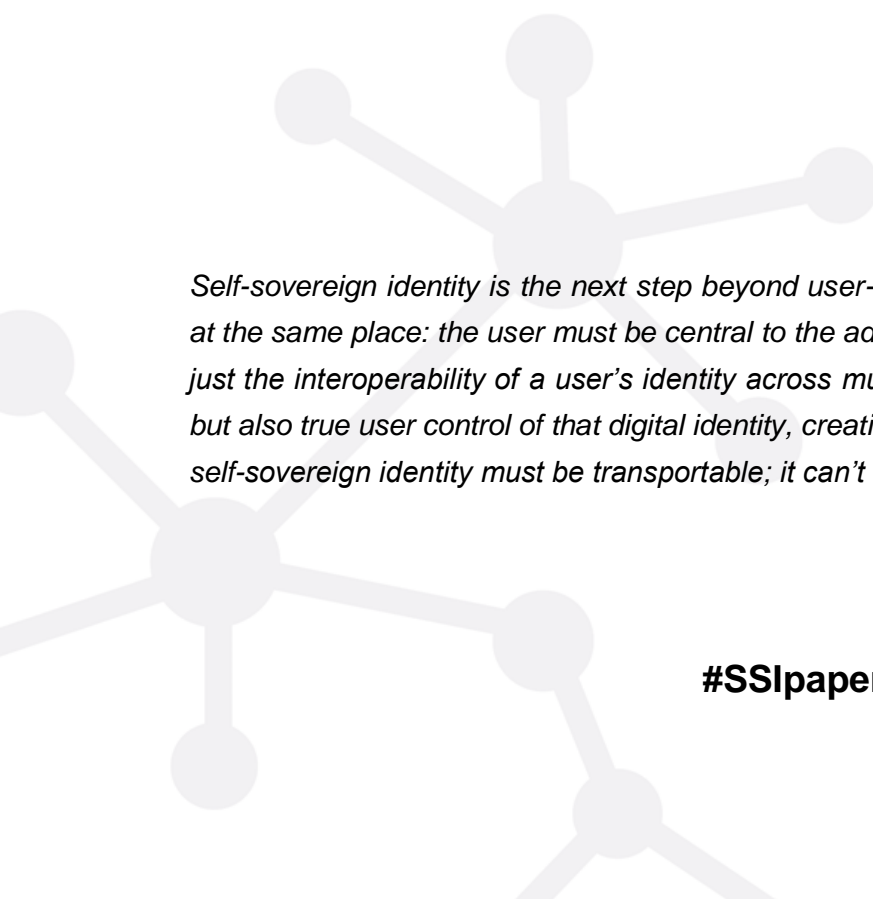


Self-sovereign Identity

A position paper on blockchain enabled identity and the road ahead

23. October 2018

Published by the Identity Working Group of the German Blockchain Association



Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale.

-Christopher Allen-

#SSIpaper

Authors

Kai Wagner	Jolocom
Balázs Némethi	Taqanu
Elizabeth Renieris	
Philipp Lang	esatus
Elliott Brunet	
Eric Holst	Klgroup

Reviewers (in alphabetical order)

Alexander Mühle	Hasso Plattner Institute
André Kudra	esatus
Clare Nelson	Sedicii
Daniel Buchner	
David Chadwick	University of Kent
Fabian Vogelsteller	Ethereum
Florian Glatz	Blockchain Bundesverband
Joachim Lohkamp	Jolocom
Johan Pouwelse	TU Delft
Jörg Rückriemen	Bundesdruckerei
Kaliya Young, Identity Woman	Merritt College
Knut Karnapp	PHP Law
Manu Sporny	Digital Bazaar / Veres One
Markus Sabadello	Danube Tech
Matthias Möller	BotLabs
Oliver Mahnke	Bundesdruckerei
Oliver Nägele	Blockchain HELIX
Peter Czaban	Web3 Foundation
Rouven Heck	ConsenSys / uPort
Silvan Jongerius	TechGDPR

Disclaimer:

Neither this Position Paper nor any information contained herein is offered, nor should be construed, as legal advice. Communication of information by or through this Position Paper and any related materials, and your receipt or use of such information or materials is not intended to create an attorney-client relationship with any organization or individual contributors to this Position Paper or their respective employers. You should not act or rely upon information contained in this Position Paper without specifically seeking professional legal advice.

Table of Contents

Abstract	4
1. Introduction	5
2. Digital Identity	7
The central role of identity	7
A universal identity layer	8
Self-sovereign Identity	9
3. Core capabilities	15
4. Building Blocks of Self-sovereign Identity	19
5. Outlook	21
Call to action	24
Appendix	25
Appendix I – Glossary	25
Appendix II – Regulation	28
Appendix III – Standardization	35
Appendix IV – Security	38
Appendix V – Open Questions	45
Appendix VI – Exemplary use cases	49
Appendix VII – Pilot Projects and Proof of Concepts	53

Abstract

The identity working group of the German Blockchain Association presents this position paper on the emerging paradigm of self-sovereign identity. As a novel framework for the creation, management and interaction of digital identities, self-sovereign identity represents a major leap for both digital and analog interactions. We are convinced that blockchain and other decentral technologies represent a fundamental infrastructural innovation, that has the potential to enable a fair and inclusive digital economy. As representatives of the blockchain industry, we see self-sovereign identity as a fundamental building block for the success of blockchain based innovation.

Identity is at the core of each and every interaction. While the required level of trust between identities can vary from one interaction to another, the necessity to exchange it in a secure and privacy preserving manner is universal.

In the self-sovereign identity paradigm, individuals and entities are enabled to create and manage their identifiers in a decentralized fashion, without relying on a third-party identity provider. Unlike existing identity solutions that are structured from the perspective of the organization that provided an identifier, self-sovereign identities are structurally set out to work from the perspective of the individual or entity that is the subject of a given identifier.

This document is primarily directed at an audience from a political and business background interested in blockchain enabled identity (mainly in Germany and Europe). Our intention behind this position paper is to provide a clear description of self-sovereign identity. By explaining the concept, the problems that motivate it, its potential use cases and questions evolving around implementation (including around Standards, Architecture, Security, Privacy, and Regulation) we intend to provide a document that can guide further development and discussion in this field. The strength of this document does not only lie in the expertise reflected by the authors and reviewers of this report, but even more so in the fact that all involved parties coming from different institutions and companies (that might even be regarded as competitors in this field) show agreement on the direction of self-sovereign identity (regarding standardization, interoperability, regulation, privacy, and security aspects).

This position paper is thus a report of the status quo on self-sovereign identity, as much as it is providing a shared vision and entry points for the road ahead.

We invite you to discuss this position paper using the following hashtag:

#SSIpaper

1. Introduction

Digital Identity is a field that matters to a seemingly infinite number of stakeholders from diverse backgrounds. Confronted with this extensive scope, we decided to structure this position paper around two major objectives:

First, to provide our readers with a structured overview of the identity field from the perspective of self-sovereign identity, and second, to motivate stakeholders in the identity community to embrace the idea of a universal identity layer and join us for the road ahead.

As a result of our collaboration in the identity working group in the German Blockchain Association, we propose the SSI model as a way to enable an identity ecosystem that is capable of solving many inefficiencies in existing identity solutions and addressing novel demands on identity in the emerging decentralised web. Whilst SSI systems can be constructed without the need for any blockchain system, blockchain systems can add significant value to SSI systems, as this paper will show. Ultimately, the universal identity layer that we describe is required to enable blockchain based decentralised systems and business models to reach their full potential.

Our aim is to present an overview that is independent from any one company's product offering. We instead present an industry-wide consensus on the model of SSI that is geared towards the establishment of a truly interoperable and modular identity system that utilizes open standards. The paper can thus be understood as the baseline of agreement between all represented businesses from the identity space. The paper is an attempt to describe the universal identity layer from a high-level perspective with a focus on shared positions and agreement instead of going into technical implementation details that certainly matter but need to be discussed further on in the debate we intend to initiate with this position paper.

We use the terminology of SSI, as an identity model that allows an individual or entity to have sole control of their digital identity expressed through the use of one or more decentralised identifiers or “DIDs.”¹ Mindful of the associations that arise from the use of the term “self-sovereign,” we want to clarify that self-sovereign refers to this ability to control the use of one’s identifiers that reveal something about their identity. It does not imply that the power of sovereign actors such as the state or public authorities is weakened by the SSI model. Quite the opposite—SSI allows the state to engage directly with citizens and organizations without depending on a third party.

¹ See Appendix I for an extensive glossary on terminology

The act of credential and certificate issuance that has been a prime area of state sovereignty in the analog world is now enabled in a digital environment for the first time with the SSI model. This identity model thus reduces the dependency of the state and its citizens on intermediaries and enables more direct interactions. In this way, the self-sovereign approach has great potential to enhance citizen or constituent engagement and even renew democratic institutions.

We want to encourage actors from politics, business, and civil society to join us for this paradigm shift in identity management and control over personal data, which has the potential to substantially change our society. We hope our position paper can be a starting point for a global debate on the need for and the possibility of building a universal digital identity layer. We are aware that our authors and reviewers do not represent this inclusive claim yet and we want this to change. We thus invite everyone to join the conversation and broaden the debate, especially in those regions and environments that we are not yet representing. We look forward to continuing this conversation and collaborative development with you.

The paper starts with a look at the status quo of digital identity, which motivates the paradigm shift. We present the concept and unique capabilities of SSI, followed by a presentation of the technical architecture in the form of a vendor agnostic model of building blocks, followed by an outlook on the adoption and scalability potential of SSI. We close the main part of this position paper with a set of clear calls to action targeted at the different identity stakeholders we intend to reach. In the appendices, we provide a glossary with the relevant terminology, as well as a rich collection of the shared expertise in our working group providing a closer assessment on the implications in the regulatory, security and standardization fields. For those interested in the practical implications of SSI, we also provide an appendix with exemplary use cases, a list of Proof of Concepts and a Pilot Project proposal that is aimed at the implementation of an interoperable identity ecosystem between a diverse set of stakeholders from the public and private sector.

2. Digital Identity

The central role of identity

Identity is at the core of all transactions and interactions between natural persons (e.g. citizens and consumers), legal entities (e.g. businesses, organizations, and governments), and other things (e.g. smart devices and artificial intelligences). People have a rich tapestry of identities made up of their own personal identities (e.g., father, husband), their social identities (e.g. employee, soccer player) and their state-issued identities (e.g. passport, driving license). Typically, these identities are not static but dynamic, evolving over a person's lifetime and across contexts. State-issued identities however are often more stable and are about the ability to uniquely identify an individual, which makes it the foundation for our interactions with the outside world. Government issued documents are manifestations of such state-issued identities, which in turn facilitate our interactions with other identities.

The substrate of identity is, however, changing profoundly with the technological evolution in social networks, artificial intelligence, autonomous vehicles, and, more recently, decentralized governance and data structures. Online as well as offline, we have the ability to create and use multiple personas, each validated in a different way, used in a flexible setting and requiring different levels of security, privacy, and verification. Beyond that, the emergence of a new interaction layer based on IoT (Internet of Things) amplifies the question of hardware security and device identity, which also need to be addressed. We will delve more into this question in the next section.

“Digital” identities in the form of “online accounts were the way to access digital services in the 1990s. One could create multiple personas and build a protective layer of privacy around oneself, as long as the state-issued identity was not disclosed or uncovered. This user proxy experience dependent on multiple unique sets of logins and passwords tied to each individual online account proved complicated and led to a push for simplicity of user experience. In the 2010s, scalable services took over the internet with “single sign-on” (SSO) or federated identities (allowing users to sign into a website using an existing account from providers like Facebook, Google or Twitter). This approach lightens the usability burden on websites and improves the conversion of visitors into active users. However, these solutions create single points of failure and correlate the user's activity over time and across contexts, requiring the user to trade their privacy for convenience.

Centralized ID Providers

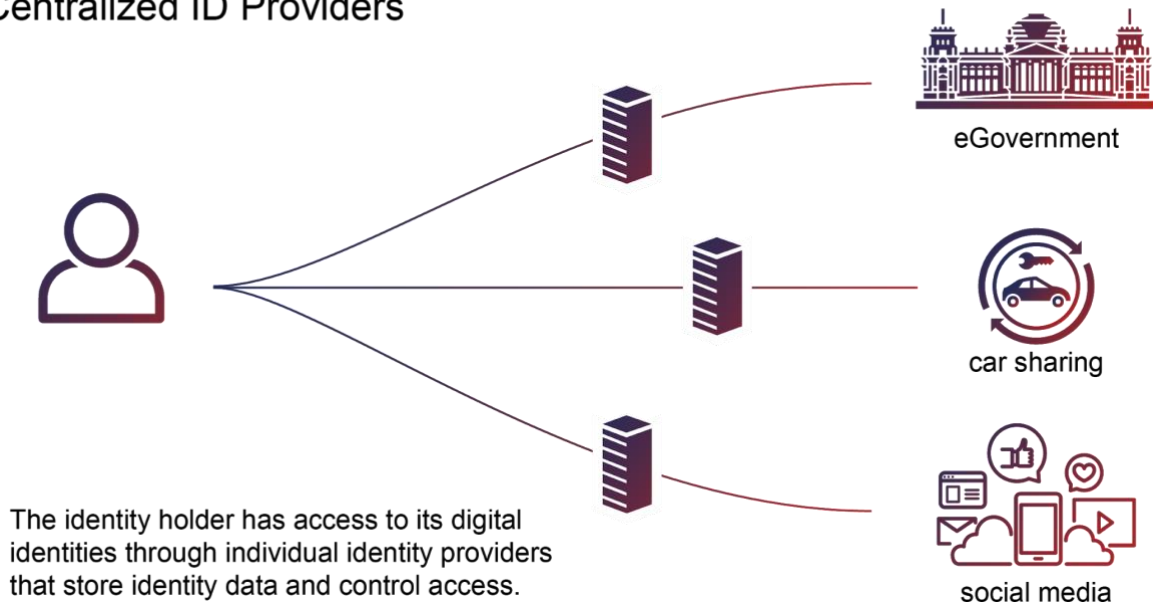


fig. 1 – Centralized Identity Providers hold a position as intermediaries in digital interaction.

Although the user arguably gained in security and usability, it ceded control to large centralized corporations with a complete view of the digital footprint of their users, compromising privacy and leading to unforeseeable uses of our data in violation of fundamental principles of data protection. It further created centralization around these IDPs or SSO providers, leading to an over-reliance on very few services and large honey pots of data that they control. This created a pain point with regard to business issues, liability, privacy and security. Also, these business-driven identity providers can deny users access to their services (and those that they mediate or gate keep) at any time.

A universal identity layer

Digital identity has traditionally been tailored for the requirements of the issuing organization, which often leaves the individual without control over his or her identifiers and other identity-related data. The result is that organizations, governments, and other entities maintain large silos of data, storing the digital identities of their users. This has led to a number of challenges that have not been solved sufficiently since the invention of the internet.

The introduction of a well-designed, universal identity layer could trigger unprecedented scales of efficiency and trust in the digital space. The current data silo-based ecosystems could be replaced by a new paradigm where self-sovereign individuals and entities have the ability to establish web-of-trust networks outside of the current silos through the entire digital space.

Until now, with great levels of efficiency came great levels of centralized control too. Therefore, the universal layer for identity has to decentralize control, by empowering myriad self-sovereign individuals and entities to have full control over how they utilize their data and manage their identity.

Ownership of systems that underpin the digital privacy of the future must not be controlled or owned by any single entity. Moreover, any viable solution also has to offer auditable trust in the underlying technology by utilizing and building on open source code and standards.

Such a decentralized approach is capable of preserving privacy and data protection to the highest standards. It introduces data management principles to move the world towards an interoperable ecosystem of connected entities. With this universal layer, services that require customer or constituent data can rely on information structured in the form of Verifiable Credentials, a data format that can be attested to by a trusted third-party. This could enable new, direct, and enhanced relationships with customers or constituents based on mutual trust.

This new mechanism for trust could drive efficiency as the existing, independent data silo providers will be able to use and rely on this trust network too. With reliable data shared directly by the subject of that data, existing barriers in the process of establishing and maintaining trust in the digital space are significantly reduced. This new trust infrastructure could also enable direct interactions via verifiable or provable interactions of all kinds (in the form of Verifiable Credentials). The possibility of this paradigm shift brings us to the concept and tooling of SSI, a codified mechanism for enabling these enhanced interactions.

Self-sovereign Identity

SSI starts with the notion that individuals and organisations have real world or offline, context-dependent identities that no one else can take away. Sometimes, these are expressed in the form of identity-related documents issued by third parties, which can be revoked though the artefact may still be retained (e.g. you can carry an expired credit card or driving licence in your wallet). Just as in the real world, self-sovereignty doesn't mean that individuals or organisations can control all aspects of their identity that are provided by external parties, such as trusted credentials that are issued by legitimate actors such as for example the state (e.g. the state can still revoke your driving licence as an individual or your liquor licence as a business). Rather, self-sovereignty implies that an individual or organization who has one or more identifiers or DIDs, can present certain Claims or Credentials relating to those DIDs without having to go through an intermediary.

At the outset, it is important to clarify some terminology and actors in the SSI ecosystem. There are various roles that exist at two distinct levels — (1) Credential-based roles where an individual or entity controls a given Credential and its uses, and (2) Identifier or DID-based roles where an individual or entity owns and/or controls certain DIDs and their uses.

There are at least four Credential-based roles we can identify as follows:

- ❓ **Subject** — the individual, entity, or thing that a given Credential is about or relates to
- ❓ **Holder** — the individual or entity in control of the digital wallet or agent that stores and controls the use of a given Credential; note, the Holder may or may not be the Subject (e.g. a child may be the Subject of a digital passport, but the child's parent may be the Holder of that passport)
- ❓ **Issuer** — the individual or entity who issues a given Credential
- ❓ **Verifier** — the individual or entity who verifies or relies upon a given Credential

There are also two DID-based roles that we can identify:

- ❓ **DID Subject** — the individual, entity, or thing that a given DID identifies
- ❓ **DID Owner (or Identity Owner)** — the individual or entity who holds and controls the private keys associated with that DID

While the Identity Owner and DID Subject will often be the same, that is not always the case because (just as with Credentials managed by a Holder on behalf of a Subject) there are situations where an DID Subject may not be able or willing to manage their own keys. In such situations, care must be taken to design legal constructs around guardianship and delegation to protect the DID Subject and preserve their rights.

Self-sovereign Identity

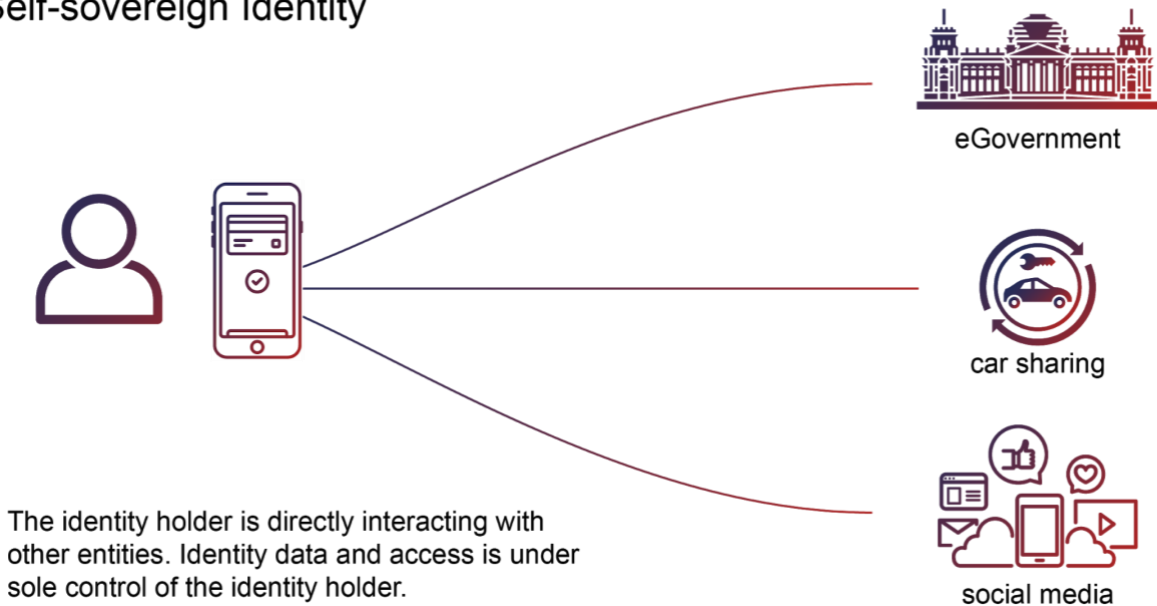


Fig. 2 – The basic interaction model of SSI with the Identity Holder as the sole controller of their identity.

Putting these roles in context, let's take the example of a Claim that an individual is over the age of 18. In the self-sovereign model, such a Claim can either be self-attested (a claim the individual makes about herself) or attested to by another entity (such as the state or a trust services provider) that can issue an attested claim in the form of a Credential to the individual who now becomes the Holder of that Credential. In the latter case, the Holder (who is in full control over the previously described Claims) can choose to present a self-attested version of the Claim or a Verifiable Credential that has been issued and cryptographically signed by another entity. If the interaction requires a degree of trust in the presented claim, the Verifier can ask for a Credential from a trusted Issuer that satisfies the Verifier's requirements for that specific interaction. It is important to say that the exchange of claims happens in a peer-to-peer manner and the Holder is always one of the peers to the interaction. No information is exchanged outside the Holder's control, a principle that is ensured by storing the Claims under the Holder's control and requiring cryptographic signatures for each interaction, based on keys only the Holder can access and control.

Attestation and Issuance of Credentials

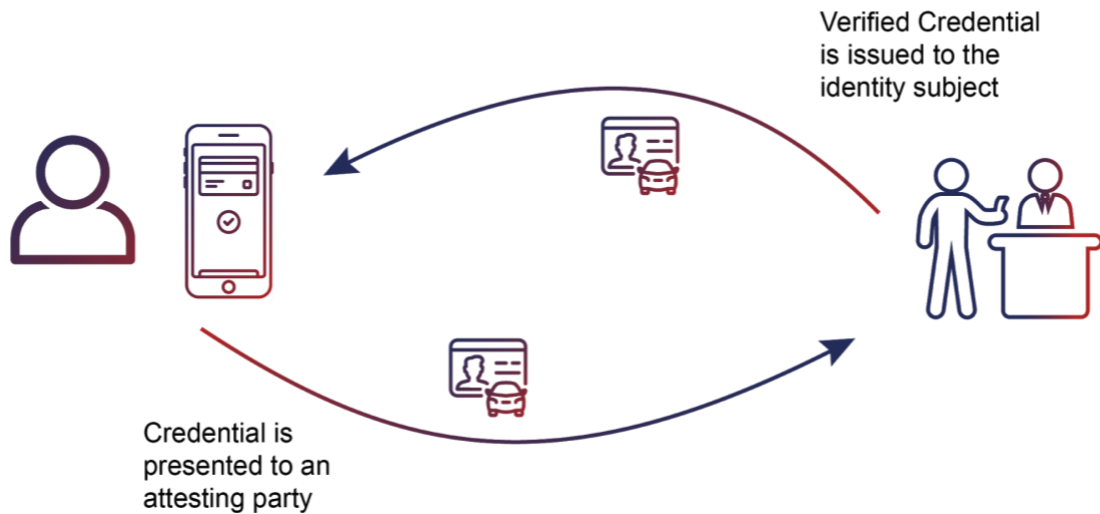


Fig. 3 – Exemplary interaction flow for the issuance and attestation of a credential.

With this model of SSI, it is possible to express virtually any kind of Claim about an individual or entity, and given the adequate verification processes and legal acceptance, these Claims can represent anything about the individual or entity who is the subject of that Credential. This adds a level of flexibility and modularity that will encourage the development of new types of identity claims and will allow a Holder to selectively reveal only the relevant data necessary for a given transaction or interaction. In fact, most interactions only require the involved parties to trust the permissions of each party (e.g. to access a building), which doesn't require the unique identification of a party to any degree. A key strength of the SSI model is its ability to support both conscious identification, as well as a pure access management and permissioning system in a privacy and data protection by design and default environment.

SSI is a powerful tool for privacy protection. In fact, it has a strong visionary alignment with the EU's General Data Protection Regulation (GDPR). SSI even has the potential to become the foundation for real world achievement of the GDPR's principles. One objective of the GDPR is to enhance individual data protection rights, just as SSI seeks to provide individuals with more control over their own personal data. A second objective of the Regulation is to enable the free movement of personal data across the European single market and stimulate economic growth, embodied in the right to data portability. SSI also promotes the free flow of data by creating a layer of trust and autonomy around identifiers and Credentials that can be portable by design.

Lastly, this new identity paradigm is the result of a series of attempts to balance the power structures underlying digital identity and personal data by bringing the individual

to the centre of her data ecosystem and giving her control over the uses of her personal data.

For that reason, we need a series of guiding principles to make sure SSI doesn't go rogue. The SSI community often uses Christopher Allen's Ten Principles of SSI as a starting point, a list built on significant community work over 10 years at the Internet Identity Workshop and echoing Kim Cameron's Laws of Identity.²

Before explaining these principles, a word of caution. Identity is a central piece of society and requires the utmost care when dealing with it. How we define and use identity can tip the scale of democracy. It can empower or imprison us. As Christophe Allen put it:

“These principles attempt to ensure the user control that's at the heart of SSI. However, they also recognize that identity can be a double-edged sword — usable for both beneficial and maleficent purposes. Thus, an identity system must balance transparency, fairness, and support of the commons with protection for the individual. “

This list is by no means perfect and things have evolved significantly in the last decade, so we offer some annotations and enhancements (in the form of “Notes”) in addition to the explanations below.

1. **Existence.** *Users must have an independent existence.* Note: This sometimes presumes that everything must be documented to exist. We disavow that notion and respect that there is an inherent quality to existence and a right to remain unknown in certain contexts.
2. **Control.** *Users must control their identities.* Note: The focus is specifically on control and not ownership (e.g. you don't own your passport, the State does, but you want the right to control the use of it).³
3. **Access.** *Users must have access to their own data*
4. **Transparency.** *Systems and algorithms must be transparent.* Note: To this end, the foundation of all technology solutions to enable SSI must be open source.
5. **Persistence.** *Identities must be long-lived.* Note: This principle can be quite controversial when understood to apply to identifiers. We believe that the persistence principle does not and should not be interpreted to mean that

² <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>

³ For more on the dangers of an ownership model of data and digital identity, see <https://medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa>.

identifiers, including decentralised identifiers, should last forever or that they cannot be revoked or abandoned by an Identity Owner. The point is that the Identity Owner must be the one in control of the degree to which that DID is persistent or not.

6. **Portability.** *Information and services about identity must be transportable.*
7. **Interoperability.** *Identities should be as widely usable as possible.*
8. **Consent.** *Users must agree to the use of their identity.* Note: We argue that consent must be real and meaningful, such as the high standard for consent set out in Article 4 of the GDPR requiring a freely given, specific, informed and unambiguous statement or clear affirmative action signifying agreement to processing. While this level of consent is nearly impossible to achieve in today's big data ecosystem with its huge volumes of data, vast information asymmetries and uneven bargaining power between individuals and organizations, we are optimistic that the SSI model combined with advances in technology could help us achieve real, meaningful consent in the future.
9. **Minimization.** *Disclosure of claims must be minimized.*
10. **Protection.** *The rights of users must be protected.*

These principles reinforce the view that the individual is in control of their identity-related information, including their identifiers, Credentials, and other personal data. In that sense, they can be understood as a true sign of the quality and values that the decentralized identity community endeavours to enforce through SSI. Nevertheless, we must not confuse principle with dogma and should not restrain ourselves from questioning and continuing to refine them as necessary.

3. Core capabilities

By aiming to be a universally applicable model for digital identity, SSI can be hard to grasp. A description of its core capabilities is thus key to understanding its implications, especially when it comes down to the different actors and their roles in the SSI model.

As a prerequisite for the following capabilities, we assume that all individuals and entities as Identity Owners have one or more DIDs, with a unique set of private keys that control each DID. Things, such as in the IoT context, may also have DIDs associated with them (and be DID Subjects) but the private keys for those DIDs will be controlled by an individual or organization acting as the Identity Owner (and will be legally liable for the thing or device associated with that DID). All self-sovereign individuals and entities are able to exchange public keys and sign data with their private keys. In the SSI model, each contextual identity of an individual, entity, or thing is made up of one or more DIDs, and Credentials relating to these DIDs that are controlled by their Holder. Attributes associated with a DID can be signed by other (trusted) entities and thereby attested to in the form of Verifiable Credentials. The private keys and Verifiable Credentials are usually controlled and stored or “held” by the Holder who is also the Subject of that Claim or Credential. A Credential may also be “held” by a Holder who is not the Subject of the Credential but who controls its use on behalf of the Subject, e.g. in the case of a child’s digital passport held by a parent.

Single Sign-On (SSO)

Unlike centralized single sign-on solutions, such as social login services (e.g. Facebook, Google, Twitter, LinkedIn, WeChat), SSI allows for fully decentralized single sign-on, circumventing the core problems of social logins, including vendor lock-in, single points of failure, and correlation and involuntary sharing of meta-data.

Verified Credentials

Credentials are a part of our daily lives. driving licences are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. These credentials provide benefits to us when used in the physical world, but their use on the Web continues to be challenging. Utilizing an interoperable data format for the creation and attestation of Verifiable Credentials allows for the utilization of credentials in the digital space for remote interactions across services.

Reusable Trust

Once issued to a Subject in one context, Verifiable Credentials can be reused or repurposed in other contexts. A key example for this would be the case of car sharing services that requires a verified driving licence—rather than a lengthy onboarding process with each individual service using the card-based licence, a Subject can reuse their existing digitally verified driving licence in the form of a Verifiable Credential to access the ride sharing service with no verification time.

Data portability

Storing identity related data as Verifiable Credentials and providing SSI-based key management, Credential sharing and storage solutions enables new forms of competition to provide these services. This can be understood as a practical implementation of data portability beyond the simple right to receive personal data in a structured, commonly used and machine-readable format. Combined with the individual's ability to repurpose Verifiable Credentials across contexts, portability takes on a new dimension.

Wallet

A digital wallet refers to an electronic device or online service that allows an individual to store data assets and make electronic transactions. A digital wallet has both a software and a data component. The software provides security and encryption for the personal information and for the actual transaction. A specific identity wallet is used to handle cryptographic keys and offers the potential to store and manage identity data in the form of Verifiable Credentials.

Competition on credential issuance

Reusable and portable Verifiable Credentials could motivate a race-to-the-top for the best or highest quality Issuers for a particular use case. Issuers of Credentials, such as verification services, trust services providers, and other entities that provide Verifiable Credentials can directly compete with each other in offering their services in the market. This effectively creates a B2C market for trusted identity data and attestations in contrast to the status quo of services are bound to B2B interactions and associated with high barriers of entry to the market.

Consent

The Holder of a Credential (who is usually also the Subject of a given Credential) has full control over the Credentials it holds, which means that each exchange of data can only be executed if the Holder gives affirmative consent to the handover of that data. Where the Holder manages a Credential on behalf of a dependent or someone else

who is the Subject of that Credential and has delegated this function to the Holder, the Holder will have already obtained consent from the Subject and may face other legal constraints and fiduciary obligations to ensure it is acting in the interests of the Subject. Further, as noted above, the innovation of mutual authentication means that both sides of that handover sign their respective requests and data packages, allowing them each to individually create a record of the interaction.

Persona-based interactions

With the ability to derive multiple personas in a way that is not backwards correlatable, individuals and entities can create a new persona for each interaction. While an individual or entity should be able to link their personas and control all of their various DIDs, the default setting should be the automated creation of unique personas for each interaction. This is a core component of the privacy and data protection by default-type of interaction that is enabled through SSI. The concept is sometimes referred to as unique pairwise DIDs.

Data minimization

The flexible format of Verifiable Credentials allows for privacy-preserving interactions following the core data protection principle of data minimization. One example for this is the use of Verifiable Credentials that only state that an identity has the minimum age or lives in a specified area, without providing the complete birthdate or address. While such minimized data exchange is very powerful, many interactions can be executed without any sort of identification, but purely with the exchange of attested permissions in the form of Verifiable Credentials.

Mutually trusted interaction between identities

With the exchange of identity-related data relying on public key exchange, both sides of an interaction are required to sign their respective exchange of information. Whereas before this trust flowed in a single direction (e.g. you authenticate yourself to your bank), the new model enables mutual authentication (e.g. you authenticate yourself to your bank *and* your bank also authenticates itself to you), as well as more security and auditability of these interaction protocols. Of course, as in the real world, the relevant interaction continues to be determined by the power balance and relative bargaining power of the participating entities.

Identity interactions across domains

With all entities utilizing the universal identity layer built on top of interoperable and open standards, flexible interaction between entities can be enabled with very low friction. Examples can be the interaction of two identity subjects that utilize different client and network solutions (see building blocks), but even more so entities that are different in their nature, such as the interaction between humans and IoT devices or devices and organizations, as well as every other thinkable connection between identity subjects in the SSI model.

Data management

SSI is a powerful tool for data management, meaning that allows to enable the right individuals to access the right resources at the right time and for the right reason. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

Interoperability

The question of interoperability in respect of digital identity and identity management systems is one of growing concern. On the one hand, there are many situations where being able to cross-match identity-related information about citizens and consumers would be of enormous benefit to them. On the other hand, without the appropriate control in the hands of data subjects, interoperability could be another weapon in the hands of the surveillance society, unwelcome in a world where privacy is still valued.

4. Building Blocks of Self-sovereign Identity

Different implementations of SSI solutions can vary to a large extent when one looks at solutions currently present in the market. While this might seem to represent disagreement about the concept of SSI, nothing could be further from the truth. With the infographic below, we present our shared understanding of the building blocks that enable an open and interoperable SSI ecosystem on the basis of shared open standards and a modular architecture.

The infographic is structured as two vertical dimensions and four horizontal layers:

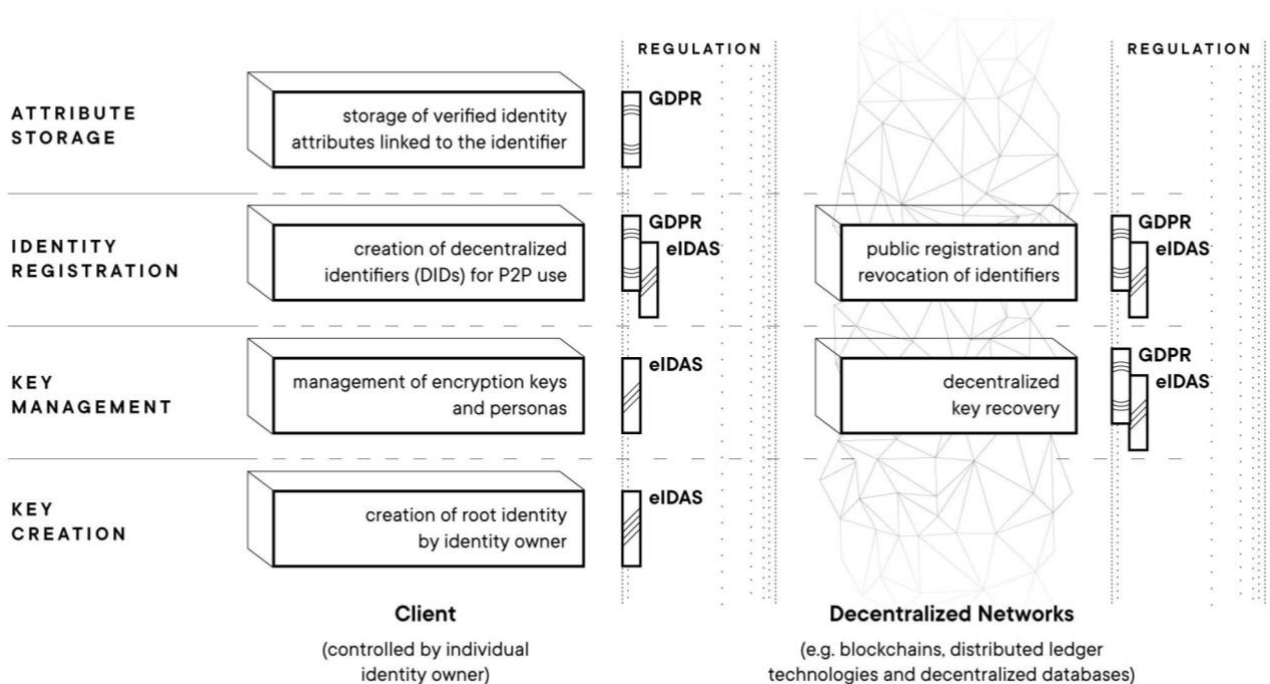
- ❑ **Client-side** building blocks that are fully controlled by the Identity Owner. Such clients can be mobile phone apps, software wallets, cloud wallets, hardware wallets or personal data stores, but their unifying property is that only the Identity Owner is able to control them. These clients are typically placed in the middle of each sharing interaction (a process that could also be automated).
- ❑ **Decentralized Networks** represent the other dimension of the SSI architecture. While this document focuses on blockchains, decentralised databases, and other Distributed Ledger Technologies, their unifying property is the public accessibility, and readability of the network.
- ❑ **Cryptographic key creation** is the fundamental layer of SSI, responsible for the creation of a root identity in full control of the Identity Owner.
- ❑ **Key management** is built on top of the underlying root identity and is used to manage cryptographic keys.
- ❑ **DID registration** is the third layer of SSI, allowing to create, register and demonstrate control of DIDs based on the underlying encryption keys. It further enables the revocation of a DID or connected identifiers.
- ❑ **Attribute storage** describes the layer where a client stores identity attributes of the respective Identity Owner as Verifiable Credentials, serving as a secure vault that can only be controlled by the Identity Owner.

In the basic architecture that we present here, decentralized networks fulfil two core functions of the SSI ecosystem. They play a vital role for the underlying decentralized public key infrastructure⁴ as they provide a decentralized, cryptographically secure root of trust for (publicly) registered DIDs.

⁴ <https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/dpki.pdf>

Further, they offer the potential to develop decentralized key recovery solutions, as one essential requirement of true SSI is that only the individual DID Subject should be able to control the private keys and DIDs that their identity is built on. Other potential use cases of decentralized networks in the realm of SSI could be incentivization via tokens (please see Appendix V) or its use for accountable storage of meta-data about an interaction. We have not included those scenarios here, as they are not essential for a basic SSI ecosystem to function and are rather implementation decisions of individual stakeholders within the ecosystem.

Self-sovereign Identity Building Blocks



Concept by Kai Wagner (Jolocom), visualization by Iryna Nezhynska (Jolocom).

Blockchain Bundesverband

Fig. 4 – Building blocks of SSI distinguished along the dimensions of clients and networks and the application of those dimensions within different layers of the system.

In addition to these two dimensions, the infographic further points out building blocks that are particularly relevant from a European regulatory compliance perspective, particularly with respect to the GDPR and the Electronic Identification and Trust Services Regulation (eIDAS). Further information on this topic can be found in Appendix II (Regulation).

5. Outlook

Given that this position paper is primarily intended to capture the community's consensus over the concept and basic implementation of SSI, as well as its regulatory and security dimensions to date, the outlook provided below considers the future of SSI. We consider points around adoption, implementation, usability and technological potentials, which can form the basis for further discussion and research. We want to encourage a lively debate around the presented ideas, as well as the points described further on. Ultimately, we aim for a universal identity layer that is global and should thus be discussed and developed by an inclusive group of individuals, and organizations worldwide.

Adoption

The model of SSI represents a paradigm shift in the management of digital identities. Besides its disruptive potential to offer new business models for all actors in the market, the need to create awareness about these potentials and the necessary changes to both conceptual and technical models are huge. On the technical side, legacy systems have to be updated in order to benefit from the increased cost efficiency and redistributed liability risk of SSI. On the business side, both services that are built on top of identity solutions and secondary identity-related services (e.g. verification and trust services providers) need to reorganize their business models in order to benefit from the potential of capabilities like reusable credentials and verified user data. On the conceptual side, SSI is facing the challenge of perceived complexity. While it practically resembles the physical worlds approach to identity (namely a physical wallet in which an individual store their credentials to identify and authenticate themselves towards others), we have to break the status quo of centrally-managed, digital identity where each interaction is routed through a third party. This habit will be very hard to break and requires SSI solutions to be tenfold better as compared to the convenience of centralized identity solutions, while being enriched with the unique capabilities of a universal identity layer.

Getting to Scale

While the above-mentioned points on adoption do a great part in describing necessary developments to bring SSI up to scale, there is also the question of timing in both technical and regulatory developments. In the technical domain, questions remain on how quickly the described building blocks of SSI will be completed and to what extent they will be in sync in order to allow for significant network effects.

We already see great traction in respect of client applications, decentralized identifiers and decentralized networks, but all building blocks are under active development and require constant collaboration on standards and implementation decisions in order to reach their potential.

Regulatory compliance and respective adaptation will further enhance or harm the dynamic of SSI and we expect that those regulatory environments that embrace SSI solutions will benefit from a significant economic potential for their economies, both due to early mover advantages, as well as legal certainty. Here, it is of particular relevance to create legal certainty in the new field of reusable credentials. To have appropriate guidance on whether some pre-issued Verifiable Credential can be reused in a given context will determine whether companies and public institutions can easily adopt SSI systems. In other instances, there may already be certainty in the law, but the law is nevertheless incompatible with the new SSI-enabled approach, such as in the case of laws that do not allow third-party reliance or that do not allow passing on regulatory liability (though they may still allow for passing on commercial liability and recouping damages from a third party).

Finally, just as domain-specific regulations such as the Fifth AML Directive (AMLD5), the Revised Payment Services Directive (PSD2), and the Electronic Identification and Trust Services Regulation (eIDAS) are emerging, other domain-specific regulations or self-regulatory frameworks, may be required to build horizontal trust across borders.

Social Acceptance

In addition to the questions raised above, there is a need for increased awareness about the capabilities of SSI (see Section 3 above). Ultimately, this model of identity can only become successful if citizens, public institutions, and businesses understand its potential and can create trust in this novel infrastructure. It is thus a key responsibility of the SSI community to be transparent and hold on to the values of interoperability and collaboration in order to build and retain trust in the SSI infrastructure, as much as it is required to engage in constant educational outreach and advocacy.

Accessibility

Another point that can by no means be underestimated is the need for accessibility. SSI solutions must ensure that everyone who is legally able to have a given identifier or Credential is able to have and use them in this new architectural construct. In the process of designing and implementing these solutions, we have to make sure that disadvantaged or vulnerable populations, including those with physical or mental disabilities, children, the elderly, and those without access to certain technologies, are not excluded or precluded from the promise of SSI. Its empowering potential can

instead only be reached if it manages to cover the society as a whole and not just tech savvy elites.

This also raises points on the technical infrastructure necessary to hold an identity. While smartphone-based identity wallets will do a great job most of the time, some individuals will require other or additional means to control their identity, making it necessary to open client application development to specialized vendors, a setting that is ensured by the interoperability and open standards of the described building blocks. It also means that we cannot rely on technology alone but that there must also be non-technical measures in place, including laws, regulations, and “off-chain” governance mechanisms, as well as the application of existing legal constructs like guardianship, delegated access, and powers of attorney and other proxy contracts. SSI is not self-sovereign unless it is truly identity for all.

Call to action

We need a global universal identity layer for all individuals, entities, and things, built on open and interoperable standards!

For individuals

□ We invite everyone to test emerging applications and services as an early adopter and thereby speed up the learning cycles of all participating actors (see existing pilots at Appendix VII). You are an integral part in this process to shape the way SSI will work, look, and feel.

For regulators

□ We ask for clarification on the implementation requirements for GDPR compliance of various kinds of data implicated in the SSI context, such as DIDs, DID documents, revocation registries (of various implementations), public keys and addresses, and the degree to which certain kinds of obfuscation methods might take this data outside the scope of GDPR (by making it sufficiently “anonymised”).

□ We ask for guidance on the potential to have eIDAS-compliant implementations of SSI up to the high level of assurance (including how to get DIDs accepted as qualified electronic signatures and how to derive DIDs from qualified signatures).

□ We ask for legal clarification on the reuse of issued credentials outside of their original regulatory environments such as for example credentials subject to the Fifth AML Directive (AMLD5), the Revised Payment Services Directive (PSD2), and eIDAS to enable horizontal comparability of credentials.

□ To explore the use of SSO in business and public administration, we call for regulatory sandboxes to build up knowledge on the practical implications of SSI especially in combination with legacy systems. The public sector needs to enable the issuance and attestation of credentials for its citizens and organizations in this new identity layer.

For business

□ We call for Pilot Projects that target the specific capacity of SSI solutions to be used in an interoperable way across services and independent from the specific implementations, by utilizing shared open standards.

□ We call companies from all industries to explore the potential of new business models built around decentralised data transactions enabled by mobilized trust.

For identity companies

□ To ensure long-term sustainability in the market, companies from the identity sector (e.g. trust services providers) should seek to understand the implications of reusable trust in the form of Verifiable Credentials, and the value-add that DIDs can bring, and adapt their business model and strategy accordingly.

Appendix

Appendix I – Glossary

Acknowledging that blockchain and decentralized identity are still in a phase of dynamic and rapid development, this glossary is intended to provide a resource for readers new to the field while at the same time providing clarity to all readers for definition of the used terms. Potential conflicting or varying terminology is avoided by using the same terminology throughout the paper, while referring to the respective optional terminology in this glossary.

Attestation an attestation is the confirmation of a Claim through evidence or verification.

Blockchain as used in this document, means a distributed ledger technology of different types. While the term is often used as a catch-all phrase, we differentiate blockchain technologies along two main characteristics of public & private read access and permissioned & permissionless write access, resulting in at least four distinct blockchain infrastructures with different implications across, legal, commercial, and technical domains. This is an oversimplification for the sake of efficiency in this Position Paper as there are other permutations of permissioning (such a permissioning of the node infrastructure or participants in a consensus protocol) that may also achieve similar ends.

A **Claim** is a statement or assertion that one DID Subject, such as a person or organization, makes about itself or another DID Subject. The Claim will relate to one or more attributes about an DID Subject. While an Attribute may be the information itself, e.g. "first name", the corresponding Claim would be is a statement involving an identity subject, e.g. "My first name is ...".⁵ A Claim is typically an assertion which is disputed or in doubt unless cryptographically signed. A Verifiable Credential existing of only one Claim is still known as a Verifiable Credential.

A **Client** is any type of software or hardware (e.g. software wallets, cloud wallets, hardware wallets, etc.) that is used to create and manage decentralized identifiers on behalf of an Identity Owner (i.e. through key creation and management) and store of Claims and Verifiable Credentials relating to that Identity Owner or any identity subjects whose decentralized identifiers they manage.

A **Credential** is a set of one or more Claims about a Subject.

⁵ http://wiki.idcommons.net/Main_Page

A **DID Document** contains a set of key descriptions, which are machine-readable descriptions of the Identity Owner's public keys, and a set of service endpoints, which are resource pointers necessary to initiate trusted interactions with the Identity Owner.

DID or decentralised identifier is a new type of identifier intended for verifiable digital identity that is "self-sovereign", i.e., fully under the control of the Identity Owner and not dependent on a centralized registry, identity provider, or certificate authority. ⁶

eIDAS electronic IDentification, Authentication and trust Services is an EU regulation on a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.

Entity refers to all types of entities that can have a SSI, ranging from individuals to legal persons such as businesses and public institutions as well as Smart Agents such as IoT devices and machines.

GDPR GDPR is (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Digital Identity is defined as the data points that identify something (whether an individual, entity, or thing) in digital form.

Holder: the individual or entity that digitally stores and controls the use of Claims or Credentials about one or more Subjects. Often the Holder and Subject will be the same entity. But there are cases where they may be different e.g. a parent may be the Holder of a digital passport for their child who is the Subject of that credential.

An **Identifier** is something that enables an individual, organization, or thing to be discovered and identified in a given context. The Decentralized Identifier or DID is the building block of SSI. In the context of this document, we refer to DIDs when speaking about Identifiers.

Identity Owner is an individual or organization who controls the private keys associated with a given DID. While all types of entities, including natural persons, processes, organizations, smart agents, and things (e.g. IoT devices, machines, etc.) may have DIDs that identify them, the private keys associated with a DID will still be controlled by an individual or organization (who will also be legally liable for it).

⁶ <https://w3c-ccg.github.io/did-spec/>

Issuer refers to an individual or entity that issues a Verifiable Credential about another individual, entity, or thing (who is the Subject of that Credential). By cryptographically signing the Credential, the Issuer attests to its accuracy and validity. Once issued, Credentials are stored by the Holder it has been issued to. A familiar example of an Issuer is a public authority that issues Credentials such as a driving licence, passport, or diploma to a Subject.

Persona refers to a sub-identity associated with an entity's root identity. Each persona is linked to the root identity in a hierarchically deterministic way, allowing it to be controlled with the root identity, while avoiding unwanted correlation of multiple personas by being not backwards correlatable.

Personal Data means "any information relating to an identified or identifiable natural person ('data subject')" as defined in Article 4(1) of the GDPR.

Root Identity refers to the core component of the presented SSI model that is based on public private key encryption. A root identity is an underlying private key that ultimately resembles the cryptographic root for all derived public and private key pairs that are used for different identity roles and associated interactions. A prerequisite for the use of one cryptographic root is the use of hierarchically deterministic key generation for the derivation of key pairs, in order to rule out potential backwards correlation of key-pairs. Using only one such root identity improves key management for the identity subjects, as it has to only remember one set of recovery information to access all of its identity.

Self-Sovereign Identity is a model of digital identity where individuals and entities alike are in full control over central aspects of their digital identity, including their underlying encryption keys; creation, registration, and use of their decentralized identifiers or DIDs; and control over how their Credentials and related personal data is shared and used. SSI can be best understood as an infrastructural innovation that solves the interoperability and security problems of isolated and federated identity by facilitating a decentralized architecture for cryptographic roots of trust in a combination with Verifiable Credentials on the basis of encryption technologies, Distributed Ledger Technology, Open Standards and interoperable protocols. The architecture gives individuals and entities the power to directly control and manage their digital identity without the need to rely on external authorities.

State-issued Identity is any document or proof which may be used to prove a person's identity. Some countries issue formal identity documents, as national identification cards which may be compulsory or non-compulsory, while others may require identity verification using regional identification or informal documents.

Subject refers to the subject of a given Claim or Credential.

A **Verifiable Credential** is a Claim or Credential that is cryptographically signed by the issuer (e.g. a trust service) and associated with a specific identifier (typically connected to a DID) following the open standard specified by the associated W3C working group.

Verifier is an individual or entity who verifies or relies upon a given Credential.

Wallet refers to a building block of SSI that handles key creation and management, as well as storage of Credentials (see Client).

Appendix II – Regulation

Having described the potential of SSI, ongoing standardization efforts, and its underlying technical architecture, we now aim to describe and, where possible, interpret the existing regulatory environment in Germany and Europe at large. Specifically, this chapter focuses on the two most relevant European regulations that may affect the evolution and adoption of SSI significantly—namely, the General Data Protection Regulation (GDPR) and the Regulation on electronic identification and trust services for electronic transactions in the European market (eIDAS). That said, these are not the only regulations that will have an impact on the future of SSI. Other relevant regulations include the Fifth Anti-Money Laundering Directive (AMLD5), the Revised Payment Services Directive (PSD2), and the e-Privacy Directive (ePD) and forthcoming e-Privacy Regulation (ePR). Any approach to SSI should assess and analyze the impact of an array of regulations before deploying or implementing such approach.

Before exploring any specific regulation in detail, it is important to appreciate the structural challenges that SSI poses for existing legal frameworks. While many of the relevant regulations were drafted for a world in which large entities own and control centralized and siloed data stores, blockchain-enabled SSI imagines a restructuring of this digital infrastructure focused on decentralized and distributed computing. Thus, where there are structural barriers to a literal or letter-of-the-law application of a given law or regulation to SSI related solutions, we may need to employ a more imaginative or spirit-of-the-law approach. Viewed through this lens, it is clear that SSI can promote many of the objectives around privacy, data protection, interoperability, transparency, and compliance in line with these laws.

GDPR

Our assessment of the GDPR as it relates to blockchain-enable SSI is, in part, based on the German Blockchain Association's May 2018 Position Paper on GDPR, Blockchain and Data Protection, adapted to the specific context of SSI and only to the extent that it utilizes blockchain technology. We do not examine blockchain-related pieces of the technology stack that do not actually require the blockchain (such as purely peer-to-peer or agent-to-agent communications that do not require referencing the blockchain or public ledger).

The GDPR has a dual purpose—it “lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.”⁷

The GDPR only protects natural persons (i.e. individual human beings) and does not apply to corporations or legal persons, organizations or other entities, or things (e.g. animals or IoT devices). Moreover, it only applies where there is **personal data**, meaning “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”⁸ Thus, in the case of SSI, the GDPR will apply where the blockchain or ledger is processing the personal data of natural persons.

While there is some uncertainty as to whether the data implicated by the SSI model is in fact personal data, all data that relates to an identified or identifiable natural person is, by definition, personal data. Recital 26 explains that the identifiability depends on “all the means reasonably liked to be used” considering “the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.” While pseudonymous data is still personal data,⁹ truly anonymous data is not.¹⁰

Thus, the GDPR will apply to all personal data, including all pseudonymous data processed via the blockchain or ledger that enables SSI but will not apply to data that has been sufficiently anonymised so as to fall outside the scope of personal data.

Two techniques that are often suggested for achieving GDPR compliance are hashing and encryption. In the following section, we explain why these techniques—in their current form—are generally inadequate to take data outside the GDPR’s scope. We attempt to provide a brief overview of the state of the law on data that constitutes the building blocks of SSI.

⁷ Article 1(1), GDPR <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

⁸ Article 4(1), GDPR. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

⁹ Article 4(5) (“Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.”).

¹⁰ As stated in recital 26: “[...]The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.” More guidance is available in the WP216: Opinion 05/2014 on Anonymisation Techniques

Public keys

Blockchains rely on decentralized public key cryptography. The public key is derived from the private key, which is a randomly generated number. The public key is in turn hashed to create a public address. Both the public key and public address, when published to the ledger, are known by anyone with access to the blockchain.

Because an individual's public key and public address can be directly linked to a natural person—in fact, that is the whole purpose of public keys (i.e. to identify the parties to any given transaction)—they are likely to constitute personal data under the GDPR unless they are sufficiently anonymized. What constitutes sufficient anonymization is an open question under the law and an important one to clarify given the importance of public keys in blockchain-enabled systems.

Hashed data

Hashing functions are algorithms which accept any data of any size as input and generate a fixed length string as an output value. Running the hashing function again on the same input data will always generate the same output hash value. But if even a single bit of the input data is changed, the output hash value will be significantly different as well, a property also called the avalanche effect. A hash value is typically smaller than the input data.

There are three primary reasons to write hashed data to a blockchain:

- to later validate data by comparing it to the hash
- to obscure plain text data
- to overcome limitations on the size of data that can be written to a single transaction (e.g. by writing a hash of a larger block of data rather than the entire block of data).

The Article 29 Working Party—predecessor to the European Data Protection Board (EDPB)—has adopted the view that hashed personal data is pseudonymous, not anonymous, and therefore still personal data.¹¹ While the EDPB has imported most of the guidance from the Working Party, we do not know how this guidance will be applied in the context of new and emerging hashing methods being utilized for blockchain-enabled SSI.

¹¹ Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques WP216 (Brussels, 10 April 2014). http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Encrypted data

There is a common misconception that encrypted personal data is not personal data and can be safely written to a public blockchain. The Article 29 Working Party has previously adopted guidance to the effect that encrypted personal data is pseudonymous, not anonymous, and therefore still personal data.¹² While it is unlikely for state-of-the-art encrypted personal data to be linked back to a natural person in the present moment, that is likely to change in the near future.

Thus, we take the position that encrypted personal data should not be written to a public blockchain.

Decentralised Identifiers (DIDs)

While public keys present a GDPR compliance challenge for public blockchains, the specific decentralized public key infrastructure proposed for SSI raises additional questions. For someone to be discoverable on a public blockchain, they would have to write a DID to the ledger. While we do not have direct guidance from the EDPB as to whether a DID is or is not personal data, we can expect the answer to be yes when it belongs to a natural person. The DID, as an identifier, is *per se* personal data. Thus, public blockchains that process the DIDs of EU persons, are subject to GDPR requirements.

Given the above, here are some best practices for a public blockchain built on a decentralized public key infrastructure utilizing DIDs:

- Each direct interaction between an individual and another individual or entity should use an identifier that is unique to this interaction, also known as a unique pairwise identifier (see HD key derivation in Appendix III below).
-
- No DID or other identifier (such as a public key or public payment address) should be written to a public blockchain without a lawful basis for processing, such as specific, unambiguous consent obtained from the owner of that identifier by a clear affirmative action.
- Underlying data, including Claims and Credentials, should not be written to or stored on a public blockchain.

¹² Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques WP216 (Brussels, 10 April 2014).

- Rather, such underlying data should be stored “off-chain” (i.e. not on the public ledger) and under the sole control of the individual who is the Subject of that data (or the Holder of a Credential who manages this data on the Subject’s behalf).
- The blockchain and related off-chain data storage methods must have a way of complying with the rights to restriction of processing and erasure, which are some of the most challenging issues in respect of the GDPR and blockchain-enabled SSI.
- Future implementations of SSI solutions should utilize DIDs that exist purely off-ledger, especially if a unique pairwise DID is used for each relationship as mentioned above. [Note: At the moment, on-ledger DIDs are the default and pose the greatest compliance challenges].

Other key challenges of applying the GDPR to decentralized, blockchain-based solutions like SSI include determining who the data controller(s) and processor(s) are, determining and enforcing rules for cross-border or extra-EU transfers of personal data, disclosing automated processing, and giving effect to the rights of restriction of processing and erasure. Rather than address these issues here, we refer you to the EU Blockchain Observatory’s recent thematic paper, which addresses these issues in depth.¹³

eIDAS

Like the GDPR, eIDAS is another EU regulation that will reshape our digital interactions. The abbreviation refers to **electronic IDentification, Authentication and trust Services**. eIDAS is aimed at achieving interoperability across the European Single Market by establishing a single set of standards for digital identity and electronic transactions, including digital signatures, timestamps, seals, registered delivery, and website authentication.

As of September 2018, all organizations delivering public digital services in an EU member state must accept eIDAS-compliant electronic IDs from all other member states.

As with the GDPR, SSI is closely aligned with the spirit and objectives of eIDAS. However, because SSI introduces a new model for all three dimensions of our digital interactions—identification, authentication, and verification— eIDAS presents similar challenges to those introduced by the GDPR.

¹³ See Blockchain and the GDPR: a thematic report by the European Union Blockchain Observatory and Forum (October 2018), available at https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf?width=1024&height=800&iframe=true.

Just as with the GDPR, eIDAS was drafted with the conventional or traditional data model for digital interactions in mind, i.e. the model of large centralized intermediaries controlling large data silos. The challenge for proponents of SSI is to translate the centralized vision of eIDAS to a more resilient decentralized infrastructure while still achieving regulatory compliance.

Because DID-based, blockchain enabled SSI involves identification, authentication, and verification (especially through the use of cryptographically verified digital signatures), eIDAS is directly relevant. DIDs are the building blocks for giving individuals and entities full control over their digital identities and uses of their digital credentials. DIDs, in a combination with public and permissionless blockchain networks, effectively comprise a decentralized public key infrastructure that allows for a cryptographic root of trust without the reliance on any centralized authority. Further, DID-based interactions can happen between peers that rely on different decentralized roots of trust, as well as registry networks. This is enabled by the open standard specification that has been designed with interoperability as a core design criterion.

As outlined in the W3C Draft Report on “Decentralized Identifiers (DIDs) v0.11, *“Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, ‘self-sovereign’ digital identity. DIDs are fully under the control of the DID subject, independent from any centralised registry, identity provider, or certificate authority.”* eIDAS takes a more conventional approach, stipulating that *“a qualified electronic signature shall have the equivalent legal effect of a handwritten signature”*.¹⁴ eIDAS defines an “electronic signature” as *“data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.”*

In order to meet the eIDAS requirements for an advanced electronic signature, the signature must be: uniquely linked to the signature; capable of identifying the signatory; created using an electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and linked to the data signed there with in a way that any subsequent change in the data is detectable.¹⁵

The requirements for an advanced electronic signature map closely to the framework of DIDs in combination with Verifiable Credentials. However, the eIDAS regulation also provides, “A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognized as a qualified electronic signature in all other Member State.”

¹⁴ Article 25(4), eIDAS.

¹⁵ Article 26(4), eIDAS.

Thus, the acceptance and interoperability of electronic signatures across borders within the EU requires a qualified certificate from a centralized authority, which is at odds with the decentralized approach to DIDs. This means that DIDs are currently not recognized or accepted by the EU as electronic signatures under eIDAS.

As discussed above, we believe that DIDs do not need to be secured by centralized trust services because of the nature of blockchain technology. Rather, we suggest that a fully transparent and decentralized SSI infrastructure built on top of open and interoperable standards allows for eIDAS-compliant solutions in line with the spirit of the law.

We urge regulators to amend the qualified advanced electronic signatures requirements to allow for these new possibilities enabled by blockchain technologies, particularly in regard to DIDs. Specifically, we would like to see technical implementation guidelines and research on:

- What can ensure eIDAS compliance of a public permissionless blockchain?
- How can we create cryptographic keys that fulfil the high level of assurance requirements?
- What implementation requirements are necessary for eIDAS-compliant Verifiable Credentials?

Appendix III – Standardization

For the successful implementation of SSI at scale, open and interoperable standards are a key requirement. The industry actors represented by the authors and peer reviewers of this document share the position that core components of SSI need to be built in close collaboration to provide a common technological basis for everyone to provide their respective services and solutions. As a public infrastructure, this open and interoperable set of standards will enable a flourishing ecosystem for identity where competition and innovation are a driving force for all participating actors. The presented standards are pushed by a diverse set of actors, with some being relevant to the whole SSI community (DIDs, HD-keys and Verifiable Credentials), while some are only relevant for specific network environments (ERC 725, 735, 1056).

On the international level, there are also ongoing efforts by the ISO (ISO/TC 307), but this is a work in progress effort that cannot be assessed in detail yet.

DID

Decentralised identifiers (DIDs)¹⁶ are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the Identity Owner, independent from any centralized registry, identity provider, or certificate authority. DIDs are URIs that relate a DID subject to means for trustable interactions with the DID Subject of that DID. DIDs resolve to DID Documents, simple documents that describe how to use that specific DID. Each DID Document contains typically three things: cryptographic material, authentication suites, and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate as the DID Subject of that DID (e.g. public keys, pseudonymous biometric protocols, etc.). Service endpoints enable trusted interactions with the DID Subject.

DID Documents

If a DID is the index key in a key-value pair, then the DID Document¹⁷ is the value to which the index key points. The combination of a DID and its associated DID Document forms the root identity record for a decentralised identity.

HD keys

¹⁶ <https://w3c-ccg.github.io/did-spec/>

¹⁷ <https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft-documents/did-implementer-draft-10.md>

Hierarchical deterministic (HD) keys¹⁸ are a type of deterministic wallet derived from a known seed, that allow for the creation of child keys from the parent key. Because the child key is generated from a known seed there is a relationship between the child and parent keys that is invisible to anyone without that seed. In identity they are used to support the creation of non correlatable personas, such as in the context of pairwise identifiers.

Verifiable Credentials

Granting a benefit requires proof and verification. Some benefits demand a formal process that includes three parties. In this process, the identity subject asks for the benefit and the inspector-verifier grants or denies the benefit based on verification of the identity subject's qualification from a trusted issuer.

For example, we use a driving licences to prove that we are capable of operating a motor vehicle, a university degree to prove our education status, and government-issued passports to grant travel between countries. This specification provides a standard way to express these claims on the Web in a way that is cryptographically secure, privacy respecting, and automatically verifiable.¹⁹

Ethereum - ERC 1056

A registry for key and attribute management of lightweight blockchain identities. It represents a standard for creating and updating identities with a limited use of blockchain resources. An identity can have an unlimited number of delegates and attributes associated with it. Identity creation is as simple as creating a regular key pair Ethereum account, which means that it's fee (no gas costs) and all Ethereum accounts are valid identities. Furthermore, this ERC is fully DID compliant.²⁰

ISO/TC 307

In 2016, the ISO Technical Committee ISO/TC 307²¹ was launched, focusing on Blockchain and distributed ledger technologies²². The secretariat is held by Standards Australia. The committee has currently 37 participating – including DIN (Deutsches Institut für Normung e. V.) from Germany – and 12 observing members. The ISO work is still in early stages and expected to reflect market dynamics towards standardization, such as the ones described above.

¹⁸ <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>

¹⁹ <https://www.w3.org/TR/verifiable-claims-data-model/>

²⁰ <https://github.com/ethereum/EIPs/issues/1056>

²¹ <https://www.iso.org/committee/6266604.html>

²² <https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0>

Appendix IV – Security

Building a decentralised ID requires a high security level and usage of best known standards. Since a solution has to work in a trustless environment (Decentralized Networks). Many aspects of the technology utilized must be highlighted. Additional fast updating processes have to be defined for potential security risks. A solution has to be secure today as in the future especially with sensitive data handled by identity management tools.

Not only security challenges could be a problem for SSI solutions. The privacy and data protection rights of users are non-negotiable requirements and can be endangered by connecting information on a public ledger. As there are many similarities on all present SSI solutions we provide a general outlook on the respective security aspects.

Cryptography

The blockchain technology is a fusion of peer-to-peer systems and cryptography. Cryptography is used in three ways. You have to be able to encrypt, decrypt and sign messages, you need a cryptographic hash function for building up the blockchain data structure and a random number generator is needed for creating key pairs. The used algorithm for asymmetric cryptography has to be secure for a long time. The 'Bundesamt für Sicherheit in der Informationstechnik (BSI)' provides continuous recommendation for technology and key length which should be followed to ensure secure cryptography in the future²³.

Nevertheless, there has to be (fast) update processes to allow the deployment of an update in case of sudden risks. Such a sudden development could for example be a quantum computer. With quantum computing, it is said that presently used cryptography isn't secure. Signing and coding processes could thus be compromised. There are also recommendations for hash functions. If a collision is able to be found within a hash algorithm it is said to be insecure. A change of the used hash function would be mandatory in such a case.

The number generator is used for building key pairs. Those keys are necessary for creating a root identity. It has to be ensured that two people are not able to create the same key pair.

²³ https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/tr02102_node.html, accessed 09.08.2018

A correct random number generator is a common research field and has many challenges on its own that will not be covered here. The BSI also provides a recommendation for creating a secure blockchain solution²⁴.

Client applications

The client application will be the tool the Identity holder is using for controlling and applying its identity. It bridges the SSI solution with customer needs especially the need for a user-friendly interface. Assuming that most SSI users aren't aware of security standards or needing technical guidance, this solution has to be continuously secured and managed by the solution provider and support has to be delivered.

The client application should provide basic identity operations like creating, deleting or changing identity related information and handling credentials for identity proofs. There are various possibilities to build a client application, all have its own features.

Software Wallets

A software solution is currently the most common way for implementing a client application given the advantage of low budget realization. But to achieve a broad market it needs to be implemented for all the major operating systems. The software has to be secure whatever hardware is used. Continuous work on new software updates on all systems are required for achieving secure solutions into the future. Depending on the software the Identity holder needs to be active. Backup or update of the system and management of settings can be dangerous and time consuming. Lacking knowledge can endanger the identity, potentially leading to identity loss or damage.

Cloud Wallets

In cloud solutions the provider is able to maintain, manage and control the software by itself. The responsibility shifts from Identity Owner to provider compared to software solutions. But this advantage comes along with a needed internet connection and with the impact of the provider. Because of the centralization the resulting identity cannot be seen as a fully SSI, as it requires a server operator. This evaluation is based the low usability of personal server infrastructures today, effectively creating a need for users to rely on third-parties.

²⁴https://www.bsi.bund.de/DE/Themen/Kryptografie_Kryptotechnologie/Kryptografie/Blockchain/blockchain_node.html, accessed 09.08.2018

□ **Hardware Wallet**

The main difference to a software solution would be the fact of storing and handling the identity on a hardware device like an USB stick or a (credit) card. It comes along with being more secure on untrusted hardware than a software solution, since it doesn't need to use the device CPU or memory for creating credentials or building private and public key pairs. But, it comes along with the need to buying this particular hardware device. This may occur as a negative point for the Identity holder due to financial concerns and the need to carry an extra device. In this solution the Identity holder is responsible for backup and managing the device as in software solutions.

All mentioned solutions help the Identity holder to control its identity. For that there has to be a user interface which has to be user friendly and secure. Security issues in the client may impact many people and endanger them. To counter this problem taking precautions to secure the client is mandatory like continuous testing and development of the client.

Networks

Blockchains vary in their respective architectures. Interactions are reading and writing transactions out or into the blockchain. The writing process can be distinguished by writing a transaction and writing transactions into the blockchain.

We can represent this with the below matrix. The Y-axis represents the read access. The X-axis represents the write access.

	Permissionless	Permissioned (Consortium)
Public	Public-Permissionless	Public-Permissioned
Private	Not applicable	Private-Permissioned

Public Permissionless

This blockchain type allows all user to interact with and to view the blockchain. It is used in common Blockchain Networks like Bitcoin or Ethereum. This type of blockchain can be used for many types of applications like cryptocurrency, SSI, supply chain

management, and many more. Due to its public nature, privacy of data in these networks cannot be ensured.

We thus argue that no personal data should be recorded on a public network. A benefit of permissionless blockchains is the high level of decentralization and the potential to completely erase single points of failure.

Public Permissioned

With public permissioned blockchains all users have the ability to view the blockchain. Only the writing process differs from permissionless types insofar that only an elected consortium is able to write given transactions into the blockchain. The ability to write a transaction could be a selected group like the consortium or can if the consortium agrees be extended to be public as well. The limitation is given by the writing into the blockchain process. Building a consortium can have advantages with regard to controlling and management of the system. In addition, it could also increase some performance indicators. But due to its governance through a consortium, it comes along with the risk of a malicious members that can endanger the whole system.

Where permissionless blockchain networks try to manage governance with technical systems, permissioned networks opt for the utilization of case specific agreements between the participating parties, a decision that introduces potential friction in a consortium. This blockchain type is able to be used for SSI as well as other use cases where a limited set of stakeholders interacts.

Private Permissioned

This type of blockchain is highly discussed because of the limited difference to distributed databases. Databases have the potential to be more secure and scale better. With a blockchain like this, it is still argued to create the potential for a trusted environment within the group of network participants, able to read the blockchain.

Storage

□ Data

Storing encrypted data on-chain is possible but, in the case of data relating to natural persons, it is not GDPR compliant for the reasons discussed in Appendix II. Even if the key to decrypt the data can be shown to have been destroyed, there is always a risk that the encryption algorithm will be compromised or advances in computing will make it trivial to expose the data. For this reason, storing encrypted data on-chain is not a wise choice. Storing hashes of the data on chain is still high risk for personal data of individuals but may, if certain steps are taken, increase security. Hashing function are deterministic: running the same hashing function on a particular input will always generate the same output.

On-Chain:

□ But if even a single bit of the input is changed, the output will be completely different. For example, providing the string “Hello world” as input to a common hashing function (MD5) will always generate a hash value of “3e25960a79dbc69b674cd4ec67a72c62”, but if we make the “h” lowercase instead of uppercase (“hello world”), the output hash is entirely different: “5eb63bbbe01eeed093cb22bb8f5acdc3”. Hashes are typically a one-way function, meaning the hash value cannot be used to reconstruct the original value. However, if a field is known to contain something predictable like a name, an attacker can run through a list of likely inputs and test the generated hashes. A solution to this is to add a secret “salt” to the data before putting it through the hashing function, making it unguessable.

□ **Data**

Off-Chain:

To limit the risk of on-chain data you are able to save the data in a separate location and save a link in the blockchain. To achieve integrity, you can put an additional hash value of the data with the time stamp to your link. This solution provides you with the ability to change the data stored off-chain (e.g. remove data), making the reference stored on-chain useless.

General Risks

Inappropriate access to identity

If an attacker is able to get access to an identity (for example by phishing attacks) the full control over this identity is lost. This may result in huge damage to the identity subject. With a SSI solution, control is given to the identity subject in the form of control over the associated cryptographic keys. This resembles a centralization of identity with the identity subject. If the cryptographic keys are compromised, an attacker could abuse an identity in many ways, like using this identity for criminal purposes, election verification, e-commerce fraud, etc. It is thus a necessary requirement for SSI to enable highly secure and usable key management. In the case of compromise, the true identity subject needs to be empowered to regain control over their identity. The root identity is of central importance in these approaches.

(Partial) Loss of Identity

In difference to the compromise of keys mentioned above, one could only lose control over parts of the identity. This can happen if a client solution is compromised or offline (e.g. cloud wallet). In this case the identity subject is not able to proof its identity.

Honey pot

In centralized identity solutions, a major risk is the so-called honey pot situation. Due to the fact that all data of all users is stored in one centralized system, a successful hacker gains access to immense amounts of data. In the case of SSI, this is not possible, as the effort required to hack one identity does not bring down the cost associated with hacking another identity. One could say that in SSI, hacking does not scale.

Quantum computing

Since cryptography is a base technology of blockchains the impact of quantum computing needs to be considered. This means that if quantum computing occurs, every wallet or identity on a blockchain would be endangered and could be corrupted by the user of the quantum computer in case the used encryption algorithms are not quantum secure. But with further research in post quantum cryptography all results there can be used for blockchains as well. Researchers are already investigating several post quantum solutions²⁵. The ability to update solutions in currently under development is thus very important.

Impact of Internet Service Provider (ISP)

The (ISP) plays a key role in connecting people and companies to the internet. With this connection it also has an impact on blockchain technologies as they are connected via the internet. A malicious ISP could for example use its role for manipulating blockchain systems by blocking transactions of particular actors.

Lack of user knowledge

With an SSI solution the responsibility will be to a large extent shifted to the identity holder. But one cannot expect that everybody is conscious about the duties connected to this responsibility. Therefore, we need to develop solutions that bridge the gap between convenience, usability and personal responsibility to enable systems that live up to their promise of full user control without leaving the individual alone.

Security problems in existing centralised identity solutions

Central storage and management of identities and related data of millions of users creates a huge incentive for hackers to break into these data silos and steal millions of identities with just one hack. Recent events put a focus on identity theft and the impact it can have on the individual, on political processes and the society overall.

Four cases show on a massive scale the possible consequences of identity theft:

²⁵ <https://www.golem.de/news/new-hope-google-testet-post-quanten-algorithmus-1607-121989.html>, accessed 10.09.2018, in German



1. Equifax Data Breach

Equifax is a US based consumer credit reporting agency. It announced in September 2017 that a massive data breach had disclosed data of millions of users between the months of May and July 2017. Due to this data breach, sensitive personal information such as first and last name, Social Security numbers, birth dates, addresses, credit card data, etc. of approximately 147.9 million US Americans were exposed²⁶

2. The Facebook Cambridge Analytica Scandal

An app called “This is Your Digital Life” by Cambridge Analytica, which purpose it was to ask several hundred thousand of Facebook users to complete a survey only for academic use, was allowed by Facebook’s design to not only collect data of the users who agreed to participate in the survey, but also to collect that data from people in those users’ social network. Because of this, data of approximately 87 million users was collected. The data included public profile, page likes, birthdate and current city.

Based on this data Cambridge Analytica was able to create and sell psychographic profiles for the subjects of the data.

3. The Facebook “View As” Hack

In September of 2018 more than 50 million Facebook accounts were breached as the result of an anonymous hacker attempting to exploit the Facebook “view as” feature, which lets people see what their own profile looks like to someone else. This allowed the hackers to steal OAuth bearer access tokens, which are the equivalent of digital keys that control access to the account. The event was made significantly worse by the fact that it enabled hackers to access not just the breached accounts but any other accounts that those users logged into via their Facebook credentials, demonstrating the big risks behind social login or SSO per the federated model of identity.

4. Estonian ID Hack

Since 2002 the national ID card of Estonia is a mandatory identification document for Estonians and it is one of the cornerstones of the Estonian e-state. The Estonian ID card enables digital identification, i.e. accessing web portals and e-services, bank transactions and digitally signing documents. Additionally, it can be used for electronic voting. In August 2017 a potential security threat was discovered that affected 750.000 ID cards issued between 16th October

²⁶ 17.09.2018

2014 and 26th October 2017. This security threat could have led to the identity theft of users holding an ID card issued during the respective time frame. It was caused by a software library used by the smartcard that allowed to compute private keys from public ones and therefore enabling attackers to steal and use the identity of users holding such an ID card. According to the ISA (Estonian Information System Authority) no identity theft on the base of this security issue has occurred.

Appendix V – Open Questions

Tokenization

The need for transparency and interoperability is most relevant in regard to the potential of token based incentivization of SSI services. The use of Blockchains is closely connected to tokens, the abstract representation of currency, utility, assets or potentially information about an identity. The tokenization of analog, digital, material or immaterial goods is a business case many startups have chosen. The use of tokens brings the benefits that they are easy to generate, safe to store and quick to transact.

However, the involvement of token-based incentive models and the market environments they create might bring potentially unwanted conflicts to the use of DIDs and DID Documents.

The well-known competitive attitude “every man for himself” has proven successful only from a perspective of a winner takes all competition (that is often seen in digital platform providers, leading to de facto monopolies that ultimately leave all participants worse off) in the provision of digital products and services. Taking the case of SSI, such a winner takes all mentality naturally rules out the concept of SSI. As a universal identity layer built on open standards, it can only succeed if we agree to leave its basic infrastructure building blocks open. While this might sound counterintuitive to some, the success factors of infrastructures like the internet and email are exactly that. The open nature of these networked infrastructures allowed for dynamic competition and innovation in the provision of products and services, while relying on a shared and open infrastructure. Looking at the success of these examples, we can start to imagine the potential of a universal and open identity infrastructure. The introduction of a token-based incentive scheme in this universal identity layer poses the risk of centralization and lock-in through token dependencies, a result that would significantly undermine the promise and potential of a universal identity layer.

While we do not want to rule out the token based incentivization of SSI services, we want to highlight that such models have to be developed with utmost caution in order to leverage the open potential of SSI rather than short term gains. The universal solutions for identity should provide a balanced scheme of incentives between all actors within the addressed ecosystem, without giving the initial issuer a power monopoly in the system. Such an open platform should allow an ecosystem of self-sovereignty without exploitation of a small group of early movers or investors but offer a shared benefit for all stakeholders instead.

While token systems could support the financial sustainability of SSI building blocks, they should not counteract its core capabilities of openness and absence of vendor lock-in.

Implications of different blockchain architectures

Linking back to the chapter on security, blockchain networks can be generally differentiated along two main dimensions (read/write access), public and private, as well as permissioned and permissionless. While there are different nuances to the permissioned and permissionless category in practice, the distinctions made in the following section hold true.

Before going into a quick outlook on the implications of these architectural decisions, we want to point out that the SSI infrastructure we describe in this position paper is not bound to any blockchain architecture in particular. While there are several blockchain networks that have been developed to cater to identity only, there is no technical limitation that rules out other types of blockchain infrastructure. Instead, the possibility to register and interact with interoperable self-sovereign identities in many different networks on the basis of the DID standard is one of the core capabilities of this identity approach.

When looking at self-sovereign identities promise that it is usable outside of one clearly distinguishable environment (such as a multinational organization), the need for public readability of such blockchains becomes apparent. Identifiers have to be registered publicly in order to enable the successful matching between two identities in the case of issuance and attestation and thus fulfil the role as a decentralised public key infrastructure for trust. Private blockchain networks might also facilitate the potential of DIDs, but those will only be of use for interactions happening inside of the private network, thus resembling the isolated structure that DIDs are built to overcome. The second dimension of permissionless vs. permissioned architecture does not offer an easy answer in the case of identity. Instead, deciding on whether to map identities on a permissionless or permissioned blockchain network depends on the identity use case, the regulatory environment and the respective governance model of the network.

Public and permissionless networks allow free access and provide users with the opportunity for everyone to freely join if they abide the opt-in rules, facilitated by the game theory mechanics which align the individual interests to follow the common health of the network. Such as with computing power for the consensus algorithm or joining the network with a node.

Public permissionless blockchains offer the potential of “social scalability”, which refers to the idea that public permissionless blockchains have no network limit and therefore offer the chance for every human being to become part of the network, while public permissionless blockchains have an intended bottleneck in onboarding new organisations. Despite the potential, scalability of public permissionless blockchains can be a challenge as the access to both read or write functionalities is not restricted. One suggested strategy against this scalability challenge is to facilitate public

permissioned networks that can employ different forms of consensus algorithms, as all actors of the network are known and trusted. This type of architecture requires a consortium of operators where the governance of the network is outsourced to the legal structure and politics of governing a consortium (of potentially hundreds and thousands of individual organizations).

Whether the built-in governance of (token economics) in public permissionless networks is trusted more than the one offered by a consortium running a public permissioned chain cannot be answered without a detailed assessment of the respective governance model and might be different for each individual use case. Ultimately, both architectural concepts should be targeted towards supplying SSI in accordance with the 10 principles of SSI and the W3C design goals²⁷

Zero Knowledge Proofs

In public blockchain networks all transactions are recorded on the public ledger. Its use as a decentralized public key infrastructure makes use of this very functionality, especially because these publicly visible interactions are stored in an immutable way with clear timestamping to proof the existence and date of creation for decentralised identifiers. This can have the consequence, that the whole history of an entity can be traced back by its transactions, once someone's identity is uncovered by a malicious actor. For this very reason, we argue for interaction specific (pairwise) identifiers that are designed to avoid correlation.

Still, the question remains on whether credentials that are connected to one identifier could be made available to another identifier without the reintroduction of said correlation risk. One approach to this technical challenge is the use of “Zero Knowledge Proofs”. Their use allows two different actors, the “prover” and the “verifier” to exchange the ownership of a piece of data, without actually revealing the data. The math, probability and cryptography behind this technology makes their application useful in for example allowing the verifier to prove the ownership of a credential to the verifier, such as a driving licence without revealing the identifier it has been initially issued to.

Current challenges to the wide application of ZKPs are, that they can be slow and expensive for proofers to process. While there are many ZKP variants, with a wide range of performance characteristics, they are still to be considered in early stages of development. Some identity solutions use ZKPs based on graph isomorphisms, and these are exceedingly fast in comparison with other ZKP variants. Furthermore, questions remain on the interoperability of ZKP based credential exchanges, as

²⁷ DID design goals by the World Wide Web Consortium, <https://w3c-ccg.github.io/did-spec/>

necessary standards for a universal applicability of zero knowledge proofs across implementations and technology suppliers are still lacking.

Appendix VI – Exemplary use cases

Based on the core functionalities of SSI described in chapter 3, the following use cases can be implemented:

Note: This preliminary list is to a large extent transcribed from the W3C document on verifiable claims use cases (currently in draft version) <https://www.w3.org/TR/verifiable-claims-use-cases/#dfn-claim>

Finance

Open a Bank Account

Today's requirements to open up a bank account are expensive in time and money. The user has to verify itself physically resulting in expensive processes. Stores with employees are needed. Especially for direct banks with no stores, this is a big factor. A SSI solution may disrupt the physical identification and may reduce the costs. Instead of physical presence for verification, the user will be able to use its already verified identity credentials for KYC and AML verification.

Reuse Know Your Customer (KYC) and Anti Money Laundering (AML) checks

The issuance of Verifiable Credentials on KYC and AML directly to the identity subject allows for on demand checks without the involvement of third parties, leading to a quicker process, as well as the ability to reuse that information for multiple interactions. This will further allow for the request of KYC/AML information in contexts where it is currently not feasible due to the associated cost.

Transfer Money

Similar to opening a bank account, KYC and AML checks are also required to send money, depending on the country the money is transferred to.

Reuse trusted credentials from the bank for other services

Credentials verified by your bank can be used for other services. One could provide a proof of bank account or liquidity without disclosing any further data.

Education

Digital Transcript

The university, college or school will be able to securely link a digital transcript to the corresponding identity. With this verified credential the identity subject can use it for applications and employers can easily verify its integrity.

Register for an online course and other e-learning

The identity holder will be able to register for different e-learning services in a secure way via that the utilization of Verifiable Credentials about her qualification to join the course. Services will be able to grade the performance and issue it as a Verifiable Credential to the identity holder. This grade can then again be used to get access to further education.

Provide verified student ID across domains

A SSI solution may help to get students benefits by utilizing verified credentials about enrollment, and other needed certificates. Depending on the university there are currently possibilities for faking the ID or the ID can be outdated and still be used. With SSI, student benefits can be fairly attributed with lower risk of faking and clear information about the validity of a credential, especially with regard to expiration dates.

Healthcare

Prescriptions

In the case of prescription drugs, the issuance of a prescription claim to the SSI of an identity subject would allow for trusted interaction with pharmacies, irrespective of the transaction online or offline. f

Insurance Claim

To provide an attested claim about existing and sufficient health insurance to a requester in a privacy preserving manner could be a great starting point to reduce the amount of health data that is exchanged unwillingly.

Sharing of Health Records (e.g. blood type)

With the introduction of SSI into the health-care industry, the Identity Owner would have the ability (and partial or full rights) to share his or her health records. The record issuer can set requirements and rules how data created and provided by them can be used by parties with the right permission to read health data.

Professional Credentials

- **Work licences (doctors, pharmacists, drivers, etc.)**

- An employee could easily hold verifiable credentials such as working permits and access rights to work facilities in the form of Verifiable Credentials, either issued by the employer or potentially by public bodies responsible for work permits and such.

- **Access right management (building/room access and digital access to programs, data, etc.)**

- Unlike current approaches to access right management, a SSI holder is enabled to carry fine-tuned access rights credentials in her identity wallet, allowing access to all types of facilities in a cryptographically secure way. Utilizing the building blocks of SSI, access could be managed for physical and digital systems, without the need to switch between identity providers.

- **Job application**

A prime example for Verified Credentials is the application to a new job. With the support of Verifiable Credentials, individuals could provide attested information to an employer, thereby reducing the risk of fake credentials in the application process. The potential to transfer this information without any identifiable information attached, and without reference to age, race, gender and the like, such privacy preserving application models could create a fairer employment situation based on qualification rather than bias.

State-issued (Legal) Identity

- **Access to E-Government services**

- Set up with a SSI and equipped with verified credentials about citizenship, tax information or residence, an identity subject can directly interact with e-government services in a frictionless and trusted way without the need to set up a separate and often cumbersome citizen identity/account in parallel to other identities used. Instead, all digital identity interaction is handled via the SSI wallet of the identity subject.

- **Voting**

Although currently in early stages, SSI systems could become a cornerstone of digital voting. At the current stage, utilizing such systems while guaranteeing the principles of democratic voting is still a challenge and further research and development in this field of application is very important.

- **Universal use of government issued credentials**

A core argument of SSI is the potential to directly provide State-issued credentials and certificates to citizens and businesses for further use in the private and public sector. Be it the driving licence, passport or proof of residence, SSI enables the direct interaction between government services and citizens without the dependency on a third-party platform.

Appendix VII – Pilot Projects and Proof of Concepts

The provided list of pilot projects and proof of concepts is only preliminary, as the number of projects grows quickly.

TheOrgBook (British Columbia - Canada)

The Province of British Columbia is currently collaborating with the Province of Ontario and the Canadian Federal Government to provide verified digital claims about businesses. The Verified Organization Network²⁸ is an initiative by the government of British Columbia to create a trusted network of organizational data. It allows organizations to claim credentials that are part of their own digital identity, using a component called TheOrgBook²⁹ that lists entities with their associated public verifiable claims. In this project businesses and their representatives are given access to streamlined government services and digital transactions in the broader economy. Areas of application could be incorporation of a new business, establishing a business licence and associated permits, as well as opening bank accounts.

TrustNet (Finland)

TrustNet³⁰ is a heavily industry-networked research project that focuses on developing a blockchain-based distributed environment for personal data management following the MyData principles. Such an environment is the cornerstone for functional personal data markets as it allows individuals to control the flow of their personal data across companies and industries and creates the foundational building blocks for creating new personal data-centric services.

Alastria (Spain)

Alastria³¹ is a non-profit consortium building a national blockchain ecosystem for Spain. The security and veracity of information will be ensured through the identification of natural and legal persons, while at the same time allowing citizens to have control over their personal information in a transparent way following the guidelines set by the European Union.

²⁸ <https://github.com/bcgov/von> accessed 30 September 2018

²⁹ <https://github.com/bcgov/theorgbook> accessed 30 September 2018

³⁰ <http://trustnet.fi/> accessed 30 September 2018

³¹ <https://alastria.io/#1> accessed 30 September 2018

Illinois blockchain initiative (United States of America)

The Illinois Blockchain Initiative³² is partnering with Evernym to develop a birth registry pilot, where self-sovereign identities are created, and government agencies issue "verifiable claims" for birth registration attributes such as legal name, date of birth, sex or blood type.

Blockchain on the Move (Antwerp, Belgium)

As a cooperation project between the city of Antwerp, the Flemish Information Agency, Digipolis and the Flemish ICT organization (V-ICT-OR), the project Blockchain on the Move is a pilot project on SSI and its application on the municipal level. It explores the potential of SSI for e-Government use cases and State-issued credentials for private sector B2B and B2C use cases.

City of Zug (UPort and ti&m)

As a first pilot project in Switzerland, the city of Zug is currently piloting a SSI solution. The local administration is cooperating with the IT consulting company ti&m, as well as UPort to provide a basic infrastructure for their citizens to attest their identity. With the SSI implemented in Zug, users can now pay their parking fees, register for elections or perform online sign on for e-government services³³. The benefits range for the city of Zug are low infrastructure requirements, decreased security risks, cost effectiveness, GDPR compliance and scalability.

Danube Tech (Austria)

In a SSI proof-of-concept during the first half of 2018, 3 banks, an insurance company, the Austrian Post, and an institution representing notaries has cooperated to implement a range of use cases based on DIDs, Verifiable Credentials, Sovrin, and the XDI protocol. The use cases included:

- digital ID onboarding for existing clients,
- SSO for new clients,
- sharing of KYC data between organizations,
- dynamic data verification (change-of-address),
- secure communication (e-mail with ID confirmation),
- change of identity service providers,
- personal ID verification in a peer-to-peer marketplace

³² <https://illinoisblockchain.tech/> accessed 30 September 2018

³³ <https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702> accessed 30 September 2018

Given the success of the PoCs, the consortium is onboarding new companies and will enter into a second phase in late 2018. Danube Tech is also licensing their technology to a consortium of banks in the US and is planning PoCs with other companies.