Delft University of Technology

Ministry of the Interior and Kingdom Relations

To obtain the degree of Master of Science

Computer Science

Industry-Grade Self-Sovereign Identity

On the Realisation of a Fully Distributed Self-Sovereign Identity Framework

[DRAFT]

Author
R.M. Chotkan

Supervisors
Dr. J.A. Pouwelse, TU Delft
A. De Kok, RvIG

June 13, 2021

Contents

Introduction

1

1.1 Self-Sovereign Identity

The need for digital empowerment has lead to a concept striving for digital sovereignty. Self-Sovereign Identity (SSI) attempts to put the user at the centre of their data by providing control over their digital identity. Where a *digital identity* refers to a piece of digital information used to of uniquely identifying and authenticate an entity. In case of a person, we refer to this as any *personally identifiable information* (PII) used to authenticate a user. Wherein a regular digital identity management systems (DIMS) any party attempting to verify the identity of a user, must communicate with some form of identity provider, SSI allows the user to be the identity provider through verifiable claims or *attestations*, making the traditional require infrastructure absolute. In SSI, users store their own data in the form of *attestations*. Attestation are verifiable claims of authenticated data attested to by an authority. In its essence, Self-Sovereign Identity has the capability of transforming one's real world (physical) identity to the digital domain. As in the real world, one often identifies itself through attestations: for instance, a driving license is an attested to piece of information indicating that the government (an authority) attests to your driving capabilities. This allows others to build confidence in your role as a driver. However, apart from such attested to claims, verifying self-attestations also becomes a possibility through SSI. For instance, one can self-attest to a set out goal, allowing others to verify this information. As becomes apparent, SSI allows one to verify and, hence, build confidence in digital information.

Attestations are the core concept of Self-Sovereign Identity. We visualised the their main application in Figure 1.1. In the general flow of SSI, an Authority attests to a specific claim (e.g. I am Alice). Next, in any instance that another party requests a specific attribute, the Subject of the attestation can present the claim and the attestation, allowing the Verifier to verify the validity of the claim. In a real world scenario, this could be an e-commerce platform requesting the address of a user in order to ship his parcel. As becomes apparent, this no longer requires interactivity with any identity provider or, with respect to SSI, the Authority of the attestation.

Often, blockchain technology is brought into the equation of Self-Sovereign Identity. Whilst definitely not a must, blockchain technology can prove to be an enabler of Self-Sovereign Identity systems.

1.2 Motivation

The motivation of this research it two-fold. Firstly, there exists a need for academic research into Self-Sovereign Identity. And secondly, there exists a need for sovereignty in digital identities. We firstly discuss the academic needs.

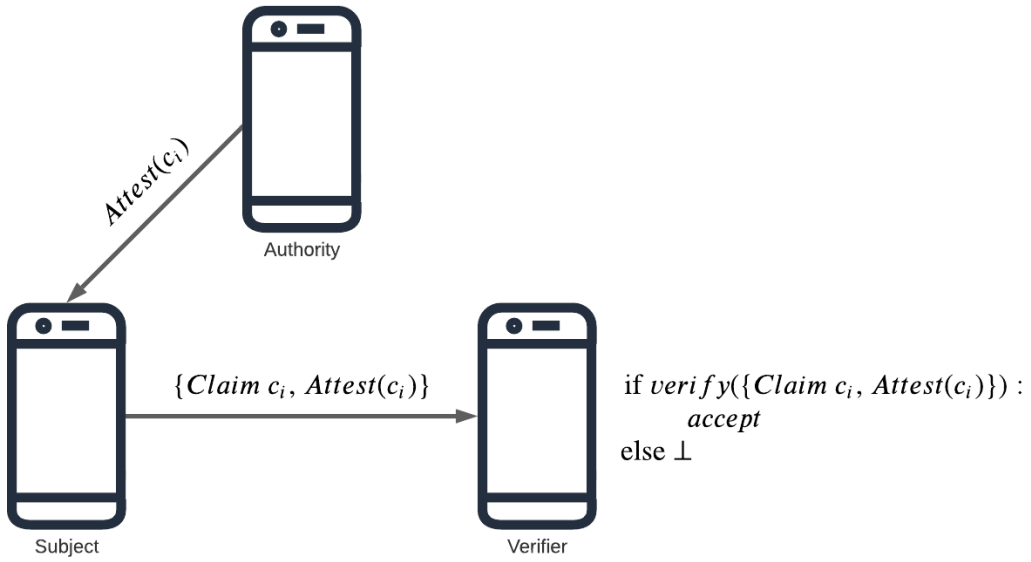


Figure 1.1: Triad of Verification

The majority of proposed Self-Sovereign Identity framework introduce inequalities in the network. These inequalities deteriorate the privacy and may even introduce censorship. Examples of this include, the usage of key splitting in Irma. Apart from censorship by the network itself, state intervention such as the Great Firewall of China, may impose restrictions on the protocol itself. This research focuses on the possibilities of a truly distributed Self-Sovereign Identity framework, where in each client is deemed to be equal from the protocol perspective. As such, there should be no necessity on external infrastructure in order to safeguard the prosperity of the network of the functioning of the protocol. Most notably, the revocation of credentials appears to be a common shortcoming in already proposed framework. For instance require special verification nodes in order to verify the validity of attestations. Whilst other solutions require full interactivity with the Authority of an attestation, introducing single points of failure into the protocol. Apart from the shortcomings in proposed frameworks, Self-Sovereign Identity has a minor presence in academia. As such, the majority of proposed and deployed solutions do not necessarily have a academic substantiation, hence, complicating the reproduction of results.

Socio-economic-wise, there exist two reasonings for the rationale of Self-Sovereign Identity's existence: the first reasoning is to devoid the current oligopoly of big-tech companies in the digital identity domain. The main issues regarding this oligopoly are lack of control, privacy. and information asymmetries. The foremost issue is lack of control: the service provider may revoke ones digital identity without warning, resulting in a loss of access to possibly countless of services. SSI attempts to resolve this issue by allowing the digital identity to be owned by the subject theirself.

These identity providers are essentially commercial parties, profiting from data received through managing these identities. This breach of privacy often comes hand in hand with the free to use service offered by the digital identity service providers. The often circulating

quote "If you are not paying for it, you're not the customer; you're the product being sold"[1] holds up in this regard. The issue with commercially available identities is that they do not provide legally valid identities and pose a huge threat on privacy, as the subject has no control over with whom their data is shared. This additionally leads to information asymmetries: as these big-tech companies posses large amount of PII of their users, any economic transaction made with them, results in them possessing more knowledge than the buyer. This effect has been regarded by [52] as the use of adhesion contracts, which go against the users' best interests.

The second reasoning is economic inclusion: residents residing in countries devoid of proper (central) identity infrastructure, are excluded from essential services enabled through identification system. [**?**] defines identification to be required for the following:

- Inclusion and access to essential services: e.g., healthcare, education, and financial services.
- Effective and efficient administration of public services, policy decisions and governance.
- Accurate measure of development progress in areas.

Hence, without any form of valid identification measures, these residents are devoid of essential services and are less likely to be able to improve their living conditions or receive aid. Globally there exist an estimated 1 billion people without a valid proof of identity [55].

As the first issue, mostly regarding privacy and control, is a far more relevant topic in Computer Science, with the second problem is more a socio-politic issue, the primary focus of this research will be targeted at combating the former phenomena.

1.3 Research Questions

The topic of Self-Sovereign Identity and the notion of *Industry-Grade Self-Sovereign Identity* shall foremost be investigated through the following research question:

"How can Self-Sovereign Identity serve as a fully decentralised digital alternative to centralised identification measures?"

This research question will allow for the investigation into and the development of a state-of-the-art SSI architecture. Based on the identified knowledge gap, the following sub-questions can be investigated:

1. *How to store verifiable claims locally in a decentralised fashion?*
2. *How to integrate the concept of 'trusted entities' into Self-Sovereign Identity?*
3. *How to perform revocation without interactivity?*
4. *How to design an open Self-Sovereign Identity standard that allows for an accessible implementation (e.g. supported by all major smartphone operating systems?)*

Based on these results, we will be able to design an SSI architecture that will overcome these shortcomings and be deemed to be of *industry-strength.*

[1] `https://www.metafilter.com/95152/Userdriven-discontent#32560467`

1.4 Contribution

The work set out by **(author?)** and **(author?)** will serve as a foundation of the IG-SSI scheme. The contributions made by this thesis will be an SSI scheme that can be said to be of *industry-strength*, which will be substantiated with a real-life trial of an implementation of said scheme. The main knowledge gap currently existing in the research area of SSI is the gap between the theoretical frameworks and the feasibility of these theories. E.g., strict processing latency requirements on mobile devices, communication overhead, and fault-tolerance. As such, this thesis will attempt to bridge this gap by constructing an SSI scheme together with developing an interaction model that allows for a practical implementation that is to be verified through real-life user tests.

1.5 Outline

Background Information

2

2.1 Identity

IDENTITY has a broad spectrum of definitions. The terminology itself stems from the Latin word for *"sameness"*, namely *identitas*. Philosophy draws the distinction between *qualitative* and *numerical* identity[34]. Qualitatively, identity is defined as entities sharing certain characteristics. Whilst numerically, we speak of total qualitative identity, thus requiring a set of characteristics which an entity only shares with itself. These characteristics are referred to as attributes[12]. The notion of the numerical identity of a person through time is referred to as the *personal identity*[35]. The foundations of this law can be traced back to Aristotle's *Law of Identity*, broadly stating that everything is equal to itself [4].

The requirements for the technical sense of identity are most fulfilled by the definition of the *numerical* variant. As it can be said that the goal of digital identity is to uniquely identify entities. Hence, *personal identity* may prove to fall short in such specification, as digital identity does not solely consider persons. Namely, [23] defines identity as "any set of attributes that describe a particular entity". We can, thus, state that identity is the set of characteristics uniquely describing an entity. When such a characterisation is transformed to the digital domain, we speak of *digital identity*. The goals of digital identity are *identification* and *authentication* [7]. Where identification can be seen as the authorisation of one's identity [12] allowing the unique identification of a user in a system [20]. Authentication is the action of proving one's identity. This can be achieved by three means:

- Something you know (e.g. a password).
- Something you have (e.g. a smartcard or key).
- Something you are (e.g. biometrics: fingerprint, face, etc.).

Often, measures are combined, referred to as *multi-factor authentication*.

2.2 Digital Identity

The Internet was not created with an identity layer. Even the conceptual OSI-model does not contain a layer specifically designed for identity. The layer which often takes on this responsibility is the Application layer. As a consequence, there is no *digital Identity*. The current digital ecosystem comprises one's digital presence through fragments of pseudo-identities. These pseudo-identities ultimately belong to a single entity and, thus, all attempt to be a digital identity. Of course, one is able to be identified digitally through these shards. However, these pseudo-identities lack the knowledge to fully uniquely identify an entity. We refer to this phenomena as

the *Sharding of Identity*. Each of these pseudo-identities often attempt to authenticate the same data. For instance, name, age, and a means of communication (e.g. e-mail). As such, all these pseudo-identities can be labelled as being derivatives of one's actual identity: the true digital identity. One that is uniformly true and does not require indefinite copies for each new encounter. The relationship between these groups are visible in Figure 2.1. As is visible, one's digital identity is a subset of one's physical identity, indicating that the digital identity is invariably linked to the entities physical identity, and the group of digital identity shards is a subset of what one's digital identity may possibly be. We note overlap between identity shards, which is caused by a non-empty union of the attributes comprised by said shards. For instance, the vast majority of services require a registration per name. As such, most digital identity shards will have at least an overlap on this attribute. As may become apparent from this description, these digital pseudo-identities fall under qualitative identity as most of them share attributes with other shards. This follows naturally from the fact that each of them attempt to identify the same entity.

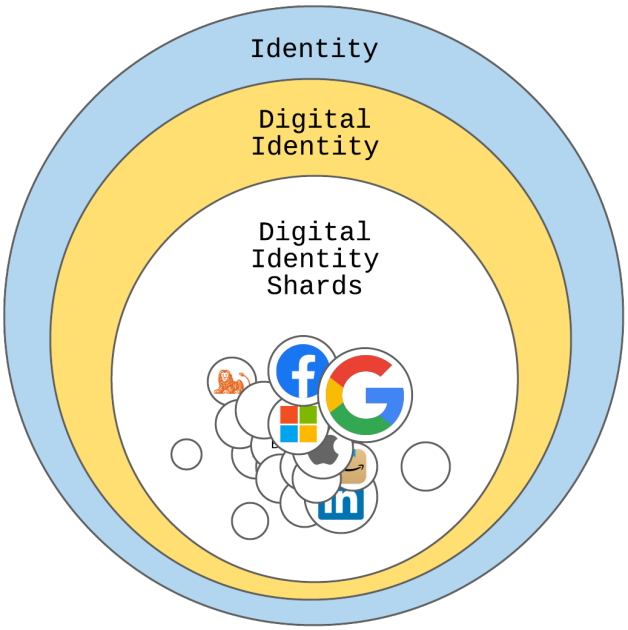


Figure 2.1: Identity Groups

so [10] describes some aspects of this phenomena. **(author?)** refers to the Internet as *"a patchwork of identity one-offs"*. With this statement, they refer to the same phenomena that resulted in the Sharding of Identity. Namely, each Internet service providing or requiring and managing its own (unique) identity system.

2.3 The Evolutions of DIMS

[3] describes four phases of digital identity. Although the chronological ordering of the phases is correct, we argue that the term *phase* is not correct for these specifications as phases indicate

non-concurrent existence. For instance, the eight phases of the Moon do not exist simultaneously. Therefore, we propose the usage of the term *evolution*. As evolution indicates gradual development, whilst allowing simultaneous existence with prior iterations. Note that evolution does not necessarily indicate improvement, which is also not insinuated by the term *phases*. Hence, the following four evaluations of digital identities exist:

Evolution One: Centralised Identity

With the onset of the Internet, centralised authorities such as IANA[1] and ICANN[2] became the issuers and authenticators of digital identities. For instance, the IANA determined the validity of IP addresses [18], whilst the IANA managed the registration of domain names [21]. Next, in order to generate trust through certificates, Certificate Authorities were created, which were able to also delegate some power through hierarchies. Finally, as mentioned by [10], the distributed nature of the internet let to online services implementing their own digital identity management systems, which for the user often led to username and password combinations. All of the aforementioned organisations present in the Internet ecosystem are inherently centralised authorities, with capabilities of revoking these identities. This comes with the consequence of users not owning any of their digital identities, as they are all either assigned to them or are managed by others. For instance, the registration of a domain name is performed on a yearly-bases, allowing one to never fully own a domain name.

Evolution Two: Federated Identity

The second generation attempted to overcome the hierarchies, by imagining a *federated identity*. An example of this is Microsoft's Passport initiative [38], allowing identities across different domains. However, this initiative soon proved to be far from optimal, as it is comprised of a single authority. This was improved upon by allowing each site to remain an authority [3]. However, users were still not provided with the means of controlling what happened with their data. Hence, there was a need for a new evolution catering to the user aspect of digital identities, as opposed to the identity management aspect.

Evolution Three: User-Centric Identity

Currently, identity management systems are in the third generation, the "*User Centric Identity Management*", originally described by [24] . This generation attempts to put the user at the centre of their identity. Open-sourced examples of these include OpenID[3], OAuth[4] and FIDO[5]. These systems focus on user centricity through consent, and interoperability, allowing users to select their own provider. Unfortunately, these efforts have resulted in the still register being the owner of the identity, instead of the user. However, the main drawback to the current phase is the introduction of initiatives such as Facebook Connect[32] (contemporary known as

Allen refers to another source (?)

[1] For IANA, see: `https://www.iana.org/`
[2] For ICANN, see: `https://www.icann.org/`
[3] For *OpenID*, see `https://openid.net/connect/`
[4] For *OAuth*, see `https://oauth.net/`
[5] For *FIDO*, see `https://fidoalliance.org/`

Facebook Login[6]) or Google Identity[7]. Whilst these initiatives do allow selective sharing of identity information and regard user consent, they still store identities in a centralised fashion and are managed by a single authority, namely a commercial party. The global adoption of these digital identity providers, has led to what we refer to as, the *oligopoly of digital identities*.

The oligopoly poses additional threats to users. The main issues regarding this oligopoly are lack of control, privacy, and information asymmetries. More prominently, Big Tech now has the ability to potentially revoke ones digital identity without warning, resulting in a loss of access to possibly countless of services. Privacy is at peril as Big Tech is enabled to gain information on their users through other services. This privacy concern can lead to market mechanisms such as information asymmetries, due to these extra opportunities for data farming. These identity providers are essentially commercial parties, profiting from data received through managing these identities. This breach of privacy often comes hand in hand with the free to use service offered by the digital identity service providers. The often circulating quote "If you are not paying for it, you're not the customer; you're the product being sold"[8] holds up in this regard. The issue with commercially available identities is that they do not provide legally valid identities and pose a huge threat on privacy, as the subject has no control over with whom their data is shared. This additionally leads to information asymmetries: as these big-tech companies posses large amount of PII of their users, any economic transaction made with them, results in them possessing more knowledge than the buyer. This effect has been regarded by [52] as the use of adhesion contracts, which go against the users' best interests. These concerns portray a need for a different approach to identification, breaking the oligopoly and creating the ability to generate trust over the Internet.

2.4 Shortcomings in the Current Ecosystem

The current ecosystem of digital identities suffers from several drawbacks and limitations, both from the perspective of identity providers as of that of the users.

Problems for Identity Providers

For identity providers, identification measures can prove to be a double-edged sword: whilst it allows them to manage their users' digital identities, allowing them to gather user statistics and information in order to improve their services, it can also prove to be a burden. Firstly identity providers must adhere to specific data compliance legislation such as the GDRP [51] or the PCI DSS [14]. Additionally, often companies strive for internation standards such as ISO/IEC 27001 [22]. The leakage of Personal Identifiable Information (PII) cannot only lead to liability in accordance to said legislation (e.g., the GDPR has the possibility to fine companies in the millions), but can also have side effects for the users. For instance, in case passwords are compromised, other services utilised by the user may be at peril or the leaked PII can be used for spear-phishing attacks. Moreover, such losses can have tremendous impact on the image of an organisation. Breaches such as the Cambridge Analytica Scandal [42], portray the impact.

[6]For *Facebook Login*, see: `https://developers.facebook.com/docs/facebook-login/`
[7]For *Google Identity*, see: `https://developers.google.com/identity`
[8]`https://www.metafilter.com/95152/Userdriven-discontent#32560467`

Problems for Users

On the other end, users suffer from these consequences and more: firstly, users must keep track of all their fragmented digital identities, often requiring to manage a multitude of digital identities. A report published by **(author?)** in **(year?)**, shows that on average employees of small businesses manage 85 passwords. With the statistic that the use of brute-forced or stolen credentials are responsible for over 80% of the vulnerabilities utilised in breaches [54], credentials continue to be a weakness in online identification measures. Secondly, users' information is stored in numerous amounts of locations, significantly increasing the chances of their personal identifiable information to be stolen, as this increases the attack surface. For instance, [50] reported that in 2020, 49% of US companies reported a digital breach of some degree.

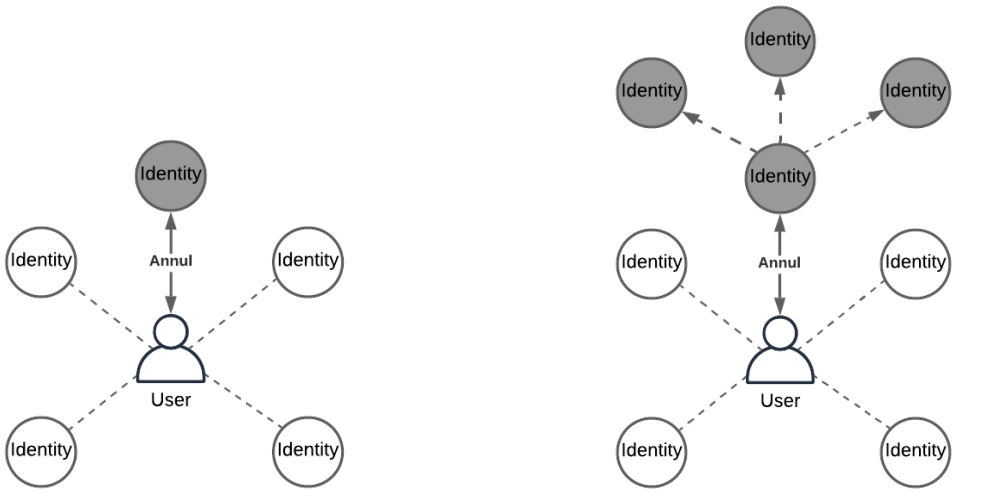
Furthermore, the oligopoly poses additional threats to users. The main issues regarding this oligopoly are (I) a disproportional balance of power, (II) privacy issues, and (III) information asymmetries.

The Balance of Power

The disproportional balance of power is caused by the connection with other services. In a central identity, i.e. one in which the service provider is also the identity provider, the user and the service provider hold relatively the same amount of power. More specifically, the user has the ability to stop their usage of the service and, thus, losing a single digital identity shard. Similarly, the service provider has the ability to refuse service to the user, revoking in turn a single digital identity shard and, thus, the revoking access to a single web service. This generates a balance of power within their relationship, as both of their abilities to annul the digital identity leads to a single loss. Hence making the balance one-to-one. This has been visualised in Figure 2.2a, portraying one-to-one annulment relationship. Of course, this lays more delicately, as often the service provider generates value for the user making the user reliant on them to some degree, hence, shifting this balance in the favour of the provider. However, when the identity provider manages a federated identity system or a user-centric variant, this balance shifts greatly. As now, a user desiring to annul his digital identity with such a provider, will cascadingly annul his access to any connected service. Hence, they are often not able to discontinue any arrangement with such an identity provider without affecting their arrangement with other service providers. On the other hand, as the identity provider has the ability to revoke ones digital identity, users may face loss of access to any connected services. For instance, in case a user is deemed to have breached a term of use. This has been visualised in Figure 2.2b, which portrays the imbalance of annulment power.

Privacy Issues

(author?) showed that 84% of the people believe that they have lost all control over how their data is used by companies. This aids in portraying the privacy issues experienced by users. The digital identities managed by Big Tech can further impact privacy, as they enable the gathering of more information on their users through other services. Any connected service has the potential to serve as a funnel for additional data on user information. The identity providers are essentially commercial parties, profiting from data received through managing these identities. This breach of privacy often comes hand in hand with the free to use service offered by the digital identity



(a) Centralised Identity

(b) Federated/User-centric Identity

Figure 2.2: Balance of Power

service providers. The often circulating quote "If you are not paying for it, you're not the customer; you're the product being sold"[9] holds up in this regard.

Information Asymmetries

The privacy concerns can lead to market mechanisms such as information asymmetries, due to the extra opportunities for data farming. As the identity providers posses large amounts of information on their users, any economic transaction made with them, results in them possessing more knowledge than the buyer. This effect has been regarded by [52] as the use of adhesion contracts, which go against the users' best interest. These concerns portray a need for a different approach to identification, breaking the oligopoly and creating the ability to generate trust over the Internet.

2.5 Self-Sovereign Identity

It can be said that Self-Sovereign Identity is not a technology, but a movement [46]. It is a term not coined by academia, but one stemming from a need in sovereignty over identity. In order to define Self-Sovereign Identity, we must first dive into the history of the movement so far. In this section we describe the history of Self-Sovereign Identity, sketch a description of the term, and discuss the properties Self-Sovereign Identity is to adhere to.

[9] `https://www.metafilter.com/95152/Userdriven-discontent#32560467`

Table 2.1: The principles by Loffreto (2016)

Principle	Description
Human Life	An SSI originates from an individual human life.
Human Identity	The human identity is the source authority of an SSI.
Attestations	An SSI has no personal control or authority until it is attested to by others.
Unpragmatic	SSI is not to be pragmatically defined as it is a function of time and place.

History

There is no clear onset of Self-Sovereign Identity. [39, 3] refer to the work of *"What is 'Sovereign Source Authority'?"* [28] in 2012 to be the onset of SSI. Allen misatributes this work to Moxie Marlinspike, the co-founder of Signal[10]. However, presumably this was performed on purpose [44]. In their work, Loffreto describes the concept of *Sovereign Source Authority* (SSA). With SSA, Loffreto calls for an overhaul of the current national administrative identities. They refer to the current systems as lacking the ability of providing a real identity, as current identities can be seen as a registration process for participation in society. SSA can be seen as a need for what Loffreto refers to as *Human identity*. This falls in line with the Identity Groups as discussed in section 2.2. Loffreto's main argument for an alternative identity system comprises of societal participation being a choice, hence one must be able to have a valid identity without participating in society. Loffreto states that *"Within any Society, Individuals have an established Right to an "identity"*. The term *Sovereign Source Authority* itself did not gain much traction. However, it did led to the coining of the term *Self-Sovereign Identity*. Whilst no key literature has been identified for coining the term itself, it can be said that SSI has gained traction due to Christopher Allen. Allen has often been erroneously credited for the invention of the term *Self-Sovereign Identity*, however, has explicitly credited Loffreto. Four years later, in 2016, Loffreto made another blog post on explicitly SSI. In [29], **(author?)** describes four properties of SSI. These principles have been summarised in Table 2.1. As becomes apparent from this description, Loffreto does not consider SSI to be a digital technology, but more a concretization of the human life, capable of authenticating the human identity.

Later in the same year, Allen released his blog post "The Path to Self-Sovereign Identity" [3], which, undeniably has been a major influence on the field, with all major publications referencing said work, e.g. [52, 33, 49, 5, 17]. In their work, [3], describes ten principles which SSI is to adhere to. However, an often uncredited piece of literature in SSI is that of **(author?)**'s "Laws of Identity"[10], where *Laws* is used in the scientific sense. In this work, published more than a decade prior to the literature directly on SSI, Cameron calls for a need for "unifying identity metasystem" [10]. Furthermore, the concepts of digital *subjects* and *claims* are introduced, making way for *claim-based* identities. This work describes a large number of fundamentals of SSI and is often disregarded in literature on SSI, whilst being a highly influencing article in DIMS in general, with laws being implemented in systems such as OpenID 2.0[40]. These laws explain the shortcomings and successes of digital identity systems and, as such, are applicable to SSI. The works of [3, 10, 29] are described more thoroughly in **??**

[10]For Signal, see: `https://signal.org/`

Critique of the Term

Sovereignty is defined as "supreme authority within a territory" [37]. In terms of *Self-Sovereign Identity*, this would translate to *supreme authority over one's identity*. This term is prone to misinterpretation. As *supreme authority* insinuates that one has the full power of some territory. However, the extent to which this power reaches is open for interpretation. For instance, Good ID defines *Self-Sovereignty* as "a feature of an ID or identity system, whereby, individual users maintain control over when, to whom, and how they assert their identity". There exists a discrepancy between this definition and the definition of the word itself posed by [37]. We identify the same discrepancy in literature. For instance, the works set out by [28, 29] portray a philosophical nature of SSI, not necessarily indicating the usage of DIMS. DIMS are merely an implementation which allows a realisation of SSI. Furthermore, proposed solutions such as [25, 17, 56, 30] do not necessarily adhere to this description. However, the case can be made that [49, 48] as well as, transitively, IG-SSI would allow for the human identity as origin of source authority, as described by [29]. It can be noted that SSI and DIMS are undeniably intertwined, having led to misinterpretations of the term itself. Concerns for the usage of the term have been raised [43, 11]. Common misconceptualisations due to the term itself, are the following [43]:

- **Self-sovereign means self-attested**
  The term sovereignty implies total domination and, as such, could lead to self-attestation. However, even in the descriptions proposed by [29], claims require attestations. We do believe that claims due allow for self-attestations, as in certain instances verifiability through others is simply not required. However, it is not the case that any self-attested nature is a given.

- **SSI attempts to reduce government's power over an identity owner**
  This claim we deem invalid due to a multitude of reasons. Firstly, SSI, as is generally true for any form of technology, is adiaphorous; SSI is not an entity that can act, hence it is inherently neutral. The realisation and usage of SSI can impact a government's power. [28, 29] does propose SSI as an alternative to the centralised governmental identities, as he deems the centralised registration unnatural. Secondly, the case can be made that the traditional governmental identity can evolve into SSI. With active plans from the European Commission to introduce a European Digital Identity, wide-spread SSI may even be introduced by government [13]. Moreover, SSI can prove to not delegate any power from governments as they can simply become an attestor for a digital identity credential, making them intrinsically an authority. As government can be considered a commonly accepted authority, the network will most probably acknowledge the government for verification of a digital identity. SSI can even prove to aid governments by reducing the need for maintaining the physical identification documentations.

- **SSI gives absolute control over identity**
  This misconceptualisation is most likely caused due to the ambiguous nature of the term *Self-Sovereignty*. As we established that *self-sovereignty* does not lead to *self-attested*, the dependency on attestation directly deteriorates the level of control one has over claims. Verifiable claims require authorities to attest to a certain piece of information. The lack of

authoritarian party, which is deemed trusted amongst the network, that attests to a claim, making it verifiable, leads to a weak claim. Hence, whilst one does have the power to self-attest and, furthermore, fully controls the actions regarding his data in terms of verifiable claims, one's self-sovereign identity will still be dependent on others. For instance, it is a possibility that a digital identity will only become valid in case it is attested to by a governmental institution, as otherwise there is no neutral party in which one can built trust in the validity of the information of the claim. Intrinsically, there is no true sovereignty over what attributes one has, but merely, sovereignty over what happens with said attributes.

The above critiques and misconceptualisation sketch the ambiguous nature of the *sovereignty* part of SSI. It leads to a need for a more defining term. [43] proposes the use of *decentralised identity* as an intermediary term. However, the major shortcoming of this term is that it does not convey the level of control that a user has. As, in order to be classified as *decentralised*, a system must simply consists of multiple parts which collaborate in order to achieve some goal. Hence, the selection of *decentralised identity* is not strict enough in order to explicitly convey the user rights. Therefore, we propose the usage of the term *Self-Governed Identity* (SGI) in order to specify and distinguish what literature most commonly refers to as SSI from the more anarchic SSI discussed by [28, 29]. To govern can be defined as "conduct the policy, actions, and affairs of (a state, organization, or people) with authority" [16]. When placing this definition in the context of *identity*, one would be able to conduct the policy, actions, and affairs of one's identity. This constraint the power of the principles behind SSI, as *self-governed* does not imply total dominion over one's identity as sovereignty does. As a consequence *self-governed* implies that one has full control of one's identity, whilst not necessarily defining what the identity is. This flows naturally from the instances in which identity is to be assigned to one. As any society decides that a government has the power to delegate identities, hence, SSI will most likely have to adhere to this structure in order to gain any form of legal validity. However, this does not mean that SSI itself must force this behaviour, as self-attestations have valid use-cases. Even more, an identity may be formed through self-attestation. However, this most likely does not lead to any legally valid identity as such an identity is only valid to the extend that it is accept by any parties with whom one will communicate and require identification. A government hence provides a (relatively) neutral party in which one can generate trust in order to only attest to valid identities, allowing verification of such identities. Hence, the term *Self-Governed Identity* can prove to encapsulate this almost inherently unavoidable unbalance of power. SSI can, hence, be seen as a digital alternative as opposed to a digital revolution, as it is unavoidable that certain existing and, most probable, required power balances must be transformed to the digital domain in order to safeguard the identity. However, we believe that the most important nature of SSI and, subsequently, the more lenient proposition of SGI is to place data back in the hands of users and providing the digital domain with legally valid identities and verifiable information without the need for a central authority.

2.6 Theoretical SSI Models

As no consensus on a formal definition of Self-Sovereign Identity has been reached, the properties of SSI are loosely defined. There are, however, returning concepts in (academic) literature and

common notions of use-cases. This section will aid in defining a set of requirements based on identified common themes in literature and will bridge the gap in unresolved issues.

2.7 The Laws of Identity

As mentioned previously, Cameron describes the seven laws of identity, which DIMS are to adhere to [10]. Whilst not directly calling for sovereignty over digital identity, the principles describes by Cameron are all visible in contemporary notion of SSI, hence, we can make the case that SSI was created in 2005, at least the foundations for it. The following laws are proposed by [10]:

1. **User control and consent**: digital identity systems must only reveal personal identifiable information (PII) given prior consent by the user. Through this law, trust can be built between the system and the user.

2. **Minimal disclosure for a constrained use**: the solution which discloses the least amount of and best limits the use of PII, is the most stable long term solution. This law minimises risk, as it is assumed that a breach is always possible.

3. **Justifiable parties**: disclosure of data with third parties must always be justifiable in a given identity relationship. Through this law, the user is aware of any third parties with whom is interacted with whilst sharing information.

4. **Directed Identity**: universal digital identity systems must support "omni-directional" identifier, which can be said to be public, and "unidirectional" identifiers, which can be said to be private, enabling identification whilst facilitating privacy.

5. **Pluralism of operators and technologies**: universal identity system must support multiple identity technologies run by multiple identity providers. This law enables the incorporate this somewhere, disallowing vendor lock-in and encourages the use of open-standards.

hnologically agnostic
perty

6. **Human integration**: universal digital identity systems must incorporate the user as a component of the system, offering protection against identity attacks. This laws attempts to bridge the discontinuity between the actual (human) users and machines with which they communicate.

7. **Consistent experience across context**: universal digital identity systems must allow for a separations of domains, whilst enabling a consistent experiences within and across them. This law thus enables interoperability across different operators and technologies.

Whilst not coining a specific term for such a system, we do identify key aspect relevant to SSI which were later—in an adapted form—reiterated in the conceptualisation by [3].

The Path to Self-Sovereign Identity

[3] is undeniably the most commonly referred to literature with respect to SSI. In their work, the following set of *principles* are posed:

1. **Existence**: users must have an independent existence. I.e., a (digital) sovereign identity does not solely exist digitally. As a result, it can be interpreted as requiring to be tied to a physical entity.

2. **Control**: users must have control over their identities. This entails a full authority over the user's own identity: the ability to share, update, and even hide.

3. **Access**: users must have access to their own data. Similarly to the above principle, users must be able to access all of their data.

4. **Transparency**: all involving systems and algorithms must be transparent. This entails open-standards and open-source software.

5. **Persistence**: identities must be long-lived. Identities should, thus, exists until destroyed by the user.

6. **Portability**: information and services about identity must be transportable. I.e., identities must not be held by a single third-party, as they may not support it live-long. This principle would be satisfied by the *Control* and *Persistence* principles.

7. **Interoperability**: identities must be as widely usable as possible. This ensures that the identities can be globally deployed and can be achieved partly by adopting the *Transparency* principle.

8. **Consent**: users must agree to the use of their identity. This principle strengthens the *Control* principle, as sharing of attributes may only occur with the consent of the user. However, the **(author?)** noted that this must not require interactivity.

9. **Minimalisation**: disclose of claims must be minimised. I.e., the minimal amount of information must be disclosed when sharing claims. This principle is focused on privacy and prevents misuse of data.

10. **Protection**: the rights of users must be protected. The right of users must take precedence over the identity network itself. This can be achieved thorough the *Transparency* principle and decentralisation.

The above set of principles is often adhered to as a set of requirements. See e.g. . These principles portray that digital identities must be tied to the human, which are the most important entity in the system. Furthermore, their control is key to the design. We note a large overlap with the work of [10]. The laws "User control and consens"; "Minimal disclosure for a constraint use"; "Pluralism of operators and technologies"; "Human integration"; and "Consistent experience across context" can be directly identified from the ten principles from [3]. In addition to these ten principles, [49] add the principle of *Provability*: claims must be provable, as otherwise they can be deemed worthless. [52] builds upon these ten principles by subdividing then into three categories:

Add references

- **Security**: aims to keep the digital identity information secure. This consists of: *Protection*, *Persistence*, and *Minimisation*

- **Controllability**: focuses on the user-centric foundation of SSI. This consists of: *Existence*, *Persistence*, *Control*, and *Consent.*
- **Portability**: this requirement results in the user not being tied to a single provider and being able to use their identity without bounds. This consist of: *Interoperability*, *Transparency*, and *Access.*

The additional principle defined by [49] can be categorised into *Security*, as the provability of claims aids in generating trust and in creating authentication.

A Model for Digital Sovereignty

[47] describes another model for digital sovereignty based on the work by [3]. The resulting model is visible in Figure 2.3. As visible, there is an overlap with [3] and [10]. Most prominently, the model is built on top of *The Human*, indicating that SSI must stem from a human. Secondly, we note that the boundaries of sovereignty are modelled. Whilst we argue that the term sovereignty is too ambiguous, insinuating more freedom than is often considered, this model restrict the sovereignty of the domain related to the human identity. However, the drawback of this is not capturing the reliance on other parties. The additional property of verifiability also noted by [49] is present. However, we argue that properties such as *convenience* and *usability* are not specifically intrinsic to the design. Especially usability does not necessarily stem from a protocol, but from a user-interface or a human interface device built around the protocol. *Convenience* can also be deemed something that is not a part of SSI, but something that can be created using the technology. Furthermore, *purpose* is a reasoning for the existence of SSI, as opposed to the technology itself.

2.8 The Pyramid of Sovereignty

The previous sections portray a crisis in terms of both definition and the naming of the principle that is referred to as *Self-Sovereign Identity.* We believe that this is mostly caused by the unacademic origin of SSI. As such, we propose a new set of principles based on the commonly cited works of [3, 10], however, also taking into account the literature that sketched the beliefs of SSI [28, 29]. We propose the pyramid of sovereignty as present in Figure 2.4.

The main pyramid consists of ten principles, having overlap with [3]. The corner stones of the framework are *existence* and *control.* Existence requires an SSI to be linked to an entity. Where most literature requires a link with a human identity [29, 47], we state that an SSI must be linked to an entity in order to exist. We argue that this is a necessity for the prosperity and long liveness of SSI as a whole. Especially for ongoing fourth industrial revolution [31], in which SSI can prove to fulfil a prominent role with the communication of IoT [45]. Hence, allowing other entities, such a IoT devices or even digital bots or artificial intelligence which facilitate any form of communication with humans or support systems which such a goal, can prove to gain valuable characteristics through SSI. *Control* enables the user-centric nature of SSI, allowing complete access, consent, and usage of the data stored by an SSI for the user. [3] splits this up in *control*, *access* and *consenst.* However, we argue that control implies requirement of consent as in full control, no action is to be performed without knowledge of the one in

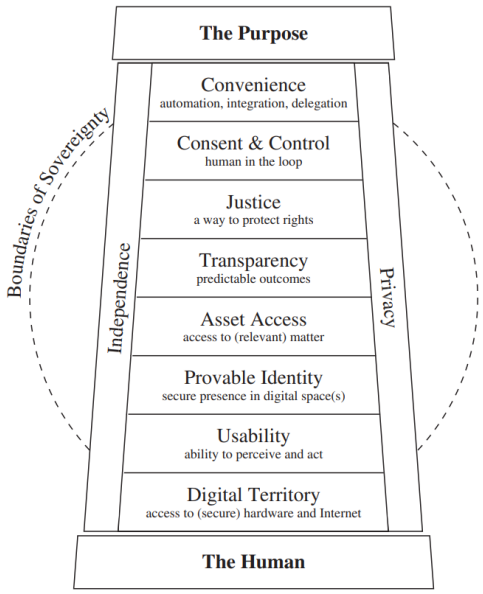


Figure 2.3: A Model for Digital Sovereignty [47]

control. Similarly, we argue that control implies access. Furthermore, control must also imply a free choice of storage. Hence, we deem the term *control* sufficient for enabling the user-centric nature. Furthermore, the bottom layer of the pyramid is reinforced by *verifiability*: a property not explicitly mentioned in literature. However, we deem verifiability to be one of the main foundations of SSI. As without verifiability, information holds no value. The second layer consists of *transparency* and *interoperability*. Where transparency strives for the usage of open standards and implementations, of which the very least the details of used algorithms and protocol are openly defined. This aids in making SSI a common good and ensuring that the principles are adhered to. *interoperability* ensures that a user is not locked in a specific implementation of SSI, allowing the communication with other services, even other systems. This aids in both ensuring user's rights as well as the adoptation of SSI through easy usage with existing solutions. The third layer is comprised of *minimalisation*: this principle ensures that no more information is shared than is required. This also entails that no information is shared with parties that do no explicitly require it. This falls in line with the comparable law posed by [10]. The final layer consists of *privacy*. All of the previous layers combined allows one to achieve a certain degree of privacy. Of course, no full privacy is ever achievable when sharing data. However, the SSI system must attempt to guarantee a certain level of privacy. Which is especially reinforced by the *control*, *transparency* and *minimalisation* principles.

Finally, the Pyramid is contained by two shells. The inner shell represent regulations imposed upon the system by for instance governments. In case legally valid credentials are introduced, legislation comes into play. This will most likely counteract, or at least deteriorate, the strength of (some of) the principles. This is visualised by the intersecting nature of the inner shell. The outer shell represents the *Domain of Sovereignty*, in which the further the pyramid nears the bounds of the domain, the higher the degree of sovereignty. As mentioned previously, [28, 29]

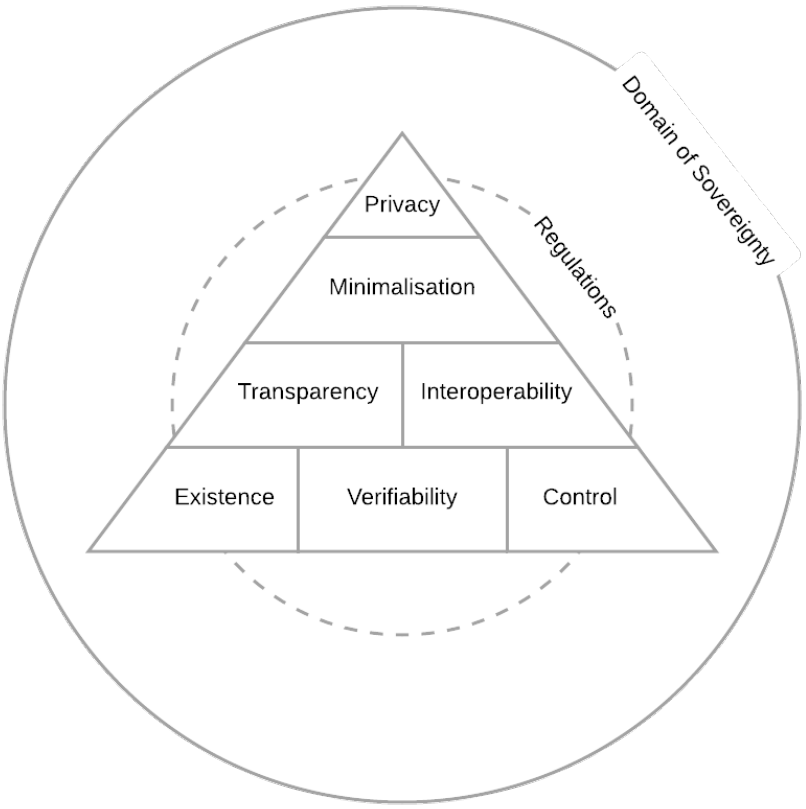


Figure 2.4: The Pyramid of Sovereignty

describes a more anarchic nature of SSI than most other literature envisions SSI to be. The outer bounds of this domain represent this level of sovereignty. As is visible, the proposed framework is more restricted in its levels of sovereignty than the notions discussed by Loffreto.

2.9 Existing Solutions

Sovrin

The Sovrin Foundation[11], focused on creating an identity layer for the Internet, notes several effects caused by the lack of identity management on the Internet. The traditional methodology for identification, i.e. unique credentials for each digital service, creates several layers of problematic side effects. Sovrin note that it is both problematic from a usability perspective and from a security perspective[52]. Firstly, from a usability perspective, managing different credentials for each service becomes problematic as users often do not take proper security measures. Secondly, the numerous storage location for these fragmented digital identities can prove to be honeypots

[11] For *Sovrin*, see `https://sovrin.org/`

for hackers, after which a possible breach affects the trust in said service and possible affects the security of a users' other credentials due to the aforementioned lack of proper security measures set into effect by the user theirself. The second phase in identity management, the so-called federated model mentioned by[3] is also sub-optimal. It foremost increased data leakage through sharing, raising privacy concerns, whilst still not allowing identity management by the user [52].

Furthermore, the impact of a missing identity layer causes large financial impacts. Services have to construct their own identity management system and they suffer from fake users, whilst user suffer from stolen records and identity theft [52].

Sovrin proposes the use of public permissioned blockchain, consisting of "Members" and "Stewards". Where the former are the user registered with their digital identity and the latter the verifying nodes. The foundation itself is to be tasked with developing, coordinating, governing and promoting the identity network [52]. They propose the use of two layers of nodes, where the nodes in the outer layer are deemed "Observer Nodes" which run read-only copies of the blockchain, and the inner layer consists of "Validator nodes" which allow for write access [2]. The reasoning behind this design choice is scalability. The principle is the same as the general concept of SSI: claims are cryptographically signed for a user, after which these can be verified by third-parties. Sovrin aims to store no private (encrypted) data on its blockchain. Additionally, Sovrin is compatible with the DID[12] standard from W3C [41]. In order to aid privacy, each relation uses new public and private keys

find citation

Serto (uPort)

. Serto[13], formally known as uPort, is an SSI solution built on Ethereum [30, 8]. Serto has a multitude of open standing project, of which their Ethereum SSI project appears to have gained the most traction. As was the case for Sovrin, Serto is being built to be compatible with the DID standard from W3C. Sovrin is built upon the concept of Ethereum smart contracts, where an identity can be represented by a smart contract of Ethereum address. The usage of Ethereum contracts, make Serto a Claim Registry Models. The contracts store the hashes of claims, of which the claims themselves are stored off-chain [**?**]. The underlying structures are built on the JSON format.

Decentralized Identifiers

The aforementioned solutions all utilise W3C's Decentralized Identifiers (DIDs). DIDs are a type of identifier that allow for verifiable, decentralised digital identities [1]. It is a specification drafted by the World Wide Web Consortium (W3C)[14]. And, being a specification, DIDs have no specific software or hardware requirements, it merely defines a generic syntax and generic requirements for the four CRUD (create, read, update, delete) operations [1]. The design goals of DID are the following [1] :

move to table

- Decentralization

[12]For *DID*, see `https://www.w3.org/TR/did-core/`
[13]For *Serto*, see `https://www.serto.id/`
[14]For *World Wide Web Consortium*, see `http://w3.org/`

- Control
- Privacy
- Security
- Proof-based
- Discoverability
- Interoperability
- Portability
- Simplicity
- Extensibility

The basic structure of DIDs consist of a DID which references a DID documents. The DID documents contains the actual information regarding identification.

2.10 Related Works

corporate this more
mlessly

[33]

[33] describe an overview of SSI. They state that ISS differentiates itself with traditional identity management systems by being a user centric model as opposed to service provider centric. They describe two architectures for SSI: the *Identifier Registry Model* and the *Claim Registry Model*. Wherein the former model the pairing of identifiers and public keys of users are stored onchain and claims offchain. In the later model, in addition to serving as a registry for identifiers and public keys, the claims themselves are also stored onchain. Next, they focus what they deem the four core components of SSI: identification, authentication, verifiable claims, and attribute storage. Identification comes done to the issue of having both uniqueness and human-readability in identifiers of clients. It is noted that the current best effort is that of *decentralised identified* (DID), which has a universal resolver by the Decentralized Identity Foundation[15]. They present a scheme capable of incorporating the four core components. The resulting scheme satisfies the ten principles by[3] and presents SSI in a intuitive fashion. The scheme sets verifiable claims at the centre: the these claims are issued by an issuer on a subject, which can be attested by other clients. These signed claims can then be verified by a verifier to whom a claim is presented to.

[15]

[15] describe the o opportunities and challenges for a digital revolution caused by SSI. The authors start with explaining the terms *digital identities* and *secure digital identities*. Where a *digital identity* is a temporal reflection of a regular identity: it merely contains specific characteristics of an identity, with varying level of detail. A digital identity can be held by any type of entity,

[15] `https://identity.foundation/`

may it be a person, a car, or a device. It usually has to function to use a particular service. In addition, a *secure digital identity* adheres to the requirements of *privacy* and *trustworthiness*. Where privacy leads to only authorised access to the identity, and trustworthiness the correctness of the attributes contained in the digital identity.

The authors then explain the general concept of Self-Sovereign Identity. They state that SSI can be the next step in identity management and mention the ten principles by [3]. SSI moves the requirements of privacy and trustworthiness to the user, requiring the user to provide evidence.

Next, three opportunities for SSI are explained. Firstly, SSI can counteract the oligopoly present in the management of current digital identities. Secondly, it can provide help to people living in crisis areas, as identities may no longer require ties to local government. Finally, SSI may help companies to adhere to the GDPR as privacy can be more easily implemented.

The challenges for SSI are also explained. It is stated that current digital identity services (e.g. Facebook connect) allow for a certain level of comfort by trading in a certain level of control of their identity. Based on that assumption, the case is made that one of the core challenges of SSI is that the additional required administrative efforts of SSI must be sufficiently comfortable. The following key challenges are outlined:

- Protection of privacy across transactions.
- Transparency between two parties during a transaction, i.e., consensus on content and conduct.
- Persistency of digital identities and logs for long-term transparency.
- Trustworthiness of digital identities and claims.
- Consistency between granted rights and real usage.
- Standardisation of data formations and interfaces.

Finally, the efforts by the ISÆN and an outlook are given with applications of SSI for the Internet of Things and institutions.

[49]

[49] present a blockchain-based digital identity solution. It is stated to be an academically pure model for SSI. They state that the first half of the problem regarding the creation of such a model, is the need for Self-Sovereign Identity: identity holders must be identity owners. The second half of the problem is the need for legally valid signatures: identities can e.g. be recognised by the governments, making them legally valid. They firstly describe the solution for the first halve of the problem, in which they state the ten principles by [3]. The blockchain-nature of their solution is said to intrinsically satisfy the majority of the principles, apart from:

- Portability
- Interoperability
- Minimalisation

- Protection
- Provability (added by authors)

The usage of zero-knowledge proofs and the chain of claims enabled by their blockchain, Trustchain, allows for the satisfaction of the remaining principles. Their solution comprises of zero-knowledge proofs also allowing for range proofs. Their claim metadata incorporates a validity term for finite claim validity as well as a "proof format" field, allowing for interchangeable signature algorithms. A reference implementation shows sub-second claim-verification performance.

[36]

[36] describe their Horcrux protocol, a decentralised biometric credential storage option via blockchain using W3C's Decentralised Identifiers (DID). The authors mention that the current drawback of traditional biometric-based authentication systems is that the systems are a single point of compromise for securing digital identities. This is caused by requiring a central authority for storing templates of biometric samples. The Horcrux protocol combines the SSI ecosystem with the h 2410-2017 IEEE Biometric Open Protocol Standard (BOPS). This is performed by dividing biometric templates into $n \leq 2$ shares, which are then stored distributed-wise. The actual shares are stored offchain, but resolvers to the DIDs are stored on onchain. Their solutions requires interaction with these BOPS-servers for enrolment into the SSI system.

[17]

[17] describe a mathematical model for SSI in order to provide a formal and rigorous treatment of the concept of SSI itself. As such, they firstly formalise a mathematical definition and identify the required properties for SSI, after which they investigate the impact SSI can have using the Laws of Identity. Finally, they investigate the implication of applying blockchain technology to SSI. Their formalised model of an SSI contains the definition of an entity. An entity has an identity which consists of of the union of all its partial identities. These partial identities are all of his attributes and values in a specific domain. Hence, an entity can be contained in multiple domains, where each partial identity can be subdivided into profiles (subsets of the attributes contained in the partial identity within a domain).

[10]

[10] describes one of the inherent flaws of the Internet being the lack of an identity layer: there is no standardised mechanism for identification, resulting in a shattered "patchwork of identity one-offs", so-called workarounds for identification.**(author?)** proposes a *unifying identity metasystem*, which, similarly to what sockets provide for networking, provides an abstraction for identification which allows application to abstain themselves from specific implementations and allow (lose) coupling of digital identities. For this, **(author?)** developed the seven *Laws of Identity*. These will be discussed more thoroughly in **??**.

[3]

[3] discusses the ten principles of SSI. Firstly, their work explains issues with traditional (physical) identity measures, e.g. driver licenses and social security cards, which are erroneously portrayed as identities. As a consequence, the issuing authority has the capability to nullify ones "identity".**(author?)** propose SSI as an improvement and solution. Next, the four phases of evolution of identity are explained.

[56]

[56] present EverSSDI: a framework based on Ethereum smart contracts allowing for unique identifiers to normalise different user identities. Additionally, they construct an authorisation method based on Hierarchical Deterministic (HD) keys, an information verification mechanism and two methods for identity recovery. Their design makes use of Ethereum smart contracts to store encrypted fingerprint variants of claims. The design uses so-called "Ever-Service" servers to generate unique IDs named "Ever-IDs". These specific servers also aid in a login procedure. It is not clear who manages the "Ever-Service" servers. They introduce two methods for identity recovery: one based on SNS authorisation and one based on Ethereum Oracles. The authors mentioned that their future research will incoroporate a custom public blockchain.

[6]

[6] propose their Self-Sovereign Identity Based Access Control (SSIBAC) model: and SSI access control scheme based on blockchain technology. Their research contributions include an access control scheme based on SSI, an implementation and evaluation. They achieve a throughput of 0.9 seconds per access control request. The design works by creating a verifiable presentation (VP) from a verifiable claim (VC). This VP is sent to a verifier, which confirms that the client holds the VC by verifying whether it satisfies a specific predicate. The drawback to the scheme is that the verifiers are a single point of failure in their design, which is acknowledged by the authors.

Design

3

This chapter describes the design of the *Industry-Grade Self-Sovereign Identity Framework* (IG-SSIF).

In its essence, the main enablers of self-sovereign identity are *attestations*: the verifiable claims capable of facilitating one's digital identity. All proposed solutions focus on public-key encryption. The selection of asymmetric encryption as opposed to symmetric encryption lays in the properties that stem from asymmetric encryption. The public and private key pair enable the possibility to encrypt a message for a certain public key, for which it is then certain that only the entity possessing the corresponding private key, has the ability to decrypt said message. Vice verse, encrypting a message with a private key, ensures that only the corresponding public key can be used for decryption. This first property enables privacy, as only the entity to which the public key belongs, can now read the contents of the message. The second property enables authenticity, as anyone can verify, using the corresponding public key, that a message was signed by a certain entity to which the private key belonging to the public key is known. This verifiability through public-keys allows for a relatively trivial implementation of attestations.

More specifically, the properties of public key encryption can prove to create a rather trivial creation of attestations: one can simply hash a specific piece of information and encrypt it using his private key. This process is referred to as creating a digital signature. Next, anyone possessing the corresponding public key can verify this signature in case he knows the corresponding plaintext value.

Continue with information already written in article

3.1 Hybrid-Revocation Model

A relatively unresolved aspect of Self-Sovereign Identity, is the ability to revoke previously signed claims. Whilst not necessarily being an issue solely present in SSI, distributed revocation is a rather unsolved issue. With distributed revocation, we speak about the notion of revoking signatures in a distributed fashion. Moreover, we append the additional requirements of non-interactivity and, as a consequence, offline usable revocation. In other words, revocation should not be dependent on (centralised) authorities, as this can have additional consequences on confidentiality and availability. As described by [**?**], the usage of authorities with revocation proofs, can lead to collusion. Therefore, relying on authorities for revocation can lead to the deterioration of privacy. More drastically, introducing authorities in revocation can lead to censorship, as these specialised nodes have the ability to either hide revoked signatures or to maliciously state signatures as being revoked. Hence, in order to address the additional raised issues, we present a truly distributed revocation mechanism.

Trivial Approaches

Revocation in general can be solved quite trivially. The first approach relies on the introduction of centralised authorities, the second approach requires the usage of distributed ledges, whilst the third relies on interactivity. These approaches can all utilise existing revocation mechanisms, designed for more closed identity ecosystems. For instance, the usage of backward unlinkable revocation described by [53]; the usage of revocable group signatures describe by [**?**]; or the usage of accumulators as described by [9**?**].

Authorities

A rather trivial approach is to construct a central storage location in which anyone can store their revoked signatures. This has the drawback of introducing a central authority, which can be said to defeat the purpose of SSI. A central "banlist" authority would be a single point of failure and has the ability to be misused. Apart from availability issues, a single authority introduces a steep inequality across the network, as this client would have the ability to arbitrarily withhold revocations or may falsely introduce new ones. This effect may be counteracted by introducing several revocation nodes, e.g. per Sovrin's design. However, this still leads to the requirement of interactivity, as communication with revocation nodes is still required for validation. Hence, we deem this trivial solution not sufficient for a truly distributed SSI system.

Distributed Ledgers

The usage of distributed storage solutions may appear to be quite suitable. The properties introduced by the usage of e.g. blockchain technology, can prove to build a resilient revocation mechanism. For instance, [26] describe a certificate revocation mechanism, tailored to Cooperative Intelligent Transportation Systems, utilising Blockchain technology. However, the introduction of distributed ledger technology, often imposes the issue of consensus. Requiring consensus algorithms such as Proof of Work or Proof of Stake, where the former introduces unnecessary power consumption, raising the entry barrier for IoT and portable devices. Apart from this drawback, offline validation of past blockchain transactions often require the storage of the entire chain. Where the most prominent blockchains, Bitcoin and Ethereum, require more than 300GB[1] and more than 200GB[2] for regular and 4TB[3] for archive nodes. Hence, offline validation would become quite infeasible for regular devices. Furthermore, requiring the communication with fully synchronised blockchain nodes, would replace transform the problem of interactivity within the SSI ecosystem, to one within the blockhain ecosystem, hence simply moving the problem instead of solving it. This makes the use of distribute ledgers not feasible for the imposed requirements.

Interactivity

The most trivial of solution may be to simply validate a credential by querying the authority of a credential. However, the imposes several restrictions on the validation process. Firstly, this requires the signee of the credential to be online. Availability in distributed systems is never a guarantee, hence, this introduces a weakness in the revocation mechanism. Secondly, interactivity with the signee removes any offline usability. As now, a connection to both the presenter and the signee must be made or the presenter must simultaneously make a connection

[1] For Bitcoin blockchain size, see: `https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/`

[2] For Ethereum blockchain size, see: `https://blockchair.com/ethereum/charts/blockchain-size`

[3] For Ethereum archive blockchain size, see: `https://etherscan.io/chartsync/chainarchive`

to the signee in order to generate a non-revocation proof to present to the verifier. This make this approach not suitable.

The trivial solution all add a degree of interactivity or impose too strict of processing requirement to clients. Hence, the trivial solutions introduce requirements directly contradicting the properties sought after in the revocation mechanism. Hence, the aforementioned solutions are not suitable to solve the issue of revocation.

Remove?

remove?

Current approaches require a large degree of interactivity between the signee and verifier. In existing distributed approaches, a verifier suspecting a claim to be invalid must actively query the signer for validating whether the presented signature is not revoked. This has the drawbacks of requiring both parties (i.e., the verifier and the signee) to be online and requires a high throughput of transaction, as otherwise this check introduces large latency in the verification process. This process has been visualised in Figure 3.1, in which it can be seen that a claim is verified with the signee. This design is prone to variations, e.g. requesting a list of all revoked signatures. It can be noted that in case verification is required for each presented claim, signatures would intrinsically longer be required, as we can now simply verify with the signee whether the claim is valid.

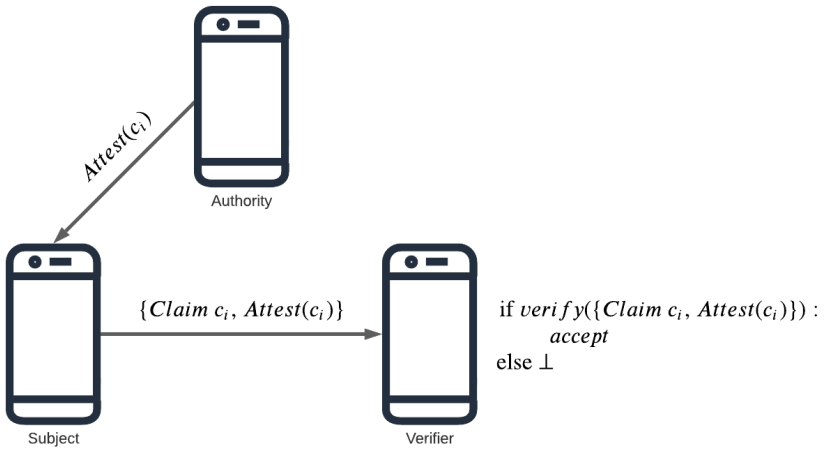


Figure 3.1: Revocation requiring interactivity

3.2 Design

In order to address the previously identified weak-points and shortcomings, we introduce a hybrid solution. This model aims to require no interactivity between a verifying party and a signing party during verification and allows for offline validation. The schematic design is visible in Figure 3.2. The scheme builds upon our previously defined notion of Trusted Entities: each client aims to accept signatures signed by a trusted entity, hence, each client trusts any revocation made by said

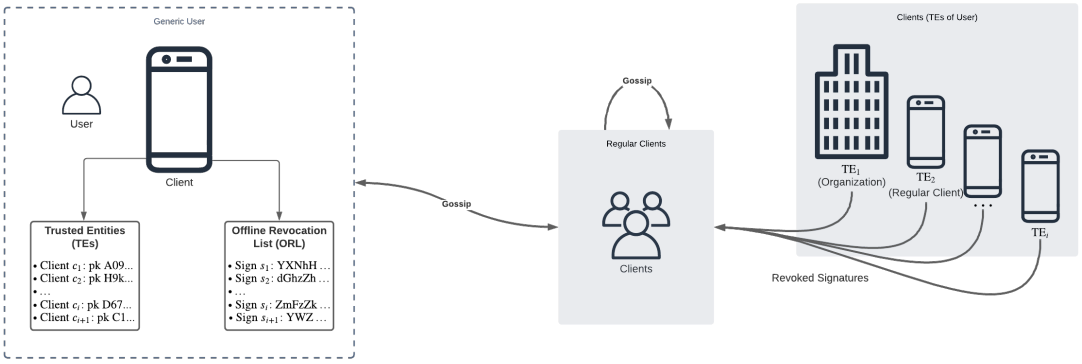


Figure 3.2: Hybrid-Revocation Model (HRM)

trusted entity. The HRM design uses a so-called Offline Revocation List (ORL), which comprises entries of revoked signatures from TEs. The ORLs are stored distributed across all clients and, hence, only contain revoked signatures from client which they trust. The ORL requires periodical syncing in order to stay up-to-date.

Synchronisation

Synchronisation in the system is dependent on the entire community of peers. Whilst consensus on revoked signatures is reached on peer-level, propagation is dependent on the entirety of peers. I.e., revocations are sent across the network in a peer-to-peer fashion. More specifically, peers are to actively propagate the latest revocations to other peers by means of gossip. Gossip protocols are modelled after epidemic spreads. Similarly to how gossip can spread throughout an office building, epidemics spread viruses across hosts. Translated to distributed systems, clients attempt to spread the latest information to as much other clients as possible. The effects of this, is that information ripples through the entire network. As with epidemics and gossip, this ripple takes time to reach all peers. This time we refer to as the *propagation time*. Propagation time is dependent on multiple factors, both digital and physical.

The affecting factors of the propagation time can be split up into two factors: (1) the protocol characteristics (2) network properties.

Protocol Properties

For protocol delays, the propagation time is dependent on the parameters imposed on the protocol. The parameters related to peer-contacting directly impact the frequency of the gossip. These are:

1. **Gossip-interval** (t_g): the time interval on which peers are gossiped to.
2. **Gossip amount** (n_g): the number of peers which are gossiped to on a time interval.
3. **Peer selection** ($\mathcal{F}_g(\mathcal{X})$): the function used to determine which peers are gossiped to.

The reasoning that the throughput of gossip can be limited are due to client restrictions. A client can impose certain restrictions regarding the frequency of gossiping to peers. This can, for instance, be due to hardware restrictions or energy consumption limitations. The gossip-interval, amount, and peer selection process, directly influence the number of peers gossiped to clients per time interval, thus, directly impacting the propagation time. The delay presented by these parameters can be summarised to the following formula:

Let $P = \{p_0, \ldots, p_{n-1}\}$ be the set of peers of size n_p in the network and let $g = t_g \cdot \frac{n_p}{n_g}$ be the minimal number of interval iterations required to gossip to all peers. The peer selection function $\mathcal{F}_g(X)$ may result in overlapping subsets. I.e., let $f_i = F_g(P)$ be the subset of peers generated at iteration i and let $f_{i+j} = F_g(P)$ be the subset generated at iteration $i + j$, then it does not necessarily hold that $f_i \cap f_{i+j} = \emptyset$. Hence, let $P_f = p_0, ..., p_{n-1}$ be the multiset of peers of size $m_p >= n_p$ selected throughout each iteration until convergence. I.e., the peer selection function $\mathcal{F}_g(X)$ selected at least $m_p >= n_p$ peers, leading to at least $t_g \cdot \frac{m_p}{n_g}$ iterations. The additional iterations can be modelled by: $h = t_g \cdot \frac{m_p - n_p}{n_g}$, where $h \geq g$ This leads to the propagation time for the protocol delays for a single client i attempting to gossip a single update to the entire visible network with size n as to be as summarised in Equation 3.1.

$$\begin{aligned} \mathcal{T}_{protocol,i} &= h + g \\ &= t_g \cdot \frac{n_p}{n_g} + t_g \cdot \frac{m_p - n_p}{n_g} \\ &= t_g \cdot \left(\frac{n_p}{n_g} + \frac{m_p - n_p}{n_g} \right) \\ &= t_g \cdot \frac{m_p}{n_g} \end{aligned} \tag{3.1}$$

As clients are not aware of their position in the network (relatively to others) or of the peers already contacted by other clients, there can only be set an upper bound on the expected runtime of the algorithm, as each peer attempts to gossip all information to all other peers. Hence, we can summarise the propagation delay to the formula presented in Equation 3.2, where $t_{g,i}, m_{p,i}, n_{g,i}$ are the gossip-interval, number of selected peers, and gossip amount for client i, respectively.

$$\begin{aligned} \mathcal{T}_{protocol} &\leq \sum_{i=0}^{n-1} \mathcal{T}_{protocol,i} \\ &\leq \sum_{i=0}^{n-1} \left(t_{g,i} \cdot \frac{m_{p,i}}{n_{g,i}} \right) \end{aligned} \tag{3.2}$$

Due to parameters being dependent on hardware and deployment restrictions, there does not exist an optimal setting for all deployments types. Depending on the expected frequency of updated data, different parameters may be suitable. Different configurations lead to different characteristics imposed on the system. Increasing the gossip-interval leads to, generally, more up-to-date peers as a client will gossip the latest information more frequently. Whilst increasing the amount of gossip will allow for more clients to receive information, whilst not necessarily

leading to more up-to-date clients. Where up-to-date refers to possessing the latest information. This is, of course, dependent on the frequency of new information. The peer selection function can influence the number of up-to-date and the number of updating clients both positively and negatively, as the peer selection function $\mathcal{F}$ allows for multiple modus operandi. E.g., the $\mathcal{F}$ can be a pseudo-random function (PRF), in which the peers are selected arbitrarily, giving each subset of clients of size n a near equal chance of being gossiped to on each interval $\mathcal{T}$. However, such an approach may lead to specific peers being selected multiple times, due to chance, at an interval. Hence, possibly negatively impacting the overall propagation time. A more sophisticated is also possible: e.g. a combination of a PRF with backtracking, in which a subset is dropped in case a member of the set has been contacted in the last m iterations. Such an approach can prove to increase the overall throughput of information, thus decreasing the propagation time.

These three parameters do not necessarily have to be static: clients can record the latest gossip sent to specific peers, hence, selectively gossiping on new information. This can be extended to decreasing the gossip-interval and amount depending on the frequency of new information. This dynamic behaviour allows for more efficient usage of resources and decreases the overhead of gossiping to peers which may already have received the latest information. However, this would increase memory usages and runtimes, as now such metadata on gossiped information must be recorded by the client.

Network Properties

Foremost, the propagation time is dependent on the amount of nodes in the system. Where a system with a single node converges in a constant time. I.e., the system converges in c time with a system of size $n = 1$ nodes. For any larger sizes ($n > 1$), several constraints on the propagation time are introduced. Firstly, the size of the information itself becomes a factor: as the throughput of data between nodes may not necessarily be equal, the time for propagation between nodes may differ. More specifically, the propagation of information in a (sub)graph with $n > 2$ with a gossiping node n_i and two uninformed directly linked nodes n_j and n_k, may result in node n_k becoming informed prior to node n_j or vice versa. Reasonings for this are the imperfections present in the network infrastructure and deployment environment differences. For instance, network congestion present in the link to a certain node can lead to queueing delays and packet loss. Lower available bandwidth may also conceive such discrepancies. Differences in deployment environments (i.e., different hardware), may also lead to different convergence timings. For instance, a faster CPU and more available memory may lead to faster processing of gossip and, thus, a faster propagation time compared to weaker hardware. Hence, each node p_i introduces a relatively unique processing delay c_i. This processing delay will be constant for a single update iteration, i.e., this delay is initiated after another client gossiped new information to this client. However, this delay may differ on subsequent gossip, as this constant is influenced by factors such as the current load of the node and the size of the gossiped data. Therefore, we assume that this delay is of arbitrarily length, which only becomes apparent after a node has gossiped new information to this node. Hence, no prior analysis can be made with regard to this delay, we simply acknowledge its existence and, thus, base the network propagation delay on the minimum link with a gossiping node.

Next, we generalise the delays imposed by the network. Let $\delta_{i,j}$ be the propagation delay from node i to node j and let function $\Delta(p_j)$ be the smallest propagation delay for node p_j to be

gossiped to. I.e., $\forall(p_i, p_k) \in \{p_0, ..., p_{n-1}\}$ it holds that $\delta_{i,j} < \delta_{k,j}$. Let $\mathcal{D} = \{\delta(p_0), \ldots, \delta(p_{n-1}\}$ be the set containing all these smallest propagation delays for each node. Finally, let $\mathcal{C} = \{c_0, \ldots, c_{n-1}$ be the the set of delays imposed by processing times on the clients on invocation $\Delta(p_j)$. This leads to the network delay for a single client i updating the entirety of the to him visible networks with size n as summarised in Equation 3.3

$$\mathcal{T}_{network,i} = \sum_{j=0}^{n-1} (\delta_{i,j} + c_j) \tag{3.3}$$

The the total propagation time in a system with a set of $P = \{p_0, \ldots, p_{n-1}\}$ nodes of size n can be modelled as visible in Equation 3.4.

$$\mathcal{T}_{network} = \sum_{i=0}^{n-1} (\Delta(p_i) + c_i) \tag{3.4}$$

Finally, we can model the entire propagation time of a single node and the entire graph. The propagation time for a single node can be seen in Equation 3.5

$$\begin{aligned} \mathcal{T}_{tot,i} &= \mathcal{T}_{protocol,i} + \mathcal{T}_{network,i} \\ &= \left(t_g \cdot \frac{m_p}{n_g}\right) + \left(\sum_{j=0}^{n-1} (\delta_{i,j} + c_j)\right) \end{aligned} \tag{3.5}$$

The propagation time for a network of size n, is visible in Equation 3.6

$$\begin{aligned} \mathcal{T}_{tot} &= \mathcal{T}_{protocol} + \mathcal{T}_{network} \\ &\leq \left(\sum_{i=0}^{n-1} \left(t_{g,i} \cdot \frac{m_{p,i}}{n_{g,i}}\right)\right) + \left(\sum_{i=0}^{n-1} \Delta(p_i) + c_i\right) \\ &\leq \sum_{i=0}^{n-1} \left(t_{g,i} \cdot \frac{m_{p,i}}{n_{g,i}} + \Delta(p_i) + c_i\right) \end{aligned} \tag{3.6}$$

Bibliography

[1] Decentralized Identifiers (DIDs) v1.0.

[2] Sovrin ™ : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust A White Paper from the Sovrin Foundation. Technical report, 2018.

[3] Christopher Allen. The Path to Self-Sovereign Identity, 5 2016.

[4] Aristotle. *Metaphysics*. 1925. Original work published 350 B.C.E.

[5] D.S. Baars. Towards self-sovereign identity using blockchain technology. 2016.

[6] Rafael Belchior, Benedikt Putz, Guenther Pernul, Miguel Correia, André Vasconcelos, and Sérgio Guerreiro. SSIBAC: Self-Sovereign Identity Based Access Control. Technical report, 2020.

[7] Elisa Bertino. Establishing and protecting digital identity in federation systems. *Article in Journal of Computer Security*, 2006.

[8] Pelle Braendgaard. What is a uPort identity?, 2 2017.

[9] Jan Camenisch and Anna Lysyanskaya. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. Technical report, 2002.

[10] Kim Cameron. The laws of identity. *Microsoft Corp*, 5:8–11, 2005.

[11] Kim Cameron. Let's find a more accurate term than 'Self-Sovereign Identity', 11 2018.

[12] L Jean Camp. Digital Identity. 2004.

[13] European Comission. Regulation of the european parliament and of the council amending regulation (eu) no 910/2014 as regards establishing a framework for a european digital identity, 6 2021.

[14] PCI Security Standards Council. Payment Card Industry Data Security Standard (PCI DSS), 2004.

[15] Uwe Der, Stefan Jähnichen, and Jan Sürmeli. Self-sovereign identity - opportunities and challenges for the digital revolution. *arXiv preprint arXiv:1712.01767*, 2017.

[16] The Oxford Dictionary. Govern.

[17] Md Sadek Ferdous, Farida Chowdhury, and Madini O Alassafi. In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, 7:103059–103079, 2019.

[18] IANA. IANA — Number Resources.

[19] IBM. Consumer Attitudes Towards Data Privacy, 2019.

[20] IBM. Identification and authentication - IBM Documentation, 6 2021.

[21] ICANN. Registering Domain Names - ICANN, 6 2017.

[22] ISO. ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT. Technical report, International Organization for Standardization, 2013.

[23] ISO. IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. Standard, International Organization for Standardization, May 2019.

[24] Audun Jøsang and Simon Pope. User Centric Identity Management. *AusCERT Conference 2005*, 2005.

[25] Dmitry Khovratovich and Jason Law. Sovrin: digital identities in the blockchain era. Technical report, 2017.

[26] Noureddine Lasla, Mohamed Younis, Wassim Znaidi, and Dhafer Ben Arbia. Efficient Distributed Admission and Revocation Using Blockchain for Cooperative ITS. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, volume 2018-January, pages 1–5. Institute of Electrical and Electronics Engineers Inc., 3 2018.

[27] LastPass. THE 3RD ANNUAL GLOBAL PASSWORD SECURITY REPORT. Technical report, LastPass, 2019.

[28] Devon Loffreto. What is "Sovereign Source Authority"?, 2 2012.

[29] Devon Loffreto. Self-Sovereign Identity, 2 2016.

[30] Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton, and Michael Sena. UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY. Technical report.

[31] Mike Moore. What is Industry 4.0? Everything you need to know, 11 2019.

[32] Dave Morin. Announcing Facebook Connect, 5 2008.

[33] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. A survey on essential components of a self-sovereign identity, 11 2018.

[34] Harold Noonan and Ben Curtis. Identity. In Edward N Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, summer 2018 edition, 2018.

[35] Eric T Olson. Personal Identity. In Edward N Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2021 edition, 2021.

[36] Asem Othman and John Callahan. The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity. In *Proceedings of the International Joint Conference on Neural Networks*, volume 2018-July. Institute of Electrical and Electronics Engineers Inc., 10 2018.

[37] Daniel Philpott. Sovereignty. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Fall 2020 edition, 2020.

[38] PressPass. Microsoft Passport: Streamlining Commerce and Communication on the Web, 10 1999.

[39] Alex Preukschat and Drummond Reed. *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Manning Publications Co. LLC, 2021.

[40] David Recordon and Drummond Reed. Openid 2.0: A platform for user-centric identity management. In *Proceedings of the Second ACM Workshop on Digital Identity Management*, DIM '06, page 11–16, New York, NY, USA, 2006. Association for Computing Machinery.

[41] Drummond Reed, Jason Law, and Daniel Hardman. The Technical Foundations of Sovrin A White Paper from the Sovrin Foundation. Technical report, 2016.

[42] Matthew Rosenberg. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, 2018.

[43] Timothy Ruff. 7 Myths of Self-Sovereign Identity, 10 2018.

[44] Philip Sheldrake. [On the misattribution in Allen (2016)], 4 2016.

[45] Sovrin. Sovrin SSI & IoT Working Group Charter, 12 2019.

[46] Sovrin Foundation. What is self-sovereign Identity?, 12 2018.

[47] Tim Speelman. *Self-Sovereign Identity: Proving Power over Legal Entities*. PhD thesis, TU Delft, 2020.

[48] Quinten Stokkink, Dick Epema, and Johan Pouwelse. A Truly Self-Sovereign Identity System. *arXiv preprint arXiv:2007.00415*, 2020.

[49] Quinten Stokkink and Johan Pouwelse. Deployment of a blockchain-based self-sovereign identity. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1336–1342, 2018.

[50] Thales. 2020 Thales Data Threat Report. Technical report, Thales, 2020.

[51] The European Parliament and Council. Regulation (EU) 2016/679 of the european parliament and of the council, 2016.

[52] Andrew Tobin and Drummond Reed. The inevitable rise of self-sovereign identity. *The Sovrin Foundation*, 29(2016), 2016.

[53] Eric R Verheul. Practical backward unlinkable revocation in FIDO, German e-ID, Idemix and U-Prove. Technical report, 2016.

[54] Verizon. 2020 Data Breach Investigations Report. Technical report, Verizon, 2020.

[55] World Bank Group. ID4D Data: Global Identification Challenge by the Numbers, 2021.

[56] Tong Zhou, Xiaofeng Li, and He Zhao. EverSSDI: Blockchain-based framework for verification, authorisation and recovery of self-sovereign identity using smart contracts. *International Journal of Computer Applications in Technology*, 60(3):281–295, 2019.