TECHNISCHE HOCHSCHULE NÜRNBERG
GEORG SIMON OHM

Bachelor thesis

The growth factors of self-sovereign identity solutions in Europe

Which factors affect the adoption of
self-sovereign identity solutions for European citizens?

Author:	Adrian Doerk
Field of study:	International business
Academic supervisor:	Prof. Dr. Matthias Fischer
Submission date:	October 14th, 2020

Acknowledgements

At this point, I would like to express my gratitude towards the whole Lissi team, which supported my research with input, feedback and organisational support. Especially, Helge Michael who supported my learning process and research within his role as project lead of the SSI for Germany consortia and Lissi. I would also like to thank Sebastian Bickerle, senior developer at Lissi, who provided valuable feedback about the technical details, Kathrin Mateoschus in her role as marketing manager at the Main Incubator GmbH, for reviewing my work as well as Franz Thomas Fürst who serves as advisor for the Main Incubator GmbH and provided input regarding regulatory processes.

I'm also grateful for the input provided by the ten experts, which took the time for a personal interview including: Oskar van Deventer, Dr. Nacho Alamillo Domingo, Dr. André Kudra, Luca Boldrin, Markus Hautala, Tim Bouma, Daniël Du Seuil, Kaliya Young, Drummond Reed and Andrea Servida.

I would also like to thank the Decentralized Identity Foundation (DIF) for hosting different working groups for the community, such as the product manager call, which facilitates collaboration to solve common product issues for SSI vendors and which I'm honored to co-organize.

Last but not least, I would like to acknowledge the work done by the different stakeholders within the SSI for Germany consortia, which collaborate as a cross-industry research initiative to enable the cross-border usage of self-sovereign identity solutions. The conversations and discussions within the consortia greatly helped to structure this thesis.

Abstract

Digital identity has traditionally been approached from an organizational point of view. While user-centric concepts were introduced to the market, these are still provided by a single entity, which dictates the rules of the interactions. In 2020 the need of a reliable infrastructure for secure identification and authentication reach reached a whole new level. But the internet has still no framework for the exchange of verified information between trusted parties. Currently, individuals either use passwords or a single sign-on provided by a big technology company and increasingly lose control and oversight of their digital life.

This thesis introduces the concept of self-sovereign identity and analysis the factors required to achieve adoption of the concept. It describes the basic components of a self-sovereign identity system and provides the reader with an overview of important conceptual theories to understand the differences to traditional identity systems and the unique approach taken instead.

It then dives into the status quo of the discussions around business, technology, legal and governance aspects. It further examines the central factors for the user and describes a know your costumer use-case as well as the current efforts and challenges for higher education certificates for learners. Furthermore, it depicts the diffusion factors of the innovation. While the legal aspects are mainly concerned with regulations from the European Union, the findings in this thesis can be applied globally.

List of abbreviations

AML	Anti-money laundering
API	Application programmable interface
BIP	Bitcoin improvement proposal
CCPA	California consumer privacy act
DID	Decentralized identifier
DIDComm	Decentralized identifier communication (protocol)
DIF	Decentralized identity foundation
DLT	Distributed ledger technology
DPKI	Decentralized public key infrastructure
EBSI	European blockchain service infrastructure
eID	electronic identification
eIDAS	Electronic identification and trust services for electronic transactions
EFF	Electronic frontier foundation
ESSIF	European self-sovereign identity framework
GDPR	General data protection regulation
IAM	Identity and access management
IDP	Identity provider
KERI	Key event receipt inftrastructre
KYC	Know your costumer
Lissi	Let's initiate self-sovereign identity
LoA	Level of assurance
NFC	Near field communication
PCTF	Pan-Canadian trust framework
PII	Personally identifiable information
PKI	Public key infrastructure
RWOT	Reboot Web of Trust
SAML	Security assertion markup language
SIOP DID	Self-issued OpenID connect provider DID profile
SSI	Self-sovereign identity
SSI4DE	Self-sovereign identity for Germany
SSO	Single sign-on
TIP	ToIP interoperability profile
ToIP	Trust over IP (Foundation)
TSP	Trust service provider
URL	Uniform resource locator
VC	Verified credential
QES	Qualified electronic signature
W3C	World wide web consortium

List of figures

Figure 1: Examples of single sign-on offerings 7
Figure 2: Agent connections 10
Figure 3: The trust triangle 11
Figure 4: Verified credential train 12
Figure 5: Mindmap of mental models enabled by SSI 17
Figure 6: Trust over IP stack 30
Figure 7: Dimensions of guardianship 35

Table of contents

Acknowledgements ..... *II*

Abstract ..... *III*

List of abbreviations ..... *IV*

List of figures ..... *IV*

Table of contents ..... *V*

1. Introduction *1*

1.1. Problem statement 1

1.2. Research question 2

1.3. Research approach 2

1.4. Literature overview 2

1.5. SSI communities, standardization bodies and service providers 4

2. Self-sovereign Identity *6*

2.1. Current identity management systems 6

2.1.1. Siloed, federated and user-centric systems 6

2.1.2. The convenience of single sign-on 6

2.1.3. Surveillance capitalism 7

2.1.4. Factors, which led to development of SSI 8

2.2. Introduction to SSI 9

2.3. An SSI enabled identity wallet for end-users 9

2.4. The trust triangle 10

2.5. Verified credentials (VC) 11

2.6. Decentralized identifiers (DID) 13

2.7. The execution of SSI with the mental models of identity 14

2.8. The community principles 17

3. The growth factors of SSI *18*

3.1. The business of SSI 19

3.1.1. Determining business value 19

3.1.2. The business model 21

3.2. Technology aspects 22

3.2.1. Standardization 22

3.2.2. Interoperability 23

3.2.3. Implementation 24

3.3. The government and regulatory compliance 25

3.3.1. The government as issuer of foundational identities 25

3.3.2. Regulatory compliancy 26

3.4. Trust infrastructure 29

3.4.1. Governance frameworks 29

3.4.2. Trust frameworks 31
3.5. The user 32
3.5.1. Publicly available knowledge 32
3.5.2. Trust of the public 33
3.5.3. Inclusivity 34
3.5.4. Convenience 36
3.5.5. The backup 36
3.6. Use cases 37
3.6.1. KYC-Reusability 38
3.6.2. Higher education certificates for learners 39
3.7. Innovation characteristics of SSI 40
4. Conclusion 42
List of sources I
Legal examination declaration VI
Attachments VII

1. Introduction

The digital age has brought us countless benefits. As of 2020 there are 4,57 billion people with an internet connection[1] who can enjoy the perks of being connected to the rest of the world. The internet is a great place to gather information, join communities, access services, publish ideas or communicate with peers. But for most of these activities we require some sort of digital identity. This can be a pseudonym one uses within an online community, the real name we like to display on social media or a verified identity when opening a new bank account. But here the problem begins. An individual creates countless online identities, which are scattered around the internet. On the one hand, this can be useful for the preservation of one's own privacy, on the other hand, it also creates the problem that users lose track of their online accounts, aren't able to remember hundreds of passwords, have very limited means to execute their data protection rights and are overwhelmed with the overall management of their digital twin. While big technology companies offer a convenient log-in service, which works by only clicking a button, the user pays for this service with behavioral data. Online identity needs to be more than user-centric – it needs to be self-sovereign!

The concept of self-sovereign identity (SSI) offers individuals more control of how they interact with third parties in the digital world. It provides them with a tool to gain agency and authority over their digital relationships and credentials. It enables them to execute their capabilities and provides them with a choice of representation. There are several factors, which have a major influence on the adoption of this technology. This includes the business and technology factors, as well as the regulatory compliance and trust infrastructure. These factors need to be offered by the market, but the user itself is also a factor, driving the adoption. Inviting people to experience SSI with actual use-cases running on a solid trust infrastructure enabled by legally binding relationships, will ultimately spur the adoption of SSI and lead to widespread usage of the concept.

1.1. Problem statement

When the internet was created, it failed to implement an infrastructure for the exchange of trusted identity information. This led to service providers offering proprietary identity and access management (IAM) systems within their domain. The outcome were siloed identity domains, which are adjusted to the needs of an organization and therefore aren't interoperable. Organizations provided users with one option only: create a username and a password to access their services. With an increasing number of services used, the number of passwords, an individual had to manage, also increased. When standardized protocols for authentication and authorization started to become more widely used around 2012 with the introduction of the OAuth 2.0 framework[2], single sign-on services (SSO) enabled by OpenID connect were step by step adopted by the market. While replacing passwords, these services are offered by platform providers, which act as a centralized identity providers (IDP).

Some of these IDPs generate income by collecting behavioral data of their users, which they use to produce sophisticated prediction products. These are traded on behavioral futures marketplaces where advertises can select a fitting target audience for their products as described by Shoshanna Zuboff in her book "The Age of Surveillance

[1] Statista, J. Clement, 'Digital Users Worldwide 2020'.
[2] 'OpenID Connect FAQ and Q&As | OpenID'.

Capitalism"[3]. The European commission recognizes the problem, without directly using the term 'surveillance capitalism' and states "these solutions are disconnected from a verified physical identity, which makes fraud (such as identity theft) and cybersecurity threats more difficult to mitigate. In addition, this practice may raise concerns of market power and of impact on the level playing field where a competitive European digital identity user-empowering services market could develop."[4] Apart from these intrusive business practices, individuals only have limited options to gain transparency of where their data is stored, with whom it is shared and how it is used. Of course, one could read the privacy statement of every service used, however in practice this is unrealistic, not constructive and furthermore doesn't provide the individual with a choice.

While the concept of self-sovereign identity holds the promise to grant the individual more sovereignty and control over their digital identity, current implementations are struggling to achieve productive status, gain adoption as well as legal recognition.

1.2. Research question

RQ1: What led to the development of the self-sovereign identity concept?

RQ2: Which factors affect the adoption of the self-sovereign identity solutions in Europe?

RQ3: How does the eIDAS regulation affect the adoption of SSI in Europe?

1.3. Research approach

For this thesis a qualitative research approach based on the grounded theory is used. This theory is used to develop new theories by combining flexible methodological strategies with the outcome of the analysis, consisting of synthesizing, analyzing and conceptualizing qualitative data.

For this thesis, data was gathered from online meetups, academic literature, legislative texts, whitepapers from SSI providers and frameworks, technical specifications by standardization bodies, internal documents from the SSI for Germany consortia, practical findings by the SSI software provider Lissi as well as ten expert interviews.

1.4. Literature overview

This chapter provides an overview of relevant academic literature in the context of self-sovereign identity. It's only a small selection of the available resources and therefore isn't exhaustive.

One paper, which is commonly cited regarding the principles of SSI is the "Path to self-sovereign identity"[5] by Christopher Allen. It explains the history of identity systems, provides a definition of SSI and outlines the ten principles, which attempt to ensure the focus on building a system, which is centered around the control of the user.

[3] Shoshana Zuboff, *The Age of Surveillance Capitalism*.

[4] European Commission, 'EU Digital ID Scheme for Online Transactions across Europe, Public Consultation, Inception Impact Assessment - Ares(2020)3899583'. Page 3

[5] Christopher Allen, 'The Path to Self-Sovereign Identity'.

Another paper from the area of self-sovereign identity published by several authors from the Reboot Web of Trust (RWOT) community explains the "Five Mental Models of Identity"[6]. It provides insights of how these mental models where constructed, provides definition to these mental models and explains how these relate to identity. While defining the mental models called space-time, presentation, attribute, relationship and capability, the paper also acknowledges that these models have intersections between each other depending on the perspective taken.

The EU Blockchain forum & observatory also published a thematic report on the topic of "Blockchain & digital identity"[7]. It illustrates the current problems with digital identity today and provides an overview of decentralized identity and its implementation. Furthermore, the report provides case studies and highlights the importance of the general data protection legislation (GDPR) and the eIDAS regulation within this context.

A. Mühle, A. Grüner, T. Gayvoronskaya and C. Meinel oft the Hasso Plattner Institute published a paper about the essential components of self-sovereign identity. The authors illustrate the relationship between verifiable claims and the connected identifiers. They continue by explaining the challenge to Zooko's triangle, which states that an identifier can't be secure, decentralized and human readable at the same time. The paper then illustrates options of mitigating centralization in the authentication process and describes the execution of attestations with verifiable claims. The paper concludes that the „concept of verifiable claims has been extended by the Identity Registry Model as well as the Claim Registry Model. These decentralised registries were enabled by blockchain technology (…) This only leaves the claim-issuers and their position of trust as centralised entities in the system."[8]

The Reboot Web of Trust paper "SSI: A roadmap for adoption"[9] creates an SSI market roadmap by defining the stakeholder within the ecosystem and describing the market as of April 2018 with a SWOT analysis. This analysis helps to formulate a go-to-market strategy by identifying potential risks or drawbacks for different stakeholders.

The European Commission and the European Blockchain Partnership launched the European Blockchain Service Infrastructure (EBSI), which includes the European Self-Sovereign Identity Framework (ESSIF) as one use-case. The documentation produced by the EBSI provides context about the joint initiative as well as other policy matters including the governance, the benefits of the infrastructure and its business relevance. It also includes practical instructions on how to leverage the infrastructure and provides an outline of future work packages.[10]

The Book "Diffusion of Innovation"[11] by Everett M. Rogers explains the process a society goes through when adopting a new technology. He defines the elements of diffusion and

[6] Joe Andrieu, Nathan George, Andrew Hughes, Christophe MacIntosh and Antoine Rondelet, 'Five Mental Models of Identity'.
[7] Tom Lyons, Ludovic Courcelas, Ken Timsit, 'EU Blockchain Observatory & Forum: Blockchain and Digital Identity'.
[8] Mühle et al., 'A Survey on Essential Components of a Self-Sovereign Identity'.
[9] Moses Ma, Claire Rumore, Dan Gisolfi, Wes Kussmaul and Dan Greening, 'SSI: A Roadmap for Adoption'.
[10] European Blockchain Service Infrastructure, 'EBSI Documentation'.
[11] Everett M. Rogers, *Diffusion of Innovations*.

describes the innovation-development process. The book also provides an overview of different categories of adopters and how innovations are communicated.

In April 2020, a legal report on the combination of SSI with the eIDAS trust framework was published by Dr. Ignacio Alamillo Domingo.[12] After introducing SSI and the eIDAS regulation, the author discusses the legal value of verified credentials. The report then presents several scenarios on how SSI can be implemented with regards to the regulation. The report includes very short-term scenarios and short-term scenarios, which are applicable to the current regulation. It also includes mid- to long-term scenarios, which offer more legal substance, but also require a change of the regulation.

1.5. SSI communities, standardization bodies and service providers

This section provides an overview of different communities, readers can join and participate in. The discussions, insights and outcomes of these communities greatly supports the progress of SSI. Although not all of these communities are solely focused on the topic of SSI, without their participation within the ecosystem the status quo would not have been possible. However, this might not necessarily apply for the SSI for Germany consortia and Lissi, which are added due to their relevance for this thesis. There are also other worthwhile communities, which aren't included in the list below.

SSI Meetup[13] is a series of webinars hosted by Alexander Preukschat. The platform offers companies, organizations, public representatives and SSI evangelists the possibility to share their insights with the community. All content is freely available and published under the open source license "attribution-sharealike 4.0 international (CC BY-SA 4.0)".[14]

The Reboot Web of Trust design workshops are "focused on the creation of the next generation of decentralized web-of-trust based identity systems."[15] The design workshop under the leadership of Christopher Allen and Joe Andrieu are hosted semi-annually in a different location each time. The results of these workshops are summarized in whitepapers, offering readers deep insights in the technical and theoretical aspects of SSI.

Since 2005, the Internet Identity Workshop (IIW) is hosted semi-annually at the computer history museum in Mountain View, California (USA). The workshop brings together interested individuals and experts, who share a common interest in "finding, probing and solving identity issues"[16]. It serves as an open forum to invent and refine identity related protocols and systems for identification, authentication and authorization among other community driven content.

The MyData non-profit organization (NGO) hosts the MyData conferences with the mission to "empower individuals by improving their right to self-determination regarding their personal data."[17] "The human-centric MyData paradigm is aimed at a fair,

[12] Dr. Ignacio Alamillo Domingo, 'SSI EIDAS Legal Report'.
[13] Alexander Preukschat, 'Self-Sovereign Identity for Everyone!'
[14] 'Creative Commons — Attribution-ShareAlike 4.0 International — CC BY-SA 4.0'.
[15] 'Rebooting the Web-Of-Trust'.
[16] 'About – IIW'.
[17] 'MyData.Org – Make It Happen, Make It Right!'

sustainable, and prosperous digital society where the collective benefits of personal data are maximised, by fairly sharing them between organizations, individuals and society."[18]

Another important organization is the Sovrin Foundation, which is "a nonprofit organization established to promote the concept of internet identity for all".[19] The foundation has contributed code, governance frameworks, operational processes as well as concepts (like guardianship) to the whole community and runs the Sovrin Network in a productive state.

The Decentralized Identity Foundation (DIF) "cultivates ideas & (sic!) emerging specifications by enabling industry-wide discussions, experimentation (testing of hypothesis) and demonstration of interoperability."[20] The foundation specifies the universal resolver as well as the DIDcomm protocol among other specifications. It hosts regular working groups on a variety of different topics, which are open to join for everybody.

The World Wide Web Consortium (W3C) is a standardization body. Its goal is to make the benefits of the web available to all people and enable internet usage on all devices.[21] The W3C standardized the data model for verified credentials and drafts the specification for decentralized identifiers (DIDs).

The Trust over IP (ToIP) Foundation is an independent project hosted at the Linux Foundation. Its mission is to "provide a robust, common standard that gives people and businesses the confidence that data is coming from a trusted source"[22]. The foundation defines standards on how to combine the governance of different technical layers for SSI implementations.

The European Blockchain service infrastructure (EBSI) was founded by the European Blockchain Partnership and the European Commission with the aim of delivering cross-border public services.[23] It currently includes four use-cases: Diploma, notarization, trusted data sharing and the European self-sovereign identity framework (ESSIF).

SSI for Germany (SSI4DE) is a public private partnership with the aim of establishing a European identity ecosystem for natural persons, institutions and things based on self-sovereign identity principles. The project is fostered by the federal ministry of economics of Germany and lead by the Main Incubator GmbH.[24]

Lissi (Let's initiate self-sovereign identity) is a software provider of SSI components, which empower individuals, companies and institutions to have data sovereignty. Lissi spawned the SSI for Germany consortia and is a brand of the main incubator GmbH.[25]

[18] Langford, J., Poikola, A., Janssen, W., Lähteenoja, V. and Rikken, M., ''Understanding MyData Operators', MyData Global'. Page 7
[19] Sovrin Foundation, 'Mission'.
[20] Decentralized Identity Foundation (DIF), 'Mission'.
[21] World Wide Web Consortium (W3C), 'Design Principles'.
[22] Trust over IP Foundation, 'FAQ'.
[23] European Blockchain Service Infrastructure, 'EBSI Documentation'.
[24] Technical University Berlin, '"SSI for Germany" Consortium Starts Decentralized Identity Network'.
[25] main incubator GmbH, 'Lissi - About'.

2. Self-sovereign Identity

2.1. Current identity management systems

"At its essence, identity management is a set of processes to manage the identification, authentication, and authorization of individuals, legal entities, devices, or other subjects in an online context. It is designed to provide the answer to two simple questions (…) 'Who are you?' and 'How can you prove it?'".[26] Before diving into a new kind of identity system, this paragraph will illustrate the history and status quo of identity systems as well as pointing out the key consequences of using single sign-on (SSO) services provided by surveillance capitalists. There are four major categories of identity management from a user-perspective: siloed identity domains, federated log-in alliances, user-centric SSO services and self-sovereign identity.

2.1.1. Siloed, federated and user-centric systems

The history of identity management can be described in three phases. Firstly, companies and institutions had siloed IAM systems, which didn't offer much choice or convenience for the end-user. These traditional siloed IAM systems require the user to choose a username and a password, which in combination grant access to the services offered. However, a user has to generate new passwords for every service to avoid being hacked if one of those passwords gets compromised. Since the passwords are stored in a central database of the service provider, it creates a so-called honey pot for attackers. According to haveibeenpwned.com, 10.196.051.455 [27] accounts were breached in total, referring to "an incident where data is inadvertently exposed in a vulnerable system, usually due to insufficient access controls or security weaknesses in the software."[27]

Hence, federated approaches were developed. Log-in alliances offer more convenience for the end-user by requiring only one log-in account for all participating companies or institutions. However, this approach again requires a username and password and is also limited to companies, which participate in this log-in alliance. In addition, it is an administrative system, which is under the control of the party offering the federated service. Thirdly, user-centric log-in options, based on open standards with the most prominent being OpenID connect, were adopted by a wide range of entities such as Google, Gakunin, Microsoft, Yahoo! Japan, Deutsche Telecom[28] among others. The SSO feature is also commonly referred to as 'social sign on' or 'federated login'.

2.1.2. The convenience of single sign-on

The usage of SSO functionalities is convenient for both the user as well as the entity, implementing the service offered by an SSO service provider. Instead of establishing their own identity management and risking further data breaches, service providers, which require a login, usually implement a variety of different SSO services as illustrated in figure 1.

[26] United Nations Commission on International Trade Law, 'Possible Future Work in the Area of Electronic Commerce - Legal Issues Related to Identity Management and Trust Services'. Page 3

[27] 'Have I Been Pwned'.

[28] 'OpenID Connect FAQ and Q&As | OpenID'.

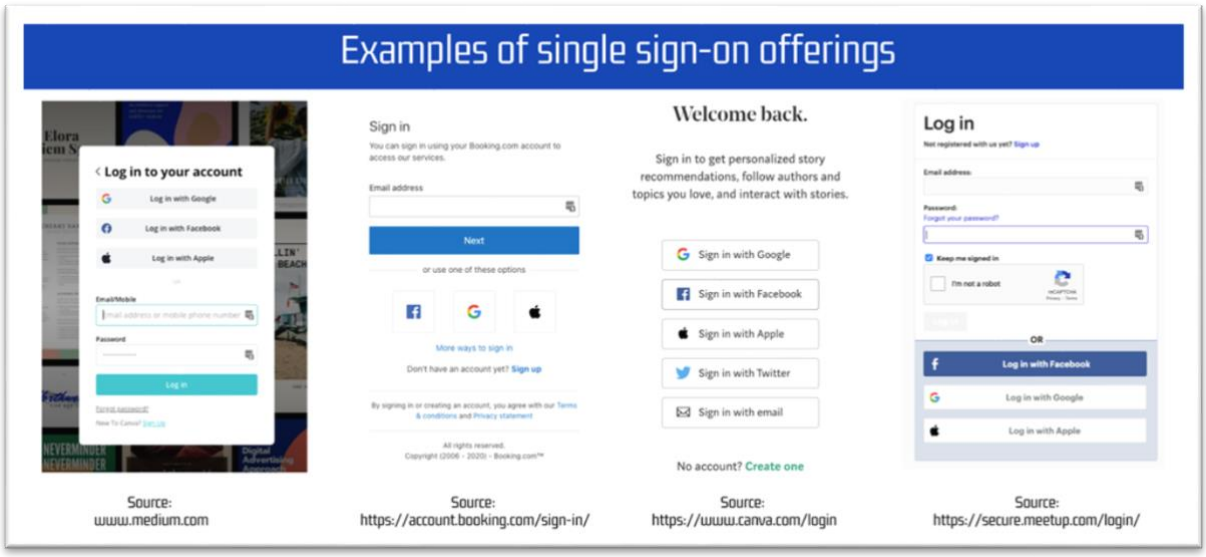

Figure 1: Examples of single sign-on offerings

It is an easy way to authenticate a user without requiring a password. While the technology implementations leverage standardized protocols, the governance of these identity domains is in total control of the entity offering the SSO service. Additionally, these SSO service providers are able to extract further data about the user, e.g. the names of third-party providers they used as well as all the meta data that comes with it.

The most prominent SSO providers are Alphabet (Google), Facebook, Microsoft, Apple and Amazon, but other entities also offer this functionality. Two of these companies, namely Facebook and Google, built their business model based on the economic logic of surveillance capitalism.

2.1.3. Surveillance capitalism

Due to the immediate relevance for the topic of online identity as well as the protection of citizen rights and our democracy, this section will explain the underlying logic of surveillance capitalism. The common saying: 'If the service is free you are the product' is not exactly right. You are not the product, your behavioral data is the raw material, the supply, to produce prediction products, which are sold to advertisers. Surveillance capitalists see your behavioral data as their proprietary and use the data to feed machine intelligence to fabricate sophisticated prediction products.[3] These prediction products are then traded on behavioral futures marketplaces. The more data is fed into this new machine intelligence-based 'means of production' the more powerful are its prediction products. Surveillance capitalism is executed by companies, which offer products and services to extract our behavioral user data to sell predictions and modifications of our future behavior.

Three major economic principles are dictating the direction of this kind of capitalism. The economies of scale imply the more behavioral data they can extract, the better the prediction is. Economies of scope mean the more varied the data sources are, the higher its predictive value is. And lastly, the economies of action describe the modification of users' behavior, being influenced towards a desired commercial outcome.

The monopoly power owned by the prominent players in this market, grants them

[3] Shoshana Zuboff, '*The Age of Surveillance Capitalism*'. Page 233-254

unprecedented control over our market economies, our society, and every single individual. Due to all this gathered detailed personal as well as behavioral data, their services are superior to everything seen before, and they can further amass power and influence to control and manipulate our society at their will.[3]

Dispossession of knowledge

This point describes the act of taking publicly available information and presenting it within the proprietary system of a company in question. It is especially eye-catching in the case of Google, which replaces search results to third parties with information provided by Google itself. A recent example of the ongoing dispossession and fraudulent business practices of Google is the case of the lyrics provider "genius", which caught Google red-handed of using their content and presenting it as their own as described by the New York Post[29]. This might seem like a minor incident but is just one out of many examples of how this company threatens the core values of our society. Societies, which have a meaningful proportion of their citizens using identity-services provided by surveillance capitalists, such as single sign-on by Facebook will suffer continued dispossession of knowledge, agency and authority. The increased reliance on proprietary platforms decreases the autonomy of the society and possibility to exercise free speech. They make a society – and therefor also its government – dependent on decisions of single companies or even single individuals in the case of Facebook, Instagram and WhatsApp.

Governments need to be present on (social) media platforms to communicate with their citizens. The recent case of twitter, which hid tweets[30] of Donald Trump or applied warning labels to the tweets[31] demonstrate the power and responsibility these platforms have. Christopher Allen puts it this way when explaining the consequences of current user-centric identity models: "It's central authorities all over again. Worse, it's like state-controlled authentication of identity, except with a self-elected 'rogue' state."[5]

2.1.4. Factors, which led to development of SSI

Users face the increasing loss of control over their digital identity and the capability to understand how their collected personal and behavioral data about them is used and shared. Individual lack options to execute data protection rights and there is no standard for consent and private data management. The president of the European Commission Ursula von der Leyen said: "Every time an App or website asks us to create a new digital identity or to easily log on via big platforms, we have no idea what happens to our data in reality"[32] in her state of the union speech 2020.

The situation is also difficult for businesses, since they increasingly feel the pressure from big technology companies, which expand into new industries. These global players already have a close relationship to the customer and can easily integrate new offerings into their existing product portfolio.

Trusted peer to peer communication already existed in the 1990s with PGP (Pretty Good

[3] Shoshana Zuboff, '*The Age of Surveillance Capitalism*'. Page 293-328

[29] Manskar, 'Google Caught "Red-Handed" Using Stolen Genius Lyrics'.

[30] Alex Hern, 'Twitter Hides Donald Trump Tweet for "Glorifying Violence"'.

[31] Donie O'Sullivan, 'Twitter Puts Warning on Trump Tweet for "threat of Harm" against DC Protesters'.

[5] Christopher Allen, 'The Path to Self-Sovereign Identity'.

[32] Ursula von der Leyen, 'State of the Union Address 2020'. Page 13

Privacy), but it wasn't able to hide the key management from the user and therefore was not appealing to non-tech savvy people. Furthermore, in most cases the usage involved proprietary systems, meaning that verifications required some sort of central third party like an e-mail provider. With the proliferation of distributed ledgers through sparked interest in blockchains and cryptocurrencies, the topic gained considerable momentum and distributed public key management (DPKM) systems were evaluated to be used as root of trust (also referred to as trust anchor). Hence, the database, which is distributed among several entities, serves as public record to store public keys and events associated with those. Further cryptographic advances in all related aspects gave people hope that a decentralized identity management would be possible.

2.2. Introduction to SSI

We use the terminology of self-sovereign identity for describing a concept of giving individuals or organizations control over their digital identity. The identity resides with the identity subject in question, who is central to its administration. Sovereignty implies that individuals are equal among peers and are not administered by a central authority. This doesn't mean that individuals can suddenly issue themselves a new passport. Instead it means that individuals have control over how their personal data is shared and used. Moreover, individuals can now choose whether they would like to reveal their personal data and also which kind of data they would like to share in the event of a transaction or interaction. Through the use of cryptographic proofs SSI enables verifiability for all involved parties.

SSI puts individuals into the driver's seat and enables them to receive, store, manage and present their personal information. This enables them to act as a carrier of their own information between different trust domains. All while the communication to third parties is directly established without intermediaries with identifiers, which don't require an administrative third party. In this context some also speak about ownership. Yet identity is something we are, not something we have. And hence, it can't be sold.

The next paragraph will provide an overview of key components of the concept of self-sovereign identity. In essence SSI empowers, individuals to control different aspects of their digital relationships, credentials, representations and capabilities.

2.3. An SSI enabled identity wallet for end-users

A digital wallet is a key management application, which provides a user with a graphical interface to store, manage and secure digital keys. These keys can be used to sign transactions, statements, credentials, documents or claims. A digital identity wallet enables a user to establish relationships to interact with third parties by establishing encrypted peer to peer connections between two parties. This encrypted communication channel can then be used by the two parties to exchange verified information. E.g. an issuer of identity information can send a verified credential. The user can store and manage these verified credentials within the wallet. Once in the wallet the verified credential can be used to answer proof request from every connection. The wallet creates a verifiable presentation, which the user can choose to send or instead decline the proof request. Users are also able to verify the identity of the other party, effectively establishing the trusted relationship, which can be leveraged to share and receive information within a defined trust framework such as the eIDAS regulation.

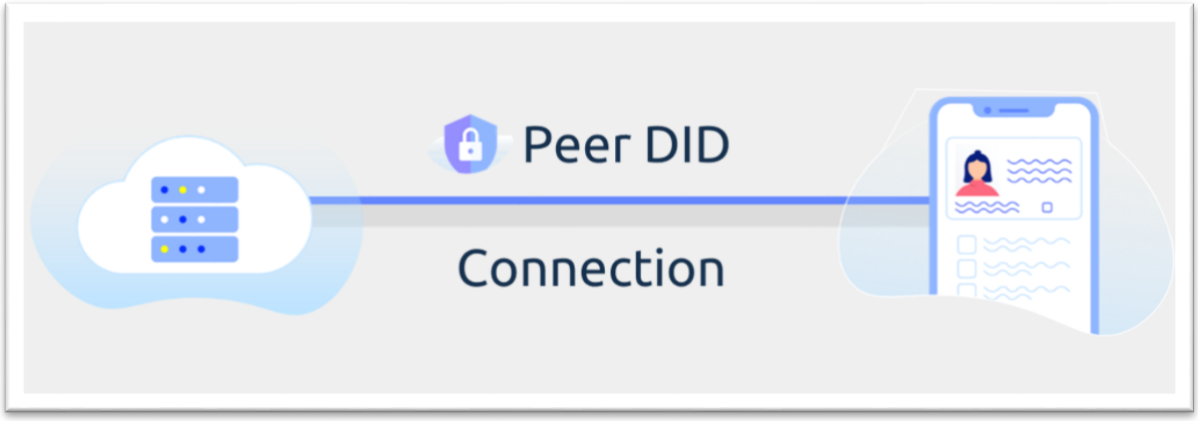

Figure 2: Agent connections *Image provided by Lissi, Main incubator GmbH*

The wallet can include a variety of additional functions and serves as central point of administration and access to services for the individual. For instance, the wallet can be used to replace traditional login mechanisms like passwords with SSO functionalities or building on existing standards such as the OpenID connect protocol. It also enables the user to keep track of the history of shared information and facilitates the execution of data protection rights.

These digital wallets run locally as application on the device of the user. From a technical perspective these wallets are similar to self-custody wallets for cryptocurrencies, which enable not only the ownership, but also the possession of digital currency. This is in strong contrast to custodial wallets, which are offered by a third party such as exchanges. These wallets, which are also referred to as 'web wallet' or 'online wallet' are hosted by a third-party provider and only enable the ownership of digital assets with traditional log-in functionalities for the user.

This means, the user also has the responsibility of having a secure backup solution to restore the wallet in case of lost access, for example when losing the phone as described in paragraph 3.5.5.

2.4. The trust triangle

Compared to traditional identity management systems, SSI puts the holder of identity information into the center of the information exchange. The act of receiving and proofing verified information is executed by the holder itself. There are three roles, which are part of the information exchange. An issuer, a holder and a verifier. The relationship between the roles is described in the trust triangle.

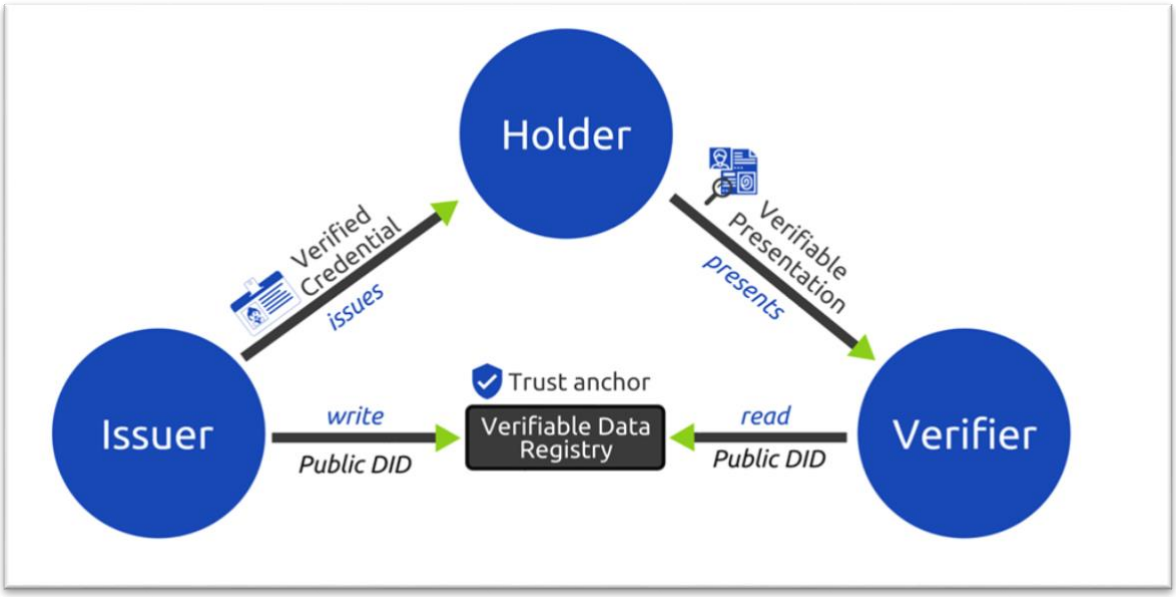

Figure 3: The trust triangle

The issuer of identity information asserts a claim and provides the proof of validity of the issued verified credential by signing it with the private key of the corresponding entity. The public key of the issuer is stored on a verifiable data registry with public read access. This enables every party to independently cross-check the accurateness and validity of the credential. The issuer sends the holder a signed version of the credential, which makes it verifiable by third parties.

The received credential can be stored locally on the device of the holder. Individuals, legal entities and IoT-devices can use a digital wallet to receive, store and manage verified credentials as well as their connections. The holder can but doesn't need to be the subject of the credential. When an owner of a dog holds a credential certifying the dog as guide dog, the subject of the credential isn't the holder, but the dog.

The holder can generate a verifiable presentation and share it with a verifier, who is also referred to as 'relying party'. Normally, this process is initiated by the relying party, which sends the holder a proof request. The holder can decide on an individual level if he wants to share the requested information with the third party. While one of the main benefits of SSI is the verifiability of presented information, it doesn't solve trust. Trust cannot be solved by technology, since trust is subjective and is individually allocated by the party in question. Trust requires social structures and legal certainty, which are provided by trust frameworks and trust service providers as explained in chapter 3.3.2.

In theory all roles can take the place of another role meaning that an issuer can also be a holder or a verifier. In practice an individual as holder might not be able to perform the role of an issuer, since permissioned verifiable data registries don't allow individuals to write their public DID on the ledger due to GDPR compliancy reasons as explained in paragraph 3.2.3.

2.5. Verified credentials (VC)

Credentials are issued to individuals, companies or institutions to certify qualification, competence or authority. Prominent examples for individuals are passports, driving

licenses or a student ID. We carry them around as physical card to assert a certain information about us. However, currently there is no widely adopted standard to express this information via the internet. The verified credentials data model as standardized by the Word Wide Web Consortium (W3C) "provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable"[33] and therefore has a good chance to be adopted as new standard on the web.

In essence these are digitally signed claims, which can incorporate the same information as the physical credentials. The digital signature leads to a more tamper-evident and trustworthy source of information compared to physical cards. But their use is not limited to credentials only, since the data format can be interpreted as a container, which can contain more than just a list of attributes. Timothy Ruff compares them to digital shipping containers, which can deliver consent, permissions, options, balances, statistics, statements, contracts, confirmations, temperature, photos and prescriptions[34] to mention a few examples of their potential payload. He goes on to make the point to rename them to "verified containers", because credentials are only a subset of information they can deliver.

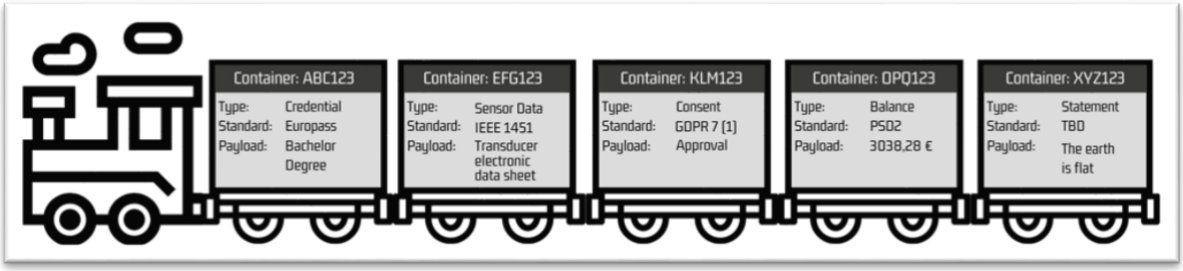

Figure 4: Verified credential train

Hence, a credential is just one of the many use-cases, which can be communicated through a verified credential. While the authenticity of the verified credential can be inspected and authenticated – meaning that it can be checked I) who issued it; II) that it has been issue to the holder in question; III) that the content hasn't been tempered with and IV) that it has not been revoked - the veracity of the payload itself cannot always be authenticated as illustrated in figure 4 with container XYZ123.

Verified credentials are meant to be under the control of the holder of the credential who might or might not be the subject of the credential as explained in the previous paragraph. Hence, the holder is the currier of his own data and can access multiple trust domains such as a university, his or her employer, a financial institution or a government service by providing the necessary claims. This reduces friction and decreases switching costs from one service provider to another to a minimum.

Within the hyperledger indy stack a verified credential is based on a pre-defined schema, which lists the attributes of the credential in question. A national ID card for instance contains the name of the holder, the current address, the issuer and the date of issuance among other information. Based on the schema an issuer can create a credential definition. When a verifier only wants to accept a verified credential issued by an

[33] World Wide Web Consortium, 'Verifiable Credentials Data Model 1.0'.
[34] Ruff, 'Verifiable Credentials Aren't Credentials. They're Containers.'

authorized party it can send a proof request to a holder with the requirement that the proof request can only be answered with the credential definition in question. An example would be that the Bundesdruckerei GmbH (the federal printing office of Germany, which has the authority to issue the German ID card) creates a credential definition, which issuers can include into their proof request. The proof request can then only be answered by credentials, which were issued by the Bundesdruckerei GmbH.

In order to be tamperproof a verifiable credential requires to be linked to some sort of verifiable data registry. While this could also be a traditional public key infrastructure (PKI) like the domain name system (DNS), most SSI implementations leverage the benefits of a DPKI as trust anchor, which is also referred to as 'root of trust'. Meaning a database with public read (and sometimes also public write) access is used to write the DID (further explained in paragraph 2.6) onto the ledger, so third parties can independently verify the authenticity of the verified credential in question. While the verified credential is stored 'off-chain', meaning not on the verifiable data registry itself, but instead in the device of the holder, the verified credential is singed with the private key of the issuer. Since the public key of the issuer is known via the DID, asymmetric cryptography can be used to proof the validity of the verified credential. The ToIP Foundation referrers to verifiable data registries as 'public utility'[35]

The communication of the identity information itself happens via peer to peer connections. There are different protocols, which specify how verified credentials are carried from one party to another. Currently, there isn't a clear standard on the market and various protocols are used to send verified credentials between two parties. The aries RFC 0037[36] defines the verifiable credential exchange within the aries framework, however there are also other protocols in use. The DIDComm protocol[37], which specifies the encrypted messaging between agents based on DIDs and has multiple proponents, which already achieved portability of verified credentials between mobile wallets[38]. Nevertheless, verified credentials can also be send with HTTPS, Bluetooth or other communication protocols.

2.6. Decentralized identifiers (DID)

An identifier helps to refer to a specific object, person, entity, product or even a planet within the galaxy. Most identifiers in usage are globally unique and therefore enable the clear international identification of the object behind it. Almost all of these identifiers are administered by a central authority. Since self-sovereign identity aims to be independent of a central authority decentralized identifiers (DIDs) were specified to enable the usage without the reliance on a third party. DIDs are aimed to be fully under the control of the controller of the DID, independent from any centralized registry, identity provider, or certificate authority. Within the introduction the specification of the W3C, it states that "this specification does not require any particular technology or cryptography to underpin the generation, persistence, resolution or interpretation of DIDs. Rather, it defines: a) the generic syntax for all DIDs, and b) the generic requirements for performing the four basic CRUD operations (create, read, update, deactivate) on the metadata

[35] Trust over IP Foundation, 'ToIP Primer.Pdf'.
[36] Nikita Khateev, 'Aries RFC 0037: Present Proof Protocol 1.0'.
[37] Decentralized Identity Foundation 'DIDComm Messaging Specification'.
[38] 'Trinsic Leads SSI Digital Wallet Portability'.

associated with a DID (called the DID document)."[39] The DID itself is created by the DID controller, which can, but doesn't need to be the DID subject. The DID points to the DID document, which contains further instructions on where to find attributes, claims or similar information and how to communicate with the identity controller.

DIDs enable the creator of it to present the identifier to a certain target audience and prove that the communication shared with the DID is indeed coming from the creator by using asymmetric cryptography. Hence, the DID has a strong relation to the public key, which is communicated to third parties, while the private key is only known by the creator of the DID and is used to sign events or interactions associated with the DID.

An important differentiation is the distinction between anywise, pairwise and n-wise DIDs. The DIF Peer DID Method specification[40] describes these as followed:

*"**Anywise** **DID***
A DID intended for use with an unknowable number of parties (e.g., the global public or some subset thereof).

Pairwise** **DID
A DID intended to be known by its subject and exactly one other party (e.g., one usable in the Alice and Bob example just above).

N-wise** **DID
A DID intended to be known by exactly *N* enumerated parties including its subject. A business partnership with 3 members might be a modeled with n-wise DIDs. Pairwise DIDs are just a special case of an N-wise DID (*N* = 2). For more on n-wise DIDs, see Groups in the appendices."

Anywise DIDs (also referred to as 'public DIDs' as stated in the W3C DID specification[39]) are stored directly on a verifiable data registry. Any third party can therefore verify information published or sent by the entity behind the public DID. A pairwise DID in contrast is not stored on a verified data registry and therefore isn't publicly resolvable. It is only used for the communication between two peers. An example DID method of pairwise DIDs is the peer DID method specified by DIF as mentioned above.

2.7. The execution of SSI with the mental models of identity

To pin down the meaning and definition of identity is a challenging task due to its uniquely human nature. It can have totally different meanings for different people. However, there are reoccurring themes when speaking about the term. The following five mental models describe what people refer to, when speaking about identity and provide a useful structure of how these models can be executed in a digital environment leveraging SSI infrastructure and components. While the concept of SSI can be applied for individuals, legal entities and things alike, the following paragraph solely focuses on individuals and explains how these models can serve as a guideline for SSI implementations. The five

[39] World Wide Web Consortium (W3C), 'Decentralized Identifiers (DIDs) v1.0'.
[40] Decentralized Identity Foundation (DIF), World Wide Web Consortium (W3C), 'Peer DID Method Specification'.

mental models were published by experts of the RWOT community[41] and are quoted as followed.

Space-time
"The space-time mental model sees identity as resolving the question of the physical continuity of an entity through space and time. (…) It answers the question: Does the physical body under evaluation have a continuous link through space and time to a known entity?".

An identity is established in the past, it acts in the present and continues to be useful in the future. To secure the sum of recorded interactions and relationships in digital form one requires a backup when using a self-custody wallet. This backup enables the user to restore the received credentials as well as established relationships. When losing access to the wallet, the backup enables the user to reestablish the aspects described in the space-time mental model as further explained in paragraph 3.5.5.

Presentation
"The presentation mental model sees identity as how we present ourselves to society. This is the mental model behind Vendor Relationship Management, user-centric identity, and self-sovereign identity. (…) It answers the question: Is this how the subject chooses to be known?"

Individuals can choose, which information about them should be known by third parties or the public. The granularity of this information varies dependent on the social context. While one might only want to provide the required minimum of information to a government authority, one might have the desire to share very personal details with a certain social circle such as family or friends. Hence, the user requires different social profiles or circles, which help to present the right information to the target audience.

Attribute
"The attribute mental model sees identity as the set of attributes related to an entity as recorded in a specific system. Enshrined in ISO/IEC 24760-1, an international standard for identity management, this mental model is the primary focus for many engineers. (…) It answers the question: Who is this data about?"

From a birth certificate to a university degree or a language certification, we collect a variety of credentials, which attest certain information about us. The sum of all these credentials can also be seen as one mental model of identity. These credentials are issued, stored and managed by the individual and are standardized within the specification of the verifiable credentials data model 1.0 by the W3C[33] as explained in paragraph 2.5. It is the only mental model with a formal specification. SSI implementations use cryptography to provide the necessary proofs that presented information is about the individual in question. There are different options of implementations to ensure that a certain identifier relates to the specific person, however most implementations use DIDs to establish the binding between the individual and the associated identifiers as explained in paragraph 2.6.

[41] Joe Andrieu, Nathan George, Andrew Hughes, Christophe MacIntosh and Antoine Rondelet, 'Five Mental Models of Identity'.
[33] World Wide Web Consortium 'Verifiable Credentials Data Model 1.0'.

Relationship
"The relationship mental model sees identity emerging through interactions and relationships with others. Our identity is not about what we are in isolation from others, but is rather defined by the relationships we have. This is the fundamental model in the South African idea of 'Ubuntu', meaning 'I am because we are.' (…) It answers the question: How is this person related?"

The relationship to other individuals or entities can help to determine the status of a person within society. We can observe different domains of relationships, which are depended on the social context like a professional, official, legal, personal, public, business or employment context to name a few. A representative of a government like a diplomat has special rights and obligations due to this relationship. Depended on the context, e.g. an interview of said diplomat, it can touch multiple domains by being an official interview, with legal consequences, which is presented to the public and can have direct effect on the employment relation for the diplomat. Generally, individuals initiate and maintain hundreds or even thousands of relationships to different entities. An SSI solution enables an individual to initiate this relationship by accepting or requesting a connection. Once established this connection serves as communication channel to facilitate the exchange of (verified) information between the two parties. Since both parties are able to validate the identity of the other party it enables the necessary trust in a digital environment.

Capability
"The capability mental model pragmatically defines identity in terms of an individual's capability to perform some task, including their physical ability now, in the past, or in the future. It is the inevitable approach for anyone in an emergency. (…) It answers the question: What can the subject actually do?"

The only reason why an identity is required in the online world in the first place are the capabilities that come with it. Without an identity one is still able to browse the web and gather information, however when it comes to online shopping, banking, applications, requests, access, control and many other aspects, a link to an identity is necessary to execute those actions. Not all of these actions require a verified identity. In most cases a self-attested identity is sufficient for the verifier. However, there are multiple cases for which the verifier either has a legitimate interest for only allowing access to verified parties or is obligated by law to verify the identity of an individual. The second case includes telecommunication providers, or financial institutions, which need to comply with know your costumer (KYC) regulations. An example for the first case can be access to information for a specific audience like a university, which wants to grant students access to internal documents. The students would not be required to verify their identity every time they want to access the repository, but instead only need to prove that they are a student of said university, without disclosing further personal details.

Figure 5: Mindmap of mental models enabled by SSI

Figure 5 provides an overview of the five mental models and their execution and integration with SSI. The list of subitems is non-exhaustive.

2.8. The community principles

Principles provide guidance and clarify the boundaries of a specific topic. Principles for SSI facilitate the interpretation, design and implementation for all involved stakeholders. In 2016 Christopher Allen drew on existing identity literature such as the “Laws of

Identity" by Kim Cameron[42], the Respect Network trust framework[43] and the W3C Verifiable Claims Task force FAQ[44] to gain additional perspective and create the ten principles of SSI.[5] These principles are:

Existence, control, access, transparency, persistence, portability, interoperability, consent, minimalization and protection.[5]

Since then these principles are frequently referenced by startups [45] [46] [47], which integrate SSI solutions. However, these are principles on which the community has a general consensus, but no SSI framework or software provider actually needs to follow these principles. Governance and trust frameworks need to define their own core principles, which can vary depending on the scope and purpose of the framework. The Sovrin governance framework[48] for instance lists:

Self-sovereignty, guardianship, openness and interoperability, accountability, sustainability, transparency, collective best interest, decentralization by design, inclusive by design, privacy by design and security by design, data protection by design and default as their core principles.[48]

The eIDAS regulation, which has not been purposely created for SSI, but can serve as a trust framework for SSI as elaborated in paragraph 3.4.2, has its own principles, which apply to the usage of SSI. For instance,

"non-discrimination of legal effects and admissibility of electronic documents in legal proceedings", or "cross-border and legally enforceable mutual recognition between Member states".[49]

Consequently, the stakeholders within the SSI ecosystem have a similar understanding of what the general principles of SSI should be, however these principles are highly influenced by principles set by the trust infrastructure consisting of governance and trust frameworks as noted in paragraph 3.4.

3. The growth factors of SSI

In the book "Diffusion of Innovation", Everett M. Rogers provides five important characteristics, which can be leveraged to explain the rate of adoption. These are relative advantage, compatibility, complexity, trialability and observability.[11] However, in order to determine these characteristics one first needs to evaluate the status quo of the elemental building blocks of SSI, which are necessary to implement use-cases. This

[42] Kim Cameron, 'The Laws of Identity'.
[43] Respect Network, 'The Respect Trust Framework V2.1'.
[44] W3C Verifiable Claims WG, '[EDITOR'S DRAFT] Verifiable Claims Working Group Frequently Asked Questions'.
[5] Christopher Allen, 'The Path to Self-Sovereign Identity'.
[45] J. Lohkamp, K. Wagner, S. Baldwin-Stevenson, 'Coopetition Rather than Competition for Self-Sovereign Identity Wallets'.
[46] Blockchain Helix AG, 'helix id'.
[47] r3, Arjun Govind, 'Is Self-Sovereign Identity the Answer to GDPR Compliance?', 3.
[48] Sovrin Foundation, 'Sovrin Governance Framework V2'. Page 3 and page 4
[49] 'EIDAS SUPPORTED SELF-SOVEREIGN IDENTITY'.
[11] Everett M. Rogers, '*Diffusion of Innovations*'. Page 15

chapter splits the different factors of SSI into thematic categories and then analyses the characteristics of innovation based on the analysis of said thematic topics.

3.1. The business of SSI

There are multiple aspects required for SSI to have adoption from a business side. This includes clear incentives for businesses to adopt SSI, but also includes non-privacy intrusive business models for software provides, which offer business agents and mobile wallets as well as sustainable business models for public infrastructure.

Current identity solutions are not satisfactory for consumers and companies alike as described in paragraph 1.1. The exact benefits for a company can vary depending on the jurisdiction (e.g. via regulatory obligations or the existing offerings in the market), the market segment and the needs of the consumer. There are plenty of reasons for European businesses to adopt SSI. Firstly, IAM solutions are very costly. The global economy spent 4,93 billion USD in 2017[50] on identity verification, however this number doesn't include financial losses due to identity fraud, regulatory compliance costs, costs for IAM systems and IT security costs. Hence, the true financial costs far exceed this number, while the consequences of not having a digital trust infrastructure has a severe adverse impact for society at large.

The aspect of cost reduction alone is a valid reason to explore SSI, since it can lower costs associated with identity verification by e.g. sending a proof request and receiving a verifiable presentation instead of receiving a photo of a physical ID and then running sophisticated artificial intelligence to spot potential fraud. This also reduces the potential options for fraud, further decreasing the associated costs. Zero knowledge proofs and selective disclosure also enable the compliancy with the minimal disclosure requirements set in the GDPR, further reducing cost associated with data protection compliancy. The cost factor is one of the main reasons to adopt SSI for many companies within the SSI4Germany consortia. However, there are more important aspects why SSI makes business sense.

3.1.1. Determining business value

The Sovrin whitepaper about the business of SSI (Attachment 1, Page 41-60) (which unfortunately wasn't finished and therefore not published) defines the value proposition for businesses. The points help to determine if SSI makes sense for the particular use-case or business.

"SSI makes business sense when:

- Verifying assertions is costly or important
- Credentials are useful in another context
- Streamlining workflows
- Personal data is a liability
- Missing data & communication
- Customer-driven workflow" (Attachment 1: Page 46)

When verifying assertions is costly or important:

[50] Statista, 'Global Identity Verification Market Size 2017-2027'.

The first point mentioned applies to companies and institutions, which currently spend significant money or time to verify identities or associated claims. A financial institution, which assigns identification tasks to contractors to comply with KYC regulations is a good example. The process is not only costly, but also introduces friction into the onboarding process causing a reduced customer conversion rate.

When credentials are useful in another context:
SSI also facilitates the verification and bridging of trust domains. A retailer, which wants to offer a student discount needs some way of verifying this claim. SSI enables the retailer to easily get an answer to the question: 'Are you currently enrolled in a university?' Another example is a doctor, who holds claims about his professional achievements and certificates e.g. that he is a certified internist. This information is not only useful for the hospital he might currently work in, but also for patients, health insurances, specialist associations or his next employer. Whenever a credential can be leveraged to access a multitude of services it benefits all participating stakeholders.

When workflows need to be streamlined:
While privacy and security are paramount when dealing with digital identity, the convenience of using the service or product and the associated usefulness are decisive for most end-users. Whenever a process has too many steps, requires too much effort or is not well understood by users, the conversion rate drops dramatically. While SSI won't be able to solve all workflow issues, it can completely reinvent and simplify processes, given the user already acquired the required credentials. A good example are applications, which obligate the applicant to fill in forms and transfer documents when applying for a university, a new job, a government grant or a kindergarden place for the new member of the family. The verifier can construct the proof request according to his needs (and regulatory requirements such as minimal disclosure) and the wallet of the holder can automatically insert the information due to the semantic standardization. This leads to significantly decreased efforts for both parties. However, filling in forms is just one out of many examples. Others being password-less single sign-on[51] or access control.[52]

When personal data is a liability:
Since the GDPR went into force in May 2016, companies are increasingly forced to pay special attention to consumer data regarding the rights of the individual using their services. Fines like the £500.000 Facebook paid for the Cambridge Analytica scandal in the UK[53] are not the only burden for companies. They also suffer from eroded trust and have to cope with increasing scrutiny of government watchdogs and the public alike. Since consumers take over the management of their data, companies can reduce their statutory liabilities prescribed in data protection laws such as GDPR or the California consumer privacy act (CCPA) by eliminating the necessity of storing vast amounts of detailed personal data of costumers and consequently also reducing data exposed in potential data breaches.

When data isn't used, communicated or existent:

[51] Dan Gisolfi, 'Decentralized Identity'.
[52] A. Doerk, P. Hansen, G. Jürgens, M. Kaminski, Dr. M. Kubach, O. Terbu, 'Bitkom: Self Sovereign Identity Use Cases – von der Vision in die Praxis'. Page 10-12
[53] Alex Hern, 'Facebook Agrees to Pay Fine over Cambridge Analytica Scandal'.

Accumulating data is one thing. To manage its secure storage, consent, communication and affiliation another. If the data isn't leveraged to derive essential insights or to improve the product or consumer relations, then its accumulation can have more negative consequences (due to costs affiliated with its storage, maintenance or compliance) then positive ones. This also applies for the communication of the data within a company. Data siloes within entities can cause the necessity to authenticate a costumer repeatedly leading to a fragmented customer experience and high drop-off rates during the process. But what if the data isn't available in the first place? For example, when customers want to order a product, but don't want to fill in delivery and payment information all over again. The easy choice is to stay at a provider, which already has the data. This favors the consolidation of established market participants, since one-click orders aren't possible without having an account in the first place. SSI can essentially eliminate the prerequisite to establish an account to initiate the payment and delivering process, since the data required is just one proof request away.

3.1.2. The business model

When we consider meaningful innovations based on their impact on society then technology is just a tool. The real innovation happens on the business side. New business models such as pay-per-use, freemium or subscription models are oftentimes the driving forces of innovation. The SSI community still has to explore these options. Probably the most innovative business model hasn't been found yet.

Business models for service providers
While the business models for institutional software agents are easier to determine, the business models for mobile wallets require more creativity. Selling software to enterprises or institutions, which facilitates onboarding and enables trusted communication to exchange verified data can be done with license agreements, pay-per use or subscription based, depending on the needs of the market segment. However, generating non-privacy intrusive income with mobile wallets is a challenging task, because people are used to free identity services. Non-representative user-acceptance tests at Lissi depicted the different expectations of users. Some clearly stated that the service of the app needs to be free of charge, while others could consider paying for the product. (Attachment 1: Page 211) Hence, wallet providers either charge the consumer directly via e.g. freemium models, premium support, feature based, cosmetic adjustments etc. or the wallet providers charges businesses for third party branding, special features, implementation efforts for connecting the wallet to existing infrastructure or generates income through other sources like affiliate marketing or white label solutions.

Business models for verifiable data registries
As explained in paragraph 3.2.3 there are different options for implementing a verifiable data registry. Some are public blockchains, which are operated regardless of the identity use-cases executed on top, others are constructed and operated specifically for digital identities. While the second option has a higher dependency on generated income, neither of both implementations currently solve a key issue. With SSI all stakeholders can asynchronously verify claims made. Hence, while the verifier obtains considerable benefits from the system, it's difficult to charge the verifier for the service. There are ideas on how to circumvent this issue and enable verifiers to be charged for premium claims[54],

[54] Sovrin Foundation, Andrew Tobin, Drummond Reed, 'The Inevitable Rise of Self-Sovereign Identity'.

however the business logic, legal circumstances and the exact implementation are still an ongoing topic.

3.2. Technology aspects

SSI is a highly technology driven concept, since the interactions oftentimes require several layers of applied cryptography to produce the required functionality. Furthermore, data sovereignty is an elemental part of the concept, which highlights the necessity to engage with the technological aspects. These include the standardization, interoperability and the implementation.

3.2.1. Standardization

Standardization is required to ensure that applications from different stakeholders flawlessly work together. Standards enable a level playing field for all stakeholders by avoiding that a single entity has too much power controlling a proprietary system and therefore aid the prevention of monopolies. But they don't only serve the private market. A report by Rishab A. Ghosh, which was supported by the FLOSSPOLS project and funded by the European Union recommends that "open standards should be mandatory for eGovernment services and preferred for all other public procurement of software and software services."[55] In addition to the standardized components referred to in paragraph 2.5 (verified credentials) and 2.6 (DIDs) SSI and digital identity in general requires other standardized protocols to function. Leaving aside core internet protocols these include several specifications, which are organized within the DIF:

DID AuthN
DID AuthN is a "method of proofing control over a DID for the purpose of authentication"[56]. One of the currently developed protocols within the working group is the SIOP DID (Self-Issued OpenID Connect provider DID Profile), which "use(ing) OpenID Connect (OIDC) together with the strong decentralization, privacy and security guarantees of Decentralized Identifiers (DID) for everyone who wants to have a generic way to integrate Identity Wallets into their web applications"[56]

DIDComm
The protocol enables "secure, private communication methodology built atop the decentralized designs of DIDs"[37] to request, issue, disclose, and verify credentials and/or presentations between agents.

Universal resolver
The universal resolver enables the discovering and resolution of identifiers including DIDs. The resolver can already resolve DIDs from several networks including "the Bitcoin Blockchain, Sovrin, Ethereum, IPFS, and others."[57]

Other
Other relevant open-source frameworks are governed by the Linux foundation. These

[55] Rishab A. Ghosh., 'An Economic Basis for Open Standards'. Page 2
[56] DIF, O. Terbu, I. Basart, K. Den Hartog, C. Lundkvist, D. Stark, D. Zagidulin, D. Strockis, O. Steele, 'Self-Issued OpenID Connect Provider DID Profile v0.1'.
[37] Decentralized Identity Foundation 'DIDComm Messaging Specification'.
[57] Markus Sabadello, 'A Universal Resolver for Self-Sovereign Identifiers'.

include the **hyperledger frameworks** such as Fabric, Besu, Indy as networks for verifiable data registries and Aries for the agent implementation as well as Ursa, which serves as a shared library for cryptography facilitating zero-knowledge proofs among other functions.

KERI (Key event receipt infrastructure) as proposed by Samuel M. Smith Ph.D. enables self-certifying identifiers for decentralized key management similar to peer DIDs, which don't require a public DID to be stored on public verifiable data registry.[58]

"**Sidetree** is a protocol for creating scalable decentralized public key infrastructure (DPKI) networks that can run atop of any existing decentralized ledger system"[59], which is e.g. used by ION (Identity Overlay Network) a second layer implementation for the bitcoin blockchain driven by Microsoft among others.[60]

3.2.2. Interoperability

„In general, interoperability refers to the ability of independent, heterogeneous systems to work together as seamlessly as possible. This allows mutual use of functions and services to exchange information."[61] Interoperability enables systems to be linked so users can seamlessly use the services offered by multiple networks and vendors. It is necessary to avoid siloed solutions, which in turn spurs innovation and competition. However, the pressure to interoperate can also have negative consequences, since the homogeneity and compatibility of different services and forced standardization can stifle the development of differentiated products.[62] Nevertheless, without technical interoperability SSI won't fulfil its promise of data portability and therefore might decrease its change of further adoption.

While most discussions about interoperability are mainly centered around the technical aspects there are also semantic and legal aspects, which need to be taken into consideration. One aspect of technical interoperability is the usage of common standards. The SSI community has widely adopted DIDs as well as verified credentials. However, currently it's not possible to use verified credentials from different verifiable data registries such as permissioned implementations based on Hyperledger Besu or Hyperledger Indy as well as permissionless networks such as Bitcoin or Ethereum.

Another aspect is the communication between agents, which has three characteristics:

1. "It acts as a fiduciary on behalf of a single identity owner (or, for agents of things like IoT devices, pets, and similar things, a single controller).
2. It holds cryptographic keys that uniquely embody its delegated authorization.
3. It interacts using interoperable DIDComm protocols."[63]

[58] Samuel M. Smith Ph.D., 'Key Event Receipt Infrastructure (KERI) Design'. Page 10 - 22
[59] DIF, Sidetree working group, 'Sidetree Protocol'.
[60] P. Dingle, D. Buchner, 'ION – Booting up the Network'.
[61] Deutscher Bundestag, 'Zehnter Zwischenberiht Der Enquete_komission "Internet Und Digitale Gesellschaft" Interoperabilität, Standards, Freie Software'.Page 5
[62] Schallbruch, Strüve, and Skierka, 'Digitale Identität in Deutschland: Ergebnispapiere von acht Workshops im Zeitraum Mai 2018 - Januar 2020'. Page 16
[63] Daniel Hardman, 'Hyperledger/Aries-Rfcs'.

If these agents use different messaging protocols the exchange of information won't be possible. Furthermore, support of the traditional identification infrastructure is required to combine systems, which are already in use with SSI. This primarily includes OpenID connect and the security assertion markup language (SAML) which are used for single sign-on (SSO) functionality.[64] Last, but no least we need standardized data models for the mobile storage of verified credentials to achieve data portability between different mobile agents. These standardization efforts are currently undertaken by a joint effort of the W3C credentials community group and DIF who published the secure data store 0.1. as unofficial draft on 20. September 2020.[65]

3.2.3. Implementation

To be used on a wide scale the technological implementation needs to fulfil certain requirements as well, including but are not limited to interoperability, reliability and adaptability. It should leverage standardized components, is preferably open-source and enables easy developer onboarding.

There are two essential components, which need further clarification to achieve the requirements requested from implementations. These are the verifiable data registries and the messaging protocol used between agents.

The verifiable data registry
In essence a verifiable data registry is a data base, which contains the necessary public data (e.g. public DIDs or public keys) used to provide proofs via asymmetric cryptography. There are multiple possibilities to achieve the anchoring of an identity with PKIs. However, most implementations use a DPKI to write public DIDs on the verifiable data registry. These data registries can either have permissioned write access or permissionless write access. Examples for permissioned implementations are Sovrin, IDunion, Bedrock or the Dutch digital trust network based on Hyperledger Indy[66] or the EBSI infrastructure, which is based on Hyperledger Fabric and Besu.[67] Permissionless implementations include ION on Bitcoin[60], Veres one on the Veres one Network[68], and 3Box[69] or uPort[70] on Ethereum among others. While the resolving of the DID Documents of different data registries is possible with the universal resolver[57], the number of different implementations and their constant evolvement make it difficult to keep the resolver working for all verifiable data registries.

Agent communication
The other important aspect, which requires implementers to adopt common standards is the protocol used for the messaging between different agents. These can be agents for businesses or institutions as well as agents for end-users (wallets). Currently there are a lot of vendor specific standards in use, which were implemented before the DIDcomm protocol became available.

---

[64] Auth0, 'Single Sign-On'.
[65] DIF, M. Sporny, D. Buchner, O. Steele. 'Secure Data Store 0.1'.
[66] ToIP Utility Foundry Working Group, 'Utility List'.
[67] European Blockchain Service Infrastructure, 'EBSI Documentation'. Page 48 and 51
[60] P. Dingle, D. Buchner, 'ION – Booting up the Network'.
[68] The Veres One Project, 'Intro - Veres One'.
[69] 3Box, 'Create a 3Box Profile'.
[70] uPort, Consensys GmbH, 'UPort - Tools for Decentralized Identity and Trusted Data'.
[57] Sabadello, 'A Universal Resolver for Self-Sovereign Identifiers'.

Integration in existing backend software
Instead of connecting existing back-end systems via each other, creating complexity and interoperability challenges, institutions can leverage the owner of the verified credential to carry claims from one system to another. Hence, existing software backends don't require a complex restructuring, but instead only need to connect an additional communication interface – commonly referred to as 'institutional agent' or 'business agent', which supports the essential SSI components. These agents can easily be connected to existing backend infrastructure with application programmable interfaces (API).

3.3. The government and regulatory compliance

When it comes to identity management the involvement of the government can be a tricky topic. It needs to be involved to enable access to public services, adapt legislature and guarantee equal access for its citizens. However, it should not be able to control or monitor all aspects and activities of its citizens. SSI doesn't mean that a citizen is suddenly able to issue his own ID-card. Governments are still the primary source of foundational identities.

3.3.1. The government as issuer of foundational identities

While individuals gain more autonomy with SSI the issuance of national IDs is still the responsibility of the public administration. The Pan Canadian Trust Framework (PCTF) differentiates between foundational and contextual identities. "A foundational identity is an identity that has been established or changed as a result of a foundational event (e.g., birth, person legal name change, immigration, legal residency, naturalized citizenship, death, organization legal name registration, organization legal name change, or bankruptcy)."[71] Hence, the government continues to be the issuer of foundational identities and still holds the authority to revoke these credentials when necessary.

However, SSI also enables the usage of other identity providers, which are context dependent – leading to a contextual identity as further explained within the PCTF. "A Contextual Identity is an identity that is used for a specific purpose within a specific identity context (e.g., banking, business permits, health services, drivers licensing, or social media). Depending on the identity context, a contextual identity may be tied to a foundational identity (e.g., a drivers licence) or may not be tied to a foundational identity (e.g., a social media profile)."[71] This means a customer of a bank can use his verified bank ID to authenticate himself at a credit bureau. Since the bank ID is based on a foundational identity, the contextual identity provided by the bank can be sufficient in this particular use-case given the regulatory environment allows such a usage. However, a contextual identity can, but doesn't have to be based on a foundational identity.

The European Commission supports the continued usage of contextual identities online and only demands the usage of fundamental identities when required by law as stated in the eIDAS public consultation regarding the option to extend the regulation for the public sector: "A European identity solution enabling trusted identification of citizens and companies in their digital interactions to access public or private online services (e.g. e-commerce), should be entirely voluntary for users to adhere to and fully protect data and

[71] PSP PCTF Working Group, 'Pan Canadian Trust Framework (PCTF) V 1.1'. Page 7

privacy. Anonymity of the internet should be ensured at all times by allowing solutions for anonymous authentication anonymously where user identification is not required for the provision of the service."[4]

3.3.2. Regulatory compliancy

Within the European Union, there are two laws, which have a significant influence on identity frameworks. The General Data Protection Regulation, better known as GDPR, determines how personal data from EU citizens can be collected and used. The other important law is the Electronic IDentification, Authentication and trust Services (eIDAS) provision specified in N°910/2014.[72] It constitutes the main electronic identification trust framework in the EU and is an elemental building block of the digital single market.

GDPR

The EBSI GDPR assessment notes that "According to this Regulation, there are two types of actors whose key role in data processing and whose relationship to the data within the data processing environment leads the European legislator to attribute them a set of obligations and responsibilities. Thus, these liable actors are subject to data protection rules."[73] These are data controllers, which are defined in article 4(7) GDPR as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law"[74], which "have to take all necessary measures so that data subjects are sufficiently informed and have the ability to exercise their data protection rights."[73]

The other actor is the data processor who acts as delegate of the data controller and is a separate legal entity.[75] With multiple nodes running a decentralized network every node acts as an data processor or data controller depending on if the node operator is processing the data as a delegate or not. The EBSI GDPR report further notes "in case of joint controllership, data controllers can contractually assign partial responsibility based on distinct stages of data processing."[73] While an agreement between these data processors can regulate the responsibilities, "data subjects will have ot (sic!) be able to exercise their rights against every joint controller"[73] and "nodes that add and process the on-chain ledger data in order to maintain the consensus will be individually qualified as joint data controllers and this, regardless of a contractual relationship stating the contrary."[73]

For public blockchains with permissionless write access such as Bitcoin or Ethereum, this means, that every miner, which is participating in the proof of work consensus is regarded as data processor given there is an unintentional personal data leakage or correlation

[4] European Commission, 'EU Digital ID Scheme for Online Transactions across Europe, Public Consultation, Inception Impact Assessment - Ares(2020)3899583'. Page 3

[72] European parliament and the council of the European union, REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[73] CEF Digital, University of Amsterdam, 'EBSI GDPR Assessment, Report on Data Protection within the EBSI Version1.0 Infrastructure.' Page 6,7 and 8

[74] 'REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (GDPR)'. Page L 119/33

[75] Working Party up under Article 29 of Directive 95/46/EC., 'Article 29 Data Protection Working Party, "Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'" (2010)'. Page 25

with an URL (Uniform resource locator) of a service endpoint within DID Documents as pointed out as critical to keep personally-identifiable information (PII) private by the DID specification of the W3C in section 10.1.[39] This threat in addition of the numerous other correlation risks mentioned in section 10.2 and 10.3 of said specification make the current implementation of SSI based on permissionless blockchains, which inhibit the capability for natural persons to write a anywise DID on the ledger a daunting privacy challenge.

Another important aspect is the question if credentials (or any other form of PII) is stored as hash on the verifiable data registry. A hash is a data digest and is considered a one-way function, which in theory leads to an anonymization of the original information. The debate around the question if a hash constitutes PII is likely to continue, since national data protection agencies are struggling to clearly define if the hashing can be considered an anonymization or pseudonymization. "According to the Spanish DPA (Data protection agency), hashing can at times be considered as anonymization or pseudonymization depending on a variety of factors varying from the entities involved to the type of the data at hand."[73] The EBSI GDPR assessment report concludes. Even if the hash constitutes a one-way obfuscation technique, which anonymizes PII, it I) requires a transaction on a public ledger and II) it puts data controllers in a higher risk position with the obligation to avoid correlation of individuals. Risk minimizing obligations for data controllers are easier to implement when there is no hash of a verified credential or verified presentation stored on a public ledger.

When it comes to the wallet itself the EBSI GDPR report notes that "there is growing consensus about the possibility of data subjects to being simultaneously considered as data controllers for the data that refer to themselves".[73] This means individuals, which act as holder of their personal information might be regarded as data controller. The report provides the recommendation that "the privacy preserving technical and organisational measures of the wallet and the personal data transmissions should ensure that the necessary safeguards are in place in order to not limit the empowerment of the data subject through the DLT chosen model."[73] The report concludes, that data within the wallet application is considered personal data and therefor is subject to the data protection regulation.

While there is a general assumption that e.g. Hyperledger Indy implementations are GDPR compliant[76], ultimately courts have to decide if that claims holds up based on a case by case evaluation on the particular implementation. Nevertheless, avoiding the exposure of PII on the verifiable data registry, by I) not allowing natural persons to write public DIDs and II) not storing PII in hashed form on the verifiable data registry facilitate the GDPR compliance obligations.

eIDAS:
The eIDAS regulation[77] is concerned with two distinct topics. One part is concerned with trust services for private businesses such as electronic signatures, seal, time stamps etc.

[39] World Wide Web Consortium (W3C), 'Decentralized Identifiers (DIDs) v1.0'.
[73] CEF Digital, University of Amsterdam, 'EBSI GDPR Assessment, Report on Data Protection within the EBSI Version1.0 Infrastructure.' Page 15 and 16
[76] Sovrin Foundation, 'GDPR Position Paper: Innovation Meets Compliance'.
[77] European parliament and the council of the European union, REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The other part is regulating the mutual recognition among member states of national implementations of electronic identification (eID) for the public sector. Is a technology-neutral approach, which has a strong influence on the international regulatory space. The main goal of mutual recognition of eID is to enable EU citizens access to cross-border public services with their own national eID means. The implementation of eID schemes vary from member state to member state and not all member states have notified an eID scheme.[78] There are three levels of assurance specified for eIDs under eIDAS referring to the "degree of confidence in the claimed identity of a person"[79], which include detailed criteria allowing member states to map their eID means against a benchmark (low, substantial and high). Current SSI implementations have the objective to be recognized with a level of assurance specified as substantial.

It's currently possible to be eIDAS compliant with SSI by leveraging one out of five scenarios described in the SSI eIDAS legal report by Dr. Ignacio Alamillo Domingo.[12] Especially interesting is the eIDAS bridge, which adds legal value to verified credentials with the use of electronic certificates and electronic seals.[80] However, it's also possible to derive national eIDs notified in eIDAS, which are eIDAS linked by deriving a national eID by issuing a verifiable credential with a qualified certificate.[12]

Nevertheless, there are also hindrances in the process of creating a qualified certificate with the derived national identity, because of the way the regulation is defining a qualified signature according to Luca Boldrin. (Attachment 1: Page 30) He also stated, that "for the short-term we might not be in the position to have full alignment with the regulation." (Attachment 1: Page 29) Additionally, he points at another issue, which is that national eID requires the keys to be in a secure element. However, current SSI wallets only offer software keys and do not leverage the security benefits of a hardware element. (Attachment 1: Page 29) Furthermore, the eIDAS regulation doesn't regulate the case of a private entity issuing an eID attribute to a natural person for the usage of it in other private interactions according to Dr. Ignacio Alamillo Domingo. (Attachment 1: Page 17) Currently, the authentication process to achieve the recognition of notified eIDAS schemes by other member states requires a national node, which provides the authentication service. While aimed to be technology neutral, the obligation to provide this authentication service as delegated authentication component has several drawbacks and also hinders the potential adoption of SSI. (Attachment 1: Page 17)

The EU has already identified the need to re-evaluate the policies set by eIDAS. "Fundamental changes in the overall societal context suggest a revision of the eIDAS Regulation. These include a dramatic increase in the use of novel technologies, such as distributed-ledger based solutions, the Internet of Thing, Artificial Intelligence and biometrics, changes in the market structure where few players with significant market power increasingly act as digital identity 'gatekeepers', changes in user behavior with increasing demand for instant, convenient and secure identification and the evolution of EU Data Protection legislation".[4] The initiative continues with its target: "The objective of this initiative is, first of all, to provide a future proof regulatory framework to support an

[78] CEF Digital, 'Overview of Pre-Notified and Notified EID Schemes under EIDAS'.

[79] CEF Digital, 'EIDAS Levels of Assurance (LoA)'.

[12] Dr. Ignacio Alamillo Domingo, 'SSI EIDAS Legal Report'. Page 86 – 117 and 95 - 101

[80] EBSI, ESSIF, 'Technical Specification (15) - EIDAS Bridge for VC-ESealing'.

[4] European Commission, 'EU Digital ID Scheme for Online Transactions across Europe, Public Consultation, Inception Impact Assessment - Ares(2020)3899583'. Page 4

EU-wide, simple, trusted and secure system to manage identities in the digital space, covering identification, authentication and the provision of attributes, credentials and attestations. Secondly, the initiative aims at creating a universal pan-European single digital ID. These objectives could be achieved through an overhaul of the eIDAS system, an extension of eIDAS to the private sector, the introduction of a European Digital Identity (EUid) building on the eIDAS system or combination of both."[4]

Dr. Ignacio Alamillo Domingo suggests embodying new technologies such as SSI into the revised regulation e.g. by not mandating the provision of an authentication facility and creating new trust services such as electronic identification. (Attachment 1: Page 17) Luca Boldrin suggests keeping national identity systems as they are but use a derivation of national identity for cross-border context for public and private businesses in parallel to current node implementation to enable a European identity. (Attachment 1: Page 31)

Dr. Ignacio Alamillo Domingo argues that having derived national eIDs and eID trust services has the benefit of increased privacy by using a peer to peer authentication instead of a delegated authentication model (the national eIDAS node). This also leads to less liability issues by shifting the authentication part to private providers as well as less costs associated with running authentication infrastructure for governments, because these are provided by DPKI instead of national eIDAS nodes. These DPKI systems also have the benefits of being more resilient to attacks compared to a single node, which represents a single point of failure. However, regulating eID as trust service also means opening up identification for the private market, which might not be in the interest of national governments. (Attachment 1: Page 19)

3.4. Trust infrastructure

The trust infrastructure is concerned with the question of how and why presented information can be trusted. It defines the rules for all stakeholders and enables legally binding relationships with the combination of governance frameworks, which are built on top of trust frameworks.

There are three core components within an identity system, which in general mainly manage relationships. These are identifiers enabling the means for "remembering, recognizing, and relying on the other parties to the relationship"[81] In case of SSI these are DIDs, which are created by a controller, which "might be a person, organization or software system".[81] Controllers can use different authentication factors, which can be possession-based factors (e.g. hardware), knowledge-based factors (e.g. keys or passwords) or inherent factors (e.g. biometrics).[82] Most of the time a combination of different authentication factors are used to demonstrate authority of an identifier.

3.4.1. Governance frameworks

The BusinessDictionary defines governance as the "establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing

[4] European Commission, 'EU Digital ID Scheme for Online Transactions across Europe, Public Consultation, Inception Impact Assessment - Ares(2020)3899583'. Page 4

[81] Phillip J. Windley, Ph.D., 'The Architecture of Identity Systems'.

[82] CEF Digital, 'Guidance for the Application of the Level of Assurance Which Support the EIDAS Regulation.' Page 2

body".[83] It includes the mechanisms required to balance powers and defines their primary duties to enhance the prosperity and viability of the organization.[83] The objective for governance entities is to ensure the alignment of involved stakeholders, the definition of the implementation and the processes and use-cases executed on top of it. The purpose of a governance framework is to define the different stakeholders, determine their rights and duties as well as defining the policies under which the network is operated. Therefore, it serves as legal foundation for the operation of the particular network. It consists of several legal documents, which are published by the governing authority.

The governance of the network (the verifiable data registry) itself is only a small part of the total governance required. According to the ToIP foundation there are four layers, which require an adapted governance framework matching the needs of the particular layer.

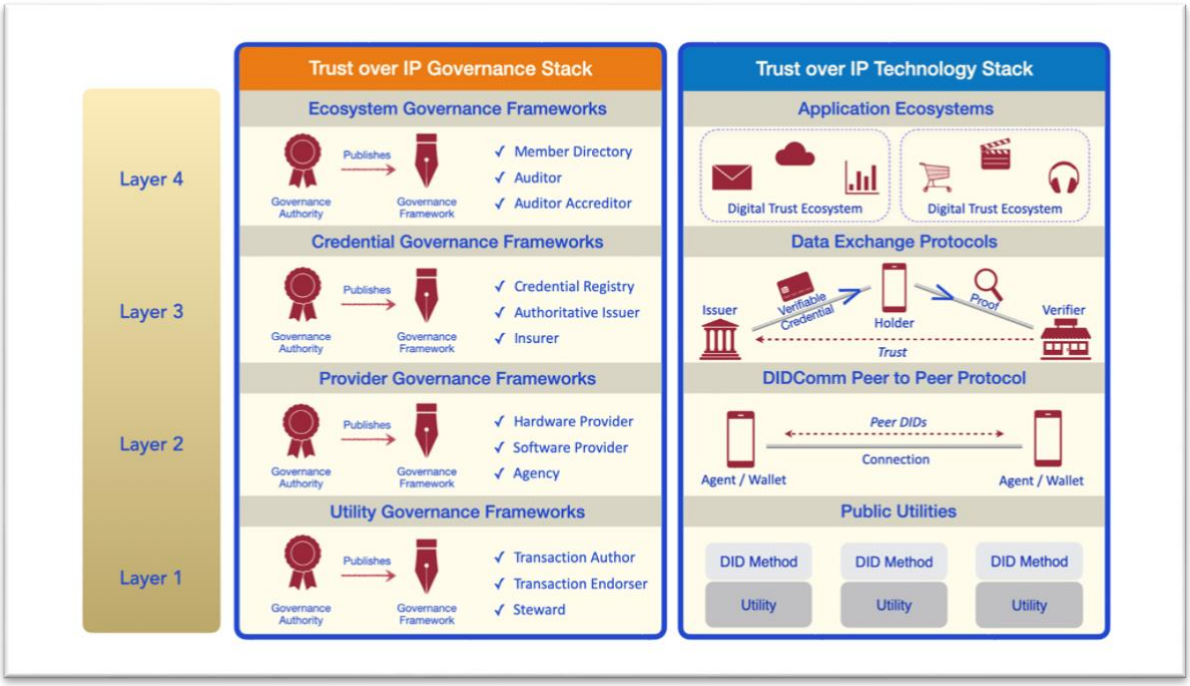

Figure 6: Trust over IP stack *Image provided by the ToIP Foundation*

As illustrated in figure 6, the Trust over IP stack is not only separated in layers, but also in technical and governance stacks within the layers. Layer one includes the verifiable data registries, which can be implemented on different technology frameworks as explained in paragraph 3.2.3. The Sovrin foundation is an example of a governance authority, which published a governance framework[48] for layer one. The second layer describes the communication between agents.

Within the ToIP stack this communication is indented to be executed via an atomic architecture such as peer DIDs with the DIDcomm protocol or KERI implementations of self-certifying identifiers.[58] However, not all SSI implementations use peer DIDs. For instance, the ESSIF-MVP1 does not currently use peer DIDs, but might add them later as

[83] BusinessDictionary, 'Governance'.
[48] Sovrin Foundation, 'Sovrin Governance Framework V2'.
[58] Samuel M. Smith Ph.D., 'Key Event Receipt Infrastructure (KERI) Design'. Page 10 - 22

deemed appropriate.[84] Hence, the same type of DID is used for both issuer and holder. Both layer one and layer two define technical or rather cryptographic trust, in contrast to layer three and four, which define human trust.

Layer three protocols support the exchange of verified credentials for different types of signatures, which enable a holder to create verifiable presentations as explained in the aries-rfcs 0289[85] as one of the potential protocols for this layer. Based on the signature a verifier can ensure that the received data is indeed legit. Layer four of the stack defines the rules for a particular digital trust ecosystem such as healthcare, finance, food products, education etc. These are led by a governance authority, which already exist or is established for this particular purpose. These ecosystem frameworks also define the semantics of verified credentials. The semantic of a verified credential defines, which attributes are part of it and their meaning in the particular context. The stack is indented to provide the certainty for higher levels that the underlying ones can be trusted.

Tim Bouma does not see the need of the government to build and operate a verifiable data registry and highlights the importance of a plurality of operators. However, he points out that the involvement and participation of the government is crucial in defining how the infrastructure is used and relied on. (Attachment 1: Page 8)

3.4.2. Trust frameworks

A trust framework sets the overall legal framework for digital interactions. These trust frameworks are technology agnostic and are uniquely adapted to the jurisdiction they serve. They set the rules for the recognition of electronic identification and specify the requirements to achieve said recognition. Within the European Union the eIDAS regulation serves as the fundamental trust framework.

The combination of the different governance frameworks as illustrated in the ToIP stack is sometimes also referred to as trust framework. However, jurisdictions have their own requirements for electronic authentication, which serve as underlying trust framework. In the case of Europe, the eIDAS regulation clearly defines the requirements for authentication factors to achieve a certain level of assurance. For instance, to achieve the level of assurance substantial, two factors are necessary. One out of the two factors needs to be either I) a presentation of an identity document or II) a verification of the possession of an evidence representing the claimed identity recognized by a member state or III) a previous procedure executed by the same member state not related to the issuance of electronic identification, which provides the equivalent assurance or IV) presenting a valid notified electronic identification mean with the LoA substantial or high.[82] While these requirements can in theory also be defined in a governance framework, the incorporation of such requirements into statutory law facilitates the enforcement of legally binding relationships. Hence, existing statutory law needs to be incorporated by different governance frameworks to achieve a holistic approach and enforce legal liability.

[84] EBSI / ESSIF, 'Technical Specification (2) - DID Modelling'.
[85] M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnel, D. Reed, O. van Deventer, 'Hyperledger/Aries-Rfcs 0289: The Trust over IP Stack'.
[82] CEF Digital, 'Guidance for the Application of the Level of Assurance Which Support the EIDAS Regulation.' Page 8 - 11

According to Tim Bouma as one of the main contributors to the PCTF and Drummond Reed these frameworks intertwine and complement each other. (Attachment 1: Page 8 and page 23) Tim Bouma suggests that policymakers have to go back to the drawing board and take a look at all the concepts to evaluate if they have the right concepts to build out a suitable framework and regulation. (Attachment 1: Page 9) The PCTF "is not a 'standard' as such, but is, instead, a framework that relates and applies existing standards, policies, guidelines, and practices, and where such standards and policies do not exist, specifies additional criteria. It's a tool to help assess a digital identity program that puts into effect the relevant legislation, policy, regulation, and agreements between parties."[71]

In the eIDAS SSI legal report Dr. Ignacio Alamillo Domingo describes the potential shift of the eIDAS regulation as trust framework as followed: „Adopting the SSI principles imply, generally speaking, an increased complexity in trust management and a shifting from hierarchical or federated trust assurance frameworks (…) to network-based socio-reputational trust models or accumulative trust assurance frameworks that use quantifiable methods to aggregate trust on claims and digital identities"[12]

3.5. The user

While the complicated discussions around the technological, regulatory and trust infrastructure will be continued by experts in the field, the user doesn't want to spend hours of reading before using a service. Most people just want a convenient solution and they do not care why the technology is better. If it's too complicated, they won't use it. Due to the unique characteristics of SSI the first onboarding might even be a little bit more complicated compared with processes the average user is already familiar with. Before a user can proof something, the necessary credential has to be obtained first. But the average user doesn't prepare his digital identity in advance, and instead acquires certificates (like a certificate of conduct or enrolment) when it is required. Once in the wallet of the holder, the credential continues to be useful, but to get it in first is the challenge we face.

In addition, SSI includes processes, which are totally new for the user. For instance, the fact that it is required to establish a connection before information can be exchanged. While connectionless proof requests are possible, a continued costumer relationship requires the creation of a connection between the two parties. Here again, once the connection has been set up, it can be used to exchange trusted information via an encrypted peer to peer channel. This opens completely new possibilities for institutions, business and the user alike. This can lead to less phishing victims, since the user has just one trusted communication channel with a business instead of receiving e-mails, which look like one from a trusted source, but are actually from a different, fraudulent party.

Given the user has these documents (such as national ID, invoices, certificates, permits etc.) already stored in the wallet, the wallet knows where to put which credential and automatically fills the form for the user. This leads to less work and more convenience for the user while the relying party gets a fast response as well as verifiable data.

3.5.1. Publicly available knowledge

While SSI grants individuals more control over their data, it also increases the necessary responsibility to take care of the data and especially the backup as explained in paragraph

[71] PSP PCTF Working Group, 'Pan Canadian Trust Framework (PCTF) V 1.1'. Page 3

[12] Dr. Ignacio Alamillo Domingo, 'SSI EIDAS Legal Report'. Page 22

3.5.5. Only informed individuals can take informed decisions. Hence, an abundance of knowledge is essential to ensure that users understand the associated risks. This includes the availability of resources in different languages, as well as in different formats (videos, infographics, texts, audio etc.). It also needs to be available on different platforms (books, articles, social media, television etc.) as well as being adjusted to the target audience (children, businesses, legal experts, government representatives, senior citizens, guardians, etc.). Especially SSI service providers, educational institutions as well as government leveraging SSI technologies need to ensure that a wide range of educational resources are provided.

3.5.2. Trust of the public

When introducing a new kind of identity management to the public it is necessary to convince the civil society as well as decision makers of the benefits of said technology. SSI does have plenty of positive aspects such as increased convince, privacy features, decentralized storage, and asynchronous verifiability. However, like every other technology, verified credentials also have the potential to be abused for surveillance purposes. For instance, governments could demand a set of verified credentials before being able to enter the country. Currently, that's only possible to a limited degree due the missing digital infrastructure.

The question is how high do we want to set the bar to get access to services and infrastructure? What information does a citizen has to prove when visiting one of the European member states the next time? Because citizens don't only have an eID as travel document, but also plenty of other verified credentials? But there are more issues, which need to be addressed:

Problems, which might arise with SSI:

- Excessive request for verified personal data to access services, products, regions or buildings.
- Implementations, which don't put privacy in the forefront can cause more harm than good.
- Fraudulent actors can offer SSI wallets, which make illicit use of the imported data.
- Backups can be lost or destroyed or even worse – stolen and used for illicit purposes.
- All the individual's private data is stored in one place making a hack of the wallet a devastating experience for an individual.
- The responsibility to manage and store data is shifted to the individual, who is always in the less powerful position in world with asynchronous power structures.
- Privacy features within the verified credential and DID specification are just recommendations, not mandates.

After mentioning the benefits of a digital citizenship Christopher Allen continues by saying: "When properly designed and implemented, self-sovereign identity can offer these benefits while also protecting individuals from the ever-increasing control of those in power, who may not have the best interests of the individual at heart."[5] It's not only a question of designing it the right way, but also implementing it with the highest standards available.

Implementations should offer:

- The choice of anonymity, not verifiability, by default.

[5] Christopher Allen, 'The Path to Self-Sovereign Identity'.

- Inform users about potential privacy hazards by e.g. "identifying field in verifiable credentials containing information that could be used to correlate individuals an warn holders when this information is shared"[33] as recommend by the W3C.
- Minimal disclosure by default enabled by selective disclosure and zero knowledge proofs
- The option to execute data protection rights such as the right to be forgotten.
- The option to complain about excessive and inappropriate proof requests.
- Continued development to decrease the potential correlation of individuals.
- Inclusion of minorities, disabled people or people without the financial resources as explained within paragraph 3.5.2.
- Multiple backup options with a cohesive user-experience, so users can choose according to their needs and don't get lost on the way.
- The usage of one-time identifiers by default instead of persisting ones.

The regulatory environment needs to consider:

- Minimal disclosure needs to be mandated – as it is already the case within the GDPR.
- Excessive requirements for verified data should be penalized by law, which is also regulated within the GDPR.
- The increased enforcement of data protection rights.
- The rigorous tracking of violations of given rights and their penalization.
- A high ceiling of SSI implementations, avoiding privacy violating implementations get adopted.
- SSI solutions must not be mandated and the option of accessing government services without digital identification should persist.
- An individual's existence is above its digital representation

SSI isn't a silver bullet for the problems of our society. It has major hurdles to take and can lead to a worse outcome if implemented the wrong way. The Electronic Frontier Foundation (EFF) already raised valid concerns and states that "the privacy recommendations in the W3C and mDL (mobile driver licence) specs must be treated as a floor and not a ceiling."[86]

A collaborative effort is required to protect the individual and a "self-sovereign identity must defend against financial and other losses, prevent human rights abuses by the powerful, and support the rights of the individual to be oneself and to freely associate."[5]

Compared to government surveillance enabled by facial recognition as we can observe in China or a private market controlled by an oligopoly of surveillance capitalists and other technology providers as the status quo in western societies, the decentralized SSI concept might offer the functionality we require in our increasingly digital society. While minimizing the threats, which accompany a digital life without eliminating them. Nevertheless, this thesis can't be confirmed yet and further discussions are necessary to ensure privacy and social equity is protected.

3.5.3. Inclusivity

[33] World Wide Web Consortium, 'Verifiable Credentials Data Model 1.0'.

[86] Alexis Hancock, 'Digital Identification Must Be Designed for Privacy and Equity'.

[5] Christopher Allen, 'The Path to Self-Sovereign Identity'.

When designing identity systems, it has to be ensured that everybody can participate. This is one of the great challenges for digital identity systems in general and especially for SSI. To ensure inclusivity a barrier-free access for e.g. blind or otherwise disabled, underprivileged, impoverished, illiterate and other disadvantaged individuals has to be enabled. However, increasing accessibility alone won't be sufficient.

Individuals, which are not able or not allowed to act on their own require a trusted entity, which acts on their behalf. This concept is referred to as 'guardianship'. It is required when an individual:

- doesn't have access to the internet
- isn't able to use digital devices or other SSI services (e.g. disabled people)
- doesn't have the right to fully control his or her identity (e.g. minors)
- doesn't have the mental capability to act on his or her own (e.g. people with dementia)

The individual, which can't, for whatever reason, act on its own is referred to as 'dependent', while the entity acting on behalf of the dependent is referred to as guardian. The guardian might instruct a delegate, which executes the orders of the guardian in the interest of the dependent. There are two dimensions of guardianship, which are explained in the guardianship whitepaper[87] by the Sovrin Foundation:

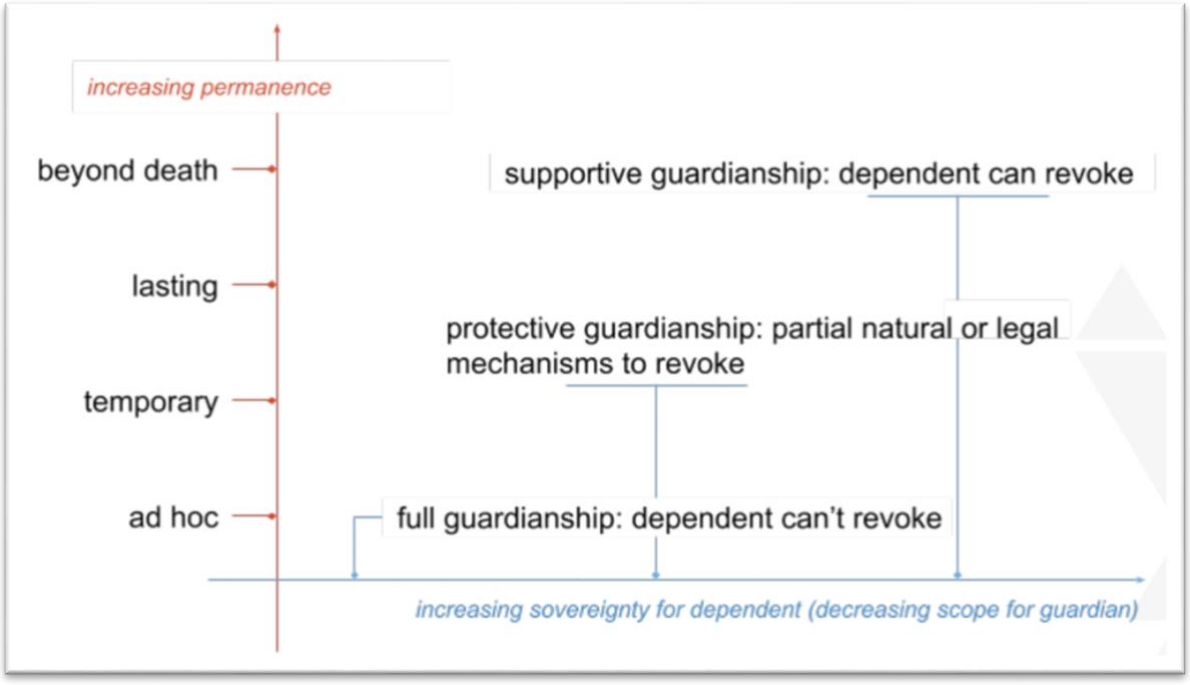

Figure 7: Dimensions of guardianship *Image provided by the Sovrin Foundation*

One is the sovereignty of the dependent, which requires the guardian to be supportive, protective or have full guardianship with increasing responsibility of the guardian and decreasing self-sovereignty of the dependent. The other dimension is the permanence of the relationship, which can be ad hoc, temporary, lasting or even go beyond death.

[87] Sovrin Guardianship Task Force, 'On Guardianship in Self-Sovereign Identity'. Page 15

Depending on the context the guardianship relationship can be based on a legal contract (power of attorney or a living will), social norms or organizational governance. While the underlying social constructs already exist in our society, their integration with SSI requires caution and a well-defined framework to protect the privacy of the involved parties and the autonomy of the dependent to the degree of totally reclaiming independence.

3.5.4. Convenience

Even if the technology is secure and offers sophisticated privacy features, it renders itself useless when it's not easy to use. While the priority of convenience is not necessarily the highest, it's without doubt a necessity for widespread adoption. Priorities of convenience, security and privacy vary depending on the age group and the use-case according to a study by IBM, which states, that security is the top priority for banking, investing, and budgeting apps.[88]

SSI Wallets act as the central application for the user, facilitating the management of digital activities, which require some sort of digital identity. These wallets need to offer a seamless user-experience and guide the user throughout the whole user-journey. Concepts such as the trust triangle, proof requests, data sovereignty as well as verified credentials are completely new to the user. Given their importance to understand SSI and its consequences, these points require special attention when onboarding new users.

One of the challenges for wallet providers is to identify the necessary stakeholders, interactions and prerequisites for every use-case scenario. While it is oftentimes easy to determine the stakeholders involved, the interactions required highly depend on the use-case in question and not only differ when authenticating on a website, ordering a product, entering in a contract or applying for a scholarship, but also vary depending on the particular circumstances of the user. Some users might already have acquired the necessary credentials to answer a proof request, while others still have to get them. Wallet providers need to be aware of all the possible scenarios and always point users in the right direction, so they don't get lost on the way.

Another challenge for the whole industry is the fact that not all wallets support all networks, functions and use-cases. Since there are different implementations of SSI networks, wallets can only communicate with a limited number of the available verifiable data registries. Furthermore, wallets can offer different features and a switch from one wallet to another might lead to a loss of functionality for the user. However, the essential features such as credential storage, the receiving of proof request and the generation of verifiable presentations are supported by all wallets.

3.5.5. The backup

The power of controlling and managing one's own data also comes with the responsibility of taking care of it and preparing for the case of losing a device or acts of nature beyond human control like fires and floods. Similar to cryptocurrencies, users require a backup strategy, which helps them to restore the accumulated data when required. Without some kind of backup, a user won't be able to restore the wallet.

[88] IBM News Room, 'IBM Future of Identity Study'.

Unfortunately, the backup requirements and procedure differ depending on the particular implementation. In general, the backup consists of two parts. An encrypted file, which contains the keys and stored information such as credentials. The second part is a key, which is used to encrypt and decrypt the file. Both are necessary to successfully restore the wallet. The encrypted file can either be stored locally by the user or be uploaded to a cloud storage. To make the key readable by a human it is given in form of a phrase (also referred to as 'recovery phrase' or 'mnemonic seed') consisting of 12 words. This procedure is standardized in the BIP39 (Bitcoin Improvement Proposal 39)[89]. The 12 words can be written down by the user and when provided in the right order can be used to decrypt the backup file. Hence, the user has the responsibility to I) actually do the backup II) store the backup file in a secure place III) write down the recovery phrase and IV) have access to both the file and the key when the backup is required. The countless stories of people who lost their bitcoin keys and were not able to access them anymore, teaches us that storing a key by itself is hard enough, let alone an additional backup file. Hence, other solutions are required for people who do not want or cannot deal with key management.

However, there are also other options available such as social key recovery. This mechanism splits the key apart and the user can send parts of the key to social contacts like friends, family colleagues or trustworthy institutions. When the backup is required the user only needs a fraction of the keys (e.g. three out of five) to restore his original key. Hence, the contacts are not able to restore the original key with their fraction alone. This procedure is easy to understand and execute, because the only decision people need to take is: 'What set of people and/or institutions are going to be their trustees?' as Drummond Reed points out. (Attachment 1: Page 24). Social key recovery is already actively used in production for cryptocurrencies e.g. by the Taiwanese technology provider htc with the HTC EXODUS.[90]

Another option is to use a fiduciary service provided by a trusted third party, which stores the backup and enables recovery for the end-user. However, there are several open questions on how to authenticate oneself to this service provider and how to avoid misuse by this third party. Nevertheless, it's quite likely that the bulk of people will have the desire to use a trusted third party, which helps them to manage their keys while still being in control.

An additional backup procedure can be a "device-based recovery" as Drummond Reed refers to it (Attachment 1: Page 25). Instead of using social contacts this mechanism uses devices, which are in the trust circle of the user such as devices of the user or devices of family members to store fractions of the key required for the recovery. Given the small probability of losing access to all devices simultaneously it can be a viable alternative for individuals, which possess access to multiple devices.

3.6. Use cases

When considering the implementation of different use-cases, one first needs to understand the performed actions of a role within the identity system. Issuer create the

[89] M. Palatinus, P. Rusnak. A. Voisine, S. Bowe, 'BIP39: Bitcoin Improvement Proposal 0039'.
[90] HTC EXODUS, 'Setting up Social Key Recovery'.

supply of verified credentials, which are demanded by verifiers. Holders are in between those and carry the credential from one trust domain to another. Hence, supply and demand do not directly meet, but instead require the holder as intermediary. The following steps help to approach an SSI use-case. The Covid Credential Initiative (CCI)[91] defined (as draft) how to determine market demand for SSI use-cases in the health sector, which served as guidance for the steps below. (Attachment 1: Page 109-110)

1. Identify the stakeholders of the three roles (issuer, holder, verifier) and evaluate the anticipated benefits and barrier to entry for every stakeholder.

2. Evaluation of the demand by the verifier, which should be high. This includes interest and the capability to implement, operate and authorize. Legal or practical hurdles also need to be evaluated.

3. Determine interest of issuers and document workflows if interest is given. Identify strategy to further incentivize or compel issuers. The less issuers have to change their processes the higher is the likelihood that they adopt SSI.

4. Given there is interest from both issuer and verifiers, as well as manageable hurdles, bring together issuer and verifier to discuss workflows, schematics, documentation, pricing, legal considerations, implementation used as well as wallets and their user experience and business agents, which can be used to execute the use-case.

5. The likelihood of holders accepting and adopting the use-case is proportional to the increased value generated compared to current processes.

3.6.1. KYC-Reusability

Financial institutions are legally required to identify individuals when offering their services. This procedure is known as know your costumer (KYC) process. In order to comply with the different obligations such as the inspection of potential money laundering or the determination of the requirement to treat the costumer as politically exposed person, the collection of personal information is necessary. While the obligations are similar, the procedure is executed differently within Europe depending on the national eID implementation and the identification solutions offered by the market. Some European countries already have a system for reuse of KYC credentials such as digital BankID in Sweden or the NemID in Denmark. The NemID is "used for identification and signing in public authorities services, online banking and other private websites." (Attachment 1: Page 117)

Currently it's not possible to reuse a KYC proof of one provider for the identification of another provider in Germany. This is due to the regulatory environment and the missing technological frameworks for verification and secure attestation.

In order to also enable this functionality for the European market based on SSI, the Main Incubator GmbH collaborates with the trust service provider Bank-Verlag GmbH to enable the reuse of KYC credentials based on verified credentials.[92] If a customer is successfully

[91] Covid Credential Initiative (CCI), 'COVID-19 Credentials Initiative'.
[92] Adrian Doerk, Sarah-Karina Lahser, 'Der Bank-Verlag tritt der Lissi-Initiative bei'.

identified (e.g. via video-ident, post-ident or any other means, which satisfy the regulatory requirements) the bank can issue a proof of identity as verified credential to the customer. The data subject (the individual) holds this claim within a mobile wallet and can use it to access other services, which require a KYC process such as trading, the purchase of cryptocurrency or the opening of a new bank account at another financial institution.

Reusability of KYC data is regulated in §11 paragraph 4. of the "Vertrauensdienstegesetz"[93] as reuse of PII, which in general allows the execution of such a use-case. The reusability of the KYC credential is possible as long the original documents are not expired, and the documents used to do the initial identification can guarantee the reliable identification of the individual every time the KYC credential is used. This complicates the execution of the use-case, since this would require the permanent storage of the video files recorded during the video-ident procedure. Since the usage of such a KYC credential requires the LoA substantial, a trust service provider is required to authenticate the conformity of the authentication process with a qualified certificate. The particular process needs to be accredited by the federal network agency (Bundesnetzagentur). However, to be permitted for official use the German federal financial supervisory authority (Bafin) also has to permit the procedure according to the money laundering act. In addition to that there are still more details required regarding the process with the Lissi wallet application and how a two-factor authentication is implemented. Hence, there are several legal challenges in addition to other hurdles related to pricing and credential storage. Nevertheless, the institutions working on the solution are experienced with addressing regulatory topics and collaborate with other financial and legal institutions as well as trust service providers and public bodies within the scope of the SSI for Germany consortia to develop a solution for the whole market.[24]

3.6.2. Higher education certificates for learners

A university degree is a tremendously valuably credential. Unfortunately, in most cases these credentials are still issued as a printed piece of paper, which makes it difficult for verifiers to authenticate their validity. Normally, the owner of the degree scans it and sends it as attachment to a potential employer. This leaves room for fraudsters to manipulate the document or create fake diplomas. The verification of these documents can't currently be automated and therefore requires manual verification efforts.

Academic credentials are considered a great case for the early adoption of SSI for a variety of reasons. These include the inability to verify the authenticity of the presented information for relying parties, which decreases the value of a legitimate degree. The issuance of educational credentials for learners also enables micro-credentialing, essential certifying a learner individual courses, workshops or online seminars. Furthermore, it can facilitate the hiring process by automating the selection process by e.g. only accepting applicants, which can prove a required qualification. Furthermore, it's easier for holders of these certificates to prove the validity of the credential, which is especially relevant for immigrants, expats, exchange students and refugees, which in are not always able to carry physical documents with them. Even if they can provide their educational credentials from outside the European Union, the interpretation of the

[93] Bundesministerium der Justiz und für Verbraucherschutz, 'Vertrauensdienstegesetz (VDG) § 11 Identitätsprüfung'.
[24] Technical University Berlin, '"SSI for Germany" Consortium Starts Decentralized Identity Network'.

documents represents a barrier for acceptance, which can be reduced by receiving the document with a defined semantic schema.

Within the self-sovereign identity space there are several initiatives, which address this issue. Such as the digital credential initiative (DCI). Their "mission is to create a trusted, distributed, and shared infrastructure that becomes the standard for issuing, storing, displaying, and verifying digital academic credentials."[94] It's a consortium consisting of a variety of different well known universities. The EBSI also includes the diploma use-case with the desired outcome of achieving "Mass adoption of EBSI solution by EU educational organisations and private companies, whereby EBSI becomes the common underlying building block to: • issue, manage and verify diplomas and other educational credentials for all citizens and employees" (Attachment 1: Page 81). Within the SSI for Germany consortia the Technical University of Berlin also evaluates the implementation of a diploma use-case based on the IDunion network.

A challenge for all the implementations is the agreement of a commonly used semantic schema, which describes the different attributes within a credential. There are several schemas in usage. According to Daniël Du Seuil the Europass schema will be used within the EBSI. He further highlights the challenge of defining a schema given the global scale of the issue. (Attachment 1: Page 14) Despite the challenges of the use-case the need and interest of issuers and verifiers is high. Educational institutions, public bodies and SSI service providers actively collaborate to solve these issues and enable individuals to hold their educational credentials.

3.7. Innovation characteristics of SSI

This section lists the five characteristics defined by Rogers in Diffusion of Innovation[11] and provides a perspective based on the analysis in the previous chapters. It focuses on the individual instead of legal entities or other stakeholders.

The **relative advantage** is the degree to which an innovation is perceived as better than the one previously used. While it might be measured in economic terms, it can also include prestige factors, convenience or satisfaction. Hence, the objective advantage doesn't matter too much, but rather subjective advantage, so if the individual sees it as advantage. The more relative advantage an individual perceives, the faster the adoption.[11]

Compared to siloed, federated or user-centric identity systems SSI offers more autonomy, choice, transparency for the user. Depending on the use-case it can decrease the time required to perform a capability and increase the access to services from the public and private sector. The aspect of data sovereignty and advanced privacy features can also be seen as a prestige factor by individuals, which are concerned with exposing to much private data online.

"The **compatibility** is the degree to, which an innovation is perceived as being consistent

[94] Kim Hamilton Duffy, Hans Pongratz, J. Philipp Schmidt Digital credential consortium, 'Building the Digital Credential Infrastructure for the Future'.
[11] Everett M. Rogers, *Diffusion of Innovations*. Page 15

with existing values, past experiences and needs of potential adapters."[11] An incompatibility with existing value structure leads to less adoption.

SSI fits well in the ongoing debate about data sovereignty, the loss of control for the individual and the accumulation of behavioral and private data by surveillance capitalists as explained in paragraph 2.1.3. It provides hope for people who almost lost their believe in a private internet. Furthermore, the experience of advertisements, which follow one around the internet on different devices, which promote goods or services the person spoke about yesterday is a daunting experience most of society already made. Additionally, the need for a new identity system is also prevalent as explained in 2.1.1.

"The **complexity** is the degree to, which an innovation is perceived as difficult to understand and use."[11] Simple ideas will be adopted faster in contrast to innovations, which require the development of new skills.

SSI is a highly complex topic. To develop an SSI solution, it requires the understanding of cryptography, multinational law, user-experience design, standardization and many other topics. It's difficult for the average person to get a superficial understanding of the concept within a short time. The usage of it requires the user to adopt to new workflows and the additional responsibility to execute a backup strategy. While guidance during the onboarding process can help the individual, a general understanding of the public for concepts like proof requests or self-custody will likely be necessary to gain further adoption.

"The **trialability** is the degree to, which an innovation can be experimented with."[11] If the innovation is easy to experiment with, it will see faster adoption by enabling learning by doing and therefore avoiding uncertainty.

Everyone with a smartphone can currently test multiple demos of SSI integrations and also experiment with some use-cases in a productive environment. In addition, the adoption of use-cases with a low-threshold regarding legal requirements (like ticketing, degrees or password-less login) will be available sooner than use-cases, which require a detailed legal assessment and have high security requirements. Hence, individuals will have enough options to experiment with the concept first-hand before using it for privacy or security sensitive topics.

"The **observability** is the degree to, which the results of an innovation are visible to others".[11] If results can be easily seen, the adoption will be higher, since it stimulates peer discussion.

The direct observability of apps on a phone is almost non-existent. However, social media makes it easy to talk about personal experiences with the app and share a screen recording of a workflow. Due to the personal nature of the identity topic however, it is likely that individuals won't share such a personal topic with the whole internet, but rather communicate it mouth to mouth. Nevertheless, most of the capabilities enabled by SSI cannot be observed by third parties.

[11] Everett M. Rogers, *Diffusion of Innovations*. Page 15

4. Conclusion

This study examined the factors, which affect the growth and adoption of SSI in Europe and inspected different issues currently faced by SSI implementations. The factors are diverse in nature and need to be articulated according to the target audience (individuals, business or public services). Businesses in particular need to enable the user to gain first-hand experiences with the concept instead of addressing a few highly regulated use-cases without prior user-feedback as pointed out in paragraph 3.7.

While the technology, legal and business factors are crucial in the long-term, short-term experimentation with use-cases accompanied with a low relevance of security and privacy should be enabled to gain more insights into the needs, problems and expectations of users. The ongoing discussions and open questions regarding technology implementations, business models and the trust framework won't be solved in the short-term, but already offer countless opportunities such as the embodying of SSI into eIDAS to enable derived eID for cross-border usage as explained in paragraph 3.3.2. Nevertheless, eIDAS compliant binding relationships are already possible.

The cross-industry discussion of stakeholders from the private and public side is especially relevant considering the standardization challenges for schemas, implementations, trust infrastructure as well as the intermediation of issuer and verifier by the user.

List of sources

1. Statista, J. Clement. 'Digital Users Worldwide 2020'. Statista, 24 July 2020. https://www.statista.com/statistics/617136/digital-population-worldwide/

2. 'OpenID Connect FAQ and Q&As | OpenID'. Accessed 29 September 2020. https://openid.net/connect/faq/

3. Shoshana Zuboff. *The Age of Surveillance Capitalism*, 2019. ISBN 978-1-61039-569-4

4. European Commission. 'EU Digital ID Scheme for Online Transactions across Europe, Public Consultation, Inception Impact Assessment - Ares(2020)3899583'. Accessed 2. October 2020 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528

5. Christopher Allen. 'The Path to Self-Sovereign Identity', 25. April 2016. https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

6. Joe Andrieu, Nathan George, Andrew Hughes, Christophe MacIntosh and Antoine Rondelet. 'Five Mental Models of Identity'. GitHub, 17 March 2020. Accessed 22. September 2020 https://github.com/WebOfTrustInfo/rwot7-toronto

7. Tom Lyons, Ludovic Courcelas, Ken Timsit. 'EU Blockchain Observatory & Forum: Blockchain and Digital Identity', n.d., 27. Accessed 21. September 2020 https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

8. Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 'A Survey on Essential Components of a Self-Sovereign Identity'. *ArXiv:1807.06346 [Cs]*, 17 July 2018. Accessed 2. September 2020. http://arxiv.org/abs/1807.06346

9. Moses Ma, Claire Rumore, Dan Gisolfi, Wes Kussmaul and Dan Greening. 'SSI: A Roadmap for Adoption'. GitHub, July 2018. Accessed 4. July 2020 https://nbviewer.jupyter.org/github/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/a-roadmap-for-ssi.pdf

10. European Blockchain Service Infrastructure. 'EBSI Documentation'. CEF Digital, n.d. Accessed 17. September 2020 https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITALEBSI/EBSI+Documentation+home

11. Everett M. Rogers. *Diffusion of Innovations*. 3th Edition. The Free Press, 1982. ISBN 0-02-926650-5

12. Dr. Ignacio Alamillo Domingo. 'SSI EIDAS Legal Report', April 2020, 150. Accessed 14. September 2020. https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

13. Alexander Preukschat. 'Self-Sovereign Identity for Everyone!' SSI Meetup. Accessed 2. August 2020 https://ssimeetup.org/

14. 'Creative Commons — Attribution-ShareAlike 4.0 International — CC BY-SA 4.0'. Accessed 3. October 2020. https://creativecommons.org/licenses/by-sa/4.0/

15. 'Rebooting the Web-Of-Trust'. Accessed 3 October 2020. https://www.weboftrust.info/#fh5co-tab-feature-center2

16. 'About – IIW', n.d. Accessed 28. September 2020. https://internetidentityworkshop.com/about/

17. 'MyData.Org – Make It Happen, Make It Right!' n.d. Accessed 3. October 2020. https://mydata.org/

18. Langford, J., Poikola, A., Janssen, W., Lähteenoja, V. and Rikken, M. ''Understanding MyData Operators', MyData Global', Eds 2020, 40. https://mydata.org/wp-content/uploads/sites/5/2020/04/Understanding-Mydata-Operators-pages.pdf

19. 'Mission'. *Sovrin* (blog). Accessed 3 October 2020. https://sovrin.org/team/

20. Decentralized Identity Foundation (DIF). 'Mission'. Accessed 3 October 2020. https://identity.foundation/governance/about

21. World Wide Web Consortium (W3C) 'Design Principles'. Accessed 3 October 2020. https://www.w3.org/Consortium/mission#vision

22. Trust over IP Foundation. 'FAQ'. *Trust Over IP* (blog). Accessed 3 October 2020. https://trustoverip.org/about/faq/

23. European Blockchain Service Infrastructure. 'EBSI Documentation'. CEF Digital. Accessed 6. October 2020. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITALEBSI/EBSI+Documentation+home

24. Technical University Berlin. '"SSI for Germany" Consortium Starts Decentralized Identity Network', 2. September 2020. Accessed 28. September 2020. https://www.snet.tu-berlin.de/menue/news/2020/2020_08_28_ssi_for_germany_consortium_starts_decentralized_identity_network/#Identity

25. Main Incubator GmbH. 'Lissi - About'. Lissi, n.d. Accessed 27. September 2020. https://www.lissi.id

26. United Nations Commission on International Trade Law. 'Possible Future Work in the Area of Electronic Commerce - Legal Issues Related to Identity Management and Trust Services', 5. May 2015. Accessed 26. September 2020. https://undocs.org/en/A/CN.9/854

27. 'Have I Been Pwned: FAQs'. n.d. Accessed 1. October 2020. https://haveibeenpwned.com/FAQs

28. OpenID Connect Foundation. 'OpenID Connect FAQ and Q&As | OpenID'. n.d. Accessed 29. September 2020. https://openid.net/connect/faq/

29. Manskar, Noah. 'Google Caught "Red-Handed" Using Stolen Genius Lyrics: Lawsuit'. *New York Post* (blog), 4 December 2019. Accessed 13. September 2020. https://nypost.com/2019/12/04/google-caught-red-handed-using-stolen-genius-lyrics-lawsuit/

30. Alex Hern, UK technology. 'Twitter Hides Donald Trump Tweet for "Glorifying Violence"'. *The Guardian*, 29 May 2020, Accessed 13. September 2020. https://www.theguardian.com/technology/2020/may/29/twitter-hides-donald-trump-tweet-glorifying-violence

31. Donie O'Sullivan, CNN. 'Twitter Puts Warning on Trump Tweet for "threat of Harm" against DC Protesters'. CNN. 23. June 2020, Accessed 30 July 2020. https://www.cnn.com/2020/06/23/tech/trump-twitter-violence-warning/index.html

32. Ursula von der Leyen. 'State of the Union Address 2020', n.d. Accessed 26. September 2020 https://ec.europa.eu/info/sites/info/files/soteu_2020_en.pdf

33. 'Verifiable Credentials Data Model 1.0'. n.d. Accessed 30 July 2020. https://www.w3.org/TR/vc-data-model/#dfn-credential

34. Timothy Ruff. 'Verifiable Credentials Aren't Credentials. They're Containers.' Medium, 23. September 2020. Accessed 24. September 2020 https://medium.com/@rufftimo/verifiable-credentials-arent-credentials-they-re-containers-

fab5b3ae5c0

35. Trust over IP Foundation. 'ToIP Primer.Pdf'. n.d. Accessed 26 September 2020. https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_050520_primer.pdf

36. Nikita Khateev. 'Aries RFC 0037: Present Proof Protocol 1.0'. GitHub, Mai 2019. Accessed 24. September 2020. https://github.com/hyperledger/aries-rfcs

37. 'DIDComm Messaging Specification'. n.d. Accessed 26 September 2020. https://identity.foundation/didcomm-messaging/spec/

38. Trinsic. 'Trinsic Leads SSI Digital Wallet Portability', 18. August 2020. Accessed 19. August 2020 2020. https://trinsic.id/ssi-digital-wallet-portability/

39. World Wide Web Consortium (W3C). 'Decentralized Identifiers (DIDs) v1.0', 7. September 2020. Accessed 24. September 2020. https://w3c.github.io/did-core/

40. Decentralized Identity Foundation (DIF), World Wide Web Consortium (W3C). 'Peer DID Method Specification', 25. August 2020. Accessed 29. August 2020 https://openssi.github.io/peer-did-method-spec/

41. Joe Andrieu, Nathan George, Andrew Hughes, Christophe MacIntosh and Antoine Rondelet. 'Five Mental Models of Identity'. GitHub, 17. March 2020. Accessed 13. September 2020 https://github.com/WebOfTrustInfo/rwot7-toronto

42. Kim, Cameron. 'The Laws of Identity', Mai 2007. Accessed 4. April 2020. https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456(v%3dmsdn.10)

43. Respect Network. 'The Respect Trust Framework V2.1', 1. February 2016. Accessed 28. September 2020. https://oixnet.org/wp-content/uploads/2016/02/respect-trust-framework-v2-1.pdf

44. W3C Verifiable Claims WG. '[EDITOR'S DRAFT] Verifiable Claims Working Group Frequently Asked Questions', n.d. Accessed 4. September 2020. https://w3c.github.io/webpayments-ig/VCTF/charter/faq.html

45. J. Lohkamp, K. Wagner, S. Baldwin-Stevenson. 'Coopetition Rather than Competition for Self-Sovereign Identity Wallets'. Jolocom (blog), 25. February 2020. Accessed 2. September 2020. http://jolocom.io/blog/coopetition-rather-than-competition-for-ssi-wallets/

46. Blockchain Helix AG. 'helix id'. helix id, n.d. Accessed 2. September 2020. https://helixid.io/

47. Arjun Govind. 'Is Self-Sovereign Identity the Answer to GDPR Compliance?' *R3* (blog), 20. April 2020. Accessed 26. August 2020. https://www.r3.com/blog/is-self-sovereign-identity-the-answer-to-gdpr-compliance/

48. 'Sovrin Governance Framework V2', 4. December 2019. https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V2.pdf

49. 'EIDAS SUPPORTED SELF-SOVEREIGN IDENTITY', n.d. Accessed 28. August 2020. https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

50. Statista. 'Global Identity Verification Market Size 2017-2027'. Statista. N.d. Accessed 4. October 2020. https://www.statista.com/statistics/1036470/worldwide-identity-verification-market-revenue/

51. Dan Gisolfi. 'Decentralized Identity: An Alternative to Password-Based Authentication'. Blockchain Pulse: IBM Blockchain Blog, Oktober 2018. Accessed 3. Mai 2020. https://www.ibm.com/blogs/blockchain/2018/10/decentralized-identity-an-alternative-to-

password-based-authentication/

52. A. Doerk, P. Hansen, G. Jürgens, M. Kaminski, Dr. M. Kubach, O. Terbu. 'Bitkom: Self Sovereign Identity Use Cases – von der Vision in die Praxis', n.d. Accessed 4. September 2020. https://www.bitkom.org/sites/default/files/2020-07/200703_lf_self-sovereign-identity-use-cases.pdf

53. Alex Hern. 'Facebook Agrees to Pay Fine over Cambridge Analytica Scandal'. the Guardian, 30 October 2019. Accessed 16. Mai 2020. http://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal

54. Sovrin Foundation, Andrew Tobin, Drummond Reed. 'The Inevitable Rise of Self-Sovereign Identity', 28 March 2017, Accessed 22. September 2020. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

55. Rishab A. Ghosh. 'An Economic Basis for Open Standards', December 2005, Accessed 8. September 2020. http://www.intgovforum.org/Substantive_1st_IGF/openstandards-IGF.pdf

56. DIF, O. Terbu, I. Basart, K. Den Hartog, C. Lundkvist, D. Stark, D. Zagidulin, D. Strockis, O. Steele. 'Self-Issued OpenID Connect Provider DID Profile v0.1', n.d. https://identity.foundation/did-siop/#did-authn

57. Markus Sabadello. 'A Universal Resolver for Self-Sovereign Identifiers'. Medium, 1. November 2017. Accessed 3. August 2020. https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c

58. Samuel M. Smith Ph.D. 'Key Event Receipt Infrastructure (KERI) Design'. GitHub, Mai 2020. Accessed 15. September 2020. https://github.com/decentralized-identity/keri/blob/master/kids/KERI_WP.pdf

59. DIF, Sidetree working group. 'Sidetree Protocol', n.d. Accessed 3. September 2020. https://identity.foundation/sidetree/spec/

60. P. Dingle, D. Buchner. 'ION – Booting up the Network'. TECHCOMMUNITY.MICROSOFT.COM, 10. June 2020. Accessed 26. August 2020. https://techcommunity.microsoft.com/t5/identity-standards-blog/ion-booting-up-the-network/ba-p/1441552

61. Deutscher Bundestag. 'Zehnter Zwischenberiht Der Enquete_komission "Internet Und Digitale Gesellschaft" Interoperabilität, Standards, Freie Software', 11. March 2013. Accessed 22. June 2020. https://dipbt.bundestag.de/dip21/btd/17/124/1712495.pdf

62. Schallbruch, Martin, Tanja Strüve, and Isabel Skierka. 'Digitale Identität in Deutschland: Ergebnispapiere von acht Workshops im Zeitraum Mai 2018 - Januar 2020', Mai 2020, Accessed 23. August 2020. https://faculty-research.esmt.berlin/sites/faculty/files/2020-05/ESMT_Reader_DigitaleIdentit%C3%A4ten_202005.pdf

63. Daniel Hardman. 'Hyperledger/Aries-Rfcs'. GitHub, 15 January 2019. Accessed 2. September 2020. https://github.com/hyperledger/aries-rfcs

64. Auth0. 'Single Sign-On'. Auth0 Docs. N.d. Accessed 26 September 2020. https://auth0.com/docs/

65. DIF, M. Sporny, D. Buchner, O. Steele. 'Secure Data Store 0.1'. n.d. Accessed 26 September 2020. https://identity.foundation/secure-data-store/

66. ToIP Utility Foundry Working Group. 'Utility List'. GitHub. N.d. Accessed 10. October 2020. https://github.com/trustoverip/utility-foundry-wg

67. European Blockchain Service Infrastructure. 'EBSI Documentation'. CEF Digital. N.d. Accessed 6 October 2020. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITALEBSI/EBSI+Documentation+home

68. The Veres One Project. 'Intro - Veres One', n.d. Accessed 19. August 2020. https://veres.one/network/

69. 3Box. 'Create a 3Box Profile'. N.d. Accessed 10. October 2020. https://docs.3box.io/try/create-profile

70. uPort, Consensys GmbH. 'UPort - Tools for Decentralized Identity and Trusted Data'. N.d. Accessed 10. October 2020. https://www.uport.me/#Product-Suites

71. PSP PCTF Working Group. 'Pan Canadian Trust Framework (PCTF) V 1.1'. GitHub, 2. June 2020. Accessed 22. June 2020. https://github.com/canada-ca/PCTF-CCP/blob/master/Version1_1/PSP-PCTF-V1.1-Consultation-Draft.pdf

72. European parliament and the council of the European union. REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014). Accessed 20. September 2020. https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

73. CEF Digital, University of Amsterdam. 'EBSI GDPR Assessment, Report on Data Protection within the EBSI Version1.0 Infrastructure.' CEF Digital, April 2020. Accessed 18. August 2020. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITALEBSI/Legal+Assessment+Reports

74. 'REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (GDPR)', 2016. Accessed 5. September 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

75. Working Party up under Article 29 of Directive 95/46/EC. 'Article 29 Data Protection Working Party, "Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'" (2010)', 16 February 2010. Accessed 5. September 2020. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

76. Sovrin Foundation. 'GDPR Position Paper: Innovation Meets Compliance', January 2020. Accessed 5. September 2020. https://sovrin.org/wp-content/uploads/GDPR-Paper_V1.pdf

77. European parliament and the council of the European union. REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014). Accessed 5. September 2020. https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

78. CEF Digital 'Overview of Pre-Notified and Notified EID Schemes under EIDAS', 2. January 2019. Accessed 6. September 2020. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

79. CEF Digital. 'EIDAS Levels of Assurance (LoA)'. CEF Digital, n.d. Accessed 6. September 2020. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+Assurance

80. EBSI, ESSIF. 'Technical Specification (15) - EIDAS Bridge for VC-ESealing'. CEF Digital, n.d. Accessed 2. September 2020. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITALEBSI/Technical+Spe

cification+%2815%29+-+eIDAS+bridge+for+VC-eSealing

81. Phillip J. Windley, Ph.D. 'The Architecture of Identity Systems', 28 September 2020. Accessed 29. September 2020. https://www.windley.com/archives/2020/09/the_architecture_of_identity_systems.shtml

82. CEF Digital 'Guidance for the Application of the Level of Assurance Which Support the EIDAS Regulation.' Accessed 10. October 2020. Accessed 6. September 2020. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents?preview=%2F40044784%2F40044786%2FGuidance+on+Levels+of+Assurance.docx

83. BusinessDictionary. 'Governance'. BusinessDictionary.com, n.d. Accessed 22. Mai 2020. http://www.businessdictionary.com/definition/governance.html

84. EBSI / ESSIF. 'Technical Specification (2) - DID Modelling'. CEF Digital, n.d. Accessed 7. October 2020. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITALEBSI/Technical+Specification+%282%29+-+DID+Modelling

85. M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnel, D. Reed, O. van Deventer. 'Hyperledger/Aries-Rfcs 0289: The Trust over IP Stack'. GitHub, 4. November 2019. Accessed 14. September 2020. https://github.com/hyperledger/aries-rfcs

86. Alexis Hancock. 'Digital Identification Must Be Designed for Privacy and Equity'. Electronic Frontier Foundation, 31. August 2020. Accessed 29. September 2020. https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10

87. Sovrin Guardianship Task Force. 'On Guardianship in Self-Sovereign Identity', December 2019. Accessed 21. Mai 2020. https://sovrin.org/wp-content/uploads/Guardianship-Whitepaper2.pdf

88. IBM News Room. 'IBM Future of Identity Study: Millennials Poised to Disrupt Authentication Landscape'. IBM News Room, 29 January 2018. Accessed 23. September 2020. https://newsroom.ibm.com/2018-01-28-IBM-Future-of-Identity-Study-Millennials-Poised-to-Disrupt-Authentication-Landscape

89. M. Palatinus, P. Rusnak. A. Voisine, S. Bowe. 'BIP39: Bitcoin Improvement Proposal 0039'. GitHub, n.d. Accessed 8. August 2020. https://github.com/bitcoin/bips

90. HTC EXODUS. 'Setting up Social Key Recovery', n.d. Accessed 24. September 2020. https://www.htcexodus.com/us/support/exodus-one-s/category_howto/setting-up-social-key-recovery.html

91. Covid Credential Initiative (CCI). 'COVID-19 Credentials Initiative : Home', n.d. Accessed 24. September 2020. https://www.covidcreds.com/

92. Adrian Doerk, Sarah-Karina Lahser. 'Der Bank-Verlag tritt der Lissi-Initiative bei', 26. June 2020. Accessed 27. June 2020. http://www.die-bank.de/home/oekosystem-fuer-selbstbestimmte-identitaeten-14752/

93. Bundesministerium der Justiz und für Verbraucherschutz. 'Vertrauensdienstegesetz (VDG) § 11 Identitätsprüfung'. N.d. Accessed 11. October 2020. https://www.gesetze-im-internet.de/vdg/__11.html

94. Kim Hamilton Duffy, Hans Pongratz, J. Philipp Schmidt, Digital credential consortium. 'Building the Digital Credential Infrastructure for the Future'. Accessed 30. September 2020. https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

Attachments

Attachment 1: Compilation of attachments