: although they might not be out there today, it is a solid guarantee that they will not appear in future. However, an exciting

thought was expressed by expert H: "*do you to invest much into something that you hope will never happen?*", which leaves a room for an open discussion about it.

All in all, SSI companies pursue the goal democratising the societies, using the conceptual and technological features of SSI: "*we're actually trying to make e-government and the democratic states work more nicely for the citizens*", expert G.

6.4.2 Economic

Economic aspects are of a particularly important for the public administration as the resources are usually limited and hence, have to be used wisely. The surrounding debate that SSI can contribute to cutting costs for processing numerous documents confronts another opinion that maintaining a public blockchain could be costly.

In essence, it is believed that by removing all the middleman parties, users will be able to interact directly and check their identity digitally, hence eliminating tons of paper-based verification processes. SSI can contribute to removing the red tape and simplify the process of linking numerous databases together, "*we can cut costs and facilitate economic processes*", as the expert I explains. Expert G complements this thought by elaborating "*currently, we have the situation where hundreds of systems exist in parallel […] Having the unified effect for all of this will create the cost efficiency and scaling effect*".

Still, more quantitative implications are needed before making any hard conclusion on SSI capacity of saving costs, which are discussed in the upcoming SSI challenges section. A good quote of expert L illustrates the uncertainty: "*searching to the self-sovereign architecture definitely takes a bit of investment, but in the long term can definitely provide cost-saving benefits as well, so it is a chicken and egg problem".*

6.4.3 Better information and processes

Self-sovereign identity promises to improve the way identity models function presently, or, as expert L argues, "*to have a healthier way of providing identity".* Experts agree that defining SSI can be confusing and impact the way public officials in making their decision regarding it. Here, expert F argues that "*we often get discussions between people who have a completely different understanding of what SSI is*". It can be explained that the ongoing debate on SSI is very dynamic and "*are likely to provide a current snapshot at what it is*", according to expert G. Despite the continuous advancements in defining the core components of SSI, several assumptions on its impact on the entire identity ecosystem can be already made, given the academic discussion and the experts' input, which expert G summarises as "*that there is a lot of implicit alignment of where*

the technology has to go, people agree that this interoperability and portability are essential".

A valid question was raised by expert C: "*how do you see the combination of sovereign identity elements and the authenticated elements?*", which bring the discussion on the difference between the self-sovereign and self-issued credentials. Mainly, as the SSI experts argue, it can easily be a combination of both.

SSI promises to eliminate the third party and hence, give more control to the citizens over their identity information: how it is shared and where it is used. With the SSI, all citizens will have their legally and technically implemented identity in one place under their control, yet still guaranteed by the authentic sources, the government in particular.

It is expected then that in case the citizen needs to present his or her identity, they will be able to decide which attributes to share. For that, a citizen will only need to have the VCs in their wallet so that when the interaction occurs, the receiving party would be able to read and understand them. Admittedly, that "*you only need to understand the verifiable credentials that are important in your business process*", according to expert K. Also, the verifying parties will be able not only to check the authenticity of the claim but also whether the party that issued it was entitled to do so, as expert G suggests. As such, citizen's wallet becomes the vehicle via which the citizens can easily exchange different proofs, as expert K believes. How this could work in Belgium, for instance, is that after requesting an attestation from FAS, the VC could be added to the wallet and re-used later on.

For the governments, it could mean that "*the main added value is about simplifying certain processes*", according to expert D, and allowing citizens to use their information outside of the particular context. Expert L elaborates that "*there are also opportunities to use the SSI as a better way of sharing those documents in the process".* Expert I also believes that "*the overall goal of the SSI movement is to minimise the trust required*", so that interaction can happen between the parties who do not necessarily need to trust each other, but rather the trust the SSI protocols. In this case, expert C provides an example in the event when the police need to check whether the person has a driving license: "*they don't want to know who you are, the only thing he needs to know if you have a driving license*".

"*Better data and integrity of the data*" are also among the benefits that the government can expect from granting citizens their self-sovereign identity, as the expert I reports. Although many features of SSI are debatable and lacking standards, it is worth discussing the possible opportunities that SSI can bring in terms of quality of data.

All in all, expert G underscores that "*the point is not to decentralize every single thing of every interaction*". The central idea should be in achieving interoperability and portability of SSI so that the citizens can freely move around, collect the credentialism from various parties and use them.

6.4.4 SSI use-cases

Merely putting a technological solution on the table is insufficient to claim that it is worth investing and researching, especially in governmental reality. SSI was initiated from a raising debate of giving users more control over their data in the light on the scatter identity information across multiple companies. In the context of the public sector, SSI could grant citizens the right to restore control over their own identity and be able to share and re-use it in the circumstances they desire. Surely, SSI cannot simply replace the infrastructure that was in place for many years, and this is impossible for many reasons.

It is also important to mention that these use-cases are in no way universal patterns that all countries can follow, it solely depends on the national context, a peculiarity of the public sector organisation and the national framework. As expert I suggests, "*if you have a good use case in Belgium, it might not be necessary that we can implement it here in Germany*". As experts agree, the processes of SSI's embedding should be gradual and start with low-risk and straightforward use-cases, which consequently involve low-risk identity credentials. This process will "*allow people to get to know the technology, understand how it works, how to keep it secure and adapt to the new technology, while already getting a lot of benefits*", as expert G believes.

More specifically, experts also anticipate some possible concrete implementations of SSI in the public sector: certifying volunteering experiences and achievements (expert I), proving identity in car-renting and other commercial services (expert A), storing refugees' personal data to guarantee their identity (expert A), university diploma verification (expert D), using QR codes to present oneself at institutions (expert J). Expert G summarised those as "*everything is the best use case. The point of SSI is that you either adopted everywhere in the long run or you can just leave it*".

A lot of comments from the interviewees regarded the cross-border interactions. As expert D suggests, "*keep SSI just merely in the public-public, or public-citizens interactions, it could help, but the most added value, of course, is if you go to the cross-sector or the cross-border*". This change of breaking the silos within sectors or even states can significantly boost cross-sector interactions and allow better mobility of citizens. Infrastructure-wise, EBSI is there to ensure that all the member states can enjoy the technology without necessarily developing it for every use-case. Then, once the ESSIF-

compliant wallets get legal value in Europe, there will be no need in the European proxy-server and interacting directly, using eIDAS as the supporting base, as expert K reports. Regarding the Belgian context, expert K believes that combining the SSI principles with resources Belgium already has, such as its robust eID scheme, FAS and the itsme-application, a secure SSI wallet can be achieved.

It is expected that in the future, all public sector processes could be run via the SSI; it is only a matter of time. However, of course, there are several processes that are easier to do the test-drives with and others which require technology to become more mature. Those include use-cases, which require high-level and high-risk credentials. Hence, starting from the easy cases, SSI can be gradually propagated to all processes, and where the eID is the final milestone to achieve because "*it's a top priority, but it's not the first thing that you implement"*, as expert G reports.

6.5 Challenges for SSI in Belgium

It is natural that SSI still has many questions unanswered. SSI is not yet there to demonstrate its performativity and efficiency with numerous use-cases. Its development at both conceptual and technological levels along with plentiful uncertainties with it suggest that there is a room for the work to be done before it gains a full adoption, both among public administrations and users. This sub-section presents the possible implementation and conceptual challenges for SSI in Belgium based on the framework employed by this study, as well as the new ones, which were identified in this study alone.

6.5.1 Legal

Compliance with the existing European and national legislation is, unquestionably, a key priority for SSI developers and practitioners. Harmonisation of SSI with the current regulations, most importantly, GDPR and eIDAS, does not happen all at once. It currently involves numerous experts to provide the compliance frameworks and to ensure that once the technology reaches a broader market, no obstacle remains on its way. Addressing this challenge might not be relevant for exclusively for Belgium but for EU member states in general, as the pan-European regulations oblige them to stay compliant.

GDPR

The definition of "self-sovereignty" in its essence is aligned with the idea of GDPR, as "*I define what is going on with my data"*, as expert F said. Yet in practice, this issue gets more complicated as it also has to be aligned at both conceptual and technical levels.

In the assumptions on how SSI could work, the public ledger would store the DID, or the hash of the DID in order to be able to have a link to an entity. However, this data can also be a subject of GDPR-violence because "*even if you encrypt personal data, it will still be pseudonymized data [...] You can decrypt it and link it to the person*", according to expert H. A more detailed discussion on what exactly gets stored on the blockchain is presented in the technical challenges section.

The lack of interpretation of GDPR in the blockchain context hurdles the alignment of SSI solutions. Still, the work is being done driven by "*a big legal risk, and a big risk of moving in a wrong direction*" for SSI developers, expert G informs. ESSIF is working on another study to illustrate the alignment of SSI with the GDPR and expects not only the technical stakeholders but also the governments to come forward. In this sense, "*next to this more technical approach, we need also a regulation approach*", as suggested by expert D.

All in all, the problem of GDPR is known and is being addressed by many contributors, *"it's not a problem of today anymore […] the questions are clear, there is no unclarity anymore"*, according to expert G. It will take time for the solutions to be fully aligned as it also involved other issues of governance, finance and trust frameworks, which are discusses later.

eIDAS

Once the technical challenges are solved, a trust framework is needed to make things work, as expert G suggests: "a*nd this is exactly where the eIDAS comes in*". eIDAS regulation has the aim of providing interoperability of services across the EU and allows European citizens to easily access services from foreign countries using their national ID schemes. While it sounds like an ideal match with what SSI stands for, there is a need for a more thoughtful discussion and development to achieve full compliance with this regulation. The eIDAS comes in practice to ensure that other means of identification and sealing are treated in the same way as the government-issues credentials, according to expert D. Also, this regulation provides additional credibility to the solution, as expert F argued in the following manner: "*if you create a trust framework around solutions, you see that businesses start to connect with each other because they rely on a digital identity, which is certified and trusted by the citizens*".

One of the examples was suggested by expert K, that at the present day eIDAS, the way it works requires making changes for every new flow, which overcomplicates the whole system. He then argues that "*if we had an open standard via which the wallets can get the*

verifiable credentials from different parties and directly exchange them, we would get a much more loosely coupled environment".

The study of ESSIF presents the outcomes of the research on the compatibility of SSI with the current version of eIDAS, as well as the relation of the verifiable attestations to the trust services under eIDAS, such as signing and sealing, expert K informs. Also, speaking from the opposite perspective, ESSIF is working on the proposal to suggest the changes that need to be made in the eIDAS to empower SSI even more, expert D explains.

Expert G also argues that at the moment eIDAS is itself quite centralised, and the "*central parties have power over the process*", and also suggest the ways how the current eIDAS could work differently:

"There is no need to put that central power that is democratically attested and democratically controlled; there is no need to put that in the context technical form. You can just accept that this is actually a central party that is allowed to issue your birth certificate".

In other words, the trust framework will be about legally ensuring that organisations follow a particular process or are registered in a certain public register. Also, it is about the way that citizens can that accept VCs so that they don't do anything illegal or they don't take too much for unnecessary or uncalculatable risk, according to expert G.

6.5.2 Institutional and organizational

Innovation in the public sector is always surrounded by so-called organisational resistance caused by the established systems and processes. In this sense, expert L explains that "*definitely, I think, in any large organization there is always this hesitance to change, it's not specifically public sector*".

Indeed, every innovation is stressful for public administrations, especially if the scale is the whole country. The implementation of SSI within different processes would be different across the EU. Notably, in the countries with the centralised architecture, like Belgium, it will face significant challenges, which are described below.

Government's role

One of the objectives of SSI seems to be removing the centralised authority over the user's identity. One theme that was present throughout the interviews was whether or not the role of government will change. In the context of the public sector, at first sight, SSI seemed to put the whole notion of governmental power, and hence, the entire public administration system, at risk. Expert A explains that unlike the commercial sector, the

issue of consent is different in the public sector reality: "*for us to function, we need data*". Expert F also underscores that "*the sovereignty of the state is the basis of all*". And if the services do not require any information about the citizen to be provided, then "*it's public information anyway*", as expert J clarifies.

A common misunderstanding lies within the name of this identity model itself: self-sovereign, which does not always mean self-issuing. Expert D explains that this is not the case: a citizen is still a part of the society and therefore, he or she has to act accordingly, they are not allowed to deny providing the tax data, for instance. Within the SSI ecosystem, governments will hold the utmost power to serve authentic sources and issue the verified credentials to the citizens, who will, therefore, store those credentials in their wallets, or vaults. While still having central authentic sources, their role will be changed, and this is where the sovereignty aspect comes into play: the citizens will get their credentials for their personal storage and give their consent for that data to be used, unlike how presently certain databases are linked without citizens' awareness, expert D explains. Essentially, not all the aspects are going to be in control of the users. Expert K provides a reasonable summary of how the citizen-government relationship in Belgium would look with SSI: the data in the wallet is under user's control but the "*Federal Government that will issue the verifiable ID, it's the Ministry of Education that issues diploma, it's the Ministry of Mobility that issues driving license*" and the citizen would then take those public-bodies issued credentials and store them at their side, meaning that those bodies will still hold their authentic sources.

Political resilience and willingness to change

To begin with, there is a philosophical question of viability: if everything is working today, what are the reasons why the government should want to change this. It is especially relevant for Belgium, where there is a robust identity infrastructure in place. Expert K argues that implementing SSI is a big cultural change both for the government and citizens, who "*need to be ready to take this initiative*", expert D said. Another problem is a limited capacity of the government to explore the technology and finance the research. Partially it could depend on the political will in the country to do so.

Expert K explains that centralisation "*is the part of our Belgian culture and changing that on the political way is very hard*". He further elaborates that "*what is missing in this country is the political support of these aspects*".

In Belgium, according to expert B, despite having visible support for digital initiatives, the top-level is still conservative in this regard. Expert D clarifies that usually, it is challenging to receive political support for projects that are not going to bring immediate

results but rather promise a long-term benefit instead. And for such an industry-reshaping initiative like SSI, merely having an administration on board is not sufficient, "*we need some political leadership*", according to expert D. The expert also argues that even though there might be private companies and other stakeholders willing to support the government of this way, they still need guidance. The case of "Blockchain on the move" project illustrated that cooperation between private and public sectors is possible with a commitment from the public administration side. Based on their experience, expert L shared that the city of Antwerp "*has always been a good partner. They have always been very transparent; we cannot complain in that sense".*

Overall, expert D believes that the SSI-momentum should be used now, otherwise "*other countries will be going ahead of us on this*". Following that further, with the COVID-19 outbreak, experts believe that there must be a shift towards more digital political agenda with a more accelerated approach towards digitalisation and new technology, in expert's B opinion. "*Corona was the ideal for everything that was blockchain, self-sovereign, anonymous, whatever you want to call it*", according to expert J. In turn, expert K elaborates in the following manner: "*we all learn that the more digital you are if you can settle legal processes, you can continue your business*". It can only be a subject of early speculations whether the pandemic can cause another boost to move towards SSI.

6.5.3 Technical

Blockchain-related factors

Undergoing the controversies such as whether or not the personal information should be stored in a distributed fashion is crucial prior to starting a political debate on SSI. Many technological questions arise from the discussion of whether or not blockchain or DLT, in general, are the necessary components of SSI. Expert H restated the widespread belief that those terms are intertwined: "*we talk about SSI, everyone thinks about blockchain*".

Still, experts mainly agree that this is not necessarily the case, even though blockchain technology can enable many features that SSI implies, "*that's just the technology […] an ICT supporting element*" according to the expert C. A constructive point was made by expert A: "*it's a term that is used in a blockchain context, but SSI only means what it means*". Following that further, expert I suggested that "*there are a lot of experts in the field who say that blockchain is just relevant for now and will be irrelevant in a couple of years*". At this moment, however, most of the SSI implementations, or SSI-wallets, are based on various types of blockchain, yet expert G believes that those can be done it a peer-to-peer fashion as well when it comes to individual usage. The reason for that could

be that if it is done in a centralised way, "*you're already missing some values of SSI",* as expert L argues.

The following challenges identified from the interviews are partially or wholly derived from blockchain properties used in the SSI ecosystem. Although the issue of "the right to be forgotten" is a part of the legal context, it was widely mentioned as a part of the technical one too, given than if the SSI is enabled using the blockchain technology, its immutability principle puts that right at risk.

What parts of identity are stored on the ledger is another controversial discussion. Because the narrative surrounding the SSI can be controversial, special care is needed. Storing the whole identity on the ledger is harmful, and it cannot be even a subject of the discussion, not in the context of the public sector at least, because "*there is no authentic source from a government anymore"*, as expert F explains.

In this manner, any information that can lead to a person, including their DID, cannot be stored there to be compliant with the regulations, as it was mentioned. Therefore, the only information to be stored on the ledger should be the public key, to serve a checkpoint for the validity of the issued claims, as expert I suggests. The identity information gets stored on the user's side in this case, which, of course, raises issues of security, audit and standardisation, as the smartphone market is extremely diverse, as expert F informs.

Also, by eliminating third parties, experts are not sure how can the identity be recovered if the wallet is lost or forgotten. Expert H gives a comparison that in a user forgets his or her PIN-code, the banks still allow getting access to the funds back. In the context of SSI, these issues are yet to be resolved. Expert K explains that the research is being conducted on the key recovery and its possible implementation via identity hubs.

Expert C also argues that with SSI it will be difficult to verify the correctness of their identity attributes: "*we don't know if the SSI elements are correct or not, but we know that they belong to that person*". Also, it is difficult at the moment to find the balance between giving the citizens the control over their identity and protecting them from misusing it, as experts D elaborates: "*you get citizens fully in control of their medical, financial information that they can easily share with the wrong people and the wrong intentions*". It is expected that once SSI is mature, these issues would be resolved.

Governance of SSI

One of the most important uncertainties is the governance and standardisation of SSI before it takes up. At the moment, the SSI development landscape seems scattered and disjoint, and not all the solutions correspond with the required security level. Today "*there*

like no fixed standards or off-the-shelf solutions, which can allow to rapidly use this technology", as expert K said. Experts agree that for SSI to mature, there must be a unification of efforts to ensure the values of SSI, namely interoperability, are consistent. Otherwise, without a coordinated effort, there is a risk of having well-functioning isolated SSI ecosystems, which would not be able to talk to each other.

Consequently, it is essential to have a clear governance framework because, in a distributed way of operating, the issue of its accountability is acute. With no central party to turn to if something goes wrong, SSI should consider the mechanism of such conflict's resolution and sustainable functionality. Expert I explains that the governance framework in the context of SSI is "*legal contracts between all the participants and the stakeholders of the system".* Expert D confirms that although there are some initiatives, "*to make the jump forward, you need a more coordinated and more political support on that*".

The private world is actively involved in building those frameworks, as expert I informs, including Linux Foundation and Hyperledger. Expert G foresees three possible scenarios on what can happen to the SSI solutions in terms of aligned the governance frameworks. First is a fully achieved portability, where everyone is using open standards. Also, there might be a case of having several major competing protocols or finally, even the scenario where everything is disjoint, namely there are well-functioning solutions. Still, neither of them would interoperable with each other.

In the public sector reality, as expert A explains, building a legal framework for instance, smart contacts, or other DLTs is difficult with the current legal base. Therefore, it must be sustainable cooperation between multiple stakeholders to make that happen.

6.5.4 User-related factors

No matter how mature and well-development is technology, it needs usage first and foremost. The findings suggest several issues associated with the users, their competence and willingness to use the technology. Expert I even calls this the most crucial factor, as "*if you don't have the user inclusivity, their adoption the user trust, then nothing is going to happen*".

To start with, implementing SSI should be an inclusive process; in other words, it should, in no case, leave any group of users behind. A heterogeneous society calls for ensuring that all users are given an equal chance to participate. As summarised by expert I, "*we still need to make sure that people who don't have a smartphone are a part of the system as well*". The expert then suggests that there is still a possibility to run only one system but in the case of the former group of people, provide them with the alternative ways of

having their identity wallets, such as physical bank-card-size item, to store their VC there. However, the questions of security will arise because the government has to ensure that the solutions are available to anyone with the same level of security. Even concerning those citizens who have smartphones, they all come in different models and functionality. For the government, it is difficult to provide the solutions that fit all: "*that is for me something […] that has been keeping us back for a long time*", as attested by expert J.

On the other hand, the question also arises whether the users are interested in having this control that SSI promises to bring. If SSI is presented as merely a technological innovation, expert J believes that, from their experience, citizens are "*not interested in having the latest of the newest tools*". Expert L also provides their view on this account: *"people don't care that the information is in the database, or it's on the blockchain, or it's in their own identity".*

Leaving the fashion and the hype technology aside, a very valid question that experts H and A are asking is "*is the citizen demanding it, is he interested to do this?".* The answer to this question can only be obtained via public discourses and surveys as it is difficult to speculate and generalise the ideas, based on several opinions.

Unlike the eID card is relatively easy to comprehend, the mobile solutions are "*more advanced, we cannot expect people to understand it easily*", as believed by expert J. Arguing in this dimension, experts raise their concern and share opinions on whether or not citizens have the competence and knowledge to utilise the SSI, should they be interested or not. Logically speaking, "*if it is difficult for the user, they will not use it*", as expert K argues. Moreover, expert L was even more persistent*: "citizens should never be exposed to the complexity of it*".

The task for the SSI is then to ensure that the solution is easy to understand and to use for everyone. Also, it can be done via providing the SSI-wallets with the necessary certifications, so that users do not need to understand the logic behind it. These certifications are something that ESSIF is working on, as stated by expert D. Some experts express their concerns that this puts too much responsibility on the users to manage their identity and secure it.

Nevertheless, most experts overall agree it is strenuous to ensure that there is no trade-off between the usability and security. If there is a comfortable user-interface that is easy to follow, as well as the good security at the backend, the users should not worry about it. Expert D thinks that "*if you let the citizens choose, they vote for usability*", which confirms the previously mentioned topic of citizens interest. Expert's H personal opinion is that in the business world "*the services and administration should be as simple as*

possible". In that direction, expert K compares it with the automobile: "*no one would buy a car if they fully understood how it works*". Still, expert D is also of an idea that "*user also wants some certification level*" before the application is used. The ESSIF is currently involved in understanding how to ensure both security and usability, "*all those usability aspects are now in place, are now being researched*", as per expert K, which indicates that the upcoming version of SSI projects will less likely cause these questions.

The governmental reality is even more difficult, as expert J admits, "*since 2009, we were looking at this, but this is very hard to find a solution that would check all the boxes: usability and security*". In the meantime, a private itsme project addresses both challenges by offering their solutions, where both user experience and security are in place: "*we didn't want them to choose anymore between the security and convenience*", expert E explains.

Finally, the additional variable comes into play: trust. Even though the application can be both secure and user-friendly, what could still harness citizens from using it is whether or not they trust its developers, according to expert I.

6.5.5 Other factors

Apart from the factors from the framework, the results suggest singling out additional factors that do not fall under the categories mentioned above and which might be SSI-specific.

Since the issue of governance and maintaining the SSI ecosystem has been already raised, a natural follow-up on them would be figuring out the finances behind it. Although on the one hand, the SSI is expected to reduce the costs of processing information and simplify processes, it is still unclear how does its economic model work. It is natural to expect installations and maintenance price when it comes to innovation and new technology. Blockchain implies having an incentive mechanism for the transactions to be executed. In the public sector context, as expert B highlights, the public services cannot imply any transaction fee, namely: *"as a government, we cannot invoice, we have to give everything for free, it's been already paid by tax money",* as expert B explains.

The point is that at this moment, it is not clear whether or not this solution will be financially viable. There is no reason for maintaining a costly ledger in the e-government context, as some can speculate. If the public sectors opt for the SSI based on the DLT, it should most probably be "*it will be public permissioned ledgers, which are super easy to maintain, very cost-efficient*", as expert G believes.

There is no clear answer to this question. Yet, the SSI community sees two possible scenarios: either an upfront payment for a certain number of transactions or a fee per single transaction, explained by expert G. In addition to that, the ESSIF conducts the study on *"economic assessment of the ecosystem of SSI*", as expert D informs, where the citizens' attitude to SSI and the expected added value is discussed. Along with that, in the light of EBSI nodes being built, a more holistic view on the related costs is required, "*we need to figure out what kind of economic model is behind*", by expert D. However, it is believed that the member states should take the initiative for financing the building blocks at their side because it would not be feasible for Europe to pay for that. As for now, this study is not yet available, and hence, the economic aspects of SSI implementation go beyond the scope of this work.

6.6 Drivers and way forward

Expert A admits that although it could be promising, SSI is just one of the existing solutions for digital identity. Expert K personally believes that SSI "*will slowly grow for the next years, once there are COTS solutions and wallet implementations available, that are also trustworthy, then, I think a very fast take-up in the market*". SSI also has a similar vision with the mobile roaming, hence ensuring portability and interoperability of different users, as expert G believes.

It is evident that SSI still needs to mature before it can be ubiquitous and adopted by the users. Following the experience from the "Blockchain on the move" project, expert L shared the vision regarding the further implementation of SSI: "*the first you need to look at when the project is done is the quick wins, where is the best balance between effort and value".*

Expert H argued that SSI could be looked from a hype cycle perspective: once it has passed the peak, "*we go to more stable mature projects, […] and I think, the stable point will be much slower than the highest point*". Seeing the number of efforts put into making sense of SSI, there is no concern if it is going to happen, but rather how and when. Expert K assumes that "*before we go to the market or 500 million European citizens, it's going to involve for three to five years, it needs time*".

Still, the evolution of SSI is not going to happen on its own. Expert I believes that the best way of enabling the SSI-words is "*if we have the public discourse about it, it needs to be on the front page*". At the moment, as this expert explains, the discourse on SSI is very niche, which is why more attention needs to be drawn.

Citizens would have their identity information on their side in the form of a vault. Still, there are concerns on what happens if this vault is damaged, lost or inaccessible. Expert K argues that "*why we need more intelligent mechanisms to recycle it*". For that, as expert H assumes, there must a stable balance between safety, reliability with the way of maintaining in in a distributed way. Expert E also believes that "*there is future in a mix of centralized and decentralized: centralised core identity and decentralised attributes*".

Also, regarding the problem of users' accountability for their own identity, "*they can be addressed with the additional services like identity custodians*", so-called intermediaries, as expert G clarifies. Expert H also argues that the "*secret sharing*" could also be applicable here, then the key is split into several parts and recompose it if one part is lost. Still, additional research is needed on how these could be implemented. Expert J explains that the government tries to be a good custodian in the current situation, but the privacy issue is difficult to be solved at the moment.

Active collaboration

Governments will play a major role in the SSI solutions to be commonly adopted, including researching and investing time and resources in it. Regardless of the type of identity scheme, as it was in the case with itsme, "go*vernment support and endorsement are the prerequisites to have a successful digital ID*", according to expert E.

Now, moving into the SSI context, expert D summaries it in the following manner: *"We have the components that we have in Belgium, the components that Europe is taking",* concluding that it is "*up to Belgian government to take the initiative*". Moreover, expert K believes, that the governments could indeed benefit from it, especially in the Belgian context: "*governments that are advanced in those authentic sources and have the centralized way, they will be getting the most advances*".

Convincing the mass audiences, especially within the government, is difficult. Also, in the context of the public administration as "*there're different layers of decision-makers*" according to expert B. Many experts mentioned that on a way of achieving this should be visionary people with enough political influence and support to advocate this identity model and set the course towards SSI. A good quote from expert B elaborates on this: "*without strong support, the ideas will not succeed, you have to have the influencers to achieve that".* Also, these actions have to be immediate, as the people's terms in the ministries are short.

However, expert C believes that not only the government should take action regarding attempting to achieve SSI, and experts D and K are of the same idea. Indeed, as was

mentioned, the dynamic of SSI development is rapid and the collaboration of various stakeholders, including public and private organisations, is needed to catch the momentum and set the right course, expert G believes. One reason for that can be seen in what expert L said: "*there is a big role that has to be played by the providers of the technology, so it (SSI) is presented in a way that the citizens are never exposed to the complexity of the technology".*

At the moment, a lot is going on in the private world, where banks and other companies experiment with SSI possibilities. "*The expectations are really high, and there are also many companies acting in this space, actually building and developing stuff, at least one hundred*", as expert G informs. As was argued in the previous sections, there is a need for a coordinated effort, given that there is a rising interest from all sides, both private and public.

Push from Europe

The European Union could be one of those drivers toward making SSI a reality, as experts believe. Expert L shares their vision that this push will not be forcing but rather encouraging member states to move towards SSI. Also, in this sense, Europe can be an accelerator on the international scene. As expert K elaborates: "*if Europe success at setting a scene and we had a few projects, where you see it really implemented, I think it would work as an accelerator*".

Expert D believes that empowerment of citizens is something within the European values, and is related to the data strategy of Europe, so there must be another way of looking at data and placing the citizens. One of the possible steps are the regulatory measures, as expert F believes, is, for instance, setting the reference framework for SSI-related notions, such as decentralised identifiers. And moreover, there is tangible support at the European level, as expert D reassures: "*now we have the budget to do certain things in the European level".* In that sense, expert L argues that "*Europe is investing so much in it to see the added value; it will play a part in the IT landscape of any government level*".

However, at this stage, it is difficult to foresee how the SSI can function across the whole of Europe, given that some member states even struggle to notify their eID schemes under eIDAS regulation. Expert K elaborates on this, stating that some members states are even moving to the centralised way of identity management, where the governments hold the central registries. Apart from that, the coordination of activities from the European level is frequently seen as a more vertical one, as even though a lot is decided on the European level, "*people who have to actually do this stuff have a lot of difficulties trying to implement these initiatives*", as expert A informs.

As a way of addressing these concerns, ESSIF works on interconnecting different SSI projects across the member states. At ESSIF, the specifications for the SSI are being developed, leaving the technical solution, or the wallets, out of scope. Here, the collaboration with the private market could come in play, as ESSIF relies on the market, in this case, to become more mature and more elaborated, according to expert D.

Overall, expert D believes that "*if we can relate […] with some private initiatives, then we can gain some momentum in a pragmatic way*". The time will tell whether or not this cooperation is successful.

6.7 Summary of chapter 6

This chapter contains an overview of the main findings of this study, collected via the interviews from the experts in the fields of identity management, self-sovereign identity, blockchain and innovation. It illustrates that there is an active development of SSI in both private and public context so that in the short term, more tangible results can be expected.

This section gave the first glance on the state of play within the identity management reality, allowing the author to reflect on why, where and how it can be benefited with SSI. The summary of the findings is depicted in the following table.

Table 5. Summary of the results

Probe	Sub-topic	Main findings
Belgian public sector	Organisational reality	• Complex public administration • High standards for security • Conservative culture • Limited capacity and resources for innovation yet the efforts are put • Difficulties with translating the high-technological concepts to everyone
	Blockchain and SSI	• Blockchain is not the absolute solution • Difficult to see a direct business value and not start from the technology • Postponed initiatives • Several projects emerged, not SSI specific • Blockchain on the move scope was reduced • Positive follow-up during phase 2
	Citizens' attitude	• Not eager to interact with the government unless they have to • Surveillance concerns • Awareness about one's identity
	itsme	• User-friendliness and security by design • Trust reached via government's endorsement • Branded identity • Centralised and in control of transactions • Possible future with decentralised attributed

	Identity management	**Benefits:** • Robust identity infrastructure (smartcards, authentic sources) • High-security standards **Drawbacks**: • Immense legacy system • Privacy concerns • Centralised control • Static ID cards • Usability challenges • Siloed usage **Future steps** • Clear positioning is needed • Seeking citizens have more control • Better services • Mobile identity
SSI	Opportunities	• Better governance • Citizens have control over their data • Foster democratic societies • Saving cost is not a strong argument at the moment • Ubiquitous identity • Simplified processes • Minimised trust • Better quality and integrity of data • Numerous use-cases possible
	Challenges	• Compliance with GDPR and eIDAS is addresses • Lacking political support • Organisational resistance • Concerns about the risk of anarchy • Blockchain-specific factors (whether it is a necessary component, what gets stored on the ledger, how to address immutability) • Lacking governance frameworks and standards, they are being developed • Diverse audience and smartphone coverage • Low user competence and awareness • More studies needed to assess the interest • A need for both usability and security
	Future steps	• SSI is expected to grow • Active collaboration from public and private actors is needed • Europe should be the driver

7 DISCUSSION

The previous chapter sketched the findings of this study, which comprise the foundations for answering the research questions of this paper and its sub-questions. The following paragraphs provide an elaborated answer for the RQ, which is "what opportunities and challenges can the Belgian public sector expect from implementing the self-sovereign identity model?", and the surrounding conclusions.

Innovations never happen in isolation (Ølnes & Jansen, 2018). The globalisation of the world and emerging technologies make it possible to look at the routine processes and systems from a different angle, which was also the case for identity management. Driven by the fact that many countries still struggle to launch secure and accessible ID schemes, several studies anticipate the evolution of identity management, both in physical and digital worlds, which poses another challenge for the public administrations. Other social, economic, political and technological drivers will determine which way the identity systems will develop towards (European Union, 2018). Among those drivers are the growing privacy and trust concerns the exposure to new technology. The identity of the future will be based on the pillars of inclusion, secure and sustainable design and governance to allow its interoperability, security preserving utilisation and legal enforcement via set standards (The World Bank, 2017). Though at first sight, it could seem that those are only relevant for the developing countries, the overall trends speak for themselves: more control over one's identity information will be ubiquitous (BBVA, 2019). The rapid technological uptakes will challenge the existing regimes of severe centralisation and attempt to return the citizens their authority over their own data, enabling them to decide how and with whom this data will be shared.

Those were the circumstances for the self-sovereign identity to emerge (Allen, 2016). It gradually gets more attention and recognition both in private and public sectors. While several benefits, such as allowing the users to have control over their identity, lie on the surface, the process of transitioning towards SSI is not a smooth one. Many factors surrounding this process should be noted and taken into the account before any concrete implementation plans are made (Ferdous et al., 2019; Zwitter et al., 2019). Countries with the existing robust identity infrastructures will face difficulties with evolving their identity systems because once the control is in one party's hands, it is troublesome to disseminate that. What this study offers are the insight at the possible opportunities for the new identity paradigm in the context of the public sector, as well as the potential hurdles associated with that, by the example of Belgium.

Based on the results of the study, it can be concluded that defining what SSI is will take a certain time. SSI came out of the enthusiasm to grants users more control, but there is

no reference framework and hence, no right or wrong interpretation of what SSI is and what is not. All SSI projects have the right to exist, depending on the context and the goals pursued. Therefore, the author proposed discussing the SSI not via its principles but rather using the overarching vision, which constitutes that the user should be in charge of his or her identity.

Belgium public sector presents a complex mechanism, where many processes depend on various information sources. An obvious takeaway from the study is that SSI holds the potential to increase the efficiency of these processes, including the cross-sectoral and cross-border interactions. Other use-cases, where SSI can be implemented, comprise the document validation (Baars, 2016) or refugees' identity verification (Syed, 2019).

Experts revealed the fact that citizens use public services out of a need, which could be caused by various factors, including the unstable trust to the government. Notably, a strong player within the identity market, itsme, achieved a high market penetration and trust from its customers within a couple of years, offering a user-friendly interface and providing a high standard of security. Belgium has a moderately high connection and smartphone provision metrics, which could, in some way, facilitate the adoption of SSI as the public solution. As itsme stated, the future of identity could be with the centralised authentic sources and decentralised attributes.

However, aligning with the pan-European regulations, GDPR and eIDAS were frequently mentioned (Der et al., 2017; Wagner et al., 2018). Ideologically, SSI goes hand in hand with what the regulations aim, namely protecting user's privacy and the explicit consent for sharing, interoperability of identity throughout Europe. Nonetheless, much work is still ahead in terms of aligning the semantics and technical solutions with these regulations. The issue has been acknowledged and is being addressed by specialised experts, only time will tell the outcome and perhaps new, offer modernised versions of SSI concept. Alternatively, possible adjustments to those regulations could be proposed, based on the experts' opinions. ESSIF works on creating the integrated governance frameworks for SSI to consolidate the initiatives in the field. The first steps have been already taken, as the first EBSI node was launched in 2020. Only the strong visionary support could guarantee the development of SSI and bringing its benefits to Belgian citizens and residents.

More importantly, Belgian national regulation on identity is there, and it takes lengthy administrative procedures to change those, also knowing that the law on the National registry has been in place since the 1980s. Therefore, a strong administrative and political support is needed to advocate SSI. However, in the Belgian reality, it is not always easy to lobby for this with the long-term added value.

Additionally, due to this confusion and lacking standards, introducing SSI within the Belgian governmental context was associated with risks of losing the government's authority and status. Hypothetically, such a plight could lead to anarchy, unstructured identity information with millions of formats and the overall chaos in a government-citizens relationship. However, SSI could mean quite the contrary: maintaining the authentic sources, including the government's, for providing the unified identity attributes to citizens while allowing them also to oversee their data (Wang & De Filippi, 2020).

This confusion was most probably caused by the term of SSI itself, where it was not clear what the "sovereign" aspect stood for (Ferdous et al., 2019). Unlike the "self-issued" identity, where the users define their own identity credentials and serve the sources of truth, the "self-sovereign", at least in the government context, would imply the users being able to collect attributes from various sources yet hold the control over their usage and sharing. This significant difference brings more clarity into what SSI and what SSI is not.

Also, although blockchain seems a necessary part of the equation, it was debated that it is not lying in the core of SSI (Mühle et al., 2018). Originally coming from the financial sector, it has found its embodiment in the public sector context as well. It was revealed that indeed blockchain has several uncertainties, such as immutability of the records and storing the information, which could reveal the person. If used correctly and in combination with other technologies, it can enhance the SSI implementation (Dunphy & Petitcolas, 2018; van Bokkem et al., 2019) Nevertheless, SSI was proven to function with other technological solutions, implying that blockchain is just a tool to achieve things (Van Wingerde, 2017).

Hence, the Belgian public sector, with its robust authentic source infrastructure, can only enhance the SSI adoption. The government of Catalunya took the similar approach, where the it aims at providing the citizens with the control over their SSIs while remaining as the identity validator. In the light of many governments, including neighbouring countries Germany and the Netherlands taking action, Belgium could gain the momentum to move forward with SSI. Within the country, "Blockchain on the move" project has examined the opportunities for deploying the SSI and has become the pioneer project for this identity model in Belgium. The pilot in the city of Antwerp taught many lessons yet proved that SSI could go beyond exploring the technology and result in real added value for citizens and city administration. The project also indicated the commitment from the public administration side, which can expect not only increased efficiency but also better reputation among the citizens.

However, another hurdle could be low citizen competence or even their low interest in decentralising their identity (Satybaldy et al., 2020). Experts acknowledge the struggles of many Belgian citizens using the eID card and installing the software. As the example of itsme has demonstrated, the complexity of SSI can be hidden behind the comfortable user interface. The SSI in Belgium has the prospect to be widely adopted if the features it offers are embedded in the solutions. One of the suggested options were introducing the identity custodians, either public bodies or banks, yet it is not very clear at the moment how those could operate.

After the conducted analysis, the framework for assessing the opportunities and challenges of SSI implementation can be further adjusted, based on the findings of this thesis. Originally, it was developed for mapping the benefits and barriers of using blockchain technology by Ølnes & Jansen (2018) and was adjusted before the empirical part of this study began, based on the findings from the literature. The "Governance and control" unit was divided into two blocks for more vocal illustration for each stakeholders group: citizens and the government. The original "economic benefit" field was removed due to the uncertainties regarding the financial contribution of SSI, leaving it for the future research to determine. Better processes from the original framework were elaborated under the new block for "use-cases", where the SSI applications within the Belgian public sector were listed.

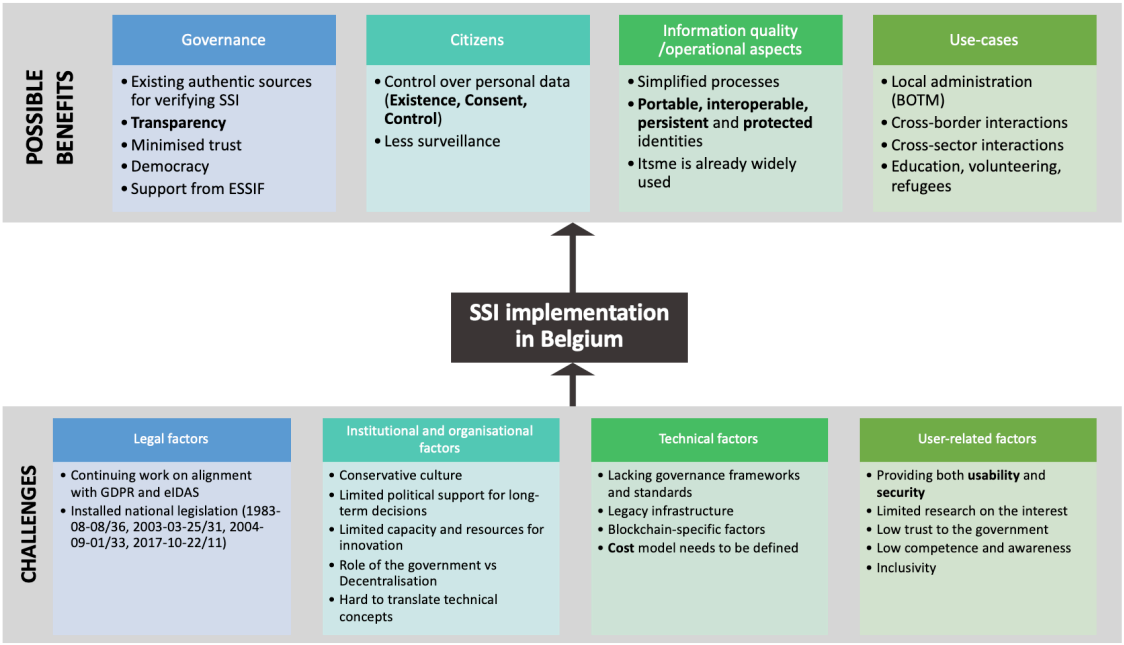

Figure 14. Opportunities and challenges of SSI implementation in Belgium

The mapped categories are by no means exhaustive and can only be speculated as to the results of this study, conducted at a particular time under particular circumstances.

8 CONCLUSION & FUTURE RESEARCH

This study intended to uncover the opportunities that the SSI can bring to the public sector and what challenges can be anticipated along this process. As the summary of the answers was presented before, this chapter will provide brief commentaries and set the foundation for future research in this direction.

Conducting an in-depth study of the current Belgian context to investigate the problem areas with the identity management domain was a part of the first sub-question. Belgium's complex public administration structure is reflected in many administrative processes as burdensome for citizens. There are difficulties with conducting cross-sector or cross-border transactions and citizens have only a static view over their identity information. The existence of state-own and controlled authentic sources guarantees the stable functioning of the state, yet it concentrates much power with one party. Citizens' careful attitude for the interactions with the government and scepticism over the possible surveillance were revealed as possible drivers for the current identity system to transform.

The second sub-question aimed at exploring features of SSI which could be applied in the public sector. Since the first mentioning of SSI as a term, it got attention from scholars and practitioners led by the ideology of having control over one's data. The research on SSI within the public sector is still to be conducted, and special care should be put to articulating about what benefits are attributed to the SSI model and what benefits describe the identity management system. As the author argued in the previous section, there is no right or wrong interpretation of SSI because this phenomenon was initially created from the public discussion and cannot be linearly described comparable to physical or mathematical algorithm. To keep in mind, the sovereignty in SSI relates to holding the authority over the usage, sharing and storing the identity, as the results show. Hence, the features of SSI suggested by Allen (2016) provide a sufficient degree of granularity when speaking about what SSI is. Many other, more advanced principles can be added depending on the context and the initial requirements. However, the overarching idea should remain the same: users should be in active control over their identity. In the context of the public sector, this can be achieved by granting each citizen a digital vault, where the identity attributes from various issuers can be stored. While some scholars would argue that this type of identity only partially resolves the centralisation problem, the current reality does not reckon for identities which are self-issuing credentials.

The third and final sub-question examined the possible hindrances for the SSI implementation. The literature initially suggested these challenges, and they were further enriched after the case analysis, provided the Belgian context and experts' opinion. A detailed elaboration on the challenges is presented in the revised conceptual framework,

with a clarification that this list is not exhaustive. One of the main takeaways was that more research is needed, which is also mentioned in the following limitations section.

Hence, in the light of the current identity scheme of Belgium and the anticipated future state, it can be argued that the SSI could bring visible improvements and still preserve the sturdy sides of Belgian identity management. Although it is impossible to derive any general conclusion for SSI in the public sector, the proposed frameworks could be used by the Belgian officials for the future agenda setting, as well as by practitioners and researchers from other countries where the SSI debate is in an infancy stage.

All in all, the objectives of the research were successfully reached. The paper concludes that for now, the way SSI can be positioned is the technology with many potentials to shift the whole identity management towards a more citizen-centred direction. Still, many issues with SSI remain either unanswered or partially answered. SSI needs to mature by being involved in public debate and attracting stakeholders from various disciplines. Conveying the knowledge and SSI values to the stakeholders should be among the priorities for SSI practitioners and researchers, given that the current academic scene is scattered and dispersed.

8.1 Limitations

With the objectives of the study met, it also, nonetheless, suffered from several limitations, which have to be kept in mind when analysing the results of the research. In terms of the selected methodology, one limitation could lie in the selected sample. Belgium was chosen for its existing identity model and the accessibility of information for the author, yet it should more countries with different profiles be taken, the results would be different. Furthermore, although the Belgian public sector bodies can use the provided results for the decision making, these results cannot demonstrate general suggestions regarding SSI in the public sector.

Also, a chosen cross-sectional study design only depicts the situation at a given moment (Levin, 2006). The rapid development of SSI outside of academia makes it difficult for the scholars to track and denote all the improvements, both on the conceptual and technical levels. Thus, several advancements might have been left behind by the cause of the frequency of academic papers published in this domain is also rather low. Moreover, the overall quantity of papers dealing with SSI in the public sector is small, which forces the author also to involve business reports and technical community blogs to enrich this study with more recent information. Finding interview partners was affected by the COVID-19 outbreak, as due to limited availability of experts working directly with the SSI reduced the number of final interviews taken and narrowed down the possible spectre

of opinions and expertise on SSI in the public sector. Another limitation in terms of the data collection lies in a possible bias. Several interviewees were coming from gov agencies and their professional standpoints might be affiliated with the interests of the agencies they represent. Also, involving a citizen as the main end-user of SSI in the research would give a more holistic overview of the problem, which opens the floor for future research.

8.2 Future research

This study attempted to look at the implementation of self-sovereign identity, yet there are still many research efforts to be taken to make this implementation happen. Although this research offers a glance into the possible opportunities and challenges of SSI in the public sector, it by no means suggests concrete benefits or negative impacts of this identity model. A more comprehensive analysis of use-cases is needed to derive those implications and make a view on SSI more complete. As the previous section indicated, this study only looked at the opportunities of SSI from the public officials and practitioners' perspective, leaving the attitude of the citizens out of scope. More elaborated research is needed to understand how citizens feel about the current identity management models and what is their expectation towards the future. At the moment, one cannot answer the question of the economic model behind the SSI as research is still being conducted. In the public sector, reality does not allow the government to charge citizens for their interactions, not in today's economy. Therefore, the SSI ecosystem has to ensure free transactions but there is no crystal-clear definition of how this could be achieved, leaving the open floor for future research. As highlighted by scholars, keeping the authentic source on the government's side still poses a risk of centralised control. There must be a specific regulatory framework describing the rules of maintaining the sources so that the user's privacy and supreme control over the identity are respected.

Hence, more research is needed in finding the balance between the centralised authentic sources and decentralised attributes. There are more questions to be answered. The future research should look at validating the authenticity of self-issued credentials, such as email address and the phone number. Also, more knowledge is needed on preventing impersonation, or ensuring that the user with the vault is the user who should have it. The author expects the future studies on SSI take these points into account for enriching the body of knowledge on SSI.

All in all, the authors anticipate more attention from scholars to this research domain, as well as more cooperation between academia and public and private sectors.

LIST OF REFERENCES

Abraham, A. (2017). *Whitepaper about the Concept of Self-Sovereign Identity including its Potential*. Retrieved from www.egiz.gv.at

Al-Saqaf, W., & Seidler, N. (2017). Blockchain technology for social impact: opportunities and challenges ahead. *Journal of Cyber Policy*, *2*(3), 338–354. https://doi.org/10.1080/23738871.2017.1400084

Allen, C. (2016). The Path to Self-Sovereign Identity. Retrieved November 10, 2019, from Life With Alacrity website: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Allen, C. (2020). (15) How to avoid another identity tragedy with SSI – Christopher Allen - YouTube. Retrieved May 19, 2020, from Youtube [Video file] website: https://www.youtube.com/watch?v=isanNSDoSnE

Baars, D. S. (2016, October). *Towards self-sovereign identity using blockchain technology*. Retrieved from http://essay.utwente.nl/71274/

Babbie, E. (2010). *The Practice of Social Research* (12th ed.). Belmont: Wadsworth, Cengage Learning.

Bartolomeu, P. C., Vieira, E., Hosseini, S. M., & Ferreira, J. (2019). Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT. *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, *2019-September*, 1173–1180. https://doi.org/10.1109/ETFA.2019.8869262

Baxter, P., & Jack, S. (2008). *The Qualitative Report Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers* (Vol. 13). Retrieved from https://nsuworks.nova.edu/tqr/vol13/iss4/2

BBVA. (2019). Digital Identity: the current state of affairs. In *BBVA Research*. Madrid.

Belgium.be. (n.d.-a). Belgium, a federal state . Retrieved April 24, 2020, from https://www.belgium.be/en/about_belgium/government/federale_staat

Belgium.be. (n.d.-b). Brochure. Retrieved April 24, 2020, from https://www.belgium.be/en/about_belgium/country/belgium_in_nutshell/films_and_brochures

Belgium.be. (n.d.-c). Federal Public Services and Public Planning Services (FPS and PPS) | Belgium.be. Retrieved April 24, 2020, from https://www.belgium.be/en/about_belgium/government/federal_authorities/federal_and_planning_public_services

Belgium.be. (n.d.-d). The Federal Authorities . Retrieved April 24, 2020, from https://www.belgium.be/en/about_belgium/government/federal_authorities

Belnet. (2020, February 24). Belnet and Smals team up in building infrastructure for European blockchain project | Belnet corporate. Retrieved May 31, 2020, from Belnet website: https://belnet.be/en/news-events/publications/press-review/belnet-and-smals-team-building-infrastructure-european

Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains Unchained: Blockcahin technology and its use in the public sector. In *OECD Working Papers on Public Governance*. https://doi.org/10.1787/3c32c429-en

BOSA. (2017). Development · Fedict/eid-mw Wiki · GitHub. Retrieved May 30, 2020, from GitHub.com website: https://github.com/Fedict/eid-mw/wiki/Development

Bouma, T. (2020, April 5). Canada: Enabling Self-Sovereign Identity . Retrieved April 24, 2020, from Medium.com website: https://medium.com/@trbouma/canada-enabling-self-sovereign-identity-efcfda2aa044

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101. https://doi.org/10.1191/1478088706qp063oa

Bryman, A. (2012). Social research strategies. *Social Research Methods*, pp. 3–25.

Bundesministerium für Wirtschaft und Energie. (2020). Self Sovereign Identity für Deutschland Ein Identitätsökosystem für natürliche Personen, Unternehmen und Dinge[Self Sovereign Identity for Germany: An identity ecosystem for natural persons, companies and things]. Retrieved April 28, 2020, from

Bundesministerium für Wirtschaft und Energie website: https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/SchaufensterSichereDigIdentProjekte/sdi-projekt_ssi.html

Cambridge Dictionary. (n.d.). SOVEREIGN | meaning in the Cambridge English Dictionary. Retrieved April 25, 2020, from https://dictionary.cambridge.org/dictionary/english/sovereign

Cameron, K. (2005). *The Laws of Identity*. Retrieved from www.identityblog.com

Canada.ca. (n.d.). Public Sector Profile of the Pan-Canadian Trust Framework Cadre de Confiance pancanadien | PCTF-CCP. Retrieved April 24, 2020, from Github.io website: https://canada-ca.github.io/PCTF-CCP/

Canadian Digital Service. (2019, May 12). Delivering digital services by 2025 . Retrieved April 24, 2020, from Government of Canada website: https://digital.canada.ca/roadmap-2025/

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, *15*(1), 5–25. https://doi.org/10.1111/j.1365-2575.2005.00183.x

CSAM. (n.d.). What is CSAM ? - CSAM.be. Retrieved February 28, 2020, from https://www.csam.be/en/about-csam.html

Deloitte. (2018). The smartphone takes the crown. Retrieved May 12, 2020, from https://mobile-consumer-survey.deloitte.be/2018_the-smartphone-takes-the-crown

Delta. (2019, July 5). TU Delft is working on a digital ID for your phone. Retrieved May 19, 2020, from TU Delft website: https://www.delta.tudelft.nl/article/tu-delft-working-digital-id-your-phone

Der, U., Jähnichen, S., & Sürmeli, J. (2017). *Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution*.

DESI. (2019). DESI — Digital Scoreboard - Data & Indicators. Retrieved April 24, 2020, from https://digital-agenda-data.eu/datasets/desi/visualizations

DG Digital Transformation. (n.d.-a). Authentic sources DG Digital Transformation. Retrieved May 31, 2020, from DG Digital Transformation (in Dutch) website: https://dt.bosa.be/nl/authentieke_bronnen

DG Digital Transformation. (n.d.-b). Dienstenintegrator | DG Digitale Transformatie. Retrieved May 31, 2020, from DG Digital Transformation website: https://dt.bosa.be/nl/gegevensuitwisseling

Digital Belgium. (2017). *Digital Belgium*.

Digital Canada. (2019a, June 11). British Columbia OrgBook - “Tell Us Once” via Blockchain and Self-Sovereign Identity . Retrieved April 24, 2020, from Digital Canada website: https://digitalcanada.io/bc-orgbook-tell-us-once/

Digital Canada. (2019b, June 19). ACE : Building Localized Self-Sovereign Identity Ecosystems . Retrieved April 24, 2020, from https://digitalcanada.io/ace-ssi/

Digital Canada. (2020, April 12). Anchors and Rails of a Digital Nation - Forging Self Sovereign Identity in the Age of the Blockchain. Retrieved April 24, 2020, from Digital Canada website: https://digitalcanada.io/forging-blockchain-ssi/

Doerk, A. (2020, April 12). The growth factors of self-sovereign identity . Retrieved April 22, 2020, from SSI Ambassador / Medium.com website: https://medium.com/@SSI_Ambassador/the-growth-factors-of-self-sovereign-identity-33aa3cc17ce7

Du Seuil, D. (2019). *European Self Sovereign identity framework*. Retrieved from https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

Dumortier, J., & Robben, F. (2010). *User and Access Management in Belgian e-Government*. https://doi.org/10.1007/978-3-8348-9363-5_9

Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security and Privacy*, *16*(4), 20–29. https://doi.org/10.1109/MSP.2018.3111247

eSSIF-Lab. (n.d.). eSSIF-LAB | eSSIF-LAB: HELP SHAPE A SAFE AND SECURE NEXT GENERATION INTERNET. Retrieved April 25, 2020, from https://essif-lab.eu/

European Commission. (n.d.). What does the General Data Protection Regulation (GDPR) govern? | European Commission. Retrieved March 2, 2020, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

European Commission. (2018a, April 10). European countries join Blockchain Partnership | Shaping Europe's digital future. Retrieved May 18, 2020, from https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

European Commission. (2018b, December 12). Trust Services and Electronic identification (eID) | Shaping Europe's digital future. Retrieved March 2, 2020, from https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

European Commission. (2019a). *Digital Government Factsheets - Belgium*.

European Commission. (2019b). eGovernment Benchmark 2019: trust in government is increasingly important for people | Shaping Europe's digital future. Retrieved May 31, 2020, from European Commission website: https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2019-trust-government-increasingly-important-people

European Commission. (2019c, May 20). SSI and eIDAS: a vision on how they are connected. Retrieved April 8, 2020, from https://ec.europa.eu/futurium/en/eidas-observatory/ssi-and-eidas-vision-how-they-are-connected-share-your-views

European Union. (2018). *Trends in electronic identification: An overview*. *1.1*(September).

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

Flemish Government. (2019). Blockchain on the Move | Departement EWI. Retrieved December 15, 2019, from http://www.innovatieveoverheidsopdrachten.be/en/projects/blockchain-move

FPS Home Affairs. (2017). *IBZ in brief*.

FPS Justice. (1983). Wet tot regeling van een Rijksregister van de natuurlijke personen [Law regulating a National Register of natural persons].

FPS Justice. (2004). Wet 2004-09-01/33. Retrieved from FPS Justice website: http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&caller=list&cn=2003032532&la=f&fromtab=loi&sql=dt=%27arrete royal%27&tri=dd+as+rank&rech=1&numero=1

FPS Justice. (2017). WET 2017-10-22/11. Retrieved from FPS Justice website: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2017102211

Gartner. (2019a). Identity and Access Management (IAM). Retrieved February 28, 2020, from Gartner Glossary website: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

Gartner. (2019b, October 8). Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact. Retrieved March 5, 2020, from https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact

GDPR.eu. (n.d.). What is GDPR, the EU's new data protection law? . Retrieved April 25, 2020, from https://gdpr.eu/what-is-gdpr/

Gemalto. (2019). *itsme® – the last word in Digital ID for Belgian citizens*.

Gisolfi, D. (2018, June 22). Self-sovereign identity: Unraveling the terminology . Retrieved April 28, 2020, from IBM website: https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-unraveling-the-terminology/

Goode, A. (2019). Digital identity: solving the problem of trust. *Biometric Technology Today*, *2019*(10), 5–8. https://doi.org/10.1016/S0969-4765(19)30142-0

Government of Catalunya. (2019, September 13). President Torra: “With IdentiCAT we will empower the citizen, because the power of the citizenry is at the center of the republican project” - Press room. Government of Catalonia. Retrieved May 8, 2020, from https://govern.cat/salapremsa/notes-premsa/377133/president-torra-amb-identicat-apoderem-ciutada-ciutadania-al-centre-del-projecte-republica

Hileman, G., & Rauchs, M. (2018). 2017 Global Blockchain Benchmarking Study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3040224

IAA. (2019). *Identity & Access Management (IAM)*.

Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. *Harvard Business Review* , (January-February), 118–127. Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain

ID2020. (2019). ID2020 | Manifesto. Retrieved May 6, 2020, from https://id2020.org/manifesto

InnoCells. (2019, February 12). Alastria launched to develop the blockchain ecosystem in Spain. Retrieved May 8, 2020, from Medium.com website: https://medium.com/innocells-insights/alastria-launched-to-develop-the-blockchain-ecosystem-in-spain-f26c86684a40

ISO/IEC. (2019). ISO/IEC 24760-1:2019(en), IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. Retrieved March 30, 2020, from https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en

ISO. (2013). ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary. Retrieved April 28, 2020, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

itsme®. (n.d.). Partners | itsme®. Retrieved April 6, 2020, from https://www.itsme.be/en/partners

itsme®. (2020, January 15). itsme® notified by Europe as a means of identification . Retrieved April 29, 2020, from https://www.itsme.be/en/blog/eidas-loa-high

Jøsang, A., & Pope, S. (2005). *User Centric Identity Management*. AusCERT Conference 2005.

Keil, J. (2019, September 5). Self-Sovereign Identity Systems: How Businesses Win From Letting Go of Customers’ Data | Hacker Noon. Retrieved May 19, 2020, from https://hackernoon.com/self-sovereign-identity-systems-how-businesses-win-from-letting-go-of-customers-data-1v3fz31n0

Kennedy, H. (2006). Beyond anonymity, or future directions for internet identity research. *New Media & Society*, *8*(6), 859–876. https://doi.org/10.1177/1461444806069641

Kondova, G., & Erbguth, J. (2020). *Self-Sovereign Identity on Public Blockchains and the GDPR*. https://doi.org/10.1145/3341105.3374066

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION*, *24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

Laurent, M., & Bouzefrane, S. (2015). Digital Identity Management. In *Digital Identity Management*. https://doi.org/10.1016/C2015-0-00282-9

Levin, K. A. (2006). Study design III: Cross-sectional studies. *Evidence-Based Dentistry*, *7*(1), 24–25. https://doi.org/10.1038/sj.ebd.6400375

Lyons, T., Courcelas, L., & Timsit, K. (2019). *Blockchain and digital identity* .

Mattila, J. (2016). *The Blockchain Phenomenon \textendash{} The Disruptive Potential of Distributed Consensus Architectures*. Retrieved from The Research Institute of the Finnish Economy (ETLA) website: http://hdl.handle.net/10419/201253

Maull, R., Godsiff, P., Mulligan, C., Brown, A., & Kewell, B. (2017). Distributed ledger technology: Applications and implications. *Strategic Change*, *26*(5), 481–489. https://doi.org/10.1002/jsc.2148

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018, November 1). A survey on essential components of a

self-sovereign identity. *Computer Science Review*, Vol. 30, pp. 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. *Cryptography Mailing List at Https://Metzdowd.Com*.

Neuman, W. L. (2011). *Social Research Methods: Qualitative and Quantitative Approaches* (7th ed.). Boston: Pearson.

OECD. (2020). *OECD Economic Surveys: Belgium 2020*. https://doi.org/10.1787/1327040c-en

Oliver, P. (2010). *Writing your thesis* (2nd ed., r). London : Sage.

Ølnes, S., & Jansen, A. (2018). *Blockchain technology as infrastructure in public sector: an analytical framework*. https://doi.org/10.1145/3209281.3209293

Ølnes, S., Ubacht, J., & Janssen, M. (2017, September 1). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, Vol. 34, pp. 355–364. https://doi.org/10.1016/j.giq.2017.09.007

PIO. (2019). Blockchain on the Move (BotM) | Innovatieve overheidsopdrachten. Retrieved April 28, 2020, from http://www.innovatieveoverheidsopdrachten.be/projecten/blockchain-move-botm

Preukschat, A., & Reed, D. (2019). *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials* (Manuscript). Retrieved from https://www.manning.com/books/self-sovereign-identity

Robins, E. M., & Foster, D. (1994). Social Identity versus Personal Identity: An Investigation into the Interaction of group and Personal Status with Collective Self-Esteem on Ingroup Favouritism. *South African Journal of Psychology*, *24*(3), 115–121. https://doi.org/10.1177/008124639402400302

Roelofs, F. (2019). *Analysis and comparison of identification and authentication systems under the eIDAS regulation*.

Ruff, T. (2018, April 24). The Three Models of Digital Identity Relationships. Retrieved April 28, 2020, from Medium.com website: https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186

Satybaldy, A., Nowostawski, M., & Ellingsen, J. (2020). *Self-Sovereign Identity Systems: Evaluation Framework*. https://doi.org/10.1007/978-3-030-42504-3_28

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*.

Schutte, M. (2016, October 26). self-sovereign-identity/Schutte-on-SSI.md at master · infominer33/self-sovereign-identity · GitHub. Retrieved May 19, 2020, from GitHub.com website: https://github.com/infominer33/self-sovereign-identity/blob/master/Schutte-on-SSI.md

Setsaas, J. E. (2020, January 1). 2019's identity buzzword- Self Sovereign Identity (SSI)- and my concerns with it. Retrieved April 29, 2020, from https://www.signicat.com/resources/2019s-identity-buzzword-self-sovereign-identity-ssi-and-my-concerns-with-it

Shavers, B., & Bair, J. (2016). Digital Identity. In *Hiding Behind the Keyboard* (pp. 187–202). https://doi.org/10.1016/b978-0-12-803340-1.00009-4

Siriwardena, P. (2017, March 27). The Role of Identity and Access Management in the Era of Digital Transformation. Retrieved February 28, 2020, from Medium website: https://medium.facilelogin.com/the-role-of-identity-and-access-management-in-the-era-of-digital-transformation-48a472ce3247

Sovrin Foundation. (2020). *Innovation Meets Compliance. Data Privacy Regulation and Distributed Ledger Technology*.

Statbel. (2019, June 17). Structure of the Population | Statbel. Retrieved March 4, 2020, from https://statbel.fgov.be/en/themes/population/structure-population

Statista. (2020, February 3). • Global digital population 2020. Retrieved March 4, 2020, from https://www.statista.com/statistics/617136/digital-population-worldwide/

Stevens, T., Elliott, J., Hoikkanen, A., Maghiros, I., & Lusoli, W. (2010). *The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies*. https://doi.org/10.2791/4851

Stokkink, Q., & Pouwelse, J. (2018). Deployment of a Blockchain-Based Self-Sovereign Identity. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1336–1342. https://doi.org/10.1109/Cybermatics_2018.2018.00230

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc."

Syed, H. (2019). *Power to The People: How Blockchain Based Digital Identity Can Empower Disadvantaged Individuals*.

Taylor, J. A., Lips, M., & Organ, J. (2008). *Identification practices in government: citizen surveillance and the quest for public service improvement*. https://doi.org/10.1007/s12394-009-0007-5

Thales. (2019). Digital Identity for Banks (federated, self sovereign). Retrieved April 28, 2020, from Thales website: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-identity

Thales. (2020). National ID cards in Belgium (2020 update) | Thales. Retrieved May 30, 2020, from Thales Group website: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/belgium

The World Bank. (2017). *PRINCIPLES ON IDENTIFICATION FOR SUSTAINABLE DEVELOPMENT: TOWARD THE DIGITAL AGE*. Retrieved from http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf

The World Bank. (2018a). *G20 Digital Identity Onboarding*. Washington, DC .

The World Bank. (2018b). ID4D Data: Global Identification Challenge by the Numbers. Retrieved February 19, 2020, from https://id4d.worldbank.org/global-dataset

The World Bank. (2019). *Identification for Development (ID4D) 2019 Annual Report* (pp. 1–25). pp. 1–25. Washington, D.C: World Bank Group.

TNO. (2019, December 16). EU Project eSSIF-Lab, aimed at faster and safer electronic transactions via the internet as well as in real life, open for start-ups and SMEs . Retrieved April 25, 2020, from https://www.tno.nl/en/about-tno/news/2019/12/essif-lab/

Tobin, A., & Reed, D. (2017). *The Inevitable Rise of Self-Sovereign Identity A white paper from the Sovrin Foundation*.

Toth, K. C., & Anderson-Priddy, A. (2019). Self-Sovereign Digital Identity: A Paradigm Shift for Identity. *IEEE Security and Privacy*, *17*(3), 17–27. https://doi.org/10.1109/MSEC.2018.2888782

Trautman, L. J. (2016). *Is Disruptive Blockchain Technology the Future of Financial Services?* Retrieved from http://ssrn.com/abstract=1271684;

TU Delft. (2018, June 7). TU Delft helps develop digital ID for use on your phone. Retrieved April 29, 2020, from https://www.tudelft.nl/en/2018/tu-delft/tu-delft-helps-develop-digital-id-for-use-on-your-phone/

Turner, D. W. (2010). Qualitative Interview Design: A Practical Guide for Novice Investigators. In *The Qualitative Report* (Vol. 15). Retrieved from http://www.nova.edu/ssss/QR/QR15-3/qid.pdf

Turner, J. C., Oakes, P. J., Haslam, S. A., & McGarty, C. (1992). Personal and social identity: Self and social context. In *psychology.anu.edu.au*. Retrieved from http://psychology.anu.edu.au/files/Abstracts-Presentations-1-Personal-and-Social-Identity-Self-and-Social-Context-Princeton-1992.pdf

United Nations. (n.d.). SDG Indicators — SDG Indicators. Retrieved February 19, 2020, from https://unstats.un.org/sdgs/metadata/?Text=&Goal=16&Target=16.9

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). *Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology*. Retrieved from http://arxiv.org/abs/1904.12816

van Dongen, W. (2019). *The potential of blockchain technology for the public sector*. Leuven : KU Leuven. Faculteit Economie en Bedrijfswetenschappen.

Van Wingerde, M. (2017). *BLOCKCHAIN-ENABLED SELF-SOVEREIGN IDENTITY An exploratory study into the concept Self-Sovereign Identity and how blockchain technology can serve the fundamental basis Self-Sovereign Identity Management View project PhD-Inter-organizational governance thro* (Tilburg University, School of Economics and Management). https://doi.org/10.13140/RG.2.2.17693.82406

Vignoles, V. (2017). *Identity: Personal AND Social*.

W3C. (2020, April 21). Decentralized Identifiers (DIDs) v1.0. Retrieved April 27, 2020, from https://w3c.github.io/did-core/

Wagner, K., Némethi, B., Renieris, E., Lang, P., Holst, E., & Eric, B. (2018). *Self-sovereign Identity: A position paper on blockchain enabled identity and the road ahead*.

Walliman, N. (2017). *Research Methods: The Basics: 2nd edition*. Retrieved from https://books.google.be/books?id=M6QzDwAAQBAJ

Wang, F., & De Filippi, P. (2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion . *Frontiers in Blockchain*, Vol. 2, p. 28. Retrieved from https://www.frontiersin.org/article/10.3389/fbloc.2019.00028

Wolfond, G. (2017). A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review October 2017 (Volume 7, Issue 10)*, *7*(10).

Yin, R. K. (2018). Case study research and applications : design and methods. In *SAGE Publications* (6th ed., Vol. 6). Los Angeles.

Yu, F. R., Liu, J., He, Y., Si, P., & Zhang, Y. (2018). Virtualization for Distributed Ledger Technology (vDLT). *IEEE Access*, *6*, 25019–25028. https://doi.org/10.1109/ACCESS.2018.2829141

Yuan, Y., & Wang, F. Y. (2018). Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *48*(9), 1421–1428. https://doi.org/10.1109/TSMC.2018.2854904

Zambrano, R., Young, A., & Verhulst, S. (2018). *Connecting Refugees to Aid through Blockchain-Enabled ID Management: World Food Programme's Building Blocks*.

Zviran, M., & Erlich, Z. (2006). Identification and Authentication: Technology and Implementation Issues. *Communications of the Association for Information Systems*, *17*, 90–105. https://doi.org/10.17705/1CAIS.01704

Zwitter, A., Gstrein, O., & Yap, E. (2019). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the 'Self-Sovereign' Individual. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3454513

Zyskind, G., Nathan, O., & Pentland, A. '. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops*, 180–184. https://doi.org/10.1109/SPW.2015.27

Appendix

A Interview partners

Interview transcripts can be provided upon request.

Interviewee	Expertise domain	Organisation	Position
A	Public sector / Blockchain / Innovation	DG DT BOSA	Innovation Manager
B	Public sector / Digital identity	IAA of DG DT at BOSA	Senior IT Manager
C	Public sector / Digital identity	IAA of DG DT at BOSA	IAA Domain Manager
D	SSI / European level	ESSIF	Convenor
E	Private sector / Digital identity	Belgian Mobile ID	Spokesperson
F			COO
H	Research / Blockchain	Smals	Cryptography and blockchain researcher
G	Private sector / SSI	Jolocom	Partnerships Developer
I	Private sector / SSI / Research	Lissi project at Main Incubator	Researcher at Lissi project
J	Public sector / Digital identity	IAA of DG DT at BOSA	Service expert
K	SSI / European level	TrustCore	External expert
L	Private sector / Innovation	BallistiX	CEO

B Interview guide

Thank you for participating in this interview. My name is Stanislav Mahula, and I am a final year student of Erasmus Mundus programme in public sector innovation and e-governance. This interview is a part of my master thesis research dedicated to revealing the opportunities and challenges of implementing Self-sovereign identity in Belgium. It

will take around 45 minutes, and now I would like to ask your permission to record the conversation for my personal use, I will also anonymise the sensitive data.

The following blocks of questions were asked depending on the profile of the interviewee, each aiming at uncovering different aspects of the RQ.

WARM-UP QUESTIONS

1. What is your experience in the field of identity management?

BELGIAN IDENTITY MANAGEMENT

1. What is the overall attitude towards new technologies within the government?
2. What were the drivers that lead to introducing new changes to the Belgian mobile ID?
3. What aspects of the current ID model are advantageous?
4. What is the downside of the existing ID model in Belgium?
5. What is the citizens' attitude towards their digital identity?
6. What is the experience of using services online?
7. Are there any projects to introduce new changes to this model?
8. What is anticipated in the future regarding identity management?

Blockchain technology

1. What is the Belgian government experiences with Blockchain?

Self-sovereign identity

2. Are you familiar with the concept of SSI?
9. Many countries already started to investigate on SSI (Netherlands, Spain, Germany). Are there any considerations to include SSI in the agenda? If no, why not?
10. Do you believe that adding some SSI features positively impact identity management?
11. How can legal challenges be addressed?

Self-sovereign identity

1. What is your experience with SSI?
2. What leads projects and organisations to embed SSI?
3. Is SSI necessarily linked to blockchain technology?
4. What costs are associated with maintaining an SSI system?

a. What is the fee model using the SSI?

b. What other costs should be expected for maintaining such a ledger and SSI system in general?

SSI in the public sector

5. How would you describe the maturity of SSI to be implemented on the state level?
6. Data usage in commercial companies and government is different; governments need data about citizens to function. How can SSI work within the government?
7. Was there a call from governments to cooperate on creating SSI-bases solutions?

a. Why would the public sector want to shift to the SSI?

8. In your opinion, what benefits can SSI bring to the public sector?
9. Security issues remain essential. In the SSI model, where the credentials would be stored?
10. What experience can SSI provide in terms of security and usability?
11. What features of SSI can be harmful?

ADDITIONAL QUESTIONS

12. What do you mean by that?
13. Anything else you would like to add?

C Codebook

NAME	DESCRIPTION	FILES	REFERENCES
BELGIAN CONTEXT	Insights from the Belgian public sector	9	239
Current state of affairs	Insights on the organisational situation, the attitude and experiences with technology	9	133
Citizens' experiences	What are the citizens' experiences with the public sector services and identity management?	5	15
Conservative culture		4	12
Innovation attitude		9	89
Attitude for new tehnology	What is the attitude of the public sector bodies to new technology	5	20
Attitude for SSI		8	20
Blockchain-related		5	42
Blockchain attitude	What is the attitude of the public sector bodies to the blockchain technology	4	27
Blockchain initiatives		1	6
BOTM	Blockchain on the Move project-related opinions	3	9
Initiatives on SSI	Experiences with the SSI within the identity management of Belgium	3	7
Organisational reality		6	17
ID systems		7	73
Benefits of the current system	What experts think are the strong sides of the current identity management system of Belgium	6	16
Drawbacks of the current system	What experts think are the downsides of the current identity management system of Belgium	5	26
itsme	Discussions about the big player in identity market of Belgium	5	31
Governance of itsme		1	4

NAME	DESCRIPTION	FILES	REFERENCES
Importance of branding		1	4
itsme experience		3	7
itsme vs SSI		1	9
Next steps	The plans of the Belgian government to move forward	5	33
Future perspectives		4	24
MyProfile		2	2
Towards mobile	Opportunities of mobile identity	3	9
CHALLENGES OF SSI	The summary of all barriers that does not allow having the SSI implemented	10	133
Financial	What costs are associated with maintaining the SSI and who should pay for it?	3	5
Legal	How SSI can be compliant with the existing legal base	6	19
eIDAS		5	12
GDPR		4	7
Organisational	Organisation and institutions-related factors that can occur on the way of SSI adoption	10	52
Data capitalism	How could government protect citizens from giving their data to big companies	2	5
Governance and standards of SSI		7	14
Government's role	Role of the government in the SSI ecosystem	7	15
Political resilience		4	8
Willingness to change		6	10
Technical	Factors dependent on technology and infrastructure	8	29
Blockchain-related	Discussing on what is the role of blockchain in achieving SSI	7	20

NAME	DESCRIPTION	FILES	REFERENCES
Blockchain is not necessary		5	10
Storing data on the ledger		5	10
Wallets		3	3
Wicked SSI		4	6
User-related	Factors related to the users, their behaviour and interest	9	28
Acessibility		2	3
Competenses		4	7
Interest		3	3
Trust to technology		3	4
Usability vs security		6	11
FUTURE STEPS	Aspects to consider for the future work	9	49
Active contributors	Players in today's market and their role	3	11
ESSIF		2	4
Private companies		3	7
Collaboration is needed	How various stakeholders can enable SSI	1	1
Government context	A role of the government in adopting the SSI	5	10
Push from government		2	6
Visionary people		3	4
Push from Europe	The EU could become a driver towards making SSI possible	5	11
SSI development	Directions where SSI needs to develop towards	9	16
Identity custodians		4	6

NAME	DESCRIPTION	FILES	REFERENCES
OPPORTUNITIES FOR SSI	The foreseen improvements that SSI can bring to the public sector	9	70
Democracy	How can SSI facilitate creating a more democratic society	5	12
Control over data		2	2
Less surveillence		3	4
More democratic states		3	6
Economic	What economic benefits can be expected from SSI	3	4
Information quality and better processes	Experts' opinions on how SSI can facilitate better processes in public administration and improve data quality	7	36
Better data quality		6	28
Better processes		3	7
Use-cases	Possible use-cases where the SSI can be implemented	6	18

Declaration of Authorship

I hereby declare that, to the best of my knowledge and belief, this Master Thesis titled "Opportunities and challenges for self-sovereign identity in the public sector: a case of Belgium" is my own work. I confirm that each significant contribution to and quotation in this thesis that originates from the work or works of others is indicated by proper use of citation and references.

Brussels, 02 June 2020

Stanislav Mahula

Consent Form

for the use of plagiarism detection software to check my thesis

Name: Mahula
Given Name: Stanislav
Student number: r0728468
Course of Study: Public Sector Innovation and eGovernance
Address: Verboekhaven 5, 1210 Brussels, Belgium
Title of the thesis: Opportunities and challenges for self-sovereign identity in the public sector: a case of Belgium

What is plagiarism? Plagiarism is defined as submitting someone else's work or ideas as your own without a complete indication of the source. It is hereby irrelevant whether the work of others is copied word by word without acknowledgment of the source, text structures (e.g. line of argumentation or outline) are borrowed or texts are translated from a foreign language.

Use of plagiarism detection software. The examination office uses plagiarism software to check each submitted bachelor and master thesis for plagiarism. For that purpose, the thesis is electronically forwarded to a software service provider where the software checks for potential matches between the submitted work and work from other sources. For future comparisons with other theses, your thesis will be permanently stored in a database. Only the School of Business and Economics of the University of Münster is allowed to access your stored thesis. The student agrees that his or her thesis may be stored and reproduced only for the purpose of plagiarism assessment. The first examiner of the thesis will be advised on the outcome of the plagiarism assessment.

Sanctions. Each case of plagiarism constitutes an attempt to deceive in terms of the examination regulations and will lead to the thesis being graded as "failed". This will be communicated to the examination office where your case will be documented. In the event of a serious case of deception the examinee can be generally excluded from any further examination. This can lead to the exarticulation of the student. Even after completion of the examination procedure and graduation from university, plagiarism can result in a withdrawal of the awarded academic degree.

I confirm that I have read and understood the information in this document. I agree to the outlined procedure for plagiarism assessment and potential sanctioning.

Brussels, 02.06.2020

Stanislav Mahula