Universiteit Leiden

ICT in Business and the Public Sector

On the internet, no one knows you are a citizen.

Name: Sebastiaan Kommers
Student-no: S1844385

Date: 08/04/2019

1st supervisor: Drs. Peter van Veen
2nd supervisor: Dr. Jelmer Schalk

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

This thesis was submitted in partial satisfaction of the requirements for the degree Master of Science in ICT in Business and the Public Sector.

Acknowledgements

Writing this thesis was quite a change from coursework at Leiden University's Snellius building together with fellow students, but it was a very enjoyable experience. My sincere thanks goes out to all the kind and helpful employees of the Ministry of the Interior and Kingdom Relations, they really made me feel welcome. They were always available to guide me and answered the questions I had for them concerning my thesis, thanks to them I have learned a lot about the functioning of the Dutch government. I have come to respect individual expertise of the civil servants and their drive to make society better for everyone.

My special gratitude goes out to Jorgen Bogaard and Wouter Welling: They have supervised me in their role in the Ministry during my progress and provided me with knowledge, insights, revisions, laughs and critical suggestions. Without them, I surely would not have finished this thesis. In particular, I want to thank them for enabling me to accompany them to the Dutch Permanent Representation, DG Connect of the European Commission and the Joint Research Centre in Brussels. That was an unexpected and brilliant experience, while it also helped with my thesis. Lastly, I want to thank fellow (part-time) student Wouter van Steenbergen for allowing me to experience his daily work as ICT advisor within the government.

However, most importantly of all I want to thank all friends and family that have always been there for me when I needed some distraction or advice during my studies. Without them, I would have never completed this epic task.

I wish the reader of this thesis much knowledge and inspiration,

Sebastiaan Kommers

Abstract

In this thesis, the reader will learn about the process to create a strategy and governance framework for an upcoming innovative technology called Self-sovereign identity. This new technology makes new forms of digital identity possible that can give citizens both increased control and increased privacy over their identities. For answering this question, concepts of self-sovereign identity tools were compared. The technology and its technical and functional aspects were also explored in a theoretical review of digital identity evolution. After this, interviews with experts followed that provided valuable insights into the role of the government in SSI: Without governance by a party that has no commercial interest in the technology, this technology might end up going in the wrong direction.

After finishing and coding these interviews, a conceptual strategy and governance framework was developed that was refined further by interviewing internal policy experts. The resulting framework is also the artefact that provides an answer to the main research question: 'How can different self-sovereign identity technology developments be governed and accelerated based on societal values?' and as such completes the design science approach this research takes.

Key findings are in the form of a possible timeline for self-sovereign identity adoption within the public sector and a set of actions the government can take to change the direction of SSI development. There is also a set of strategies and public values to continually govern and discuss with stakeholders in this exciting digital identity technology.

Keywords: Public Sector, Digital Identity, Design Science, Self-sovereign Identity, IDEMIX, Attribute Based Credentials, Governance, Digital Strategy, eID, Future technology.

List of Abbreviations

ABC's – Attribute based credentials, see section 1.5.6 for an in-depth explanation.
BC3 – The Dutch blockchain coalition is a cooperation of research and business to research and develop blockchain solutions in The Netherlands.
CEF (call) – Connecting Europe Facility call for funding, European union research projects.
DQ – Data Quality, a measure of how 'reliable' a set of information is.
eIDAS – The European regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market.
eID – An electronic form of identification, usually in national context as a digital government identity.
GDPR – The General Data Protection Regulation, a May 2018 EU-wide privacy regulation with widespread implications.
ICAO – International Civil Aviation Organization, part of the United Nations. Sets passport standards.
IDEMIX – IBM Identity Mixer. A cryptographic protocol enabling Attribute Based Credentials by IBM research.
SSI - Self-sovereign Identity.
SSIF – Self Sovereign Identity Framework, a standardization and research effort by research agency TNO.
SQ(A) – Software Quality (Assurance)
TNO – The Netherlands Organization for Applied Scientific Research. A national science institute.

Index

Acknowledgements 1

Abstract 2

List of Abbreviations 3

1. Research Introduction 3

1.1 Introduction to the topic 4

1.2 Problem Statement 7

1.2 Research Questions 9

Main question 9

Sub-questions 10

Partial sub-questions 10

1.3 Scope definition 11

1.4 Research Purpose 11

1.4.1 Public sector relevance 12

1.4.2 Relevance for Academia 12

1.5 Research Methodology 13

1.5.1 The Design Science methodology 13

1.5.2 Research structure 15

1.5.3 The Relevance Cycle (conceptual foundations) 16

1.5.4 The Rigor cycle (validation of concepts) 17

1.5.5 The Design cycle (finalizing and testing) 17

1.5.6 Expected Research Outcomes 17

2. Theoretical review 18

2.1 Previous research literature on self-sovereign identity 18

2.1.1 Electronic Voting (e-Voting) and SSI 22

2.1.2 Results of prior research projects 22

2.1.3 Digital Identity as a concept 24

2.1.4 Digital Identity as the synergy of several concepts 25

2.1.5 Self-Sovereign digital identity 26

2.1.6 Verifiable claims and existing architectural constraints 27

2.1.7 Functional SSI considerations 28

2.1.8 Technologic concepts of SSI 29

2.1.9 Post-Quantum encryption safety 30

2.1.10 Conclusion on state of research concerning Self-sovereign Identity 30

2.2 Existing self-sovereign identity concepts 31

2.2.1 Evaluation criteria 31
2.2.2 Conclusion on software quality 34
2.3 Review of existing SSI concepts 35
2.3.1 The Sovrin Trust Network 35
2.3.2 uPort: An Etherium blockchain-based identity 36
2.3.3 Dappre: subscription update model identity 38
2.3.4 I Reveal My Attributes (IRMA) 40
2.3.5 Conclusions on the state of SSI software 43
3 First round expert interviews and conceptual framework 45
3.1 Interviews and expert insights 45
3.1.1 Interview targets and persons interviewed 45
3.1.2 Interview questions 46
3.1.3 Expert opinions on the role of the government in Self-sovereign identity 47
3.2 Interview coding strategy and results 49
3.2.1 Transcription 49
3.2.2 Method of open coding 49
3.2.3 Coding categories resulting in dimensions for the framework 50
4 Design cycle of the framework (finalization) 51
4.1 Conceptual version of the SSI public value framework 51
4.2 Second round interviews: improving the concept framework 55
4.2.1 Digital Identity Strategy 56
4.2.2 Legal and eID-law influences on SSI 57
4.2.3 Public Values 57
4.2.4 Innovation and public-private cooperation 58
4.2.5 Public Sector Governance and Frameworks 59
4.3 Final version of the governance framework 59
4.3.1 Strategic outlook 60
4.3.2 Governance: Manage based on the Public Values 62
4.3.3 Three moments of interaction with SSI development and possible actions. 64
5 Conclusions and discussion 66
5.1 Conclusions of the research 66
5.2 Discussion 67
5.3 Limitations and possible future research 67
List of Cited Works 69
List of Attachments 73

1. Research Introduction

In this chapter, we first explore the topic of this thesis by reviewing the history of digital identity. The scope will be defined after that. This scope definition serves to define what is in the research scope and what is outside of it, as the concept of digital identity is very broad. After doing so, we will introduce the problem of the research and why it is relevant to society and the government. Then in the fourth part of this chapter, purpose and relevance of the research will be discussed. Lastly, in the fifth part of this chapter, the main theoretical concepts of this thesis will be reviewed.

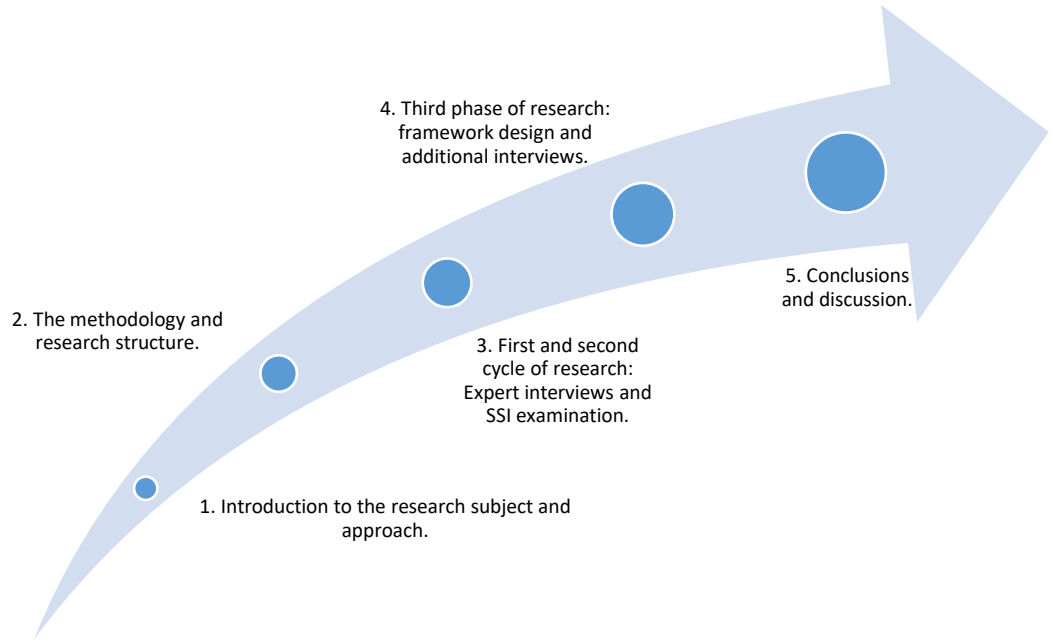

Fig. 1: Chapters of this thesis.

In **chapter 1**, the reader is introduced to the research and subject area. In **chapter 2**, the research methodology is explained in more depth and literature and existing concepts are reviewed. In **chapter 3**, the first round of interviews with experts and subsequent analysis are presented to the reader. Then, in **chapter 4**, the governance framework is conceptualized and refined with help of policy subject experts. Lastly, in **chapter 5**, the results of the thesis are discussed and a conclusion reached.

1.1 Introduction to the topic

Since the beginning of the 'digital world' we call the internet, there has been a fundamental difference with the physical world: There is a high degree of uncertainty about identity claims while communicating and exchanging information with others. In 1993, a famous cartoon in the magazine 'The New Yorker' penned by Peter Steiner visualized this situation.

Fig. 2: The famous cartoon about internet anonymity. (Steiner, 1993)

As this cartoon so befittingly illustrates, anyone can pretend to be anything on the internet. Interestingly enough the cartoon did not have a purpose of capturing the *internet zeitgeist* of that period by the illustrator, but still ended up doing so to great effect.[1] In the physical world, a claimed aspect of your identity (a *claimed* identity attribute) such as - age or nationality - can often be verified to some degree of reliability by simply using any our senses to validate a paper document such as the passport.

To the contrary, the digital realm is a chaotic situation where it is often not clear who someone *really* is at all. Some systems exist to identify and authenticate citizens such as DigID in The Netherlands, but these are more a centralized identity system for the public sector than a digital identity holder.[2]

As (Cameron, 2005) explains, "The Internet was built without a way to know who and what you are connecting to, a patchwork of identity one-offs. Since this essential capability is missing, everyone offering an Internet service has had to come up with a workaround. It is fair to say that today's Internet, absent a native identity layer, is based on a patchwork of *identity one-offs*."
While Cameron made this statement a good decade ago, it still is largely true today. Digital Identity has not moved much towards homogeneity at all during the years that followed his article.

The number of accounts a person has online can measure this fragmentation of digital identity. Estimates vary, but a 2015 study based on scanning the e-mail boxes of 20.000 persons found that that they have on average 95 (France) to 130 (USA) accounts on the internet alone.

[1] http://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html
[2] https://www.digid.nl/en/about-digid/

This study also estimates that in 2020 the number of 'forgotten passwords' per person would average 22 while in 2025 they estimate it will average 46. (Le Bras, 2015) Thus, it can be said that this is a serious concern for the future of digital identity and privacy.

When seen from a historical perspective, digital identity has evolved through four distinct phases. (Allen, 2016) (Gartner, 2016) During the start of the public internet in the 80's and 90's, a *centralized identity* was the internet standard where organizations such as The Internet Corporation for Assigned Names (ICANN)[3] acted as digital identity agencies. This centralized identity on the internet to few companies, leading to an oligarchy.

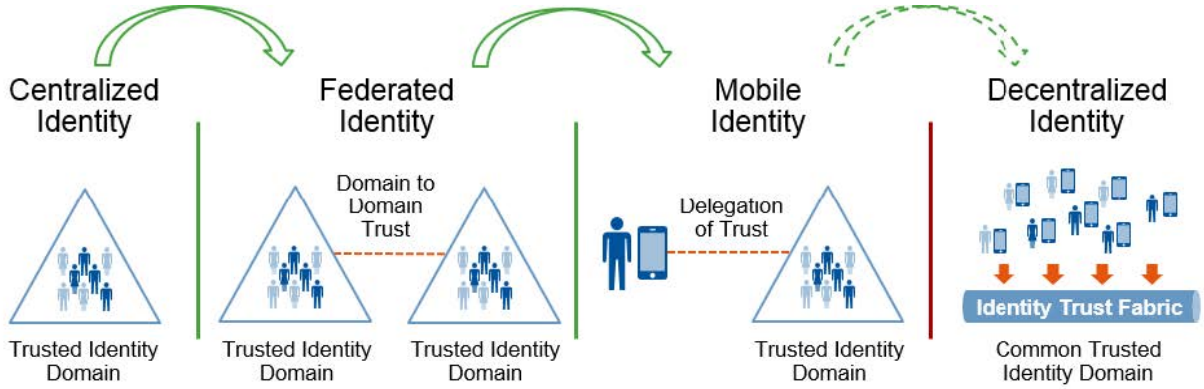

Fig. 3: The evolution of digital identity management. (Gartner, 2016)

At the start of the 21st century, *federated identity provisioning* appeared as an alternative to this centralized identity. A notable early example is Microsoft Passport, a single sign-on and wallet service that used the MSN credentials of users to provide them access to third parties. (Microsoft, 1999)

Later, this concept was refined using the concept of *user centricity* to refine the experience of authentication. (Norman & Draper, 1986) This led to a more mobile identity where Social media accounts are useable to identify on the internet and share attributes directly from those sources. Notable examples are OpenID, Google and Facebook connect. An Issue here for the user is that, while they have control over the content and attributes shared, there is still total reliance on the party providing the service. While it is federated, within that federation it is centralized.

When Facebook, for example, is in doubt about the authenticity of an account, a scanned photo ID is required. Not complying with this request means losing access to the Facebook account and by effect, other services that use the Facebook identity as the identity source. Tracking across the web where a certain user authenticates is also a privacy concern while using such identity management forms. For example, Facebook actively tracks its users across the web to become a more targeted advertising platform.[4] One might even say that privacy is the payment for the ease these single sign on platforms deliver to the citizen.

This also leads to a situation where it is no longer possible to use the (anonymous) identity the user wants or needs, due to the restrictions Facebook places on using their social network: 'Consider political dissidents who use a pseudonym to protect their families and livelihoods on the ground.

[3] The Internet Corporation for Assigned Names and Numbers handles (amongst other things) the domain naming system of the World Wide Web. See: https://www.icann.org/

[4] For example with the 'tracking pixel' https://nos.nl/artikel/2226957-aantal-zorgsites-stopt-met-tracking-pixel-van-facebook.html (in Dutch)

Providing Facebook with additional personal information and context to explain the use of a pseudonym is potentially risky, especially if Facebook collaborates with the government in question. (Galperin & Ben Hassine, 2015)

Fig. 4: ID proofing use cases. (RvIG, 2018)

Identity attributes are most frequently used in the sense of proofing identity such as authentication or Know Your Customer compliance. The Dutch agency responsible for governmental identity of citizens such as the base registry and physical identification methods is aware of many interactions for ID proofing. (Fig. 4)

Giving citizens 'a greater role in managing their own personal information is an explicit goal of the 2017-2021 agreement of the Dutch government coalition. (Rutte, Buma, Pechtold, & Segers, 2017, p. 11) Self-Sovereign Identity to some degree could contribute to this goal.
The field of digital identity is an evolving concept that is widely discussed in conferences and workshops globally by the IT community. [5]

A current and on-going development in this domain of digital identity is the concept of *self-sovereign identity*, which aims to put the user in control of its digital identity by giving back complete ownership and control. This also includes empowering users to share 'just enough' information, using new concepts of Self-sovereign identity, like the attribute-based credentials: which allows minimal disclosure. The concept of attribute-based credentials is explained in section 1.5.6 of this thesis. Such a new technology is the next logical step in the evolution of digital identity management towards a decentralized identity fabric or ecosystem as shown in figure 3.[6]

[5] The Internet Identity Workshop (California, USA) and IDNext (Europe) are large conferences on this subject.
[6] In paragraph 1.5 of this document, the exact definitions of the research concepts will be defined.

It is worth noting that this concept is relatively new, therefor limited academic literature on the subject of self-sovereign digital identity exists, a Google Scholar search for "Self-sovereign identity" only yields 55 results (6th of February 2018). One of the Academic goals of this thesis is to advance knowledge in the field of self-sovereign digital identity, by gaining insight in the possible societal success factors. Another research goal is to give the government more direction on how to approach this subject and accelerate it in a beneficial direction for society.

Over time, self-sovereign identity could lead to the end of the age of 'not knowing who someone really is' on the internet. It will become possible to exchange just enough verified identity attributes for a transaction, benefitting both trust in the validity and privacy due to the minimal disclosure. This new level of digital trust can enable new economic models to flourish and change the way we interact digitally. To properly interact with this development, the Dutch Government needs a method of valuation for this new form of identity: What are the existing technologic advances in this field and the risks and benefits for society? This thesis aims to provide a framework to select an interaction with this on-going evolution from the unique government perspective.

1.2 Problem Statement

A consistent identity across the digital domain does not exist; a different location will often require a different digital identity. As such, a citizen might have a 'Facebook identity', 'Google identity', 'Government eID identity' and many more. Figure 5 shows this 'patchwork' of identities overlapping. These different identities might contain vastly different attributes and claims that do not necessarily claim the same for each attribute. Verifying claimed attributes for a digital citizen is difficult and often leads asking for a scan of a photo id or other physical proof of identity as a digital equivalent does not exist.

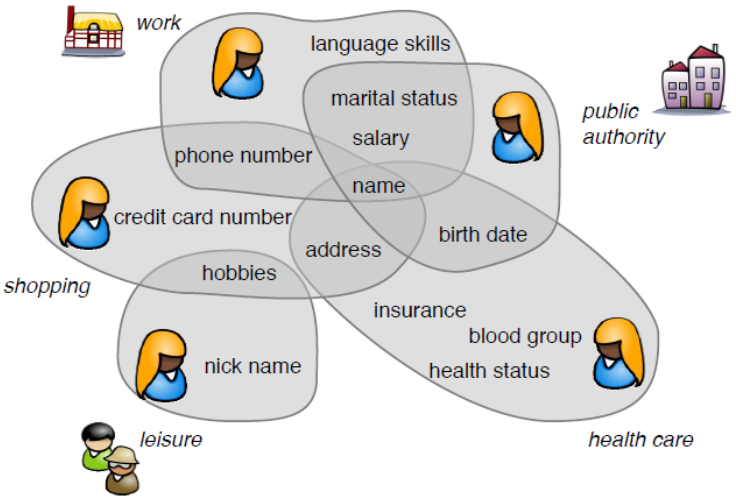

Fig. 5: A patchwork of different digital identities. (Camenisch, 2016)

Aside from the 'double work' and opportunities for fraud there are distinct privacy and security issues for citizens. Re-use of passwords is very problematic: research shows that 43% to 51% of users re-use passwords on multiple sites. Worse still, passwords that users do transform between sites are often still easy to guess. Often the same basic transformations are employed by users to 'renew' them, such as simply adding a different number to the end. That results in easily guessed passwords across the digital presence of the user, when the password database of just one website is compromised. (Das, Bonneau, Caesar, Borisov, & Wang, 2014) Increasing the risk of a hack or data breach.

When such a data breach happens, the citizen's private information such as birthdate, address and credit card details are exposed to an often malicious, third party. A notable example is the massive data theft of social security numbers from credit scoring agency Equifax.[7]

As such, a decentralized and non-traceable digital identity that is securely kept by the identity owner itself, with strong (two-factor or biometric) authentication for the identity holder can lead to higher account security.[8] This is in the advantage of citizens and businesses as they suffer reputational damage and incur fines. The government is responsible for physical identification methods of citizens, such as a passport and thus would be a logical party to provide a re-usable digital identity for citizens.

Advancement of a homogenous digital identity is also a government goal in different countries. The 'eIDAS' European regulation requires member states to accept other states' national 'digital identification' and as such puts this on the national agendas. (European Commission, 2014) Compliance with this means both creating an interoperable national digital identification and creating governmental compatibility with foreign digital identities that adhere to the eIDAS standards.

The Estonian 'ID-kaart' national digital identity smartcard proves that it is possible for governments to offer a versatile digital identity to citizens; Estonian citizens use it for many purposes not directly government-related, such as using public transit and doing business. Currently, for a fee, it is even possible to become an 'e-resident' of Estonia and receive a personal eID card at an embassy to do business digitally. (Estonian Republic, 2018) While this is not yet a true self-sovereign digital identity, it shows that putting citizens in control can work. [9] Germany is also working on a smartcard eID with attribute-based credentials that could in the future become self-sovereign in nature. (Alpár, 2015, p. 132)

With this development ongoing and the technology showing some promise in helping public values such as privacy, the Dutch government will eventually have to take a position on how to interact with self-sovereign identity. This can only be accomplished when there is a clear overview of what exactly the technologic state of affairs is, what citizens and municipalities want in their digital identity interactions and how the Dutch government can play a role in that. Solving these issues was the goal of this thesis, resulting in a framework for strategy and governance of Self-sovereign identity. That framework can help the government in finding a position and long-term goals to shape the interaction with this evolving technology.

[7] http://www.zdnet.com/article/equifax-confirms-more-americans-were-affected-by-hack-than-first-thought/
[8] Two Factor authentication adds a second layer of security, such as a mobile phone token. Cracking the password alone will thus not grant access to the user's identity.
[9] Of the ten norms for self-sovereignty (Allen, 2016) especially the self-control is only partially at the user: The eID card is controlled by the Estonian Government alone. The same goes for the German eID.

1.2 Research Questions

In the following section, the main and sub-questions of the research will be introduced to the reader. Figure 6 shows the connection of our main- and sub-questions in a diagram. The description of the question in the diagram is only a summary of the research question, for purposes of legibility.

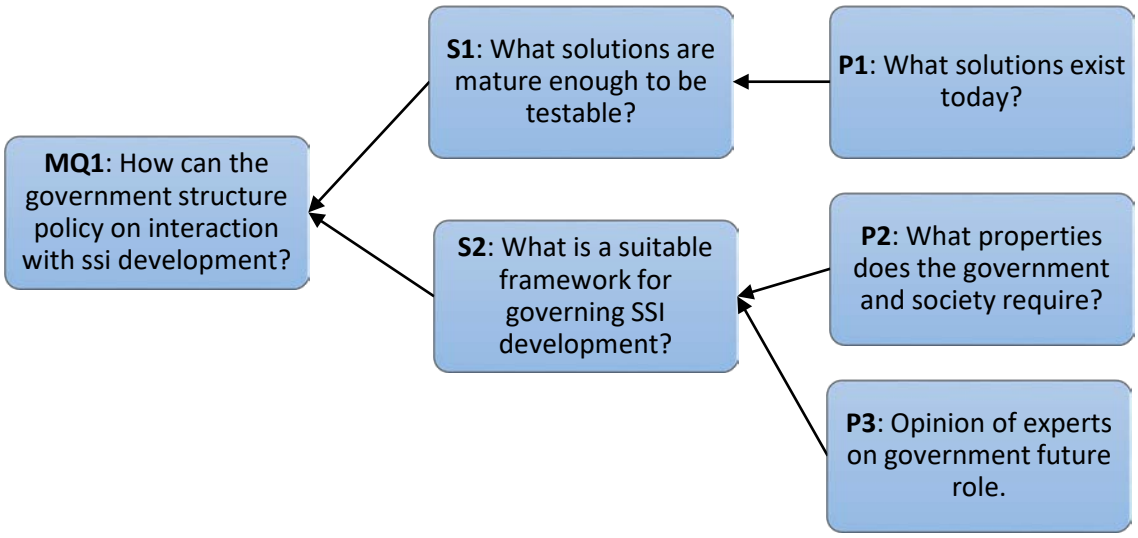

Fig. 6: Diagram of main and sub-questions. Note that they are shortened in this overview.

Main question

MQ1: How can the government structure policy on interaction with the on-going development of self-sovereign identity?

The Dutch government is searching for its correct role in the future of self-sovereign identity. The technology can potentially be beneficial for society by improving digital privacy, handing control back to the citizen, improving base registry data quality and making identity theft harder to name a few examples. There are many more potential benefits for society. Potentially it could also introduce societal dangers by reducing the possibility of oversight and handing valuable data to vulnerable citizens. However, as of yet there is no complete picture of what the state of the technology is and how the government can decide on how to interact with SSI in the future in a structured way in the form of a framework and strategy model.

The final answer to this question is two-fold. On one side, there will be a list of testable and hopeful SSI concepts based on sub-questions **S1** and **S2** together with a method to measure suitability of solutions. Hands-on experience with the technology will provide policy makers and organization's insight into the possibilities and challenges implementing SSI into societal interactions. There will also be a governance framework with a set of possible actions for the government. These actions can serve to accelerate and manage the development of this socio-technical concept.

Sub-questions

S1: What SSI solutions are mature enough to be testable and/or have been tested in an International Public Sector context?

The selection of SSI solutions that exist currently (**S1**) serves as the input for this question. It is answered in part 2.2 of this thesis. By using a conceptual benchmark and literature search for self-sovereign identity experimentation in an international context. It is an important question for the upcoming policy lab: What solutions can we actually test in simple use-cases with the citizen?

S2: What is a suitable framework for governing the development of digital identity holders based on societal values?

Based on the input of the rigor cycle and the results of questions **P2** and **P3** a governance framework has to be designed and improved to create the basis for answering **MQ1**. This iterative process is documented in chapter 4 of this thesis.

Partial sub-questions

P1: What SSI solutions or concepts exist today and what are their functional properties?

This partial sub-question is discussed in section 3.1 of this thesis. This question is closely related to **S2** and as such is relevant for the upcoming policy lab. There was no complete overview of self-sovereign identity solutions and their status available for the Ministry upfront. The definition in section 1.5 aims to give policymakers and interviewees a definition of the concepts behind this new form of identity. This sub question will be answered using a combination of desk research and literature review. It is also related to sub question two, which continues on assessing the found and indexed SSI solutions or concepts.

P2: What functional and technical characteristics do the Dutch government and other stakeholders require from a self-sovereign identity holder?

This partial sub-question answers the technical part of the framework. Based on the expert interviews with SSI experts, functional and technical characteristics (public values, requirements) can be identified. These are refined with internal expertise in the second round of interviews with internal policy experts. See sections 2.2, 2.3 and chapter 4.

P3: What is the opinion of experts on the SSI and the future role of the Dutch government in the SSI socio-technological process?

This partial sub-question is answered in parts 3.3 and 3.4 of this thesis. The persons interviewed were asked what their professional opinion was. This was then validated during the design of the iterative governance framework using interviews with policy experts. The goal is to propose a number of possible roles the government could take, not select one to be used.

1.3 Scope definition

Scope of research can be defined by categorizing in-scope and out-of-scope aspects based on the research objectives. Legal aspects such as GDPR compliance of SSI tools are defined as out-of-scope, as this is not a legal thesis. While the research does look at the international perspective of self-sovereign digital identity, solutions that merely provide a digital government identity with little to no control for the user will also be out-of-scope. In scope will be the technologies that have been identified in the review of existing technologies as sufficiently testable. This scope definition can be seen in Table 1.1.

Table 1.1: Scope definition of the research.

In-scope of research	Out-of-scope of research
• Previous research funded by the EU such as ABC4Trust and PrimeLife.[10] • Functional aspects of self-sovereign digital identity tools. • Existing technical solutions, in either concept or demo phase with a clear self-sovereign identity approach to digital identity. • Evolving the 'seven laws of identity' (Cameron, 2005) and 'the ten principles of Self-Sovereign Identity' (Allen, 2016) into part of the benchmark.	• Legal benchmarking criteria based on GDPR PSD2 and other legal aspects. This is existing research in an MSc thesis. (van Wingerde, 2017) • Digital identity prototypes that would not be usable for the public sector. (in the evaluation of concepts) • Technical implementation of identity on the blockchain: Sovrin, Trustchain and other previous research cover this aspect already.[11] • Projects that focus exclusively on eID and eIDAS compliance and do not have an aspect of self-sovereignty (based on the research definition). • Security evaluation of cryptographic properties, other than the information given by interviewees. • Citizen's direct opinions about SSI.[12]

1.4 Research Purpose

We have established that there are many societal challenges that self-sovereign digital identity can help solve and that a successful digital identity method can (in the future) exist in the public sector. Several different vendors and communities are working on realizing self-sovereign digital identity in differing technological ways: The identity can be stored on a blockchain or on a citizen's mobile phone, for example.

Prior research on the subject of SSI concluded that '... government is trusted the most. The reason for this was that according to passengers, the government does not benefit of having personal data' and 'the government already has my personal information'. For these interviewed airport travelers, the ideal SSI provider would thus be the government. (Poot, 2017, p. 80)

[10] See: https://abc4trust.eu/ and http://primelife.ercim.eu/

[11] See: (Sovrin Foundation, 2018), (Stokkink & Pouwelse, 2018) and (Lundkvist et al. , 2017)

[12] After some deliberation we decided that it is too technologically advanced a subject for a citizen opinion panel.

As such, the research and gradual societal acceptation of a SSI standard and the corresponding technologies can in turn enable new technologies to be based on this new form of digital identity management.

This research intends to result in a SSI governance framework for the government. That framework will help with making the decision on how to interact with SSI as a government, from the role as societal warder and enabler.

1.4.1 Public sector relevance

The Dutch government is interested in testing different possible (prototype) solutions. It plans to do that together with several municipalities in a so-called 'policy lab'. For this policy R&D, several preconditions have to be satisfied. First, an inventory has to be made of different existing solutions and concepts, to gain a more complete overview of ongoing SSI technologic innovation. Several concepts exist, with different technological approaches. They might be suitable as a basis for self-sovereign digital identity in the public sector, which is why the second step of this research takes place after inventorying them: It is measuring the citizen's response to the technology. Self-sovereign identity could accomplish the goal of the government to put citizens more in charge of their own data as formalized in the coalition agreement. (Rutte, Buma, Pechtold, & Segers, 2017, p. 11)

It is of importance for the public sector to know the exact constraints of self-sovereign identity from the bottom-up, to use in further related testing. A method fitting the new approach to information technology projects, putting needs and preferences of stakeholders (such as citizens) in the first place while designing solutions. (Information Society and Government Study Group, 2017, pp. 39-40)

Creating a set of demands and wishes that are applicable to different digital identity technologies, based on functionality instead of technology, will enable objective governance of different (possible) solutions on suitability. That *can* lead to better thought-out choices later in this process; other governments can use this document as a baseline for their own digital identity solution search process.

1.4.2 Relevance for Academia

The concept of self-sovereign digital identity, as introduced at the start of this chapter has only limited exposure to academic research. Previous research is available on blockchain applicability for self-sovereign identity and legal benchmarking based on GDPR and PSD2 but not on public values and governmental requirements. Through the process of knowledge discovery during the writing of this thesis this knowledge will be expanded (especially) concerning the public values surrounding digital identity.

For reorienting the digital identity policy of the Dutch government - a goal of the planned digital identity policy lab - the framework will be of value: It can be used as a way to shape future government decisions in interaction with self-sovereign identity, together with the results of the policy lab. Research organization TNO is also working on a self-sovereign identity framework (SSIF) to facilitate interoperability.[13]

[13] TNO's introductory video for SSI(F) can be found at https://www.youtube.com/watch?v=7goOGMmWO90

The knowledge gained from this thesis research will also be applicable to future digital identity projects in other countries. Helping their respective governments to select the right approach in testing solutions with the citizen. Lastly, it is generalizable to the government searching a strategic and governance role in other technologic innovation processes.

1.5 Research Methodology

In this section of the thesis, the reader is informed about the chosen research methods and phases. The objectives and guidelines for each of the research phases will be discussed as well as their expected results. The chosen approach for research is a design science in information systems delivery-oriented approach, which has been slightly adjusted for use in this specific research scenario.

1.5.1 The Design Science methodology

Design science in Information Systems (IS) research is a goal-oriented methodology, which focusses on the delivery of an information systems artefact. (Hevner & Chatterjee, 2010) This research methodology is focused around a thematic, three-stage, cyclic method. The IS research paradigm consists of both design science and behavioural science. The design science methodology offers an iterative and structured method of researching needs and creating a prototype solution, this is shown in figure 7.

A first cycle, called the relevance cycle allows the researcher to explore the context of the design research. It analyses the environment of the research to further shape the result to match the requirements of this domain. The second cycle is the so-called rigor cycle. In this cycle, the scientific foundation in environmental relevance and organizational needs is enhanced further with literature and expertise knowledge. The final research cycle designs the artefacts and evaluates them. This cycle also refines the IS Research artefacts based on the evaluative feedback loop if there are iterative cycles in the research design. (Hevner, 2007)

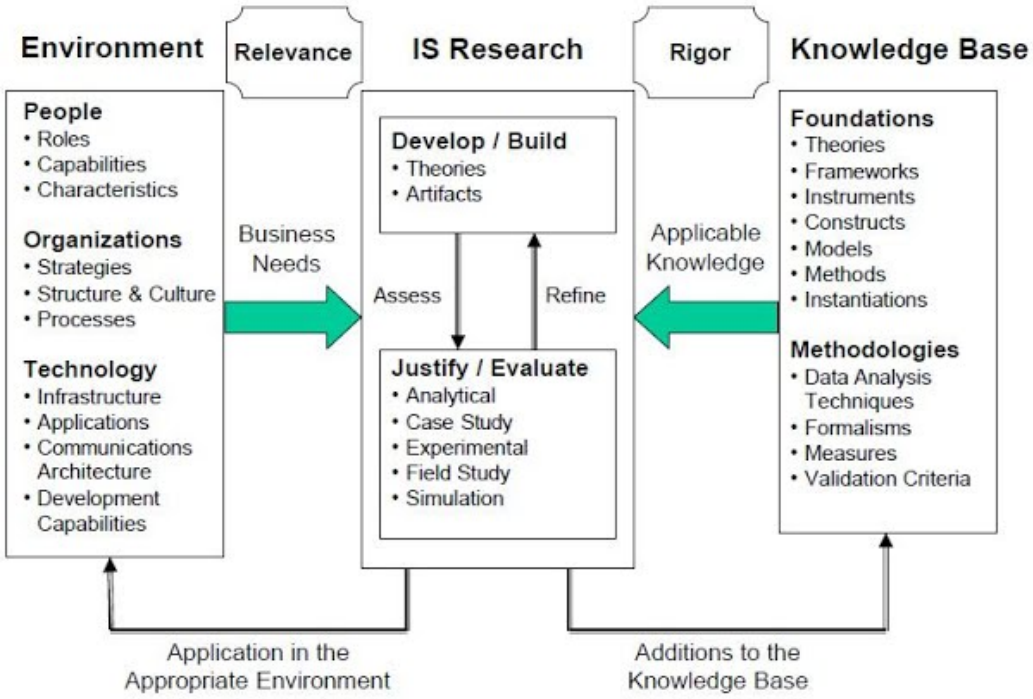

Fig. 7: Design Science cycle. (Hevner, 2007)

Some changes from this research methodology to accommodate the specific situation and the public sector were made. The relevance cycle of the research is used to examine societal values than business needs, since the public sector already sees the relevance of the digital identity problem. The focus is on technology knowledge and review, combined with exploring the gap in the knowledge of societal qualities of SSI. The current knowledge of existing SSI concepts is insufficient: Several concepts exist, but have not been evaluated on actual maturity and SSI qualities. A paper is currently the only publicly available comparison between five different SSI concepts based on blockchain technology and concluding that some of the concepts are not mature enough to evaluate at all. (Abraham, 2017)

Secondly, a Rigor cycle containing literature review, review of existing solutions and expert interviews is planned. During this cycle, a conceptual set of criteria is discussed with experts from different fields.

Lastly, in the design cycle the framework will be designed based on the input from the two earlier cycles and enhanced based on the information found in the rigor cycle. This can then be used to evaluate self-sovereign identity in the policy lab and beyond.

1.5.2 Research structure

The structure of the research is based on the cyclic nature of the design science approach as discussed in *section 2.1* of this document. The six-month timeframe allotted is split into the three cycles and finishing of the final research report.

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Fig. 8: IS Design-Science Research Guidelines. (Hevner & Chatterjee, 2010)

The Research Guidelines in figure 8 have to be taken into account while designing the contents of the research phases for successful design research. They were integrated in the planning of each cycle, under the relevant paragraph the integration is discussed further.

1.5.3 The Relevance Cycle (conceptual foundations)

Research Guidelines: Problem Relevance, Design as a search Process, knowledge building.

In the first cycle of the project, the relevance to the environment and exact nature of digital self-sovereign identity is researched. Goals are getting knowledge of the field and technological advancements and learning from previous documents what aspects of a digital identity solution might be relevant to the proposed benchmark for the public sector. Experts are interviewed in this cycle for their opinion and insights to support these goals.

Literature review was realized in this cycle. This literature has the goal of enhancing knowledge of available self-sovereign identity solutions and their properties as well as identifying key players in the field.

Interviews were taken within the government and related organizations to find out how they interact with citizen's digital identity and would envision the government's role in a future self-sovereign digital identity system. These interviews also provide input for the rigor cycle.

The interview is set up as semi-structured by using a set of eleven questions (See section 3.1.2) to guide the interview. Before interviewing a selection was made based on the criteria in Table 1.2. The experts were encouraged to somewhat expand on the questions that are asked. After the interview, a recording will be transcribed word for word into a transcript if the interviewee does not object. The transcript is then sent back to the interviewee for final review. The respondents are also encouraged to add any drawings or models that they would like to share to illustrate their answers. This final reviewed version is the version attached to this document.

Table 1.2: The criteria for selecting interviewees.

Selection criterion	Specific requirement
Experienced in SSI concepts	Professional or academic experience with self-sovereign identity.
Public sector relevance	Must be organizational context that is related to the public sector.
Unique perspective	Compared to the other (earlier) interviewees, the participant is expected to have a unique viewpoint on SSI. Based on their background.
Interview availability	Must be available for interviewing and willing to share the information publicly.
Expertise must be SSI concept Independent	Not an employee of one of the solutions, or someone only having experienced a single SSI concept to gain a more balanced view.

A Preliminary output in the form of a technical / functional comparison will be created that is based on the answers of the expert interviews round. It serves as the conceptual input for the rigor cycle.

1.5.4 The Rigor cycle (validation of concepts)

Research Guidelines: Validation of concepts, expert review and research rigor.

Follow-up expertise to validate the public values and key performance indicators found in the literature and first-round interviews and where applicable expand on them.

Validation of the self-sovereign identity governance framework (concept version), by means of expert review by policymakers and experts.

Building on the results of the initial technology research, in this cycle the findings will be discussed with policymakers. This enables improvement and refinement by engaging policy experts in conversation. Goal is to find out how they think about the issues and opportunities we have found in the first round of interviews.

1.5.5 The Design cycle (finalizing and testing)

Research Guidelines: Design evaluation, Communication of research, Design as an artefact.

Reducing bias of the interviews: Interviews with SSI experts are likely to be biased due to their unique viewpoint. Due to there being a limited amount of experts in this field that can be interviewed in the time available, the results have to be validated.

Iterative improvement of the framework with input from the policy makers and interested parties to come to a higher-quality framework.

Design and improve the final self-sovereign identity framework, by engaging many experts in policy to contribute on their experiences and expertise. This will be an iterative process to improve the framework and add knowledge due to review and call for framework concept feedback in a final workshop.

1.5.6 Expected Research Outcomes

Outcomes of the research should be two-fold. On one hand, the outcomes should offer more insight in the available Self-sovereign identity concepts and developments in this field. On the other hand, they should offer the government a framework that can help decide on whether to interact with the technology, and – if so – what possible ways of interacting are. These interactions can in turn benefit both the technologic development and society.

Research Output Artefacts (ROA's)

The output will consist of three artefacts. These are:

- A Strategy and governance model.
- Framework with the possible roles and interventions the government has in SSI according to research.
- A set of recommendations on how to proceed in strategic and tactical positioning and next steps to take.

Together, these artefacts will answer our main question by giving the government possible qualitative options for governance and acceleration based on the 'Design Science' methodology.

2. Theoretical review

In this section of this thesis, we will explore different concepts related to the subject. First, the definitions following from literature review are set for purposes of the study. Then the concept of self-sovereign digital identity and its main functional components will be explained to the reader and existing normative documents concerning the concept will be investigated, in the form of the seminal work by Kim Cameron in which he sets qualitative criteria for digital identity.

This is followed by Christopher Allen's ten norms for SSI, which are based in part on Cameron's 'Laws of digital identity'. Lastly, we discuss how Allen's work was analysed from a more philosophical perspective by Holochain director and decentralized identity philosopher, Matthew Schutte.

After this literature review, we will examine the current state of technological prototypes to answer our research question "What SSI solutions are mature enough to be testable and/or have been tested in an International Public Sector context?"

2.1 Previous research literature on self-sovereign identity

For understanding the subject of self-sovereign identity and the qualities of a 'good' digital identity from a societal viewpoint, literature was reviewed. In this section this literature, which partially shaped the comparison of existing SSI solutions, is discussed. While (Allen, 2016) and (Cameron, 2005) have laid down some normative qualities for digital identity, they are also broad and especially in case of Cameron's Laws based on old technologic paradigms.

Microsoft researcher Kim Cameron sets forth seven 'laws' of internet identity. (Cameron, 2005) These laws and Cameron's work have served as an influence to the Internet Identity Workshop, a yearly conference on future digital identity. As such, these laws are still an integral part of future identity thinking. While Cameron's laws are still quite relevant, it has to be noted that they are by now almost fifteen years old and do not take into account new technology that can influence identity in the digital domain. These laws have each been compared to the current state of identity, to research whether SSI tools that exist today adhere to them in a later section of this thesis.

This, in part, decided whether they were feasible for testing. The articles by Cameron also served as important input for Christopher Allen's 10 SSI principles. (Allen, 2016) Those ten principles will also be discussed below.

1. **User control and consent:** *Technical identity systems must only reveal information identifying a user with the user's consent.*

User control and consent is nowadays a 'hot item' in government policy, initiatives aim to give citizens more control over their personal data with the government. A problematic issue with this as shown by the 'cookie-law' is that citizens are more likely to click agree without actually reading what is consented to. This law, forcing websites to ask for consent before placing some data on the user's computer that can be used for both tracking and website functionality caused annoyance with users.[14]

[14] https://www.bbc.com/news/business-38583001

Furthermore, non-clear and lengthy agreements or policies are often impossible to understand for users without legal backgrounds. To **what** is given consent to should be explained in a maximum of one paragraph, preferably one or two sentences. Some of the SSI tools that exist such as IRMA tackle the issue well by simply listing exactly which attributes are requested in each interaction. Then, it is up to the user to accept or decline based on that overview.

> **2. Minimal Disclosure for a Constrained Use:** *The solution, which discloses the least amount of identifying information and best limits its use, is the most stabile long-term solution.*

This is an interesting position. This 'law' is very compatible with the stronger demands the GDPR places on storing personally identifying data: it means there is less data that requires protection against leakage and of which the use has to have a mandate in the new Privacy Impact Assessments (PIA's). (European Parliament, 2016, p. $84) With this new regulation, this statement by Kim Cameron is now closer to the norm, at least for European Union citizens.

> **3. Justifiable Parties:** *Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.*

Selective disclosure as stated by Cameron is an integral part of any privacy-conscious identity metasystem. This is a design and governance role, Sovrin and Qiy set standards that their 'stewards' must adhere to concerning this 'law'. While IRMA transfers the decision to the end user, who can then decide exactly which attributes to reveal (or not).

> **4. Directed Identity:** *A universal identity system must support both "Omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.*

This directionality described by Cameron can be construed as a demand: A good identity system makes transactional correlation difficult by limiting re-use of unique identifiers. Balance between ease of use and privacy is paramount.

> **5. Pluralism of Operators and Technologies:** *A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.*

Interoperability of identity systems is a long-term goal. This is one that eIDAS explicitly sets for the European Union, but for SSI it is hard to accomplish as long as there are no standards set. Parties such as TNO (Joosten, 2018) and W3C (World Wide Web Consortium, 2017) are working on these standards, which are not finished or widely accepted as of yet. This standardization effort could be a government role in the process; opinions about this were explored in the interviews with experts, which can be found in **chapter 3** of this thesis.

6. **Human Integration:** *The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.*

Cameron acknowledges here that the human user is often seen as merely the 'subject' of a digital identity rather than the director. This is a call for being in control, while also being offered protection against attacks. In 2005 biometric and two-factor authentication were not common for end users as they are now, mobile phone based solutions for self-sovereign identity make use of these new secure ways of storing identity attributes which did not exist at the time this piece was written. The most important attention point is that the user should really be in the driver's seat, there is in the European context also some progress on giving citizens the control over digital information pertaining to their identities such as the 'right to be forgotten'. (European Parliament, 2016)

7. **Consistent Experience across Contexts:** *The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.*

This is likely the most demanding 'law' of identity that Cameron has put forth. With mobile applications, which take up an entirely new (since Cameron's 2005 writing) user experience approach to software, the ambition to unify their experience is ambitious at the very least.

Cameron's laws provide a normative measure for the quality of digital identity, especially from the view of the end user. They can be used as norms by which to assess (in part) the user qualities of a digital identity, in section 3.1 of this thesis several Self-sovereign identity tools are assessed based on these seven laws, while others have already been assessed on them by previous research. (Dunphy & Petitcolas, 2018)

Researcher Christopher Allen defines ten principles for self-sovereign identity; he has published these on his weblog. (Allen, 2016) The Dutch authority for financial markets (AFM) in its capacity as a blockchain coalition partner is working on a paper in which 40+ identity solutions are measured based on these ten principles of SSI. In the words of their research member: "what we are doing now is looking at which ones comply with all ten, which ones comply to none at all. But that doesn't mean by definition that they are ok, or not ok." (Franken, 2018)

Christopher Allen's ten principles for Self-Sovereign Identity are:

1. **Existence.** Users must have an independent existence
2. **Control.** Users must control their identities.
3. **Access.** Users must have access to their own data.
4. **Transparency.** Systems and algorithms must be transparent.
5. **Persistence.** Identities must be long-lived.
6. **Portability.** Information and services about identity must be transportable.
7. **Interoperability.** Identities should be as widely usable as possible.
8. **Consent.** Users must agree to the use of their identity.
9. **Minimization.** Disclosure of claims must be minimized.
10. **Protection.** The rights of users must be protected.

These ten principles are largely comparable to the seven laws of identity set forth by Cameron in 2005. In the table on the next page of this document, these ten principles are compared to the seven laws for SSI. While comparing these two sets of norms for the quality of digital identity it was noticeable that both have the same qualities in mind, while Allen has more focus on transparency of

systems due to upcoming selective algorithms (for example, automated risk scoring) and their controversy. The ten principles overlap and expand on Cameron's laws but do not completely replace them, they are more up to date with technologic debate such as whether algorithmic automatized decisions should always be understandable for humans. Furthermore, they are also more abstract in nature, where Cameron provides a more direct 'check list' type of explanation. To illustrate the similarity, they are compared in Table 2.1.

Considering that the seven laws are described in more detail and that Allen's ten principles overlap them by a large degree, the decision was made to only use the seven laws in evaluating self-sovereign identity tools out of these two normative measures for user quality.

Table 2.1: Comparison of Cameron's seven laws and Allen's ten principles.

Cameron's seven laws (Cameron, 2005)	**Allen's ten principles** (Allen, 2016)
User control and consent	User control Consent Protection
Minimal Disclosure for a Constrained Use	Minimization Protection
Justifiable Parties	Access to own data Transparency of systems and algorithms
Directed Identity	Independent existence
Pluralism of Operators and Technologies	Transparency Portability Interoperability
Human Integration	Persistence Independent existence
Consistent Experience across Contexts	Persistence Portability

Technology thinker Matthew Schutte analyses and provides critique on the principles set forth by Allen from a more philosophical perspective. (Schutte, 2016) His foremost conclusion on identity governance (in SSI) is a word of caution: Identity is not a set concept; we should keep that in mind when governing identity ecosystems. Governance should be not limit the development to a set of rigid requirements, which in turn will limit the innovativeness and possibilities.

2.1.1 Electronic Voting (e-Voting) and SSI

A paper by (Spirakis & Stamatiou, 2013) positions that "E-voting systems must satisfy the same basic requirements as traditional voting systems." These researchers also name the eight specific requirements for e-voting plausibility:

- **Democracy:** Persons that vote can do so once and are legally allowed to vote.
- **Accuracy:** Outcome is correct and counts all valid votes.
- **Secrecy:** A specific vote cannot be seen by anyone else.
- **Receipt-freeness:** No evidence of voting is given that can be used to prove a specific vote.
- **Uncoercibility:** Protection from outside enforcement of voting a specific way.
- **Fairness:** Vote remains secret until ballots are closed.
- **Verifiability:** Auditable voting result.
- **Verifiable participation:** Participation of voters can be checked by the voting authority.

This leads to a digital system with two very differing sets of requirements just like real-life voting: Absolute voting secrecy and privacy while also having absolute proof of electoral fairness. The researchers conclude after analysing the cryptographic protocol of Attribute Based Credentials - in this case the IDEMIX cryptography of which the creators claim that it indeed can offer to satisfy all these requirements for a reliable and trustworthy e-voting system. (Camenisch & Lysyanskaya, 2002) Thus, Attribute Based Credentials could possibly in due time be used for e-Democracy in the form of digital ballots and citizen enquiries.

2.1.2 Results of prior research projects

Some documentation from previous Self-sovereign identity research projects exists; small scale testing of the underlying technology (Attribute Based Credentials) for feasibility. Previous research has examined the German electronic Identity card. (Alpár, Attribute-Based Identity Management, 2015, pp. 131-134) This project of the German government is - according to the researcher – notable for using SSI technology: it uses some of the Attribute Based Credential technology that IBM's IDEMIX also proposed. The only attribute issuer is the German Government, resulting in a less dynamic (monoculture) ecosystem. In his words: "This makes applications much less dynamic, because other issuers cannot participate, unlike in an ABC ecosystem."

The author also names three technical and functional limitations of such a government issued and controlled eID compared to an ABC ecosystem: "Another consequence of this technical approach is that attributes in the German model are sent unsigned and thus the security relies heavily on the smart card. Secondly, a German eID card is enforced to create a (scope-specific) pseudonym for each transaction. This is not the case in an ABC ecosystem where authentication not necessarily includes a pseudonym.

He also notes that there is no card management application that would enable a citizen to manage his personal information stored on his card." Other past projects that are discussed in this piece are Future ID in Information Society and FutureID, which resulted in the eIDAS regulations we now know. (FIDIS, 2004-2009)

Another project called PrimeLife was the first international project within the European Union focused on developing technical application of privacy and trust in the digital domain. [15] PrimeLife's core focus were digital privacy enhancing techniques (PET's) and the project team has developed working code for some of those, one of which was 'self-sovereign' in nature: Attribute Based Credentials. (Camenisch & Lysyanskaya, 2002) A follow-up project called ABC4Trust was fully funded by the European Union's seventh Framework program. (Rannenberg, Camenisch, & Sabouri, 2015)

This project entailed two pilots with attribute-based credentials in a European context: The first pilot tested the use of ABC's to enable students to give anonymous course feedback. For this purpose, they were given a smartcard. Three conditions had to be met to give course feedback: The student is *enrolled* at the University, *registered* as participant of the course and *present* at the majority of the course's lectures. These three attributes were issued by the university to the students who put them on a smartcard they had received. Then, without revealing their identity but proving they were eligible to, they could provide course feedback.

The second pilot gave students pseudonymous access to a chat where they could talk about school problems. The results and technology of these two pilots are discussed in great depth in the final documents. Lastly, the Secure identity across borders linked (STORK) research project has led to the input that later became part of the eIDAS regulation. This regulation is now accelerating National eID acceptance across national borders in the Union. (European Commission, 2014)

There was also a follow-up in 2015 with the (not very original) name STORK 2.0. This follow-up project focused on designing a more concrete framework for cross border identities.[16] Four small-scale cross-border pilots were set up to help with this standardization goal: eLearning and Academic Qualifications, Public Services for Business, eHealth and eBanking.

Currently there is an ongoing CEF call called Erasmus without Papers 2.0 that focusses on student mobility across borders. Attribute based credentials could be explored for this purpose in the future, but right now this not the focus of this research project.

One interviewee explained that Dutch research agency TNO is involved in several with external organizations in which the concept of Self Sovereign identity is explored further. (Joosten, 2018) As the researcher interviewed put it, the main goal of TNO research participation is to 'find out what is in the way of rolling this out broadly within The Netherlands, and if possible internationally.'

On February 14, 2018, the Ministry of the Interior and Kingdom relations hosted the Identity Deep Dive of blockchain enthusiast's organization Blockchaingers.[17] Goal of this congress was informing and ideating teams that signed up to participate in the follow-up hackathon. The state secretary opened the deep dive, showing participants that there was a true government level interest in their ideas and the future of identity. During this event, several speakers of several vendors and digital identity stakeholders such as the Ministry itself presented and debated. Afterwards there was a social setting for bringing the participants into contact, serving to exchange ideas and foster new contacts. A report (in Dutch) of this deep dive is included with this document as attachment I.

[15] See http://primelife.ercim.eu/about/factsheet
[16] The project website can be found at https://www.eid-stork2.eu/
[17] See the event information at https://blockchaingers.org/events/global-digital-identity

2.1.3 Digital Identity as a concept

The American National Institute of Standards and Technology introduces the reader to digital identity and sets guidelines. She defines digital identity as "...the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to be traceable back to a specific real-life subject. In other words, accessing a digital service may not mean that the underlying subject's real-life representation is known." (Grassi, et al., 2017, p. 2) The focus of this definition is on the unicity of a representation that does not by nature have to be realistic (it could be a dog, claiming to be a human) or traceable to a real life entity (anonymity).

Researcher Kim Cameron describes digital identity as "a set of claims made by one digital subject about itself or another digital subject." He defines a digital subject as "…a person or thing represented or existing in the digital realm which is being described or dealt with". (Cameron, 2005) He also states that a claim is "…an assertion of the truth of something, *typically one which is disputed or in doubt*".
Here the author describes a claim-based digital identity, a suitable framework for self-sovereign digital identity because by nature it allows the subject to divulge 'just enough' information to prove an assertion. Interestingly the researcher also introduces *doubt* as a concept in digital identity management, to emphasize the evaluative nature of a claim-based digital identity.

Another research document concludes that "A digital identity is a snapshot of the actual identity of a person, a company, a device, a car – more generally: an entity" and that "The actual identity encompasses all the determining characteristics of an entity, which makes an entity distinguishable from others. (Der, Jähnichen, & Sürmeli, 2017) Each digital identity consists of only a fragment of the identity and is usually created for a specific purpose in a specific context – to use a particular service or to interact with another entity."

The authors of this document also state that "The individual digital identities differ in their level of detail: With respect to the supplied properties… the accuracy of their description and the degree of abstraction.... Furthermore, a digital identity has a clear temporal point of reference: Characteristics of an entity can change at least partially…. Each entity therefore has only one identity but an unlimited number of digital identities." Thus, it introduces a one-to-many relationship in 'real-life' and digital identities, while also defining the accuracy and temporal aspects as key characteristics of digital identity. An entity is interchangeable with Cameron's term 'digital subject'.

Having considered these definitions in previous research of digital identity. Based on the focus on attribute-based credentials (ABC's) in self-sovereign identity. The research definition of 'digital identity' will be defined as follows:

"A Digital Identity is the set of claims made by an entity about itself or another entity in the digital domain. A claim being a disputable attribute that is of changeable nature. A real identity can have a one-to-many relationship with a digital identity"

Part of the research in this thesis consists of interviewing SSI experts and policy experts, to make sure they have the same definition of digital identity in mind this definition will be discussed with them before starting the interview.

2.1.4 Digital Identity as the synergy of several concepts

For understanding that digital identity is an evolving concept, it is important to know that Digital Identity can be viewed as starting to combine several 'traditional' concepts into a new digital concept. Here we define the three key analogue concepts that for purposes of the research are contained within the realm.

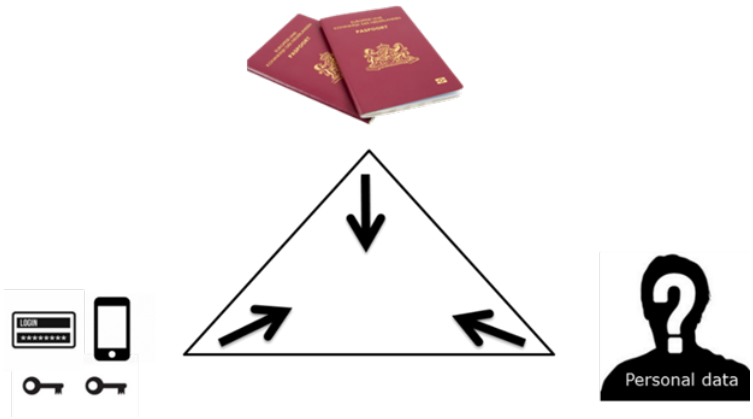

Fig. 9: Three analogue concepts as a new digital identity concept (van Weel, 2018)

Travel documents serve as governmental proof of certain attributes being valid, such as Nationality and Name. However, allergies or other (medical) information might be very important to know in a given situation, but are not to be found on a Dutch Passport

Digital Authentication and identification is (in a computing sense) "The process or action of verifying the identity of a user or process." (Oxford English Dictionary, 2018) The most common form this digital identification would be a password. Other methods such as biometrics or a one-time code can also positively authenticate the user as long as they can ascertain to the required degree of certainty that Authenticator X corresponds to User X. Newer forms of authentication and identification use biometrics such as a fingerprint scan or facial recognition to do this. In a Digital Identity authentication is no longer a separate concept. It is a work-around for not having digital proof of identity; knowing a password is a verified identity attribute in the analogue world. The verifying party is the entity storing the password that only the identity associated with it knows, although it can be compromised and therefor part of the identity stolen.

Personal identity data that travel documents, such as a government-issued ID's, do not provide, but are used by citizens in daily life. These could also be other personal data that is considered (by the entity) as part of an entity's identity. Note that an attribute can also be non-textual in nature, such as a photograph. (van Lieshout & Hoepman, 2015, p. 27)

Eventually the boundary between these three concepts will blur and they will become one digital identity, according to this policy researcher it could possibly take the shape of the so-called 'four-corner banking model' (van Weel, 2018) This is a model where institutions such as banks provide the identity vault, transactions and assurance on behalf of the owner. It is based on the existing financial system. (Ingenico Systems, 2018)

2.1.5 Self-Sovereign digital identity

The concept of self-sovereign digital identity builds on the established definitions of digital identity by centralizing the user. Dictionary definitions of the word Sovereignty are “Supreme power or authority.”, “The authority of a state to govern itself or another state”, “A self-governing state.” Self-sovereignty would thus mean ‘Supreme power or authority over oneself’. (Oxford English Dictionary, 2018)

In the context of digital identity management, the term is also defined by researchers. (Faisca & Rogado, 2016) They surmise that that “Centralized digital identity ties the individuals to the administrative domains of the identity provider. A self-sovereign identity on the contrary, is created and maintained by individuals, for their own specific usage.”

Another scholar defines Sovereignty as “per definition, a supreme power or authority, which governs itself without any outside influences.” In his research-specific context, he surmises, “Sovereignty for identity management means that the user’s identity data are fully owned and controlled by herself.” (Abraham, 2017) Taking these definitions in account, we will define the working definition of Self-Sovereign Digital Identity for purposes of this research as:

“A Self-Sovereign Digital Identity is the set of claims made by an entity about itself or another entity in the digital domain. A claim being a disputable attribute that is of changeable nature. A real identity or its owner can have a one-to-many relationship with a digital identity, is in complete control, maintains and owns the digital identity.”

A real identity can also be an object or entity such as a company; in this case, the legal owner(s) manage the identity. One of the interviewed experts talked about a new financial phenomenon called ‘decentralized autonomous organizations’. The actions of these virtual entities are completely based on software code instead of human interactions. They do not have anyone to legally point at for responsibility, an issue for the Financial Markets Authority. (Franken, 2018)

2.1.6 Verifiable claims and existing architectural constraints

A verifiable claim can be defined as a "machine-readable statement made by an entity that is cryptographically authentic, non-repudiable". (World Wide Web Consortium, 2017)
(Sovrin Foundation, 2016, p. 17) Explains the term as a synonym: "…Verified identity attributes, also known as "verifiable claims". Abraham defines verifiable claims as "non-reputable sets of statements made by an entity about another entity. These claims are cryptographically generated." (Abraham, 2017, p. 35)
All three definitions have in common that the verifiable claim is a signed attribute, which is cryptographically underwritten by a third (trusted) party. Thus, on the 'verifiable' property or aspect of a digital claim we can conclude that:

Verifiable means that a specific claim or attribute in the digital identity has a cryptographic signature of a trusted third party proving its authenticity to a certain degree of assurance. A claim is a statement such as 'is older than 21', while an attribute is a property '01-01-1990' on which a claim can be based on for minimal disclosure proof.

A concrete example would be a digital claim of having a diploma "Master's degree in Computer Science" signed by Leiden University cryptographically. This signature would prove to the receiver of the claim that it is underwritten by Leiden University as authentic. A non-trusted party or the entity itself can also underwrite an attribute or claim; it is totally up to the receiver to decide on the quality of the underwriting. The digital identity framework or attribute validity could be limited to trusted third parties for signing claims only. That would in turn limit the freedom to participate and require some form of authority over the ecosystem. Now a short explanation will be given of the fundamental roles in such a digital identity framework.

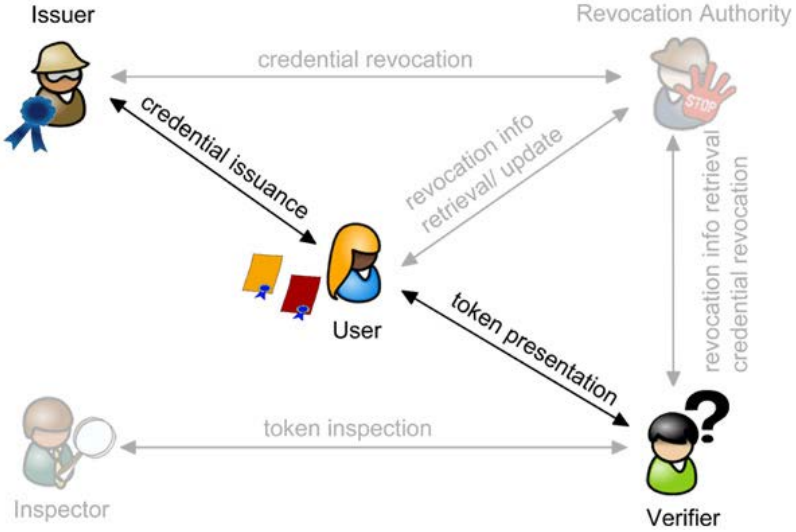

Fig. 10: Issuing, verifying, inspecting, revoking (Camenisch, 2013)

The Issuer
Each attribute is signed by the user itself or an issuer. In the example, Leiden University would be the issuer of the attribute "Master's degree in Computer Science". Self-signing is also possible, with personal attributes such as 'favourite food is pizza', which are not likely to need to be underwritten by a trusted third party. It is up to the acceptant party of the attribute to decide whether 'Leiden University' underwriting the attribute satisfies the trust level.

The Subject or User
The subject or entity is in control of the digital self-sovereign identity; it collects underwritten attributes and then selectively reveals them to parties requiring proofs.

The Verifying parties
The verifying parties are the stakeholders that need certain attributes for their business processes. For example, a bank must comply with Know Your Customer (KYC) regulations, therefor certain information about the accountholder must be known from verified sources in the digital ecosystem.

The Revocation and the Inspection authority
Another feature of digital self-sovereign identity is that, while the user is in ownership of the verified attributes, there is also the possibility of the issuer retracting them. For a functioning ecosystem, revocation has to be implemented while at the same time protecting privacy features. The exact cryptographic properties of such a revocation system have been subject of research for some time.

Brands, in his PhD thesis proposes a cryptographic method of Attribute Based Credentials. (Brands, 2000)
Cryptography researchers Jan Camenisch (IBM Research) and Anna Lysyanskaya (Brown University) also propose a cryptography for credentials, called Identity Mixer. (Camenisch & Lysyanskaya, 2002)
Lastly, Microsoft researchers have done some research leading to the U-prove Attribute Based Credential cryptography concept. (Paquin & Zaverucha, 2013). The in-depth examination of these cryptographic properties is not part of this thesis.

2.1.7 Functional SSI considerations

Three functional considerations that are part of ongoing research but not part of the SSI ecosystem as proposed by Camenisch are reviewed in this section of the theoretical review. (Camenisch, 2013)
Key recovery is an important part of usability: Identity has to be persistent according to the theory, thus losing access should be recoverable for the citizen. Secondly, when an attribute has become invalidated (revoked, for example) or invalid (old address) there should be a method of disputation, to improve the data quality and validity. Lastly, we will look at a possible future impact on trust in the digital domain: quantum computing will break certain secure communication protocols and weaken others.

Method of Key recovery
Adi Shamir, in his seminal paper about cryptographic key recovery, proposed a cryptographic solution for a shared secret, where majority decisions are possible.[18] (Shamir, 1979) Evolution of this solution is still ongoing, especially concerning its applicability in digital identity recovery.[19] Prototype self-sovereign digital identity solution uPort also has a recovery system in place based on Etherium smart-contract code. (Lundkvist, Heck, Torstensson, Mitton, & Sena, 2017, pp. 8-9) As such it possible in a self-sovereign identity to recover a key by assigning 'stakeholders' and defining a majority needed for recovery.

[18] A form of key escrow, where a pre-set majority of key group keys grants access. In the example named by Shamir, only six or more out of the eleven scientists when *together* can open the secret e.g. a majority level of which the threshold can be set. SSI-application uPort is a notable example of usage.
[19] https://github.com/Tribler/tribler/issues/3246#issuecomment-358076552 – TU Delft blockchain lab students are also working on this recovery issue.

Possibility of Data quality disputation
The working definition of digital identity, along with the research that we have explored, defines that digital identity attributes are of a changing nature. (Der, Jähnichen, & Sürmeli, 2017) As such, the Data Quality (DQ) of digital identity attributes can change over time. When attributes become invalid or outdated, the identity owner could be invoked to dispute the data quality with the supplier of the attribute; for this, an architectural standard should exist.

Assessing correlation risk of credentials
An in-progress standardization effort for verifiable credentials that includes best practices. They note, "Privacy is a spectrum that ranges from pseudo-anonymous to fully identified". This is further illustrated by a model of categorizing credentials by level of correlatable-ness as seen in figure 11. (World Wide Web Consortium, 2018)

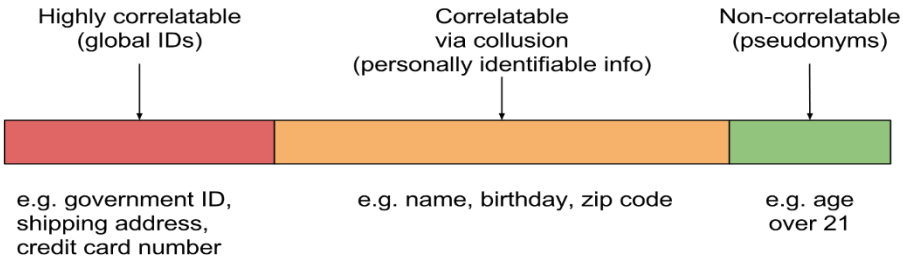

Fig. 11: Level of correlation influences privacy concerns.

It makes sense to use this as a guide for minimal disclosure of attributes and privacy impact assessment. Self-sovereign identity therefor implies that the user (citizen) is aware of exactly how privacy sensitive the information shared in a transaction is and whether it is proportionate to the situation.

2.1.8 Technologic concepts of SSI

Two technical concepts concerning SSI have also been explored for the theoretical review:

- A technical description of Attribute Based Credentials, which are the form in which the citizen's identity data is stored in these systems
- The (future) safety of encryption used in the SSI ecosystem, which is also a measure of its quality.

Technical description of credentials and attributes
For understanding the challenges and possibilities of self-sovereign identity, the technology was also explored. Attribute-based credentials (ABC) technologies using cryptography such the three discussed (Brands, Identity Mixer and u-prove) platform agnostic. While they do require some form of computing technology, they are not limited to a device. The IRMA team engineered a prototype smartcard for holding ABC's in the past; this is now no longer developed, as a mobile application was favoured.

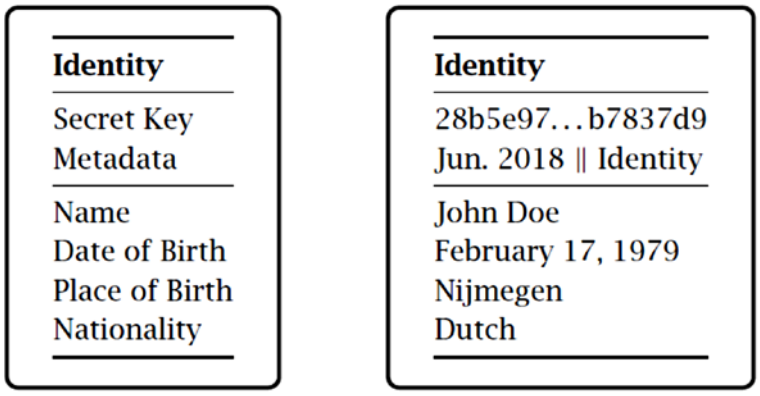

Fig. 12 An example of attributes in a credential, which can be cryptographically signed by the originator. (van Lieshout & Hoepman, 2015, p. 53)

Credentials are a set of attributes, issued by a certain issuer. An example real life representation would be a library membership card, it contains multiple identity attributes such as Name, Birthdate, membership number that were in some form validated by the issuer: the library. As such, this resembles the form in which we reveal validated identity attributes in the analogue world. Where 'trustworthy enough' is up to the acceptant, as a library attestation might be good enough for many use-cases but not for opening a bank account.

2.1.9 Post-Quantum encryption safety

Wide spread usage of a self-sovereign digital identity will likely happen in the longer-term (5 to 10 years) future. (Poot, 2017) Estimated advances in Quantum computing propose a timeline in which around 2030 the first cryptography-breaking quantum computer will exist.[20] This means that certain cryptographic protocols that rely on integer factorization will become effectively useless once such a computer exists with sufficient capacity. (Blanda, 2014)

Important for the future proofing of self-sovereign digital identity is that these future-weak cryptographic standards are not to be used in the underlying technology. An example of future-weak cryptography in SSI concepts is the Diffie-Hellman for Attribute Based Credentials (ABCDH) key exchange proposed by Alpár. (Alpár, 2015, pp. 79-83) This long-term cryptographic security is an important factor of a good SSI technology: After all, the identity should be persistent and durable according to Cameron and Allen.

2.1.10 Conclusion on state of research concerning Self-sovereign Identity

While previously the European Union funded self-sovereign identity research, this is nowadays not the case. During our visit to the DG CONNECT of the European Union, we found that no real follow-up on the results of the ABC4TRUST pilot is known at this level. The upcoming policy lab might therefor be one of the few initiatives researching self-sovereign identity in the public sector, EU-wide.

There is currently no push towards SSI from the European level; the Dutch government could be first-mover if it decides to pilot SSI in daily interactions with citizens. Other countries are likely to be interested, if they become aware of the potential advantages SSI can bring. Positive effects on privacy, citizen's sense of digital self-control and data minimisation resulting from re-use are possible.

[20] https://www.europol.europa.eu/iocta/2016/app-1.html

2.2 Existing self-sovereign identity concepts

In this section of the document, we take a more in-depth look at existing identity concepts that could possibly be 'self-sovereign' in nature. First, we set forth maturity criteria based on software quality theory. Then, for possible SSI capable concepts, the status and qualities are reviewed in more depth. This in-depth review is based on the work of Cameron and available technical literature of the concept in individual subsections. Table 2.2 shows the different concepts that have been found and of which the software quality was established with our maturity scan.

Table 2.2: The different SSI concepts that we have tested.

Concept name:	Website or source:
IRMA	https://privacybydesign.foundation/irma/
Sovrin	https://sovrin.org/
Dappre	https://dappre.com/
IBM Identity Mixer	https://www.zurich.ibm.com/identity_mixer/
uPort	https://www.uport.me/
Schluss	https://www.schluss.org/
Digi.me	https://digi.me/
Securekey	https://securekey.com/
Open Mustard Seed	https://www.w3.org/2013/socialweb/papers/OMS.pdf
Shocard	https://shocard.com/
Qiy	https://www.qiyfoundation.org/
Tykn	https://tykn.tech/

2.2.1 Evaluation criteria

System qualities were compared based on the available (technical) literature and hands-on testing of the application. Due to the changing nature of the solutions by further development and our focus on the maturity, the results of individual aspects can change quickly with new releases.

Reyes compares three particular software quality sets. (Reyes, 2008) These sets are as follows:

- McCall's Factors in Software Quality, the first proposal for a software quality criteria set. (McCall, Richards, & Walters, 1977)
- Boehm's Characteristics for software quality. (Boehm, Brown, & Kaspar, 1978)
- The ISO 9126 standard for software quality. (International Organisation for Standardisation, 1991) The conclusion of Reyes is that no 'fit all' set measures for software quality exists and it that quality depends on a more holistic view.

We have compared these three quality sets from the comparison by Reyes to our own maturity scan quality set in Table 2.3.

Table 2.3: The three discussed quality sets compared to our SSI maturity scan

Criteria / Goals	McCall, 1977	Boehm, 1978	ISO 9126, 1993	SSI Maturity scan, 2018
Correctness	X	X	maintainability	
Reliability	X	X	X	
Integrity	X	X		Privacy and Security
Usability	X	X	X	Maturity
Efficiency	X	X	X	
Maintainability	X	X	X	Community
Testability	X		maintainability	
Interoperability	X			
Flexibility	X	X		
Reusability	X	X		
Portability	X	X	X	
Clarity		X		
Modifiability		X	maintainability	Community
Documentation		X		Community
Resilience		X		Security Redundancy
Understandability		X		
Validity		X	maintainability	Security Retractability
Functionality			X	User functionality Business functionality
Generality		X		
Economy		X		

He goes on to use the IEEE definitions for Software Quality:

- The degree to which a system, component, or process meets specified requirements.
- The degree to which a system, component or process meets customer or user needs or expectations.

IEEE also defines Software Quality Assurance (SQA) as:

- A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements.
- A set of activities designed to evaluate the process by which products are developed or manufactured. Contrast with quality control.

The focus of the Software Quality evaluation for purposes of this thesis is on the *both* definitions of SQ and the *second* definition of SQA, as our goal is purely evaluative. This is done by defining a set of software quality criteria based on a long list and short list of possible quality aspects that were discussed with the company supervisor. This resulted in a scoring methodology and six categories of SSI software quality. In figure 13, our categories of SSI maturity are compared to these three traditional SQ sets.

Scoring methodology

Scores are in good / neutral / bad (or unknown) with green, yellow or red colours respectively. Total scoring can then be compared in the table by either majority colour or colours on specific questions. Since this is a qualitative benchmark, the guideline is that only when a question is satisfied

completely it can be scored 'GOOD'. If it somewhat is satisfied but not completely 'NEUTRAL' is used. If neither is the case, 'BAD' is the result. The categories are based on figure 13 categories but split or renamed where applicable to enhance clarity of the comparison spreadsheet. See figure 14 for an example of what this comparison looks like.

User functionality (Functionality): What the user expects to be able to do with the solution.
Four questions:

- What is the user experience like? (completeness, usability)
- What technology and knowledge is required of the user? (entry barriers)
- Is it possible to use the solution on simple hardware such as a smart card? (simplicity, entry barriers)
- What is the solution's approach to digital inheritance?

Business functionality (Functionality): The selling points there for businesses that can lead to adoption of the system by actual businesses (both accepting and handing out credentials).
Two questions:

- What are costs for businesses? (feasibility)
- Is there a business model and financial plan? (feasibility, maturity of the concept)

Maturity (Usability): Is there active development, is there something testable such as active software. Not just a whitepaper.
Three questions:

- Is a demo available?
- Can or do users test the concept currently?
- Is there a public development path or schedule available?

Privacy (Integrity): How is the privacy of the user guaranteed, what is the design focus on privacy. This category of quality was used because the Self-sovereign identity movement is very privacy-aware, so this is one of the core 'features' of any application.
Four questions:
Is repeated use of an attribute traceable for the attribute provider?

- Can repeated use of the same attribute lead be traced?
- Can the user remove identity data on request?
- Is a revocation agency that can also revoke anonymity in special cases possible?
- What is the vision of the developers on privacy and digital identity?

Security (Resilience, Validity, and Integrity): Are attributes stored safely and locally. Another important quality of SSI software, because it requires a high level of assurance for the attributes and measures against misuse.
Two questions:

- How are the attributes secured against misuse?
- How is the system developed with adversaries in mind?

Redundancy (Resilience): How fault-tolerant is the system, is it decentralized and what other redundancy measures are planned or in place. For viability as an identity ecosystem there have to be resilient qualities of the SSI solution.
Three questions:

- Does the system work when the attribute issuer isn't reachable?
- What measures by design have been taken to guarantee stability?
- Is it possible to prove a transaction afterwards?

Retractability (Validity): Is a system of retracting attributes possible, this is required for government attributes such as a driver's license to become possible.
One question:

- Is an attribute retractable? If yes: what are conditions for retraction?

Community (Documentation, Modifyability, Maintainablity): How active is the development community and is it code open source.
Three questions:

- Are there active developers?
- If so, are they profit or non-profit?
- Is the source code available?

From this exploratory maturity scan of different concepts that were discovered the conclusion was that four out of the twelve solutions are in a testable prototype state. These four solutions are: Sovrin, uPort, Dappre and I Reveal My Attributes (IRMA). These four concepts were after this initial maturity benchmarked in more depth, both by hands-on testing and reading their respective whitepapers and comparing their functionality and 'SSI-ness' based on the Laws of Identity by Cameron. This was then totalized in a level of feasibility at the end of this section.

Maturity	
Is er een demo?	Ja, meerdere demo's op website
Is het door gebruikers testbaar?	Ja, zeker: applicatie kan bijv. iDin inladen en gebruiken op demosites.
Is er een ontwikkelpad of tijdslijn beschikbaar?	drie maal per jaar voortgangspresentatie en meetup

Fig. 13: excerpt of the maturity scan. (In Dutch) Complete maturity scan is attached with this document

Figure 13 shows an excerpt of the maturity scan document, in which the tools were compared and the quality was established.

2.2.2 Conclusion on software quality

While many different technological concepts claim to approach digital identity in a self-sovereign way we found that they lack maturity. After investigation, they are generally (eight out of twelve) not in a testable state, the software quality aspects that we have defined could not be sufficiently answered based on the available information. Thus, we decided to continue with these four concepts and explored them in more depth in section 2.2 of this thesis.

2.3 Review of existing SSI concepts

In this section, the 'testable' mature prototype solutions are reviewed from a technical and functional point-of-view. The process of selection on 'mature enough' qualities is also explained. First, a selection of digital identity tools was made based on the preliminary desk research and input from experts. [21] A list of area-specific questions was then finalized in close cooperation with the company supervisor to compare tools on suitability of testing in the upcoming digital identity policy lab. This evaluation also helped to gain more knowledge of the SSI field and its developments.

2.3.1 The Sovrin Trust Network

Sovrin is in essence a blockchain built from the start as a self-sovereign identity solution. (Sovrin Foundation, 2018) The blockchain is 'managed' by so called trust-stewards. These organizations have signed the Sovrin charter; they provide the network's decentralized infrastructure.

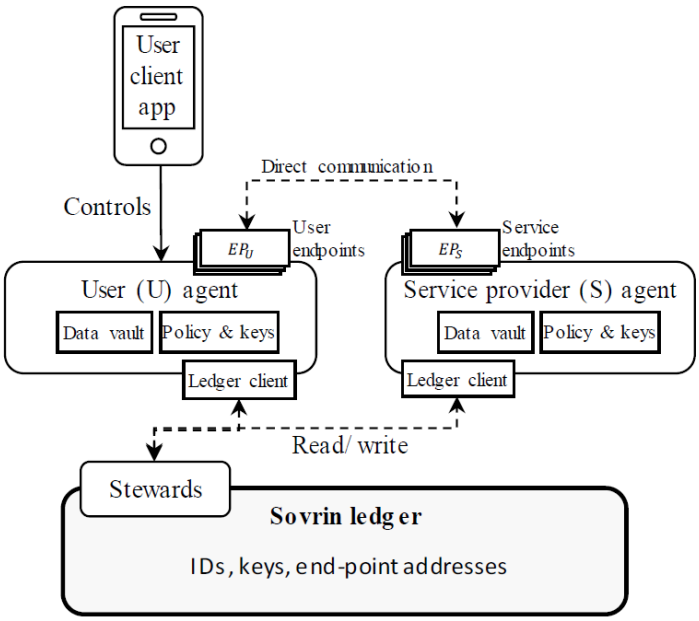

Fig. 14: Sovrin concept infrastructure (Dunphy & Petitcolas, 2018, p. 9)

As (Abraham, 2017) concludes on the Sovrin trust network "Out of all the evaluated technologies, Sovrin checks most of the boxes when developing a Self-Sovereign identity system. Sovrin got the best result especially because its design is made to realize a SSI system. Additionally, the documentation provided by Sovrin made the evaluation much easier."

Sovrin is a blockchain for identity management, leaving open the interface to the business and users. (Fig. 15) Closely related company Evernym is working on the software to provide the user (agent) functionality on top of the Sovrin blockchain, notably a Verifiable Claims Exchange prototype.[22] The eventual goal is to provide the user with an 'agent' that contains the identity, the application will then serve as a means to control this agent. This agent interacts with a service endpoint; this endpoint can either provide attestation or inspect verified attributes.

[21] Twelve concepts were found by desk research and included in the evaluation on maturity: IRMA, Sovrin, uPort, Schluss, IBM Identity Mixer, Dappre, Digi.me, SecureKey's Canadian identity project, Open Mustard Seed, ShoCard, Qiy and Tykn.

[22] https://www.youtube.com/watch?v=p0p-oSn_2kw

Evaluation on the seven laws of identity

Previous research evaluates Sovrin on the seven laws as set out by Kim Cameron. (Dunphy & Petitcolas, 2018, p. 15) The laws concerning 'Human integration' and 'Consistent experience across contexts' are seen by this evaluation as problematic. Usability is unclear due to the focus on the technology rather than the user interface and consistency in interaction is doubtful, as the user will likely use different applications for different contexts as an agent.

Total core (as scored by Dunphy & Petitcolas: 5 out of 7

2.3.2 uPort: An Etherium blockchain-based identity

This software makes use of the Etherium blockchain, which has the possibility of programming 'autonomous agents' that are usually referred to as so-called 'smart contracts'. In reality they are not 'smart' nor 'contracts' in the literal sense of the words. (Etherium, 2018) They are described more accurately as event-based distributed programming code that can for example be used to hold a sum of the cryptocurrency until a condition is met.

The developers of uPort explain the four smart contract elements and their functionalities in technical document. (Lundkvist, Heck, Torstensson, Mitton, & Sena, 2017) They are:

1. The Proxy Contract is a minimal contract, used to forward transactions and its address is the core identifier of an uPort identity.
2. The Controller Contract maintains access control over the Proxy contract, and allows for additional functionalities.
3. The Recovery Quorum Contract facilitates identity recovery in case of key loss.
4. The Registry Contract maintains cryptographic bindings between an uPort identifier and the off-chain data attributes associated with it.

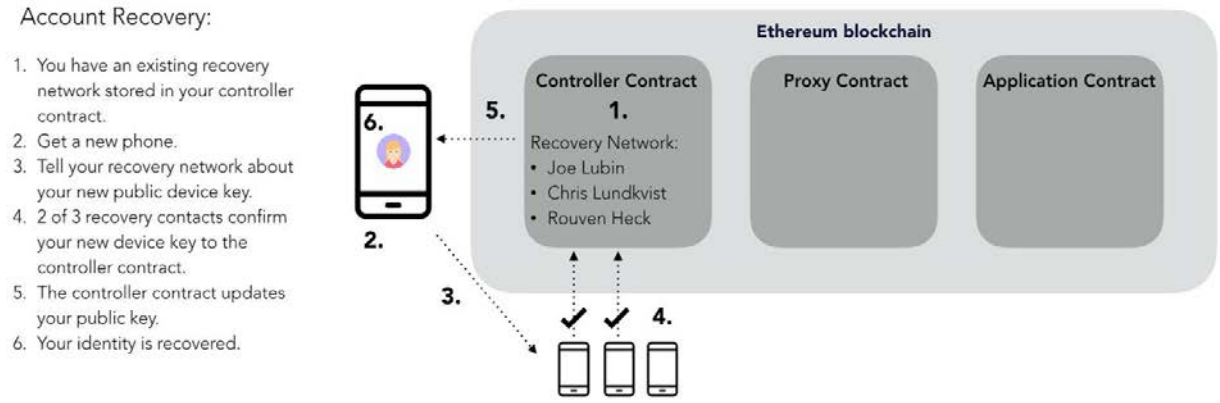

Fig. 15: uPort smart contracts (Lundkvist, Heck, Torstensson, Mitton, & Sena, 2017)

The illustration shown in figure 16 is presented by the developers as a visualisation of an account recovery using the controller and recovery quorum contracts. While figure 17 shows the information request screen of uPort.

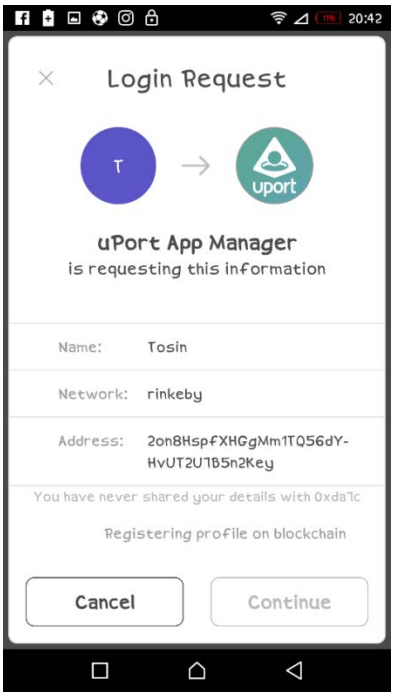

Fig. 16: uPort application selective disclosure

This prompt gives the uPort user a simple overview of what information is asked to be shared to facilitate minimal disclosure and user consent.

Ongoing pilot with uPort

The Swiss village of Zug has been offering its inhabitants the possibility of having their government identity digitally verified and stored in the uPort application of software firm Consensys since November 2017.[23] About 170 inhabitants of the city are currently testing this technology concept. An e-voting test using the application started in May 2018.[24]

Scoring on maturity aspects

Abraham concludes in his comparative review of blockchain based SSI that uPort "is in a very premature stage where there is only an alpha version available." (Abraham, 2017) This seems to have changed somewhat since the publication of his document, with the ongoing pilot in Zug and new releases of the application.
The uPort app scores especially favourably on the aspects of User Functionality and Maturity: There is a relatively user-friendly application and testing is ongoing. Redundancy is also a strong aspect, due to the basis on smart-contracts and the Etherium blockchain it is relatively hardened by distributed computing.

[23] https://medium.com/uport/first-official-registration-of-a-zug-citizen-on-ethereum-3554b5c2c238
[24] http://www.luzernerzeitung.ch/nachrichten/zentralschweiz/zug/digitale-id-abstimmung-kommt-im-mai;art9648,1229620

Main attention points & weaknesses are that uPort uses 'pseudonyms' coupled to one app identity and that the blockchain smart contracts will be archived forever due to the nature of blockchain, which leads to irrevocable proof of (historical) ownership. That is a real concern if unlinkability is required in the SSI solution. It seems that user function and commercialization aspects take priority of the development team - which is very active – over privacy-first. As such, it is not yet an ideal solution from privacy viewpoint but a strong contender in other domains. What also remains to be a consideration is the very nature of the Etherium blockchain: Transactions cost 'gas', this means an user has to have ether on his or her account to be able to interact with the smart contracts (and uPort identity) considering this cost. Currently uPort operates on a 'test net', a special network where new Etherium technology is tested. The Ether currency of this 'test net' holds no real-world value unlike 'main net' Etherium which at the moment holds a value jumping between 450 and 600 euro per unit in the last months.[25] The move to the 'main net' could well mean wide scale adoption becomes cost prohibitive due to this requirement.

Another weakness of the Etherium network is that it can become sluggish to a point where transactions and smart contract firing can be delayed by days. A notable example of this happening was the hype of owning and breeding virtual pets that used smart contracts, called Crypto kitties. (BBC Technology, 2017) As such, it is a realistic concern when Etherium becomes the host platform for a widely used identity.
On a positive note, it is very interesting that uPort is implementing the social recovery in its technology, this is something the other solutions we have investigated do not do at the current time and can have added value in societal usability.

Evaluation on the seven laws of identity

Previous research evaluates uPort on the seven laws as set out by Kim Cameron. (Dunphy & Petitcolas, 2018, p. 15) The laws concerning 'User control & consent', 'justifiable parties' and 'Human integration' are seen by this evaluation as problematic.

Total core (as scored by Dunphy & Petitcolas): 4 out of 7

2.3.3 Dappre: subscription update model identity

Dappre is an application that is being developed with the Qiy foundation's scheme as its driving force. These principles 'define a framework for individual Users, companies and governmental organizations to safely control and exchange personal information.' (Qiy foundation, 2016) The application is used by AEGON - a Dutch financial services company – to authenticate and interact with her customers.

Functionality is like a digital business card - with the addition of encrypted chat functionality between contact parties, - where according to the Qiy scheme – the user gives opt-in subscription to attributes: if he or she changes an attribute all subscribed parties will be given this updated version. That means your contact cards of Dappre users are always up-to-date.

[25] https://coinmarketcap.com/currencies/ethereum/

Scoring on maturity aspects

The data is according to the FAQ largely stored on a server in The Netherlands, hosted by information services provider KPN.[26] This implies that it is not completely self-sovereign, users do not have control over this information and the hosting specifics (security and privacy assurance) remain a 'black hole'. As such, it is currently not possible to score completely on the maturity aspects, although the concept shows promise and the application is testable.

Evaluation on the seven laws of identity

Previous research does not evaluate Dappre on the seven laws as set out by Kim Cameron. (Dunphy & Petitcolas, 2018, p. 15) Therefor it was evaluated in the table below on these aspects, while attempting to use the same reasoning these researchers used for scoring on each of the aspects. For Dappre not all information is available, it is a closed source software. Therefor this evaluation is strictly informative and exploratory in nature.

Table 2.4: Scoring table based on the seven laws of Cameron for Dappre

Law	Dappre
1 – User control and consent	The user controls which other parties are 'subscribed' to the information. But the storage of the identity on the servers of Dappre remains out of control of the user. Therefor there is only partial control by the user.
2 – Minimal disclosure for a constrained use	The Dappre application - at the moment - does not allow selective disclosure through zero-knowledge proofing or attribute selection.
3 – Justifiable parties	The user chooses with whom to share information. Not considering potential data breaches on the part of Dappre itself the data is only shared with these justifiable parties.
4 – Directed identity	Both unidirectional and omnidirectional sharing is implemented in the Dappre application.
5 – Design for a pluralism of operators and technology	As of now, the only standardization would be adhering to the QIY foundation principles. There is no interoperability outlined for the Dappre ecosystem.
6 – Human integration	The application is easy to use, in part because known contacts on the mobile phone are listed when they also use Dappre as possible information sharing parties.
7 – Consistent experience across contexts	Since the Dappre app is currently the only functioning interface, there is no cross-context experience.

Total score: 3 out of 7

[26] https://dappre.com/faq/general-questions/where-is-my-data-stored/

2.3.4 I Reveal My Attributes (IRMA)

The IRMA project is - in its core - an evolution of the IBM Identity Mixer concept. (Alpár, IRMA: I Reveal My Attributes, Privacy and Attribute-Based Identity Management, 2016) Development is in the hands of a spin-off foundation originating from the Radboud University's digital security research group. The stated goal of this Privacy by Design-foundation is to "improve the development and the use of open, privacy-friendly and secure software."[27] They actively contribute to academic research in the subject of digital privacy and attribute based credentials. (Privacy by Design Foundation, 2018) Provides a list of their relevant contributions in the field.

IRMA claims to offer a privacy-friendly, flexible and secure solution to many authentication problems, putting the user in full control over his/her data. The IRMA app manages the user's IRMA attributes: receiving new attributes, selectively disclosing them to others, and attaching them to signed statements. These attributes can be relevant properties, such as "I am over 18", "my name is ..." and "I am entitled to access ...." They are only stored on the user's device and nowhere else. According to the Github code project's Readme file.[28] Figure 18 shows a prompt from the application asking for permission to reveal an attribute with the counterparty.

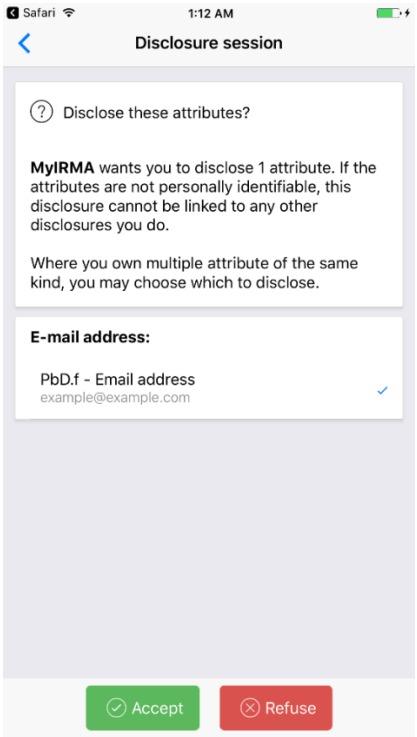

Fig. 17: IRMA selective disclosure prompt

[27] https://privacybydesign.foundation/goals/
[28] https://github.com/privacybydesign/irma_mobile/blob/master/README.md

IRMA technology demonstrators and current development

The foundation also hosts an occasional IRMA meet-up where progress in digital identity and privacy and latest technologic advances are discussed and presented with any interested parties followed by discussion and drinks. These meetups take place about once every four months. For purposes of this research the June 1, 2018 meetup was visited at SURFnet in Utrecht. Slide decks of this meet-up are available online.[29]

Current development progress is in the form of a (desktop) application in which messages can be created in the ".irma" file format. This format allows the creator to ask for a digital signature on the message, with certain IRMA attributes. The signer can do this on his or her mobile phone with the app installed by opening the mail attachment. This can open up new use cases, as it is cryptographically provable that a message is signed by a party that possesses attributes X and Y. A notable example use case is when a doctor who is entitled to write medical subscriptions digitally signs a message that 'patient X needs medicine Y' with his 'is registered in the BIG registry a doctor' attribute. Thus, it can cryptographically prove that someone is authorized to sign off on the message.

There are currently several (small) prototypes using this technology on the IRMA platform:

- The IRMA application itself is available for both Android and Apple IOS mobile operating systems.
- Alliander R&D is testing IRMA use for objects instead of persons.
- IRMA-on-chip: the IRMAcard was developed using expertise of NXP. It has not been developed since 2015, when the decision was made to switch to a mobile app based version.
- The digital concept personal budgeting assistance application called 'digitale huishoudboekje' of the Dutch municipality Utrecht uses the signing technology to enable citizens to sign permission digitally.[30]
- Several parties that work as an issuer for the actual application. Notably the municipality of Nijmegen is in the process of providing a 'pass-through' service, where Dutch citizens can log in using government authentication DigID and receive base registry identity attributes.
- SURF is in the process of using the IRMA application for two Factor Authentication (2FA).
- Professor Jacobs, head of the Radboud University's security research group and involved in the development of IRMA, used the application to take student attendance at his lectures while allowing them to find workarounds. Students quickly found that a photograph of the QR code was sufficient to allow non-attendees to sign in as attendees. The solution is being engineered: Bluetooth connectivity to share attributes peer-to-peer in physical vicinity. After this is tested in class and suitable for other scholarly contexts, the code will be shared. This also has potential for stores with age-checks for example.

During the meet-up, the conclusion of the development team was that more use-cases are now needed. The software and ecosystem are in a testable state with some valuable attributes already available through, for example, iDIN. More usage will lead to more usability testing and daily use for the citizen. The Nijmegen municipality sees the fact that iDIN might be used for identification and authentication as part of the eHerkenning system as problematic for citizen privacy: The Dutch banks run this iDIN system. The gateway can see where (what URL) a citizen logs in, it might be a website to request financial support of the government. Which then leads to financial risk of the bank, and as such is commercially very interesting information to collect.

[29] https://privacybydesign.foundation/meetings/

[30] https://www.gemeentenvandetoekomst.nl/themas/sociaal-domein/artikel/armoede-en-blockchain-het-huishoudboekje/

Scoring on maturity aspects

I Reveal My Attributes is currently – as far as we can discern - the most mature solution of the four discussed concepts. The foundation is actively working on improving the code and theoretical foundations. On a more personal note, I tried getting Leiden University to give (through SURFnet) me the option to add my student attributes to the IRMA application. This was unsuccessful, due to uncertainty on how this would interact with the upcoming GDPR, which had priority for the information management department. (Brock, 2018) Thus, it can be said that the technology is far from being embraced as privacy empowering and widely useable when fellow universities in The Netherlands are unaware of the possibilities that arise from connecting to the IRMA infrastructure to provide attributes to their students. This lack of awareness hinders the usefulness and implementation of SSI technology.

Another issue is the lack of development on the smartcard implementation, which was put on hold in favour of a more advanced solution in the form of a mobile application; the smartcard would increase technology penetration due to its lower entry barrier for non tech-savvy citizens. Lastly, the revocation aspect is especially immature, the attributes have a 'valid until' date and this is the only measure of the temporal validity dimension of the credential or attribute issued.

Evaluation on the seven laws of identity

Previous research does not evaluate I Reveal My Attributes on the seven laws as set out by Kim Cameron. (Dunphy & Petitcolas, 2018, p. 15) Therefor it was evaluated in the table below on these seven laws, while attempting to use the same reasoning these researchers used for scoring on each of the aspects.

Table 2.5: Scoring table based on the seven laws of Cameron for IRMA

Law	I Reveal My Attributes
1 – User control and consent	The user gets a prompt detailing exactly which attributes are requested by the other party. There has to be explicit consent to share these in the application.
2 – Minimal disclosure for a constrained use	Minimal disclose is possible in IRMA. A good example of this is the 'I am older than 18' attribute that can be loaded into the application. These so-called zero-knowledge proofs enable the user to constrain disclosure.
3 – Justifiable parties	Attributes are only accessible to relying parties that the user chooses explicitly by accepting the request to 'reveal' them.
4 – Directed identity	Omnidirectional identifiers are supported in IRMA, when the interacting party is both issuer and verifier.
5 – Design for a pluralism of operators and technology	IRMA currently only works for parties that use the specific technology; there is no interoperability with other standards. Which is understandable due to the identity mixer approach chosen for identity. The software of the foundation is all open source though, so other parties are free to create interoperability themselves.
6 – Human integration	The application provides decent user functionality; the requirement of having a smart phone is prohibitive. The IRMAcard smartcard is no longer developed but could aid in a wider adaptability for less digitally capable citizens.

7 – Consistent experience across contexts	User interaction driven by the mobile application. Consistently follows a QR code-scanning paradigm for all uses. The smart card implementation could make this experience even more consistent but has downsides due to the limited processing power available.

Total score: 6 out of 7

2.3.5 Conclusions on the state of SSI software

Of the four SSI projects discussed, Dappre appears to be quite different from the others. It is not possible to compare Dappre completely due to the lack of information that is available. One interesting aspect to note is that it works on subscriber-basis, so when attributes change the subscriber will be updated; this is unique at the moment for Dappre.

On the other hand, the blockchain-tech solution Sovrin shows a lot of potential but is an ecosystem rather than a useable application. There is not much opportunity right now to test it with agent software.

The other blockchain-based solution uPort is innovative in its use of smart contracts for recovery and digital identity management, but might not be optimal in terms of pseudonymity (due to the entire identity pivoting around a single controller contract). Furthermore, once it moves to the Etherium 'main net' the required input of cryptocurrency as transaction fuel will be an important factor cost-wise.

IRMA appears to be the most promising concept of the four due to the very active development of a dedicated team of University experts. The foundation spin-off is actively developing the software while the Radboud cybersecurity research group provides the academic research needed to advance the concept further. Recovery has as of yet not been a feature of IRMA, making it potentially troublesome when a citizen loses or accidently wipes their phone. The stopped development of the IRMAcard is also - from the viewpoint of inclusion – not optimal.

The table below summarizes the findings of this technical and functional review. Feasibility score can be 'Low', 'Medium' or 'High' and generalizes the results:
A. How 'self-sovereign' the concept is, by looking at the review of the tool and the maturity scan on this aspect.
B. How mature and realistic the concept is, by using the maturity scan outcomes.
C. How well it scores based on Cameron's identity laws.

Table 2.6: Maturity comparison of the four discussed identity concepts.

Tool	Positives (+)	Attention points (-)	Cameron	Feasibility
Sovrin	- Trust fabric layer based on blockchain from the start. - Innovative use of blockchain for identity.	- No testable agent application available. - Unknown token and profit model. - Scheme is heavy on financial institutions	5 of 7	**Medium**
uPort	- Innovative with recovery. - Ongoing pilot and relatively mature app. - Active development community.	- Etherium dependency (cost, size limits) - Single point of identity: the controller contract. - Requires smartphone	4 of 7	**High**
Dappre	- Subscription basis sharing means no outdated attributes. - Great for improving data quality.	- Many unknown factors: data stored out of sphere of control of user. - Requires smartphone	3 of 7	**Low**
IRMA	- Active R&D - Strong application - Developers are easy to contact	- Lack of real world use-cases. - Requires smartphone.	6 of 7	**High**

IRMA and uPort are definitely testable in a policy lab and other prototype SSI R&D projects. For Sovrin hands-on experience is also an option. The Agent front-end solution (web-based or app-based) will have to be developed or procured to be able to test the Sovrin network.

On the other end of the spectrum we find Dappre. It is a functional concept, but it is not self-sovereign in a sense that the user controls the data and that its technical functionality is largely unknown. It might be interesting to test, but only if there is more clearness on the properties and development direction.

3 First round expert interviews and conceptual framework

In this chapter, the results of the first round of expert interviews will be presented to the reader.

"Do I have to trust the government or some technology? Trust is something you often intuitionally decide yourself. When I buy an orange on the market, I look into the eyes of the salesperson and I do that to ascertain myself that he will sell me a good quality orange. Privacy, the same thing."

Four experts have been interviewed on the subject of Self-Sovereign identity as discussed in 2.2 Research structure.

3.1 Interviews and expert insights

The goal of the interviews was to find people with hands-on experience in Self-sovereign identity and enhance available knowledge of the situation and technologic possibilities. The interviewed persons have kindly shared their valuable insight into SSI.

3.1.1 Interview targets and persons interviewed

The original target for interviews with experts was five people; unfortunately, SSI experts are scarce in both number and availability, so the final number of first round interviews was one below this target. See also 2.2.1 for the considerations of this first round interview set.

Table 3.1: The Interviewed experts and their expertise area

Interviewee and organization:	**Expertise area:**
Senior researcher at TNO research	Self-sovereign Identity Framework. Standard setting and involved in several pilots to test the semantic concepts of self-sovereign identity in practice and learn from them.
Information Architect at Rijksdienst voor Identiteitsgegevens. The governmental agency for identity information and holders.	Expert in the field of identity and participant from RvIG in the blockchain coalition's identity research track.
Alliander R&D employee and freelance identity solutions software developer.	Alliander R&D: Energy infrastructure company, solution research based on IRMA self-sovereign identity concept.
Financial markets authority senior researcher and TU Delft guest lecturer.	A financial view of self-sovereign identity and consumer protection.

A more informal interview was also held with the writer of a thesis that visualized blockchain based self-sovereign identity. Her vision was that of a future passport-replacing scenario for Schiphol Airport. (Poot, 2017) This interview was not a planned interview for this thesis but the input on the subject and explanation of the user centric side was of value to the policy lab and the understanding of SSI future possibilities. A clear take-away from her research was that the government is the most trusted party with identity attributes because it has no commercial goal as also described in the introduction of this thesis.

3.1.2 Interview questions

This section will introduce the reader to the questions that were asked during the interviews. The transcribed answers to the questions are used to shape the SSI framework and advice on the government role in digital identity.

The first three questions that were asked created understanding of the interviewed person's role in the public sector and their interactions with identity in this role.

1. What is your role and that of your department in the Dutch public sector?
2. How does your department interact with the topic of digital identity?
3. What are the points during this interaction that could be better? How could Self Sovereign Identity help with that?

The second set of two questions has the goal of finding out what are current research topics the experts have ongoing concerning digital identity and how they see the challenges in this domain. These questions are:

4. What research is currently being done within your organization concerning digital identity?
5. From your professional viewpoint, do you see digital identity challenges as trust-related or privacy-related?

The third set consists of two questions that are more concrete. These questions are asked to gain understanding in the potential benefits and challenges of SSI. They are:

6. What should from your departments perspective, be the most important qualities of a self-sovereign digital identity system? Make a top 3 or top 5 list.
7. Can you name one or two challenges within your organization concerning citizen's digital identity?

The last set of subject oriented interview questions consists of three questions about the role of the government in a future digital identity. The results of these questions are discussed in section 3.2.3 of this document.

8. Should the citizen have complete control over digital identity or should the government keep control?
9. Should the government in five years offer a digital 'passport' to citizens?
    - **If yes:** Can you envision such a passport, what technological form would it take? Can you draw it out?
    - **If no:** What would be bad about that proposition?
10. Would the role of the government in digital identity, according to your professional vision, be only standard setting or should the government build an actual solution? Why?

The last question had the purpose of finishing the interview and finding out what other organizations or persons in the opinion of the interviewee might have valuable input.

11. Do you know of any other persons, departments, which could have valuable input on this subject?

In the next section, the expert opinions on governmental role in SSI are discussed for each of the three relevant questions.

3.1.3 Expert opinions on the role of the government in Self-sovereign identity

Three of the interview questions were especially aimed at finding which role the experts envision for the government in the future of self-sovereign identity. These questions are discussed in this section of the document.

Q1. Should the citizen have complete control over digital identity or should the government keep control?

"But the basics for example your name, birthdate, city or residence and maybe some more attributes... Why would you not give out an attestation for that?"

One interviewed person names Identity fraud as a specific concern that requires oversight in the digital identity future.
Someone should also be legally responsible for the digital identity and its interactions. Another interviewed expert adds that the power is in the split roles possible due to attribute-based identity, the government can attest to the validity of others (such as municipalities) that provide attestations and in this way help the ecosystem. This person also thinks that the same 'governance' should apply as with a physical passport: against impersonation and identity theft, but no control over and knowledge of where and how it is used.
Another expert thinks that the government should not decide what attributes are 'reliable' and leave this up to the acceptant. Lastly, one expert answered that for the Dutch government it should give citizens at the base registry information in a digital way. Maybe look at whether the person is capable of using it responsibly, but not more than that. He also notes that by providing attestations the citizen can become the connection between different systems and organizations, so there is less of a need to interconnect information technology for sharing identity information, reducing privacy risks.

Summarizing, the experts all see a form of governance in the ecosystem for the government. This role is boundary setting (no loaning-out digital identity or impersonation) rather than controlling in nature.

Q2. Should the government in five years offer a digital 'passport' to citizens?

" .. The user can become the connection between your systems."

From the perspective of the RvIG interesting information was shared that an internationally accepted digital passport would have to adhere to the standards that the ICAO (International Civil Aviation Organization) sets. They are involved in the blockchain identity pilots that the RvIG is also involved in at the blockchain coalition. The interviewed person could see a digital passport arriving sometime in the future, but replacing the physical passport is not something they see happening in the near future. Standardization is still very much ongoing and, an international standard for SSI would accelerate the development.

Another interviewer says 'I think the government should issue attributes, like the ones on the passport. However, the 'passport' itself could be the IRMA application or a comparable solution that is maintained by a non-profit organization. Yet another expert sees the redundancy in issued physical identity holders, in his example the driver's license. As he puts it '... I think that a driver's license is harmless enough to be digitized and put wherever', he recommends starting with these kinds of 'low hanging fruit' identity cards to pilot SSI.

Concluding based on the interviews: all experts see the government as an important partner for future SSI ecosystems. A 'digital passport' in some form should be possible but they agree that this could be just issuing attributes and letting a non-profit market party serve as the 'holder' of this identity. The suggestion that future pilots could involve digital driver's licenses was very interesting; it is discussed further in the framework concept.

Q3. Would the role of the government in digital identity, according to your professional vision, be only standard setting or should the government build an actual solution? Why?

"I think the government is the only one with a non-commercial role in digital identity and from that point of view can go for the highest security and privacy without caving in to commercial pressures."

This question served to get a response from the experts in what they see as the future role of the government in SSI development. Responses were (paraphrasing) that 'I think that the government is the only one that can play a non-commercial role in it', 'create some test locations where people can get attestations in a couple of different ways', 'I don't think the government is in a good position to actually build something like that. .. We are not an IT company, not a software company and do not think it is a good idea to build software ourselves.'

From this, we can clearly conclude that they do not think the government should actively develop digital identity software at the current time.
The experts see market parties as capable enough, but also think the government should play a role in governing the way self-sovereign identity evolves for the societal greater good. Being a primary source for valuable identity attributes and trusted validator, the government has the power to steer the development from a higher level without development investments.

3.2 Interview coding strategy and results

In this section, the method of interpreting the interview results will be discussed. The coding technique was based on the methodology explained in the advanced research methodology lectures. (Heijstek, 2017) The complete list of coded and translated sentences is included with this document as a separate attachment together with the interview transcripts (in Dutch). (Attachments II and III) His coding enabled the qualitative examination of concepts mentioned, which are then used in the framework that has to be designed.

3.2.1 Transcription

First, the interviews were transcribed literally from a recording that was made with the permission of the interviewed person. This transcribed version was sent to the interviewees for a final review and open coded after revisions. After coding the contents of these interviews the quotes were grouped as explained in section 3.3.2 and 3.3.3 of this document.

3.2.2 Method of open coding

> *"Open coding simply means code everything for everything"*
> *(Heijstek, 2017, p. 17)*

The transcribed interviews were labelled with this open coding strategy in mind. Difference is that only meaningful sentences of the interview were first labelled by content with a coloured marker, so not filler conversation or irrelevant sentences for this SSI research: Some interviewees diverted a bit to explain related concepts that were only related to understanding their role as a professional, for example.

All marked sentences were then inserted into an Excel spreadsheet together with content labels. Then these content labels were in turn used to form the code categories.

3.2.3 Coding categories resulting in dimensions for the framework

After forming initial categories these were reviewed once more together with the policy officer in charge of materializing the policy lab. After this review, they were combined into the final six dimensions.

The final six dimensions of governance based on the coding are:

- **Input / acceleration.** Input that can be added into the process to accelerate the technologic development by the public sector.
- **Output and benefits.** Societal and governmental gain from the results of SSI development.
- **Performance indicators.** What makes SSI 'good' quality for society?
- **Public values.** The public values that come in to play concerning SSI.
- **R&D.** What development or theoretical questions remain?
- **Requirements.** What requirements does society and the government have in a SSI concept?

These dimensions and the quotes from the interviews for each of them have then served as the foundation for a first conceptual framework. An example of the coding is shown below.

Table 3.2: Example of the coding tables as used for analysis of the interviews.

Category:	**Subject:**	**Text:**
public values	Vulnerable customers with SSI	Vulnerable customers will sit on a lot of information, what we see now is that everyone gives that away to Facebook and Google.
public values	governance	I think as a society we still cling too much to entities. I do not know how much you have heard about decentral markets; in a decentral market actually no one is responsible for the market. .. You cannot govern it, because there is no one to talk to.

Significant quotes not fitting these dimensions are not labelled. This framework was discussed during the 'Governance and boundary-setting of eGovernment' (Dutch: Regie & Kaderstelling i-Overheid) department. In the following chapter, this process will be explained in more depth. The complete code document is found as one of the attachments.

4 Design cycle of the framework (finalization)

After delivery of a first concept, according to the design science methodology of (Hevner & Chatterjee, 2010) the design phase focusses on designing and then refining this artefact. In this thesis, the artefacts as listed in the 2.2.5 are:

- Strategy and governance model.
- Possible roles and interventions the government has in SSI according to research.
- Recommendations on how to proceed in strategic and tactical positioning.

In this chapter, the creation of these artefacts based on the relevance cycle and rigor cycle is explained to the reader. The sources for the content of the framework such as interviews or theory are found in the finalized version (chapter 5 of this thesis).

4.1 Conceptual version of the SSI public value framework

Management can be split into traditional levels of three levels of scope: The Strategic, Tactical and Operational level. (Anthony, 1965) In their classic paper Gorry & Morton discuss these three dimensions and how they could be used for managing information systems development. (Gorry & Morton, 1989) In our framework the information from the expert interviews was combined with this triangle or pyramid to show more clearly on which levels – and how – the government should get involved according to the knowledge gained and future expectations. The result of this is shown in figure 19.

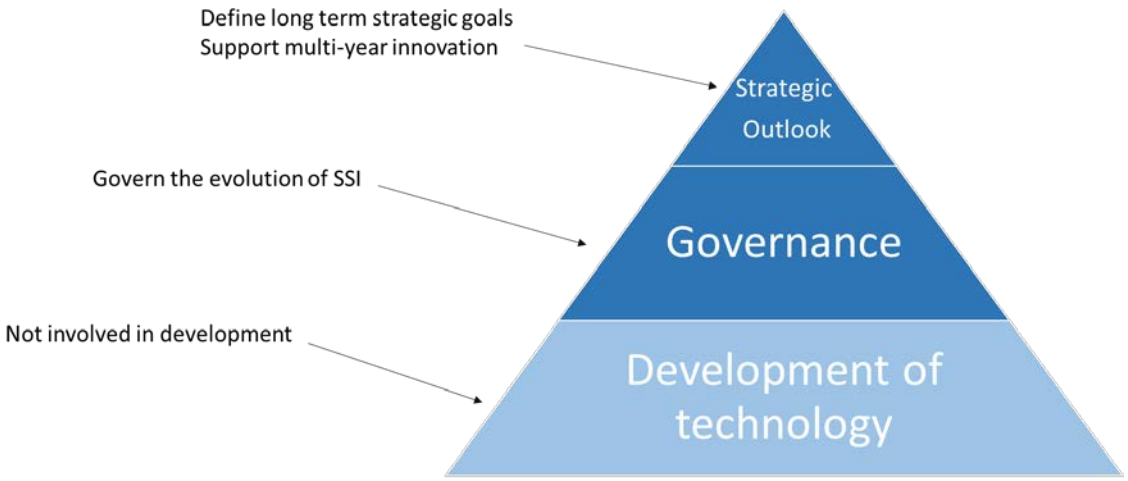

Fig. 18: adapted from the IS management pyramid (Gorry & Morton, 1989)

Logic models for program management have existed in practice at least since the late 1960's. (Weiss, 1972) Their main goal is to aid planning and decision-making of long-term programs. Taking the concept to a new level of maturity, McCawley introduces a clear document on how to implement program planning in practice. (McCawley, 2001) This researcher's most significant addition to the body of knowledge is a simple model for program management based on three moments: Inputs, Outputs and Outcomes, it is shown in figure 20.

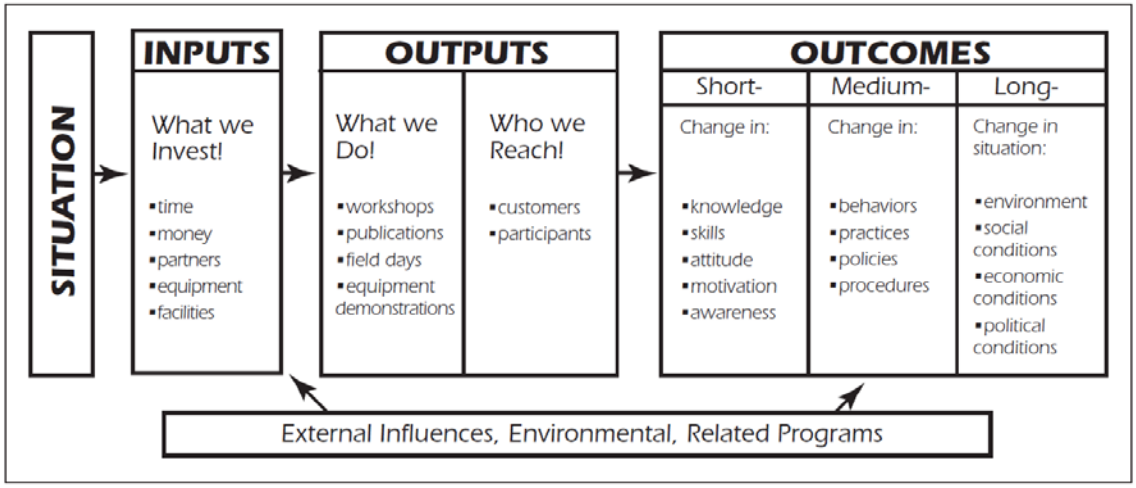

Fig. 19: The Program Logic Model (McCawley, 2001)

The logic model of McCawley is designed for internal company information systems programs. This means that it is not directly applicable in its original form for managing external programs, or software development. Therefor the model was adapted to create an iterative model, due to the evolving nature of self-sovereign identity. The situation is in our model the strategy from which the government wants to participate, then the inputs remain inputs, the outputs become the development and the outcomes become the output. The output of the cycle is in this model seen as new technologic advances or research results, resulting in change. The term strategic goals are also present in the model by McCawley: a change in situation of both economic and social conditions.

In figure 21, the adjusted model is shown as an iterative process. In this case the development of self-sovereign identity is modelled in it. By taking these three moments of interaction and changing them into governance questions, that we can find roles for the government:

- What can we provide as input to aid the development and use of SSI technology?
- What can we do to help speed up development?
- What do we gain as societal benefits when the development cycle is complete?

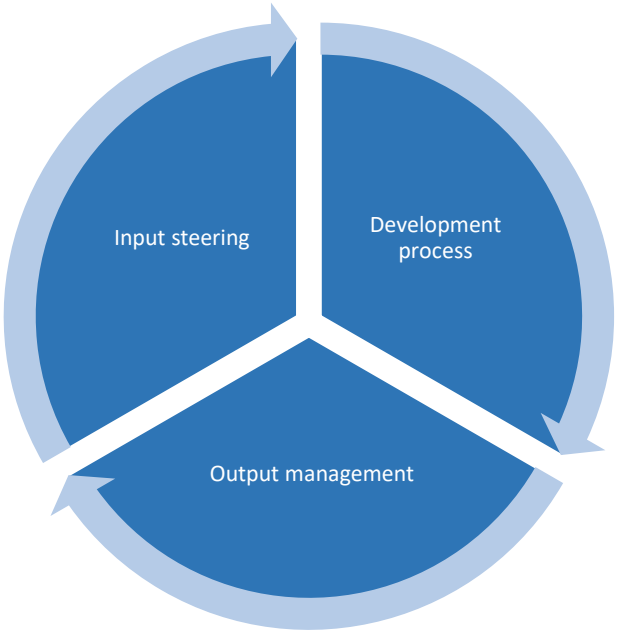

Fig. 20: Three possible governance moments of SSI development.

Accordingly, the suggestions of the first round interviewees were converted to actions the government can take in each of these domains or areas of concern. This gives the ministry some 'a-la-carte' options to respond to development and more effectively govern the technology advance of SSI. For each of the three moments, the following table lists possible government interactions and considerations.

An initial version was presented to R&K team for review. Sources are listed at the final version in this document. (Section 4.3 of this thesis)

Table 4.1: Initial version of framework contents.

Input:	**Development:**	**Output:**	**Strategy:**	**Public values:**
RvIG identity data.	Policy lab R&D	economic possibilities and effects	Secure and trustworthy identity, with high quality identity attributes.	Pseudonymity: privacy due to seperation of complete identity.
Funding based on challenges .	Standardisation effort	Form of a 'Digital passport'	citizens get 'regie op gegevens'	Paper and low-tech versions available as alternatives.
Innovation grants. (BADO)	Identity fraud detection and reducing with SSI	Dataminimalisation and dataquality	Is the government ready to 'lose control'?	Understandable for the end users.
Funding in NWO identity track	Create actual use and promote use.	SSI can make many processes with an analog identity as start faster and easier	create SSI coopration with interested parties in the public sector	Inclusion and exclusion: cheaper products for users, need new smartphone, no alternative
Verify municipalities as issuers	Test the crypto to aid development.	SSI attested statements make for example medicine recipes easier digital.	Only interested non-commercial party to govern SSI technology.	Vulnerable citizens will 'sit' on a lot of valuable identity information
Legal power of SSI solutions	Assuring the link between 'real' and digital identity.		Replace low risk analog ID's with digital version: Drivers license?	Higher level of privacy control
	Can SSI concepts comply with eHerkenning (eIDAS) scheme assurance levels?			Safety of digital identity (reliable and fraud proof)
	Find the barriers for issuing SSI attributes, what are requirements exactly.			Acceptance and validity at the accepting party not the government
	Create a self-service data quality improvement based on and with SSI tools.			Prevent vendor lock-in

Two questions were asked in this first round of expert review:

1. What is your view on these proposed forms of governance for the Ministry of the Interior?
2. Where and how would you advise me to test and discuss this framework?

Due to the short timeslot allotted for this meeting there was, unfortunately, not enough room to discuss them in depth. The participants were positive about the global framework presentation that was able to be presented. After some discussion on how to proceed, another strategy was chosen. This strategy consisted of selecting public sector employees that can provide feedback on the concept framework completing expert review. Constraints are five subjects with two experts each.

In total ten experts were asked for review. These questions and information about this second round of interviews can be found in section 4.2 of this document. The complete first version 'concept framework' presentation (in Dutch) can be found attached to this document. (Attachment V) Another 'task' for this round of interviews consisted of creating a (possible) timeline for the future of SSI in the public domain. This can spark discussion about the actions that can be taken and the direction that is visualized. Thinking ahead about possibilities and uncertainties can lead to better management of technology. An example of this is the Scenario Planning methodology widely used in international enterprises. (Schoemaker, 1995)

4.2 Second round interviews: improving the concept framework

The second round of interviews will focus on improving the governance framework. Five subject area questions are the focus of these interviews, which are based on the concept framework to increase knowledge and maturity. These are to be discussed with two internal policy experts each, which helps strengthen the framework with their policy experience. These interviews are summarized, due to their simple and informal nature they have not been recorded and literally transcribed. Some notes were taken during the discussion to document them but not literally.

Table 4.2: Second round interview subjects and selection

Which policy expertise	**Policy question(s)**	**Number of Interviews realized**
Digital strategy policy makers.	How can we – being the government – form a long-term strategy for a subject such as Self-Sovereign Identity?	2
Legal: especially eID-law.	How much room is there for experimentation with digital identity solutions? Are there set requirements which a SSI tool has to meet to use identity attributes?	1 out of 2
Inclusion and public values.	Are any important attention points in the framework missing concerning public values and inclusion? How do we govern based on these values?	2
Innovation and public-private cooperation.	When a certain SSI application shows a lot of promise, what is the correct way to accelerate development from a tactical level? (With both knowledge and resources)	2
Public sector governance and fram eworks.	How do you get a broad base of support for a framework? What can I improve in the concept framework?	1 out of 2

For each of these five subject areas the expert interviews are discussed below in the corresponding section.

4.2.1 Digital Identity Strategy

According to one of the interviewed experts on government strategy formulation concerning technology, there are several success factors involved.

From this person's experience strategy in the government will typically arise from policy makers rather than the 'top management group'. Therefor it is important to know about the subject and then convey the importance of a long-term strategy to the top management.

This expert mentioned five specific steps of successful government strategy development, where stage 0 is the preparation stage of said development process:

0. Find the different stakeholders and forces and analyse their unique perspective and role.
1. Build up expertise, do not just look while others (are hired to) experiment but partake as a policy department also. Do **not**: endlessly pilot, build solo solutions.
2. Create a group of like-minded organizations and show others the benefits, from their own perspective of the new technology. Become a platform or covenant. Immediately involve citizens.
3. Ask for a formal strategy in a policy note. Keep in mind that public values are the goal. However, do know what other parties want.
4. Propose adjusting the law to facilitate the change.

Lastly, he proposes that: A good combination for enabling top down change is the lead of the manifest group + Secretary General + CEO of an organization in the public sector that interacts directly with the citizens like the chamber of commerce or tax office. The stakeholder of such an organization often has quite concrete views on how it can improve public sector interactions.

Another government strategy expert that spoke at the Blockchaingers Identity Deep Dive for the Ministry gave feedback on the conceptual strategy models. First, from this person's experience with self-sovereign identity concepts in public sector his concept framework remark was that within the government identity is approached as an 'institutional identity', not as the 'personal identity' a self-sovereign identity is. This distinction should be made clearer in the final version of the framework, he argued.

He also proposed that the two important competing public values from the government perspective in identity are 'trust in societal interactions' and 'protection of the individual's integrity'. These can be seen as facilitating on one hand, protecting on the other. An example, a passport shows this fact: On one side, it facilitates trust and societal interactions while on the other it is protected by authenticity features and government regulations and laws. These protections are not always compatible with ease of use in society. A concern of SSI from this viewpoint is that the ecosystem is vulnerable: valuable identity data is placed at the citizens who often do not know the real value of such data. Therefor he proposes identity brokers acting on behalf of citizens in an interaction, which the government can then verify and govern. These brokers could for example be banks, as they already have expertise and core competency in protecting data and trust.

The issue with such a system is that it again leads to someone else (the broker) controlling the identity, which conflicts with the cyber anarchistic mind-set of some SSI developers such as the IRMA team.

This expert defined the following strategies as possible routes for the government in SSI:

1. Against this development: The risks of combining identity and giving citizens control are too high, on an international level try to halt the development.
2. Facilitate: Help the development in a beneficial direction, with the governance possibilities.
3. Don't interact: keep doing identity as we are doing now, leads to a disconnect between societal expectations and government service delivery.

Lastly he proposed that the government should start with some simple attestations, on regional or national level, to try self-sovereign identity in society and see the risks and possibilities.

4.2.2 Legal and eID-law influences on SSI

One of the important factors for self-sovereign identity experiments is legal in nature. (European Commission, 2014) The Dutch upcoming 'Digital Government law' (Dutch: Wet Digitale Overheid) is also of influence in the authentication and identification of citizens in the (semi) public sector. The final version of this law will be available to the public soon. According to one expert, the Digital Government Law requires the parties it applies to accept:

- The eHerkenning scheme for companies.
- The national DigID eID system.
- A yet to be defined private system or systems.
- Functionality to authorize others: Out of free will, allow someone to use the eID on your behalf.
- Nothing else. It is not allowed to accept any other solution (unless experimental, see below)

Additionally, when they accept eID with a 'substantial' or 'high' level they have to:

- Decide to notify. If a notification is started, acceptance of the level will mean it has to be usable EU-wide but also implies that all other 'substantial' and 'high' level eID's (that are successfully notified by other parties) have to be accepted.

That also applies to experimental eID's, but it is possible to not claim one of these levels for the experimental solution: When not claimed, neither of the levels is assumed. Such an experiment is possible for a maximum of four years, through the 'algemene maatregel van bestuur'. After this period the solution has to be registered by legal route. Experimentation is certainly possible under article 28 and 29 of the Digital Government law. To private companies, these rules do not apply unless they are specifically included such as healthcare insurers.

4.2.3 Public Values

Three of the public values are specifically towards the digital inclusion of the end user:

1. The application should be understandable for non-digitally savvy users.
2. There should not be any incentive for use that disadvantages people not using (or able to use) the digital solution.
3. Vulnerable user groups will sit on a valuable information store with their self-sovereign identity.

To find out what they think of the role of the government in these values, and other public values concerning technology, two short interviews with expert policy makers in this field were scheduled. During these interviews the public values we found in the coding of our expert interviews were also discussed, in an attempt to give them a ranking or priority.

One of the two interviewed policy experts started by clarifying that the goal of the coalition that 'people will be given a greater role in managing their own personal information' is a nightmare for quite some citizens. (Rutte, Buma, Pechtold, & Segers, 2017, p. 11) They are not very digitally capable or do not understand the implications of using technology and are digitally averse due to perceived risk of trusting something they do not understand well at all. This group does **not** exclusively include old or relatively less educated people: The Ministry's experience is that these challenges are present in each layer of the citizenry in The Netherlands. To further illustrate this fact, the interviewed expert named an example where a person with a PhD and a very strong job position in the legal system avoided digital interactions as much as possible. Having 100% of the target group use a digital project is (in the subject of digital inclusion) never possible, but educating and informing the public well and gradual implementation can help achieve a higher 'market penetration'.

Another recommendation is to write the citizen interactions in the more basic 'B1' language level to make the application accessible and understandable to a higher percentage of citizens. Being able to authorize another person to do things on your behalf is an important factor for achieving an inclusive digital identity. This should be an item on the R&D agenda of Self-sovereign Identity, so it is more widely useable.

When discussing our list of relevant public values with the policy experts they noted that it was not possible to rank them in a meaningful way, they were all seen as important factors for success.

4.2.4 Innovation and public-private cooperation

One interviewed expert has extensive experience with the eHerkenning digital authentication method for businesses coming from the Ministry of Economic affairs. The government took a more high-level goal, it left the actual solutions to the market but managed the eHerkenning 'brand' closely: if a solution wanted to participate in the scheme and receive permission to participate as an identity gateway they have to abide by principles set forth by the government and a list of norms and requirements. The scheme provides independence of a single vendor and provides interoperability and choice of the authentication method. Such a scheme already exists in the eHerkenning governance framework where several parties provide certified authentication services on eIDAS levels basic, substantial and high.[31]

Then shortly after this interview, at the IRMA meetup discussed earlier, these levels were also discussed as important to the societal viability of the application. This could possibly be a good connection between the government and the developers of SSI tools in giving them a goal to work towards and helping them with a set of standards to adhere to that (when met) lead to advantages in usability.

Another expert that was asked for input is the product owner of the 'machtigen' functionality of DigID. This functionality enables citizens to authorize others to use DigID on their behalf, for example their caregiver. His experience with the public private cooperation is that it helps development to first define a set of requirements that you have as the government. Then when these requirements are satisfied, the government can give the software a valuable approval. This approval often comes from acceptance into a public-private scheme, but can also be in the form of an innovation grant from a secondary Ngo. He also names the eIDAS levels as possible requirements that should be met by a self-sovereign identity, which in turn makes it valuable for usage.

[31] For more info about eHerkenning see https://www.eherkenning.nl/english/

This expert also emphasizes that building a business case can encourage public-private cooperation, if there is a more clear understanding of what benefits SSI has for a business they are more likely to get on board. Concluding with the notion that 'you have to focus on getting it widely used, both private sector and public sector'.

4.2.5 Public Sector Governance and Frameworks

Two experienced policy makers were asked about their experiences with governance and frameworks. One expert discussed experiences with setting up Standard Business Reporting, a digital way of sending financial 'messages' to parties within the scheme. The Government has the role to keep supervision on these schemes and enable them: that is where the expertise is according to the experiences of this policy maker. By setting up such a scheme, the technologic advances can be more actively managed and adjusted to maturity. Sharing knowledge with the scheme partners can lead to developments in the direction that the government prefers.

The expert also explained that another attention point in the governance of private-public sector cooperation is that it benefits greatly from a mandate of someone held in high regard in the ministry: a former Secretary General was named as a very powerful and positive influencer of a past cooperation project. It helps to set clear goals for the cooperation and communicate these views to all participants so they know what to expect of the government and what the government expects from them. Lastly, in the policymaker's experience it helped to draft a cooperation agreement, this commits parties to the common scheme.

4.3 Final version of the governance framework

In this section, only the changes from the initial version of the framework will be presented to the reader to prevent duplication. In the finalized version, interview or other sources for each item in the framework are also noted. The complete final version is also available as an attachment with this document in the form of a presentation. The final version is split in two sub-sections: first, a set of models will be shown to guide towards an interaction strategy and strategic long term outlook, then in the second part of the framework the options for interaction to work towards the envisioned timeline are presented to the user.

The framework has three steps that will result in a structured interaction with SSI:

1. Decide whether the government wants something to do with this technology at all, if so: what. This is based on the two competing roles of the government as shown in figure 22. This results in the strategic outlook, as explained in part 4.3.1 of this thesis.
2. Decide on Governance: Investigate the qualities and weaknesses of the SSI development based on several public values. This is discussed in part 4.3.2 of this thesis.
3. Manage the development: Based on the qualities and weaknesses, the government can now in a structured way encourage development in the 'right' ways by adjusting the development of SSI technology in three different ways: By providing input to the process, by aiding the development and by managing the output. This is discussed in part 4.3.3 of this thesis.

4.3.1 Strategic outlook

The strategy part of the framework will define the five year strategy concerning SSI of the Ministry. To do so, a strategic question should be asked that is the first part of the strategy formulation. In turn, the first part of the framework intends to help policymakers answer. It is based on both Strategy decisions and possible interactions to manage the technology from a governance level.

Strategic direction: How do we want to interact with SSI in five years as the Ministry of the Interior and Kingdom Relations and society?

This question should be discussed on the decision making level, so a clear mandate exists if it is chosen to interact with the technologic development. The first change from the concept is that the two public values mentioned by a strategy expert were added to the framework. This gives persons examining the SSI governance framework insight into the forces of enablement and caution on behalf of citizens.

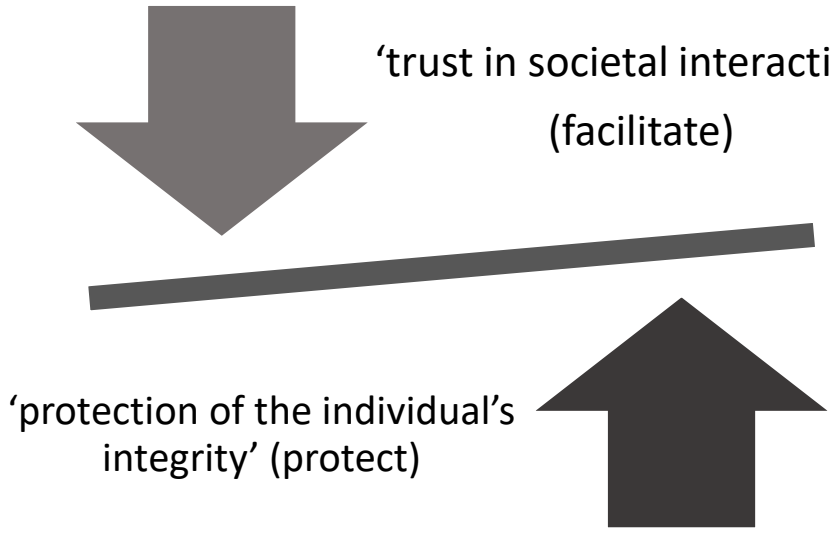

Fig. 21: Competing public values in self-sovereign identity

The two values in figure 22 are equally important, so a decision has to be reached on how these senior decision makers see the future of SSI technology and the government's preferential role in it. According to the policy experts there are three logical strategic direction decisions following from this discussion:

1. Do not condone this development. For example because the protection outweighs the facilitation public value. (Then do not continue with the framework, seek ways to prevent technology usage for prevention of societal risks.)
2. Facilitate and manage the development of SSI. An example would be a cooperation that leads to a 'four-corner' model. (Then use this framework to govern development.)
3. Let this technology evolve without any interaction. (re-evaluate the decision one year from now)

If the second option of these three interactions is chosen as the current government position, the governance part of the framework can be used to then help develop and cooperate. The public values found in section 4.3.2 of this thesis are the first part of this governance: They give the government 'requirements' that can be managed in development for societal benefits. The second part of this Governance level consists of the actual interactions there can be with the evolving technology, these can serve to guide the development in different ways.

Then, proceed by creating a strategic timeline for self-sovereign identity. Ambitions decide the possible timeline. This is an example (ambitious) timeline for SSI development in the public sector. Such a timeline can be made in cooperation with municipalities and other partners, after the results of the digital identity policy lab, to find follow-up possibilities. The 'optimistic' timeline, which was compiled based on the interviews and leading to the 2030 target of the Schiphol passenger research is shown below as an example of how the SSI technology could evolve. (Poot, 2017) This can then be presented to the decision makers to discuss whether it is a timeline that can be realistically supported.

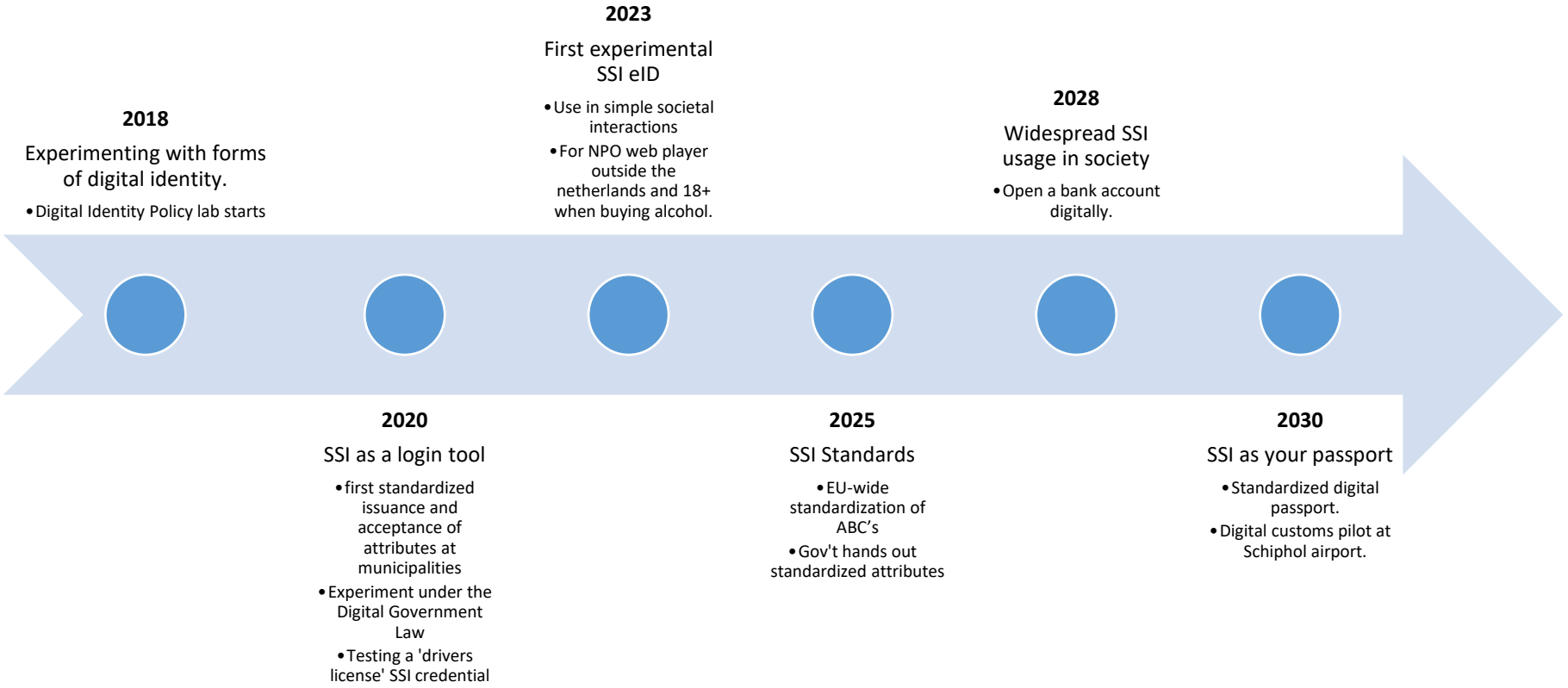

Fig. 22: A Possible strategic outlook timeline for SSI.

The finalized strategic positions the government can take are listed in the table 4.3 below. These goals can be used to create a 'business case' for investing in SSI concepts as the government.

Table 4.3: The strategies of the framework and their sources in our research.

Strategy:	Interview Source(s):	Interview code sheet codes and notes:
Secure and trustworthy identity, with high quality identity attributes.	Interview RvIG	Interview Codes: Requirements / Software development
Giving citizens more control over their information.	Interviews TNO and AFM	Interview code: SSI as key to privacy, coalition accord 'regie op gegevens' program.
Cooperation with other organizations in self-sovereign identity.	Interview TNO	Interview code: partner up with expertise
Governance of self-sovereign identity with societal values in mind.	Interviews RvIG and AFM	Interview code: Social value of SSI
Greater efficiency due to digital possibilities of SSI.	Interviews TNO + AFM + RvIG	Interview codes: Qualities for the relying party, qualities for the issuer, qualities for the holder.

4.3.2 Governance: Manage based on the Public Values

On the governance level, the technologic advances of SSI are monitored and when required, adjusted using the options on the interaction level. This serves to adjust the technology in a direction that is not only beneficial for privacy aware citizens and developers of the tools. This wider usability can then, in turn, lead to usability in citizen-government interactions such as digital signing or electronic voting in the future.

The public values from the conceptual framework were discussed with policy experts, after doing so it became clear that they could fit well within the Governance decision making. Several of the policy experts noted that the public values could be used to decide on interaction with self-sovereign identity in the future. Table 4.4 contains these public values, their interview sources and notes.

The most important public values based on the interviews with SSI experts and Policy experts were 'Right to be anonymous' and 'Right to privacy'. All of the experts named these in their interviews, which might be logical as these are the core values of the Self Sovereign Identity paradigm. The policy officers however were more focused on the protective role of the government and named Inclusion and Accessibility as important public values to manage.

In the Governance level, decisions can be taken on how to manage the development based on how the technologic concepts perform on each of these values. They, as such, serve as qualitative indicators rather than a set of priorities.

Table 4.4: The public values of the framework and their sources in our research.

Public Value:	Interview Source(s):	Notes:
Right to be anonymous: Users should not be forced to be identifed unneededly.	All expert interviews	Interview code: Privacy
Accessibility: Low tech alternative and understandable for end users (also language-wise).	Policy expert review: digital inclusion Interview TO.	Thesis section 4.2.3. Interview code: Digital inclusion.
Inclusion: Not using SSI should not lead to disadvantages.	Policy expert review: digital inclusion	Thesis section 4.2.3.
Equality and safety: Protect vulnerable users against misuse.	All expert interviews. Expert review: digital inclusion	Interview code: Role of the government
Right to privacy: Give users more privacy controls.	Coalition accord, all interviewed experts	Interview code: Privacy
Safety: Tested to be reliable and fraud-proof.	Policy expert review interview: eIDAS levels as standards for reliability and security.	Thesis section 4.2.2 and 4.2.4.
Freedom of choice: Acceptance validity at the accepting party not the government.	Policy expert review interview: eIDAS levels as standards for reliability and security. Cameron's Digital Identity Laws	Section 4.2.4 of this thesis. eIDAS gives the citizen choice of authentication provider.
Efficient and fair government: Prevent vendor lock-in.	Policy review: eIDAS and Expert interviews	eIDAS aims to prevent vendor lock in with identity provisioning. Interview code: Benefits for the Holder.
Democracy: Self-sovereign identity can strengthen digital democracy.	Theoretical input.	The PrimeLife pilots and other research. (Spirakis & Stamatiou, 2013)

4.3.3 Three moments of interaction with SSI development and possible actions.

For interaction, the strategies are designed based on the two rounds (with internal and external experts) of interviews. The second round of policy experts that were interviewed has improved the quality of the interactions and added new interactions. Table 4.5 shows these interactions, the relevant development phase, sources and notes.

Table 4.5: The development interactions of the framework and their sources in our research.

Development step:	Action:	Interview source(s):	Notes:
Input	Providing some RvIG identity data as SSI attributes.	All interviews: Question 9 and 10 answers.	All experts think that the government can help development by providing (some of) her identity attributes.
Input	Funding based on challenges.	Policy expert review: Innovation and public-private cooperation	Start-up in Residence where start-ups that provide innovative solutions to societal challenges receive funding and support. Government approval has business value.
Input	Innovation grants.	Policy expert review: innovation	Section 4.2.4 of this thesis
Input	Funding in NWO identity track.	Interview RvIG	Interview code: NOW research track.
Input	Verify municipalities as issuers.	Interview TO + TNO	Interview code: verifying municipalities
Input	Legal power of SSI solutions.	Policy expert review: eIDAS law.	Section 4.2.2 of this Thesis.
Input	High level commitment.	Policy expert review: Governance and Frameworks.	Section 4.2.5 of this thesis: High level mandate.
Development	Involved in the Standardisation effort.	Interview RvIG	Interview code: Standardization effort.
Development	Identity fraud detection and reducing risk with SSI.	Interviews RvIG + AFM	Interview code: fraud protection
Development	Create actual use and promote use.	Interviews RvIG + TNO + AFM	Interview code: role of the government
Development	Test the cryptographic properties to aid development.	Interview AFM	Interviewee stressed that using SSI technology will put a lot of confidence in the crypto. Interview code: Cryptography of SSI
Development	Assuring the link between 'real' and digital identity.	Interviews AFM + TNO	Interview Codes: Easier identity, implementation possibilities

Development	Help SSI concepts comply with eHerkenning (eIDAS) scheme assurance levels.	Policy expert review: eIDAS and legal	Section 4.2.2 of this Thesis.
Development	Find the barriers for issuing SSI attributes, what are requirements exactly.	Several interviews	Interview code: Requirements.
Development	Create a self-service data quality improvement based on and with SSI tools.	Interview RvIG + TNO	Interview code: Data Quality
Development	Authorization (machtigen) in SSI architecture.	Policy expert interviews: Innovation and Public-Private cooperation	The 'machtigen' functionality in DigID is named as an example of cooperation and a challenging problem in identity.
Output / Outcome	Economic possibilities and effects.	Interview RvIG	Interview code: economic effect
Output / Outcome	Form of a 'Digital passport'.	Interviewed persons.	Explicit Interview Question 2.
Output / Outcome	Dataminimalisation and data quality.	Interview RvIG	Interview code: Dataminimalisation, Data quality.
Output / Outcome	SSI can make many processes with an analogue identity as start faster and easier	Interviews AFM + TNO	Interview code: easier identity
Output / Outcome	SSI attested statements make for example medicine recipes easier digital.	Interviews TNO + AFM	Talked about SSIF pilots with SSI statements serving as 'recipes'. Interview code: easier identity

The three-cycle design is retained from the conceptual version. The table above shows the interactions that are possible according to the research results. This list is not definitive, but once the choice is made to pursue a strategic timeline, these interactions can be used while they can also be expanded with new knowledge from citizen interaction and policy R&D.

5 Conclusions and discussion

At the start of this thesis, the goal was to answer the research question: 'How can different self-sovereign identity technology developments be governed and accelerated based on societal values?' To answer this, the resulting framework gives the user a set of decision-making tools at the strategic and tactical levels of policy making. For this, the sub-questions served as input and guidance. In section 5.1 we will summarize the conclusions of the research, in section 5.2 we will discuss these as a whole and in section 5.3 we will reflect on our research and discuss future directions of research.

5.1 Conclusions of the research

Previous research on the matter of SSI was completed and some research is ongoing currently, notably the uPort pilot in Switzerland and IRMA development. The past EU-sponsored projects have resulted in testing of the IBM identity mixer code to a degree of satisfaction and some of the attribute based credentials technology that enables a form of Self-sovereign identity was implemented in eID cards but not used to enable SSI itself due to the single source of attributes on these cards. More research is needed, especially on how to make SSI useable in government-citizen interactions, so it can be tested in practise.

During our technology study we found twelve concepts that can be categorized as Self-sovereign identity concepts, listed in section 2.3 of this thesis. Four of these were in a testable state of completion, these were compared using Cameron's seven laws of identity and both descriptive documents and hands-on testing. This resulted in a feasibility score for each of the four concepts, leading to uPort and IRMA scoring a high feasibility, Sovrin scoring a medium feasibility and Dappre scoring a low feasibility. As such we can conclude that the technology is there to enable SSI. This process of analysing SSI concepts can be repeated, to find out how this comparison changes over time.

Several Self Sovereign Identity experts that were not bound to a certain technologic solution were asked what their opinion on the technologic paradigm and the role of the government in it was. They agreed that the government should take a strategic and governing role as the only non-commercial party involved in identity. They also saw getting involved in the development as a move the government should not make, as this is not the natural role of the government and the current developers are capable of delivering quality software.

These experts, together with internal policy subject matter experts, were also asked what they thought was important for success. We can conclude from their answers that there are many factors important for success. The SSI experts leaned towards factors of 'self-sovereignty' such as control over your own data, which is no surprise as this technology attracts privacy-conscious people. Policy experts were more focussed on the role of the government as protecting the citizen against misuse and getting (digitally) left behind due to incapability to partake in new technology, while they also thought citizen self-sovereignty was an important factor.

Finally, we adapted the IS pyramid model of Gorry & Morton into a new model suitable for public sector technology management levels. (Gorry & Morton, 1989) Then for the actual interaction on the governance level, we based our three moments of interaction on McCawley's work on managing information systems. (McCawley, 2001) This enabled us to answer the main question by using this combination and the data gathered to create a SSI framework that enables the government to find a way of interaction befitting public values and her role in society.

According to this SSI framework the government should critically look at the technology and societal possibilities and decide whether (and if so, how) to interact with the technology based on the governance framework. The final framework was also explained in section 4.3 of this thesis.

5.2 Discussion

The way society thinks about digital identity is changing: It is evolving from institutionalized identity, where institutions such as banks and governments decide who we are and what identity attributes we possess and control the single version of the truth and every step of the process. There is an ongoing shift towards personal identity, where the citizen actually is (part) owner of the identity and as such has more control over it. Self-Sovereign Identity is a promising direction for reshaping global digital identity in a positive way and this shift to personal identity.

The Ministry can take an important role in accelerating this innovative development by encouraging and fostering it. Designing a procedure for identifying hopeful technologic advances and quickly creating a 'plan of attack' on the strategic and tactical level would help the government make faster decisions. Decisions that do not just follow technology, but also guide it ahead. The Dutch government should be involved in this paradigm shift as it can bring many advantages to society, when failing to do so she neglects her role as societal enabler and warder.

The dichotomy of both facilitative and protective government roles will be leading for decisions on how Self-sovereign identity can take shape within society. Many of the parties involved are weary of government interference in what citizens can or cannot do, as they are averse to anyone but the citizen having a say over the digital identity. A balance has to be found where both citizens are given control over their own digital self and protection against misuse is adequate, this will take time and discussion between government, SSI developers and citizens to find a suitable balance.

Also, with ever faster technologic advances and potentially disruptive innovations for society such as AI, a faster way of formulating policy is needed. This technology interaction framework can serve as a way to approach other innovative technologies in a faster and structured way, while keeping in mind that the Government is there to serve the public values involved. The gap between policy-making and up to date IT knowledge can be large, leading to incomplete understanding of technology drivers within society. Early identification and elaboration on these new technologies can help create more thought-out policies earlier.

5.3 Limitations and possible future research

The most important limitation of the research was the limited availability of experts in the specific digital identity niche of Self Sovereign Identity. The SSI technology and paradigm are still green fields, so it was impossible to create a very concrete list of requirements for the technology to become a success. A core value of Self Sovereign Identity is that the ownership of one's identity rests with the person it concerns alone, which is incompatible with the role of the government as guardian of citizen's identity and preventer of identity fraud. Due to this, the validity of the research results can diminish somewhat over time as the technology crystallizes and becomes mature.

Persons interested in SSI are likely to be more privacy-conscious than the general population, based on this interest. Because of this, we cannot assume that their opinions are free of bias or positive about government 'interference' in their ideal. To counteract this, in the second round policy experts are interviewed, who are in general trusting in the capabilities and protective role of the government because they are part of the bureaucratic system. Therefor their opinions might be

biased towards government interaction with any type of identity system, because they feel this is the natural role of the government.

Another limitation was the very much conceptual state of Self-sovereign identity software and the limited usability of such software. This research area is very much 'greenfield' in nature so there is not much previous research to fall back on. As a whole, there is not much actual use of the technology, which limits the possibility to find out whether it is actually feasible for wide-scale usage. While the results of this research are certainly usable in practice, creating a test situation where citizens actually use this SSI technology and can reflect on it will give us more insight into whether the technology is really as feasible for society as it intends to be.

Future research can be focused on how to integrate and streamline governance and strategy decisions concerning emerging technologies. Self-sovereign identity would benefit from more research into how it can fit into wide use within society and how protection against misuse could be realized in the ecosystem or scheme. A good follow-up research would answer the question "How can the Dutch Government become faster in creating policy to interact with innovative technologies?" The Digital Identity Policy Lab could be a possible answer to this question. Integrating this relatively new (in The Netherlands) form of 'policy R&D' into data-driven policy making could be a good subject for a future thesis.

Another interesting possible direction of future research is whether minimal disclosure such as only proving 'age is 18+' is preferred by citizens and corporations over the traditional way of doing business by showing a full identity credential. The persons interviewed and informed were enthusiastic about this privacy enhancing technique but is this really the case for a broader audience or not.

Lastly, one of the interviewed experts mentioned the possible economic effects of the increased level of trust SSI can bring to society, it might be challenging to quantify but certainly an interesting 'future economy' research topic.

List of Cited Works

Abraham, A. (2017). *Whitepaper Self-Sovereign Identity.* Graz, Austria: E-Government Innovationszentrum.

Allen, C. (2016, 04 25). *The Path to Self-Sovereign identity*. Retrieved from Life With Alacrity: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Alpár, G. (2015). *Attribute-Based Identity Management.* Nijmegen: Radboud University.

Alpár, G. (2016). IRMA: I Reveal My Attributes, Privacy and Attribute-Based Identity Management. Nijmegen, The Netherlands: Radboud University Institute for Computing and Information Sciences.

Anthony, R. (1965). Planning and Control Systems: A Framework for Analysis. *Division of Research, Graduate School of Business Administration, Harvard University.*

BBC Technology. (2017, 12 05). *CryptoKitties craze slows down transactions on Ethereum*. Retrieved from BBC News UK: http://www.bbc.com/news/technology-42237162

Bhaskar, R., Chandrasekaran, K., Lokam, S., Montgomery, P., Venkatesan, R., & Yacobi, Y. (2008). Vulnerabilities in Anonymous Credential Systems. *Electronic Notes in Theoretical Computer Science 197*, 141-148.

Blanda, S. (2014, 04 30). *American Mathematical Society*. Retrieved from Shor's Algorithm – Breaking RSA Encryption: https://blogs.ams.org/mathgradblog/2014/04/30/shors-algorithm-breaking-rsa-encryption/

Boehm, B., Brown, J., & Kaspar, H. (1978). *Characteristics of software quality.*

Brands, S. (2000). *Rethinking public key infrastructures and digital certificates: Building in Privacy.* Cambridge, United States of America: MIT Press.

Brock, J.-W. (2018). Personal communication with Leiden University's head of Information Management. Leiden.

Camenisch, J. (2013). Concepts Around Privacy-Preserving Attribute-Based Credentials. *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life.* (pp. 53-63). Berlin: Springer.

Camenisch, J. (2016). Authentication without Identification. *Summer School Trento.* Trento, Italy: IBM Research Zurich.

Camenisch, J., & Lysyanskaya, A. (2002). A signature scheme with efficient protocols. *Security in Communication Networks, Third International Conference* (pp. 268-289). Amalfi, Italy: Springer Verschlag.

Cameron, K. (2005). *The Laws of Identity.* Retrieved from MSDN: https://msdn.microsoft.com/en-us/library/ms996456.aspx

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse. *NDSS vol. 14*, 23-26.

Der, U., Jähnichen, S., & Sürmeli, J. (2017). *Self-sovereign Identity – Opportunities and Challenges (preprint).* arXiv.org - Cornell University Repository.

Dunphy, P., & Petitcolas, F. (2018). *A First Look at Identity Management Schemes.* Illinois, United States of America: VASCO Data Security.

Estonian Republic. (2018, 2 5). *Become an e-resident*. Retrieved from Republic of Estonia E-residency: https://e-resident.gov.ee/become-an-e-resident/

Etherium. (2018, 04 22). *Etherium Whitepaper.* Retrieved from Github: https://github.com/ethereum/wiki/wiki/White-Paper

European Commission. (2014). *EU Regulation No 910: eIDAS.* Retrieved from EULex: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

European Parliament. (2016). *REGULATION (EU) 2016/679 (GDPR).* Brussels, Belgium: European Parliament.

Faisca, J., & Rogado, J. (2016). Decentralized Semantic Identity. *Proceedings of the 12th International Conference on Semantic Systems*, 177-180.

Franken, L. (2018, 03 21). Interview with AFM Blockchain Coalition member. (S. Kommers, Interviewer)

Galperin, E., & Ben Hassine, W. (2015, 12 18). *Changes to Facebook's "Real Names" Policy Still Don't Fix the Problem*. Retrieved from Electronic Frontier Foundation: https://www.eff.org/deeplinks/2015/12/changes-facebooks-real-names-policy-still-dont-fix-problem

Gartner. (2016). *Blockchain: The Dawn of Decentralized Identity.* Stamford, United States of America: Gartner Market Research.

Gartner. (2017). *Blockchain: Evolving Decentralized Identity Design.* Stamford, United States of America: Gartner Market Research.

Gorry, G. A., & Morton, M. S. (1989). A framework for management information systems. *MIT Sloan Management Review*, 49-61.

Grassi, P., Fenton, J., Newton, E., Perlner, R., Regenscheid, A., Burr, W., & Richer, J. (2017). *Special Publication 800-63-3 Digital Identity Guidelines.* Gaithersburg, Maryland, United States: National Institute of Standards and Technology.

Heijstek, W. (2017). Lecture 4: Grounded Theory. *Applied Research Methodology.* Leiden, The Netherlands: Leiden University.

Hevner, A. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, 4.

Hevner, A., & Chatterjee, S. (2010). Design Science Research in Information Systems. *Design Research in Information Systems*, 9-22.

Information Society and Government Study Group. (2017). *Make it Happen!* The Hague: The Ministry of the Interior and Kingdom Relations.

Ingenico Systems. (2018, 06 08). *Four Corners of Global Payments.* Retrieved from Ingenico NL: https://ingenico.nl/binaries/content/assets/epayments/resources/four-corners-of-global-payments.pdf

International Organisation for Standardisation. (1991). *ISO/IEC 9126:1991 Software enginnering -- Product quality.*

Joosten, R. (2017). Self-Sovereign Identity: Much More Than Just a Disruptive Technology. *IDNext.* TNO Research.

Joosten, R. (2018, 04 03). Interview with Rieks Joosten - TNO research.

Le Bras, T. (2015, 07 21). *Infographic: Online overload, it's worse than you think.* Retrieved from Dashlane inc.: https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/

Lewis, A. (2017, 05 17). *A gentle introduction to self-sovereign identity*. Retrieved from Bits on Blocks: https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., & Sena, M. (2017). *uPort: A platform for Self-Sovereign Identity.* uPort.

McCall, J., Richards, P., & Walters, G. (1977). *Factors in Software Quality. Volume I. Concepts and Definitions of Software Quality.* Sunnyvale, California, USA: General Electric Co.

McCawley, P. (2001). The Logic Model for Program Planning and Evaluation. *University of Idaho Extension*.

Microsoft. (1999, 10 11). *Microsoft Passport: Streamlining Commerce and Communication on the Web*. Retrieved from Microsoft.com: https://news.microsoft.com/1999/10/11/microsoft-passport-streamlining-commerce-and-communication-on-the-web/

Norman, D., & Draper, S. (1986). *User Centered System Design; New Perspectives on Human-Computer Interaction.* Hillsdale, NJ, USA: L. Erlbaum Associates Inc.

Oxford English Dictionary. (2018). *Oxford Dictionaries*. Retrieved from Oxford English Dictionary: https://en.oxforddictionaries.com

Paquin, C., & Zaverucha, G. (2013). *U-Prove Cryptographic Specification.* Redmond, United States of America: Microsoft Corporation.

Poot, T. (2017). *Blockchain for an enhanced passenger experience at Amsterdam Airport Schiphol.* Delft: Delft University of Technology.

Privacy by Design Foundation. (2018, 04 23). *Privacy by Design Foundation Publication list*. Retrieved from Privacy by Design Foundation: https://privacybydesign.foundation/publications/

Qiy foundation. (2016). *Definitions of the 'Qiy Scheme V1.2'.* Boxtel, The Netherlands: Qiy foundation.

Qiy foundation. (2017). *Governance Model 'Qiy Scheme V1.1'.* Boxtel, The Netherlands: Qiy foundation.

Rannenberg, K., Camenisch, J., & Sabouri, A. (2015). *Attribute-based Credentials for Trust: Identity in the Information Society.* Springer.

Reyes, A. (2008). *Introduction to Software Quality.* Austin, USA: University of Texas.

Rutte, M., Buma, S., Pechtold, A., & Segers, G.-J. (2017). *Confidence in the Future - 2017–2021 Coalition Agreement.* The Hague, Netherlands: Ministery of State.

Schoemaker, P. (1995). Scenario planning: a tool for strategic thinking. *Sloan management review, 36(2)*, 25-39.

Schutte, M. (2016, 10 25). *Schutte's Critique of the Self-Sovereign Identity Principles*. Retrieved from Matthew Schutte: http://matthewschutte.com/2016/10/25/schuttes-critique-of-the-self-sovereign-identity-principles/

Servida, A., & Sestini, F. (2018, 02 22). European Union, DG Connect unit. (S. Kommers, J. Bogaard, & W. Welling, Interviewers)

Shamir, A. (1979). How to share a secret. *Communications of the ACM 22(11)*, 612-613.

Sovrin Foundation. (2016). *The Inevitable Rise of Self-Sovereign.* Utah, United States of America.

Sovrin Foundation. (2018). *Sovrin: A Protocol and Token for Self-Sovereign Identity & Decentralized Trust.* Utah, United States.

Spirakis, P., & Stamatiou, Y. (2013). Attribute Based Credentials Towards Refined Public Consulation and Effective eGovernance. *CSP EU Forum 2013* (pp. 115-126). Springer-Verlag.

Steiner, P. (1993, 05 07). On the Internet, nobody knows you're a dog. *The New Yorker*.

Stokkink, Q., & Pouwelse, J. (2018). Deployment of a Blockchain-Based Self-Sovereign Identity. *rXiv preprint arXiv:1806.01926*.

van Lieshout, M., & Hoepman, J.-H. (2015). *The PI.lab - Four years later.* Tilburg, The Netherlands: PI.Lab.
van Weel, A. (2018). Digital Identity – Policy perspective. *Global Digital Identity Deep Dive* (p. 6). The Hague: Blockchaingers.
van Wingerde, M. (2017). *Blockchain-enabled Self-Sovereign Identity.* Tilburg, The Netherlands: Tilburg University.
Weiss, C. (1972). *Evaluation research, Methods for Assessing Programme Effectiveness.* New Jersey, United States: Prentice Hall.
World Wide Web Consortium. (2017). *Proposed Verifiable Claims Architecture*. Retrieved from W3C.org: https://w3c.github.io/webpayments-ig/VCTF/architecture/detailed/
World Wide Web Consortium. (2017, 04 17). *Verifiable Claims Working Group Charter*. Retrieved from W3C.org: https://www.w3.org/2017/vc/charter.html
World Wide Web Consortium. (2018). *Verifiable Credentials Data Model v1.0.* Retrieved from Github: https://w3c.github.io/vc-data-model/

List of Attachments

Attachments available with this document.

Attachment I: Blockchaingers Digital Identity Deep Dive report.
Attachment II: Expert Interviews transcripts.
Attachment III: Coded expert interview sentences.
Attachment IV: Comparison of SSI concepts (Dutch).
Attachment V: Concept framework presentation.
Attachment VI: Final framework presentation.