Fraunhofer
FIT

FRAUNHOFER INSTITUTE FOR APPLIED INFORMATION TECHNOLOGY FIT

Self-Sovereign Identity

Foundations, Applications, and Potentials of Portable Digital Identities

Project Group Business & Information Systems Engineering

Self-Sovereign Identity

Foundations, Applications, and Potentials of Portable Digital Identities

Authors

Prof. Dr. Jens Strüker, Prof. Dr. Nils Urbach, Tobias Guggenberger, Jonathan Lautenschlager, Nicolas Ruhland, Vincent Schlatt, Johannes Sedlmeir, Jens-Christian Stoetzer, Fabiane Völter

The Project Group Business & Information Systems Engineering of the Fraunhofer FIT combines finance and information management research areas in Augsburg and Bayreuth. The expertise at the interface of financial management, information management, and business informatics, and the ability to combine methodical know-how at the highest scientific level with a customer-, target- and solution-oriented approach are its special features.

Fraunhofer Institute for Applied Information Technology FIT

Project Group Business & Information Systems Engineering

Wittelsbacherring 10

95444 Bayreuth

Acknowledgments

We want to thank our colleagues Dr. Jannik Lockl, Benjamin Schellinger, and Jonathan Schmid for their active support in preparing this white paper. Furthermore, we want to thank our colleagues Martin Brennecke, Jan Stramm, and Anna Walter for the translation of this paper.

Disclaimer

This white paper has been prepared by the Fraunhofer Institute for Applied Information Technology FIT to the best of its knowledge and belief, using professional diligence. The original form was published in German with the title "Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten" by the same authors is and is available at https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Fraunhofer%20FIT_SSI_Whitepaper.pdf.

Fraunhofer FIT, its legal representatives and/or vicarious agents do not guarantee that the contents of this white paper are secure, completely usable for specific purposes or otherwise free of errors. The use of this white Paper is entirely at the user's own risk.

In no event shall Fraunhofer FIT, its legal representatives and/or agents be liable for any damages whatsoever, whether direct or indirect, arising out of or in connection with the use of this white Paper.

Recommended citation

Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Völter, F. (2021): Self-Sovereign Identity - Foundations, applications, and potentials of portable digital identities. Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Bayreuth.

Image sources

© https://stock.adobe.com/de/

Table of contents

Decentralized identity management enables interoperable and secure digital identities for people, organisations, and machines.

Preface of the editors

Within the last decades, our world has changed even faster and more fundamentally than before due to technical progress. Digital technologies influence many areas of our social life. At the same time, privacy and security issues in the digital environment are constantly coming to the foreground. These aspects have become increasingly important, especially regarding the use of personal data on the internet. The unauthorized forwarding of user data or so-called data breaches resulting from carelessness or cyber-attacks have repeatedly demonstrated the vulnerabilities of today's handling of sensitive data. Our personal data characterize our own digital identity and thus the way we use services on the internet. At the same time, managing the numerous accounts of internet users with different passwords and, if necessary, the technical implementation of additional mechanisms for multi-factor authentication is becoming increasingly complicated and inefficient.

Ensuring the smooth digital interaction with customers and managing employee access and authorizations has become a considerable challenge for companies. This challenge arises from the present centralized approach to managing digital identities and the personal data of internet users. Such an approach has several disadvantages for users, including portability restrictions or the far-reaching transparency of the digital identity towards centralized identity providers. One example of this are single sign-on (SSO) procedures, which are offered by social networks, among others. The related services are convenient, but user activities are entirely transparent to identity providers, and there is only limited portability of the digital identity. While for private individuals, the use of such services is only a trade-off between convenience and privacy, companies' fears of becoming dependent on a dominant market player through such identity management systems prevail, as they are often of strategic relevance to their long-term economic success. At the same time, cross-company collaboration in identity management is increasingly important for service providers who aim to offer their customers a high degree of flexibility. In stark contrast to these requirements, existing identity management systems are hardly interoperable. Platform-based solutions either have acceptance problems due to their hierarchical structures or face massive regulatory challenges, for instance, related to data protection.

Through the further development of cryptographic procedures in combination with blockchain technology, a new paradigm has been able to gain attention in recent years that could remedy significant disadvantages of established digital identity management. The concept of these portable, user-controlled self-sovereign identities envisages that users themselves can determine their domain-spanning digital identities. Self-sovereign identities can receive verifiable proofs of properties and authorizations and easily use them in different interactions across domains utilizing interoperable standards. Moreover, self-sovereign identities apply to individuals and companies or networked objects on the Internet of Things. This results in a broad field of applications in which SSI can unleash a tremendous economic potential by increasing the security and efficiency of processes.

This white paper outlines the most important conceptual and technical foundations of self-sovereign identities before presenting some use cases in detail. Subsequently, we will take a closer look at both the economic potential and the challenges of self-sovereign identities. We hope you enjoy reading this white paper and invite all readers to enter a dialogue with us. We are available for questions, discussions, and suggestions.

© Hochschule Fresenius/ John M. John

Prof. Dr. Jens Strüker

Professor for Business Information Systems and Digital Energy Management

University of Bayreuth

Project Group Business & Information Systems Engineering

© Björn Seitz – kontender.Fotografie

Prof. Dr. Nils Urbach

Professor of Information Systems, Digital Business and Mobility

Frankfurt University of Applied Sciences

Project Group Business & Information Systems Engineering

Glossary

AML	Anti-Money Laundering
CA	Certificate Authority
DID	Decentralized Identifier
DKMS	Decentralized Key Management System
DLT	Distributed Ledger Technology
GDPR	General Data Protection Regulation
ESSIF	European Self-Sovereign Identity Framework
EU	European Union
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
JSON	JavaScript Object Notation
KYC	Know-Your-Customer
SSI	Self-Sovereign Identity
SSO	Single Sign-On
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
VC	Verifiable Credential
VID	Vehicle Identity
VIN	Vehicle Identification Number
VP	Verifiable Presentation
ZKP	Zero-Knowledge Proof

1 Introduction

Introduction

The spread of the internet has led to profound changes in many areas of society. The internet makes it possible to use various digital services, such as researching information, ordering clothes and food, and communicating with friends and work colleagues via social networks. Since the early 1990s, a central challenge in using the internet has been managing one's digital identity. When communicating via the internet, it is complicated to prove one's identity or related attributes (e.g., age, place of residence, and others). The cartoon "On the Internet, nobody knows you're a dog" by Peter Steiner describes this central problem as early as 1993 - a few years after the invention of the World Wide Web.

In contrast to the status quo of identity management on the internet, identities in the paper-based world are almost always verifiable by official or non-official documents such as an ID or a customer card. Usually, these documents are designed to be copy- and forgery-proof to a certain degree. Thus, a particular person can prove that they bear a certain name or have a certain age. In this respect, in the analog world, every user can have complete control over their identity documents and other proofs without asking a third-party or the issuer of these documents for their permission. This makes identity management in the analog world "self-sovereign". For example, our analog ID card is based on this same self-sovereign concept to a certain extent. Specifically, the presentation of an ID card offers interoperability and security because it is internationally recognized and standardized in its form. This means that almost any party who trusts the German administration can verify an ID card issued by the Federal Government simply by verifying it, without asking any authority or the like for permission. Furthermore, users' personal data is protected by this construction, as data is stored on the ID card, which is only in the wallet of the ID card owner and is not additionally stored in the form of copies in numerous other places. Interoperability is also widely used in the business-to-business sector, for example, in credit cards, which many companies accept without the need for cross-company identity management.

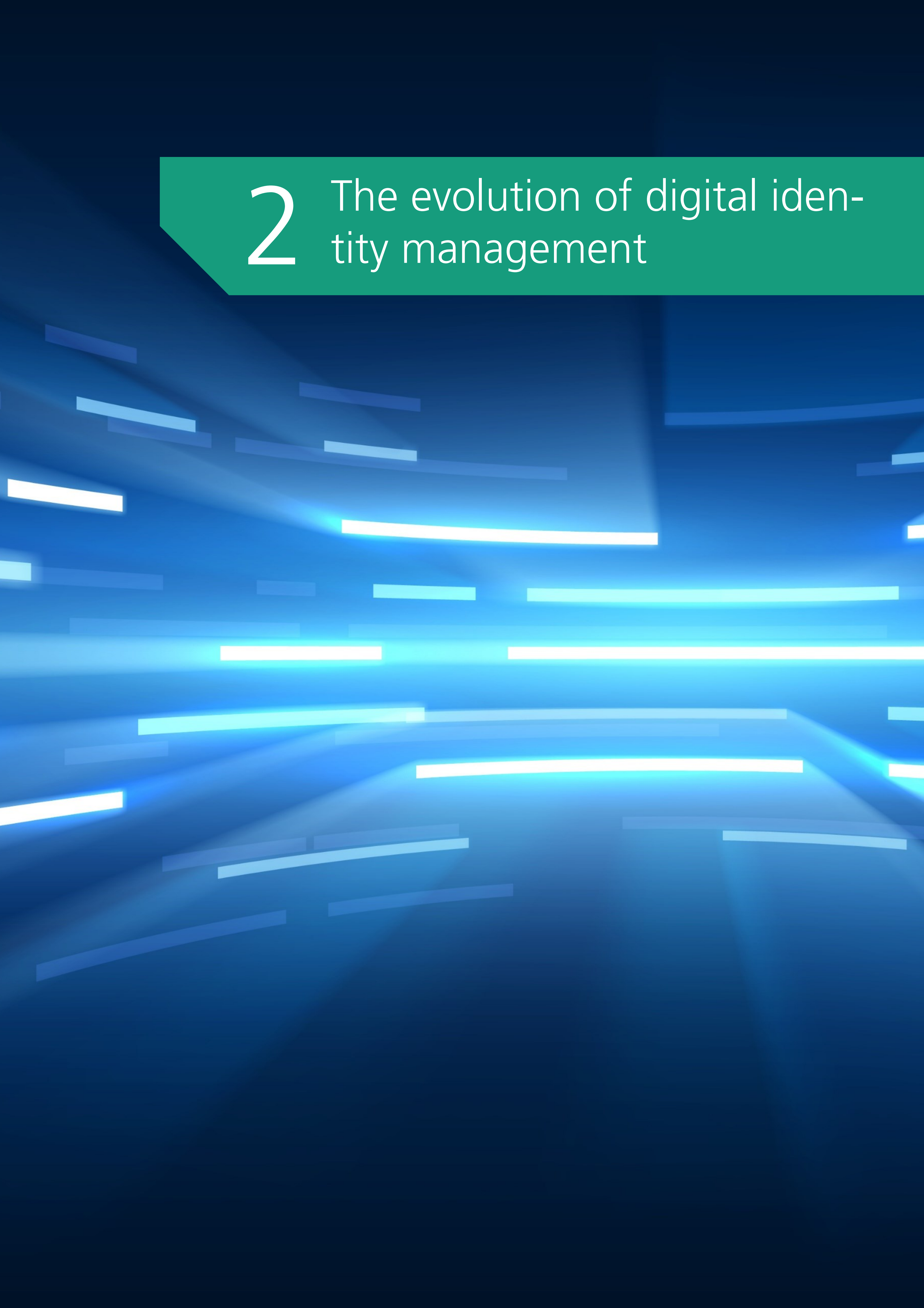
The use of such physical, relatively forgery-proof documents that are issued by trustworthy authorities and that can be easily verified by many users is not established in this form in the digital world today. Instead, identity management on the internet corresponds to a kind of "patchwork". As a result, users usually have numerous accounts with different service providers that they must manage and where they hardly have any options to use attributes that have been confirmed once - such as a driving license with a car-sharing provider or valid bank details with an e-commerce store - in other contexts. SSO services such as Facebook or Google can remedy this to a certain extent and create interoperability, but this is at the expense of data sovereignty and privacy and gives these companies a great deal of information and market dominance. All in all, users today must decide between the dimensions of interoperability, security, and data protection. They do not have a digital identity that is self-sovereign like their analog identity.

In recent years, various technical and conceptual approaches have tried to establish solutions for proving identities in the digital world that address this lack of privacy, interoperability, and security. Technical advances in cryptography and decentralized data storage have led to the novel concept of digital self-sovereign identity (SSI), which aims to solve the problems of previous identity management systems and offers new advantages for users. The role model for this is always how attributes and authorizations can be proven in the non-digital world with the help of "plastic cards" to third parties who trust the issuer of the corresponding "plastic cards".

Several consortia and initiatives are working on the SSI concept and its implementations worldwide, especially in North America and Europe. As a result, numerous documentations and studies on pilot projects and publications in scientific journals have already been published. Standard and open-source applications that bilaterally exchange digital equivalents of these "plastic cards" between universal smartphone apps and applications are currently developing quickly and have a growing developer community. Therefore, this white paper aims to compile essential information on identity management according to the SSI paradigm in a compact form to provide the audience with a broad overview of the current state of research, technical developments, and practical potential on this topic.

Self-Sovereign Identity is the next development stage of digital identity management.

2 The evolution of digital identity management



The evolution of digital identity management

Interoperable digital identity management is becoming increasingly relevant

A person's identity - whether analog or digital - consists of several partial identities. One or more partial identities can be used, for example, for work, leisure, Internet services, or going to the supermarket. Each partial identity contains information that can overlap with other partial identities, although it does not necessarily have to (see figure 1). In this context, the same information does not always have to be used. For example, a person's real name on a website can be replaced by a pseudonym. These partial identities are used continuously in everyday life and require the digital identity's portability, interoperability with different systems, and the self-determined management of the partial identities by the user. In turn, these partial identities have several attributes, e.g., name, address, qualifications, and others, in working life. Some of these partial identities uniquely identify a person, while others do not. Depending on the specific context and situation, a person can be represented by different partial identities (Clauß & Köhntopp, 2001).

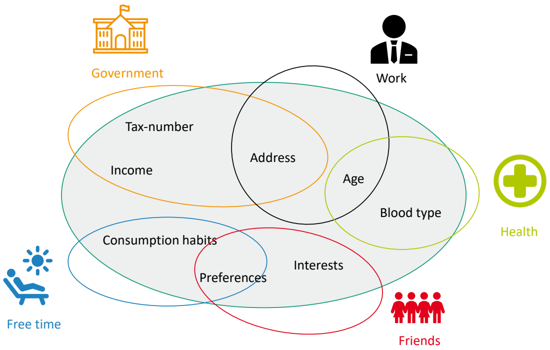


Figure 1: Partial identities (based on Clauß and Köhntopp 2001)

Challenges for identity management in the digital age

Identity management is becoming increasingly important in the digital age due to the sharp rise in digital interactions. Physical systems cannot be transferred to the digital world or only to a limited extent. Nevertheless, it is crucial to transfer the advantages of physical identity management systems into a digital equivalent. A digital identity management system describes a digital system through which users can determine their identity shared with third parties (Clauß & Köhntopp, 2001). In the analog world, identity is often established utilizing a physical object (e.g., identity card, driver's license, or passport). This is not readily possible in the digital world today. A physical identity document is traditionally protected against misuse by features and photos that are almost impossible to forge (Tönsing, 2015). In contrast, a user’s identity on the Internet is traditionally managed by creating numerous domain-specific user accounts, usually accessible by combining a username and a password. In the best-case scenario, this combination should be different for every account on the Internet, but this is often not the case in practice. On average, an Internet user has 25 accounts, for which individual rules may apply for creating the username/password combination. For reasons of convenience, password management is often not security compliant. For example, only six to seven different passwords are distributed among the 25 accounts on average (Tönsing, 2015). Compromising a single password often enables access to several services at the same time. This significantly increases the risks for possible misuse of the identity by third-party actors. On the other hand, the use of different passwords leads to rapidly increasing complexity in the management of access since either special password managers or notes have to be used to remember the individual passwords. This results in either a high level of effort on the users’ side or high sensitivity to attacks and the associated security risks. Moreover, the identity-related data stored by online services cannot be (re)used across multiple domains in most cases. This implies the need for costly and time-consuming recurring registrations with different service providers. In today's digital, account-based identity management, the identity of users, therefore, relates only to the specific context of the corresponding application. The data and information used there are mostly not usable or meaningless outside this specific context (Tobin & Reed, 2017)and cannot be (re)used across domains.

Development stages of digital identity management

Currently, there are various types of identity management in the digital world. Centralized identities, user-oriented identities, federated identities, and self-sovereign identities (Allen, 2016), as illustrated in figure 2, can be highlighted:

(1) Centralized identity

A centralized identity is managed at the system level by entities, such as administrators. The user's identity therefore depends on these entities. Deleting the identity is only possible through the respective entity, which is difficult for users to monitor and poses a risk of misuse. Furthermore, the dependence on a centralized entity often results in a lack of interoperability. As a result, the user's identity must also be recreated for another service since it cannot be transferred without further ado. In addition, user interactions become transparent for the centralized entity. Furthermore, data storage is inevitably redundant for different services requiring the same information, but the data is not synchronized and can quickly become outdated.

(2) User-oriented identity

To counteract the disadvantages of a centralized identity, the concept of a user-oriented identity was developed. Users manage their access to various services (and thus partial identities) themselves. However, the multiple uses of passwords and the difficulty to transfer account information to other services create security risks and a lack of user-friendliness. Identity attributes (e.g., a driver's license) must be repeatedly proven for each service individually. A local application for storing and managing access data for different services enables users to access different services with a single password (or authentication step). However, the data about attributes of their partial identities remain stored with the respective provider. Therefore, they can also be passed on between different web services (Allen, 2016; Tobin & Reed, 2017).

(3) Federated identity

Federated identity management represents a further development stage of a digital identity. A central log-in instance (online or offline) enables users to share their partial identities with other providers. This principle is known as SSO and is offered primarily by companies and social networks like Facebook and Google. Using the SSO of an identity provider, users can transfer their identity from one provider to another by simply pushing a button. The transfer of data always requires access to the central log-in service. The disadvantage from the user's point of view is the high degree of dependence on the log-in service as the identity provider. The central log-in service serves as the cryptographic key to all partial identities and can always track which services users access with their partial identities. In addition, the risk of misuse of the identity increases if the access data to the central login service is passed on to third parties. Therefore, access to a service could also give access to all associated partial identities. In summary, it can be said that existing approaches to managing digital identities have various disadvantages, such as a lack of interoperability or dependence on certain parties. So far, no broadly deployed system has managed to address all the problems of current identity management systems and users' needs.

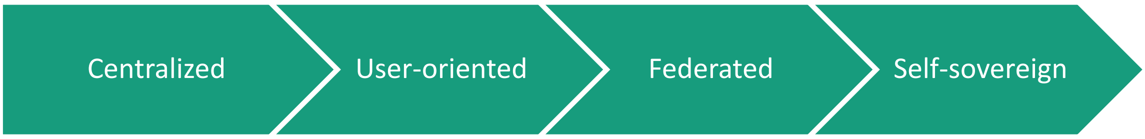


Figure 2: Development of digital identities

The evolution of digital identity management

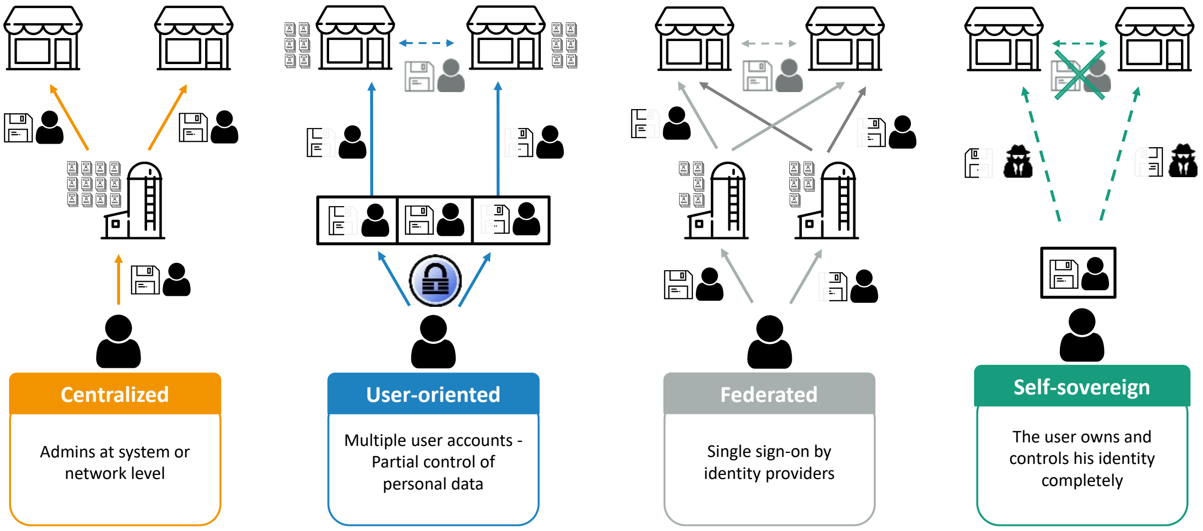

Centralized
Admins at system or network level
User-oriented
Multiple user accounts - Partial control of personal data
Federated
Single sign-on by identity providers
Self-sovereign
The user owns and controls his identity completely

Figure 3: Comparison of different identity management systems

Self-Sovereign Identity as a new paradigm in identity management

Based on the challenges described in the previous chapter, the paradigm of SSI has evolved in recent years. SSI is intended to solve the challenges and problems of existing digital identity management systems and is considered to be the next evolutionary stage of digital identities. However, there is still no uniform understanding and no generally accepted definition of the term (Mühle, Grüner, Gayvoronskaya, & Meinel, 2018). Tobin and Reed (2017) define SSI as the final stage in the development of digital identities. This is intended to ensure individual control, security, and the full portability of digital identities across different services. Allen (2016) considers users as the central administrators of their identity, including all existing partial identities. Therefore, it must be possible for users to maintain control over their identity across all different services and thus to achieve autonomy in managing these services. It follows that an SSI must be interoperable and portable. Users must be able to make assertions about their identity that become verifiable attributes through third-party confirmation. Third parties must also be able to add attributes to an identity that the user can confirm. The basic principle of SSI compared to other identity management systems is illustrated in figure 3. The differentiation from other identity management systems is clarified by the ten principles of SSI (Allen, 2016), which are listed in table 1.

Allen's principles are based on the work of Cameron (2005), who outlined the basic conditions for successful digital identity management systems. Allen (2016) defined the ten principles of SSI as a response to the drawbacks of previous digital identity management systems but did not describe a specific technical solution. Therefore, we first present the principle of SSI in a technology-neutral manner.

The evolution of digital identity management

Controllability	Existence	Users must be able to have an independent digital identity.
	Control	Users of SSI must have full authority and control over their identity. This must be achieved through secure and well-researched algorithms, giving all users the ability to set their privacy preferences as they wish.
	Consent	Users must always consent to the use of their identity by an entity. Because identity management relies on sharing information with entities, user consent is required to share data.
	Access	Users must be able to access all aspects of their identity, even if other entities manage individual sub-identities.
Portability	Transparency	Any implementation of SSI must provide sufficient transparency in its systems and algorithms. The system should be available to all, usable, and investigable through open-source code to establish trust in the technology.
	Transferability	The information and data in an SSI must always be transferable. This ensures that identities are not lost and are always owned by the users when entities disappear over time or regulation and systems change.
	Interoperability	An SSI must be usable in as many application areas as possible and work independently of borders and existing systems.
Security	Minimization	Data disclosure must be minimized. Any (partial) identities must disclose as little data as possible, i.e., only as much as is necessary to accomplish the task. An example of this principle is the purchase of alcoholic beverages: users must prove that they have reached the legal minimum age for purchase but should not need to disclose their exact birth date.
	Protection	Users' rights must be protected in every case of use; if the needs of the network conflict with the users' rights, the users' rights should be weighted higher.
	Longevity	The individual identities managed by the SSI must be usable for as long as the users wish. Even if the underlying algorithms may change, the information and thus the identity must remain untouched in the best case. However, at the same time, there is a compelling need for the right to be forgotten. Therefore, the SSI must ensure that users can delete their identity and thus revoke the previously granted rights for identity information by third parties.

Table 1: Ten principles of SSI (Allen, 2016)

3 Technical foundations of Self-Sovereign Identity

Technical foundations

The ten principles of SSI act as a catalog of requirements for the implementation of an SSI solution. Therefore, in addition to the ten principles of SSI, it is necessary to understand how an SSI solution can be implemented technically. This makes it possible to understand which of the basic components of SSI can be implemented with already known technologies and, in combination, can form an SSI solution. Therefore, we now illustrate the functionalities of the individual basic components and the key technologies involved.

Basic components: The elementary building blocks of an SSI System

The components of an SSI solution, which in combination form the foundation of an SSI architecture, can be divided into five main artifacts: Verifiable Credentials (VCs), Roles (Issuer, Holder, and Verifier), Identifiers, Digital Wallets, Agents and Hubs.

The central building blocks of any SSI solution are digital certificates. They can either contain self-attested identity attributes or those attested by third parties. Attested credentials are defined as VCs (1), for which a standard already exists that specifies the structure of such a certificate. Furthermore, VCs form the central artifacts for proving identity attributes between the central roles of an SSI solution (2). These roles form the basic framework of interaction within the issuer-holder-verifier relationship. Each VC is created by an issuer. The holder stores and controls the VC and can selectively present the information contained to a verifier.

The DID standard (3) enables the parties to provide end-to-end encrypted bilateral communication on different infrastructures to ensure the most secure communication possible and protect privacy. In contrast to current encrypted communication protocols such as HTTPS, i.e., Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS), where at least one of the communication parties requires an SSL certificate issued by a Certificate Authority (CA), the DIDComm standard enables end-to-end encrypted communication even without this certification and is thus less dependent on CAs. The individual VCs and cryptographic keys are stored in digital wallets (4). Agents and hubs (5) are needed as technical endpoints and custodians for the identifier in this context and as points of connection for bilateral communication. They ensure the protected communication between individual identities and should be accessible permanently, analogous to e-mail servers. These five basic building blocks (1-5, see table 2) make up the core conceptual architecture of an SSI solution and are therefore explained in detail below.

(1) Verifiable Credentials	Standard for SSI architectures Digitally signed collection of attributes
(2) Roles (issuer, holder, verifier)	Protagonists of the SSI solution (are related to each other)
(3) Decentralized Identifiers (DID)	Standard that allows self-certified identifiers to be used for end-to-end encrypted communication (privacy protection, anonymization)
(4) Digital Wallets	Software to store private keys, VCs and, if applicable, DID documents for the holder
(5) Digital Agents and Hubs	Technical endpoints and custodians for identifiers (ensure communication between identities)

Table 2: Building blocks of the SSI concept

Verifiable credentials

Digital certificates are subject to the trust relationship of a party to a third, neutral authority. Specifically, in current implementations of certificate management, users must trust one or more CAs (Goodell & Aste, 2019). CAs assign certain properties to an identity using a digitally signed certificate. In principle, any trusted party can assume the role of CA. In this context, various organizations exist that are exclusively concerned with issuing certificates. Nonetheless, there are also approaches in which organizations issue certificates themselves and make them verifiable utilizing overarching infrastructures in their own domain. This prevents the emergence of far-reaching ecosystems of parties issuing identity certificates and inhibits portability and interoperability.

It is also problematic that two parties wanting to communicate securely with each other, are generally dependent on the integrity of the corresponding CAs: The system is subject to the assumption that CAs are always trustworthy and will not be compromised. The CA is thus the single point of failure that leaves the system vulnerable to corrupt operators and inadequate security measures (Goodell & Aste, 2019). In addition, certification by a CA involves time and cost and can, thus, make the process cumbersome. Using VCs, CAs no longer occupy such a central role in an SSI architecture (McKenna, Reed, Schneider, & Tobin, 2020). This is primarily because VCs used in self-sovereign identity management allow the coupling of identifiers and public keys (which can be done cryptographically or by public self-attestation) separately from the coupling of attributes to identifiers (which is usually done by issuing certificates by trusted institutions). Architectures in which identity management is self-managed by organizations in a public registry as an alternative to CAs often lever a blockchain or distributed ledger.

Definition: Verifiable Credentials

In the context of identity management, identity is the representation of an entity in a specific context. On one hand, it consists of identifiers that uniquely identify an organization, an object, or a person. On the other hand, it consists of the entity's attributes, such as an authorization or demographic data. Together, these components form the "digital plastic card" described above.

These attributes serve the purpose of being verifiable to third parties. The more sensitive the attributes are, the more important it is to ensure the data sovereignty of the respective entity. To create far-reaching ecosystems of digital identity management, it must also be possible for organizations to certify attributes for entities and issue corresponding credentials for verification. Verification of these credentials must be possible for third-party actors in a secure, efficient, and clearly defined manner. Specifically, this implies the need for a holistic trust relationship between actors and CAs, and a guarantee for user privacy in functional interoperable systems.

The W3C consortium standardizes VCs intending to establish digital trust to reconcile users' privacy with the advantages of digital certificates. VCs allow for a verifiable digital exchange of credentials and properties over any communication channel, e.g., classic TLS, which is distinct from DIDs. DIDs enable the creation of a secure bilateral communication channel and provide an end-to-end encrypted connection between the actors involved (e.g., verifier and prover) without being dependent on a CA. Additionally, aspects of usage authorization are also defined within the framework of a DID - e.g., for modifying information or claiming control. Ultimately, the main difference compared to X.509 certificates is the splitting of purposes: VCs pursue the establishment of digital trust, while DIDs create a secure communication channel for the same purpose.

For the standardized use of digital certificates, digital signatures are currently implemented, for example, applying the widely used X.509 standard or the JWS standard (JSON Web Signature Standard). Both standards make it possible to prove the integrity of information in a highly serialized and machine-readable format. On the other hand, VCs often use the JSON-LD extension (JSON-based serialization for linked data) in conjunction with established or new signature procedures to guarantee forgery-proof VCs - "digital plastic cards". Thus, they certify that a signed VC is information that has not changed since it was signed. The implementation using JSON-LD additionally enables semantic interoperability (uniform semantics of the machine code) but still requires the careful investigation from a security perspective.

Choosing a suitable digital signature and the attributes presented in interaction typically represents a trade-off between authenticity and data protection. So-called zero-knowledge proofs (ZKPs) represent a more privacy-oriented solution. They enable selective and (apart from the attribute's value) uncorrectable proof of attributes confirmed in certificates utilizing advanced signature and verification protocols. In addition, interoperability also requires "open" access to revocation states, which only works to a limited extent with current X.509 certificates.

However, from a purely technical point of view, the interoperability of systems on a protocol layer does not necessarily imply that identity management will work at scale across domains. Large companies often use many software applications and highly standardized procedures for federated identity management, such as Open ID Connect. Nevertheless, the certificates issued have no meaning outside the respective domain because there is no cross-domain identity management for the respective organizations. Users can only use their "tokens" contextually.

The SSI paradigm attempts to solve these challenges. SSI follows a user-centric approach so that the sovereignty and control over identity data lie with their respective users. At the same time, users should be provided with a high degree of convenience for activities in the context of their digital identity. To implement such a user-centric approach, which does not require a third party, credentials must be designed securely and efficiently verified by third parties. However, this also means that standards must be created without an existing central authority. Only through uniform standardization can VCs become interoperable and do not have to be reissued for each context. Consequently, the international web content standardization community (W3C) has defined a standard that classifies digital credentials that conform to this concept as VCs (Sporny, Longley, & Chadwick, 2019). In addition, these VCs have various characteristics that are necessary for their technical functioning. These components and characteristics are presented below.

Components and characteristics of VCs

SSI is based on asymmetric cryptography (public-key cryptography) and key pairs (keys). The VC creator, referred to below as the issuer, creates a digital signature for the VC using their private key. This signature is attached to the VC, and anyone can use the issuer's public key to verify that the signature was calculated using the associated private key without ever having seen this private key. This process can be used to confirm the integrity of any given VC, provided the verifier is convinced that the issuer is keeping its private key secret.

For this purpose, a VC consists of a set of claims about the properties of an entity. VCs may also contain metadata describing properties of the VC, such as the issuer, the expiration date, a public key for verification purposes, or a revocation mechanism (Sporny et al., 2019). In addition, the use of a public key to sign VCs can cryptographically prove who issued the VC and what the contents of the VC were when it was issued. The typical contents of a VC are shown in figure 4.

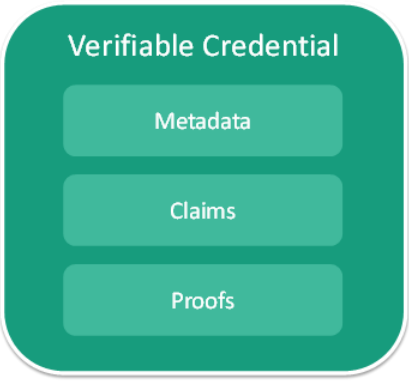


Figure 4: Components of a VC

Various properties characterize VCs. The most important ones are explained in more detail below:

(1) Privacy characteristic

One of the central goals of the SSI architecture is to protect personal information and to reveal only as much data about the subject of the VC as is necessary. For example, at the entrance of a discotheque, the security guard does not need to know the entire content of an ID card; two pieces of information would be enough: proof that the party guest is the certificate's subject (in this case shown by the photo in the ID document, the eye color and body size), and proof that the guest is at least 18 years old. This minimization of personal data transmitted is difficult to achieve with a physical ID card, but possible using an SSI architecture: The SSI architecture enables the cross-domain exchange of verifiable data between verifier and holder without the issuer's involvement in the interaction. This alone creates added value for efficiency (repeated and highly automated use of existing certificates) and privacy (the issuer does not experience every interaction, in contrast to federated identity management, where the identity provider can be regarded as issuer and holder of an identity certificate that is universal within the domain).

The information contained can be verified for authenticity using signature procedures. This is made possible by ZKPs, which can be used, for example, to demonstrate that a person is older than 18 years without revealing the date of birth.

(2) Characteristic of (active) proof of eligibility

However, VCs have the characteristic that they only ever represent an "active" credential. Thus, VCs can never restrict users in their actions but must enable freedoms or benefits for the credential subject. For example, it is easy to prove that one is a club member as a private person using a verified club membership. However, it is difficult or impossible to prove that a private person is not a member of an association. Specifically, certificates cannot be used to prove that a particular characteristic (e.g., membership of an association) does not exist, as holders cannot be forced to present the corresponding certificates from their digital wallet (Tobin, 2019).

(3) Characteristic of standardization

For the uniform use of VCs, all parties must agree on the structure of the VC, which makes the standardization of VCs a crucial foundation for their adoption. Further, all parties must also understand what each specific VC should look like. Only if all participants perform their calculations based on the same structure, consensus on the v of the VC’s validity can be reached. For this reason, a standardized credential scheme is referenced in each VC, if possible, which specifies how such a VC must be structured. The schema should be accessible to all parties, ensuring the VC's usability across domains. Accordingly, the advantage of complete access by all parties is increased interoperability (Hardman, 2019b).

(4) Characteristic of authentication

Each VC must be uniquely tied to a person, organization, animal, or object. However, for the holder to later appear under different pseudonyms, the VC must be bound to the subject as a whole, not just to the pseudonym by which the subject of identity is known. Cryptographic methods make it possible to link the control of credentials to a secret known only to the owner, the link secret (often also called the master key). Similar to a private key, it is a randomly generated number that always remains secret. It links different digital certificates to each other and thus to a person without disclosing a correlatable identifier.

In summary, VCs consist of a series of provable attributes that are cryptographically signed and can be interpreted and verified based on VC schemes (Sporny et al., 2019).

Roles in an SSI system: Issuer, holder, and verifier

VCs consist of individually provable claims that have been cryptographically signed and thus confirmed by a party. They also have a specific verifier, depending on the context. In the following, the roles that occur in the context of interactions with VCs are introduced and defined:

(1) Issuer

The issuer's role is assumed by trusted parties whose identity and, thus, public key are publicly

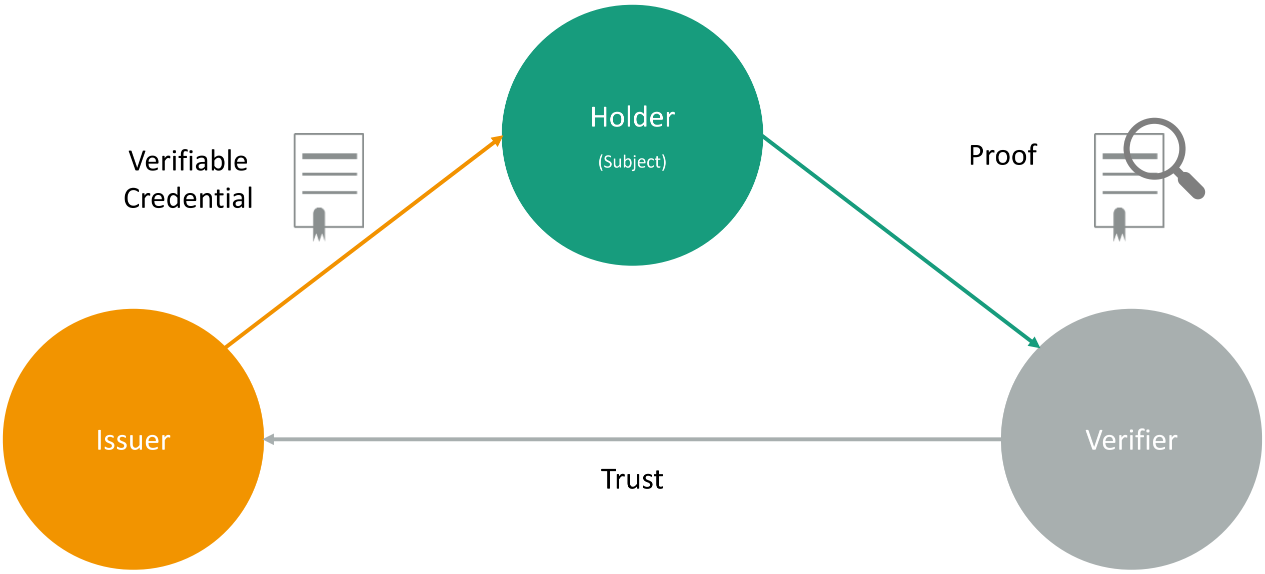


Figure 5: Roles in an SSI system

visible. Whether an issuer is trustworthy or not is evaluated by the respective verifier itself. An issuer can be a public institution such as a university. The issuer creates a VC that confirms the attributes of the respective identity holder, e.g., a university certificate. Finally, the issuer digitally signs the VC. The resulting digital documents are issued to holders, such as students, who are usually the subject of the VC, and store it in their digital wallet (Sporny et al., 2019).

(2) Holder

The holder is the owner who can assert claims based on acquired VCs. A VC's holder can be a human, an organization, or a smart device. In addition to these interacting parties, there is another role: the subject of the certificate. The certificate attests to an attribute of the subject. In SSI solutions, the holder is often the subject of the VC. However, the VC does not need be tied to the holder (Sporny et al., 2019). For example, a vehicle's registration certificate or MOT sticker is not tied to the vehicle owner but to the vehicle itself. Currently, few vehicles would be able to store and manage their VCs themselves in their digital wallet, but this may change in the future when vehicles become increasingly autonomous.

(3) Verifier

The verifier requests identity information or attributes from the respective holder. It receives this information in the form of a Verifiable Presentation (VP) based on one or more previously defined claims and proof of their correctness. The verifier uses this request, a so-called proof request, to determine which information must be proven. The proof request is a message to the holder that describes the claims to be verified and corresponding conditions that the holder must fulfill (Nauta & Joosten, 2019). This typically includes, for example, proof of the validity (non-revocation, non-expiration) of the VCs at a certain point in time or the identity (public key) of the issuing organization.

To illustrate, consider the following example:

A holder wishes to create a new bank account. When opening a bank account, the bank requires their customer's full name and other personal information to open the account. Thus, the bank requests the required information from the holder using a proof request. Now acting as a prover, the holder can accept the requests and transmit the associated VP to the verifier.

For comparison, the example of entering a club only requires a link-secret reference, which guarantees a higher degree of privacy through the ZKP. Ultimately, the verifier must issue a proof request for authentication that is appropriate for the use case. A verifier can be a police officer, a website where the holder wants to log in, or even the security staff of a given club. The important aspects are that the verifier knows the identity of the issuer, trusts the issuer, and acknowledges the issuer's authority to issue such a certificate.In the VP, the verifier does not actively communicate with the issuer. The cryptographic signature allows to check whether the certificate has been forged without direct contact with the issuer (Sporny et al., 2019).[1] Only the issuer's signature public key must be known to the verifier.

In summary, SSI's interacting roles can be described as follows:

(1) The issuer issues the VC with the attributes specified in the Credential scheme.
(2) The holder/prover manages the VC and presents it to the verifier in the context of the VP.
(3) The verifier checks that the attributes of the VC are correct and meet specific requirements.

These three roles constantly interact with each other in SSI systems and are called the Trust Triangle. Both issuer and holder as well as holder and verifier are in direct exchange during the lifecycle of a VC. There is not necessarily a direct information exchange taking place between the issuer and the verifier at the time of the VP. Still, there is a relationship of trust between the verifier and the issuer. This scheme is illustrated in figure 5.

For clarity, consider the following example: In federated identity structures, where identity providers manage the users' identities, one identity provider simultaneously assumes the role of the issuer and the holder. The users who want to log in to a website are only the subject of the

[1] This is also the case with the X.509 certificate but SSI solutions do not require a third party (CA) with which a mutual trust relationship must exist.

certificate, not the holder. The users ask the identity provider to make the data available to a website but are entirely dependent on the identity provider. The website is a verifier in this construct, but it must also have registered with the identity provider beforehand and trust it.

SSI solutions seek to combine the ease of using a federated architecture with a user-centric approach in a new architecture.

Decentralized identifiers

To design interoperable SSI solutions between identity holders, a standard has been defined that uniquely assigns identities to so-called DIDs. A DID is a Universally Unique Identifier (UUID) with specific properties and thus enables the DID controller to mark its information in a universally applicable way.

DIDs are a new type of identifier that provides a verifiable, decentralized digital identity. A DID identifies an arbitrary subject (e.g., a person, an organization, a thing, a data model, etc.) whose identification is decided by the controller of the DID (Reed et al., 2020). A DID consists of the URL scheme DID, followed by a DID method and a DID method-specific identifier (see figure 6).

DIDs are used to identify participants. Users can have any number of different DIDs because a separate DID could map each interaction. This diversity allows the privacy of individual users to be protected since each individual DID opens up a separate communication channel (Reed et al., 2020).

A DID resolver (see figure 7) executes a DID resolution function that takes a DID as input and returns a so-called DID document. DID documents

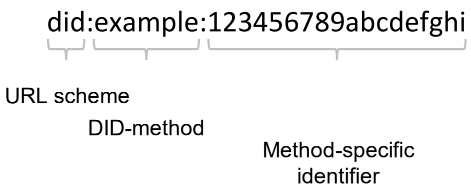


Figure 6: Components of a DID

specify how to interact with the DID subject. The subject is the respective participants identified by the DID and described by the DID document. Each DID document references exactly one DID. In contrast, participants who can make changes to a DID document are called DID controllers. A DID may have more than one DID controller. At the same time, a DID controller can also be the DID subject (Reed et al., 2020). On which technical infrastructure the DID documents are stored is handled differently for the different DID methods. DID documents are typically written in JSON-LD format. An example is shown in figure 8 (Reed et al., 2020).

To understand the structure of a DID document, one or more Uniform Resource Identifiers (URIs) are referenced in the "@context" section. The DID subject is listed under "id". The DID controllers are specified in the "controller" section. Who can communicate on behalf of this DID is listed in the "authentication" section. The specified public keys and the corresponding authentication algorithm can be used to check whether the proof specified for authentication is valid. In addition to "authentication", other methods will not be discussed in detail here. These and other components of a DID document are described in detail in the DID W3C standard (Reed et al.,

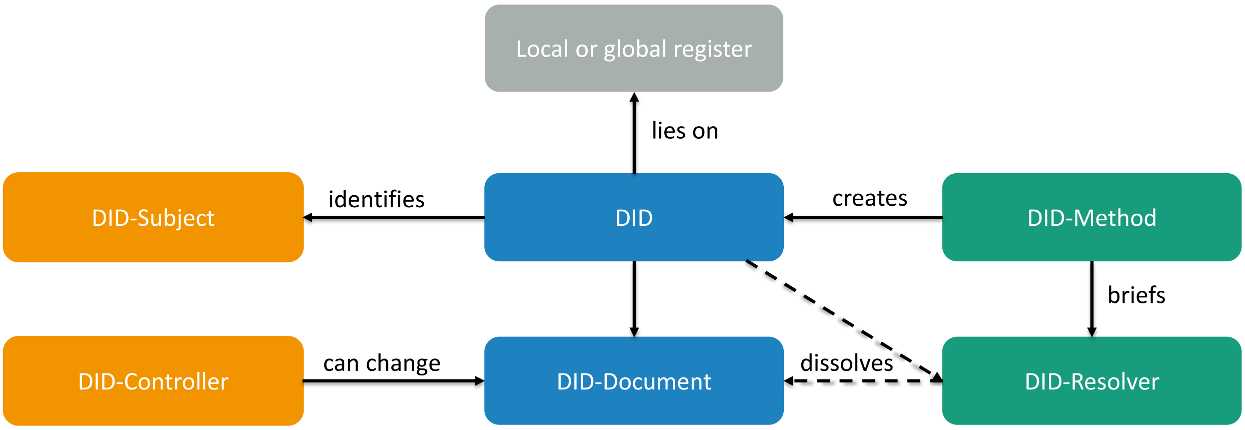
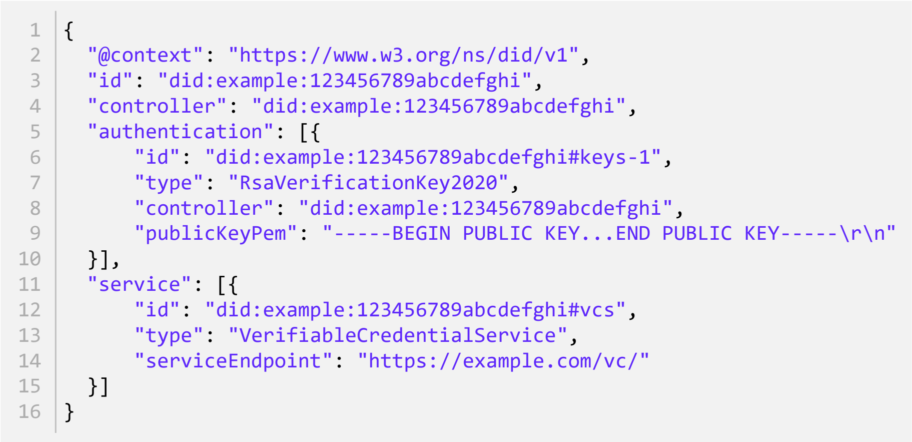


Figure 7: DID-Architecture



```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "controller": "did:example:123456789abcdefghi",
  "authentication": [{
      "id": "did:example:123456789abcdefghi#keys-1",
      "type": "RsaVerificationKey2020",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{
      "id": "did:example:123456789abcdefghi#vcs",
      "type": "VerifiableCredentialService",
      "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

Figure 8: Example of a DID document (JSON-LD)

2020). The “service” section can define the various endpoints with which the DID subject can be addressed. Depending on which service is to be invoked, different endpoints may exist. However, endpoints that reference the same domain can determine correlations between different DID documents and thus DIDs.

Digital signatures can be used to verify DID documents. The signatures do not directly reveal the current owner of the DID since the keys can change over time owing to rotations. Instead, a valid chain of changes must be presented, each of which was signed with the then authorized key. Only in this way can current ownership relationships be clarified. However, the ownership of the private key can be queried at any time after the DID document has been created. The owner of the DID is sent a request via a service endpoint specified in the DID document, which contains, for example, a nonce (random number) encrypted with the public key (Reed et al., 2020). Only with the correct response can ownership be proven.

It depends on the application who and how many participants in a network know a particular DID and the associated DID document. Therefore, there are different approaches for data registries, how DIDs and DID documents are stored. The two most important approaches are explained below.

(1) Microledgers

From a data protection perspective, especially for compliance with data protection regulations such as the European Union’s (EU) General Data Protection Regulation (GDPR), the ideal identifier is a pairwise, pseudonymous DID. This DID (and the associated DID document) is known only to the two parties in a relationship. The parties thus have their private communication channel, which is referred to as a microledger. It must be possible to establish a formal connection via the microledger and DID documents must be exchanged and updated. The peer DID method is probably the best-known approach for this architecture (Reed, Law, Hardman, & Lodder, 2019). It has the following form:

did:peer:abcdefghi1234

The DID documents are stored in a private location known only to the other party. An initial check of who is behind a DID (DID authentication) can be done based on a VC or an existing communication channel.

(2) Public/private ledger

It may make sense for an entire (company) network to know the identifier in a company-specific context. The DID can then be recorded in a registry that is best provided in a decentralized manner. This registry can be accessible to anyone (public) or only to a specific group (private), depending on the requirements. Distributed ledger technologies (DLT), especially blockchains, have many advantages here, so they are used in many SSI solutions for this purpose. The resulting architecture can be compared to a telephone book: Like how telephone numbers are written to the phone book, DIDs can be stored in a decentralized storage to provide universal identifiers for contacting.

Although in SSI, the initial contact between two peers is often established utilizing a public DID, individual peer DIDs are exchanged for further interaction based on this tight connection (Preukschat, 2019).

(3) Mixed Forms

Currently, there is ongoing work to establish non-blockchain based microledgers that allow to prove the control over a key – potentially preceded by several rotations – and at the same time prove that different microledgers do not include contradicting information. An example of this is the Key Event Receipt Infrastructure (KERI).

Digital wallets

Digital wallets are required for storing the cryptographic keys and VCs that are required in an SSI system. These are used to handle the most common types of interaction with other Self-Sovereign Identities. These include signing messages, authentication (DID-Auth), or receiving VCs and answering proof requests through VPs (Vescent et al., 2018). A digital wallet can also be used as an address book to store various contacts and evidence of past interactions in the SSI context.

The Decentralized Key Management System (DKMS) is a standard designed to manage private keys. This standard aims to avoid lock-in effects for digital wallets (Reed et al., 2019). In addition to storage, it is also necessary to support key recovery for everyday use. In case of loss of a digital wallet (e.g., loss of the smartphone), the keys and thus, in the worst case, the access to the identity must not be lost but must be restored; on the other hand, this must be balanced with protection from theft or intentional sharing. The DKMS offers these two approaches to key recovery:

(1) Offline recovery

One solution approach supported by DKMS is offline recovery. In this approach, an encrypted backup of the wallet is stored in a cloud infrastructure. The encrypted backup can only be decrypted with the so-called recovery key. This key is stored in a secure location, such as on a USB stick or printed on paper and deposited in a bank safe, guaranteeing that the wallet can be decrypted again with the corresponding keys (Reed et al., 2019). This procedure prevents the associated keys from being lost if the smartphone and the wallet stored are lost. However, similar to a bitcoin wallet, a critical key must be managed. Therefore, this approach alone does not protect against the loss of keys in general but only of a locally used technical infrastructure.

(2) Social Recovery

A second approach is a social recovery. In this approach, one or more trusted identities are designated to hold data that can be recovered. An example of social recovery is the Shamir secret-sharing method. Here, a pre-determined subset of all trusted identities is needed to recover the cryptographic keys. The process is similar to a treasure map torn into pieces, but only a certain number of which are required, and none of the pieces are essential for recovery. For example, a minimum of three out of five signatures from trusted entities, such as friends or family members, may be necessary to enable key recovery (Reed et al., 2019).

Digital Agents and Hubs

To enable users to interact with an SSI network as securely as possible and without downtime, there are so-called agents. These agents update contact data for other identities (Vescent et al. 2018) and respond to requests in the context of an identity as a service endpoint. An agent for SSI solutions should have three basic characteristics (Hardman, 2019a):

(1) It acts as a trustee on behalf of a single identity holder.

(2) It contains cryptographic keys that authorize it to do the former.

(3) It interacts with interoperable DID protocols. The DIDComm Working Group aims to standardize this interaction with the DIDComm protocol (DID Communication Working Group, 2019).

Agents form the link between the digital wallets of their users and, where appropriate, for communication between digital wallets and distributed ledgers. Thus, agents are an essential element of the interaction between holders, issuers, and verifiers.

According to their respective environments, a distinction is made between two types of agents (Preukschat, 2019). Edge agents run on a local device owned by the identity holder. Edge agents do not need to be permanently online. In

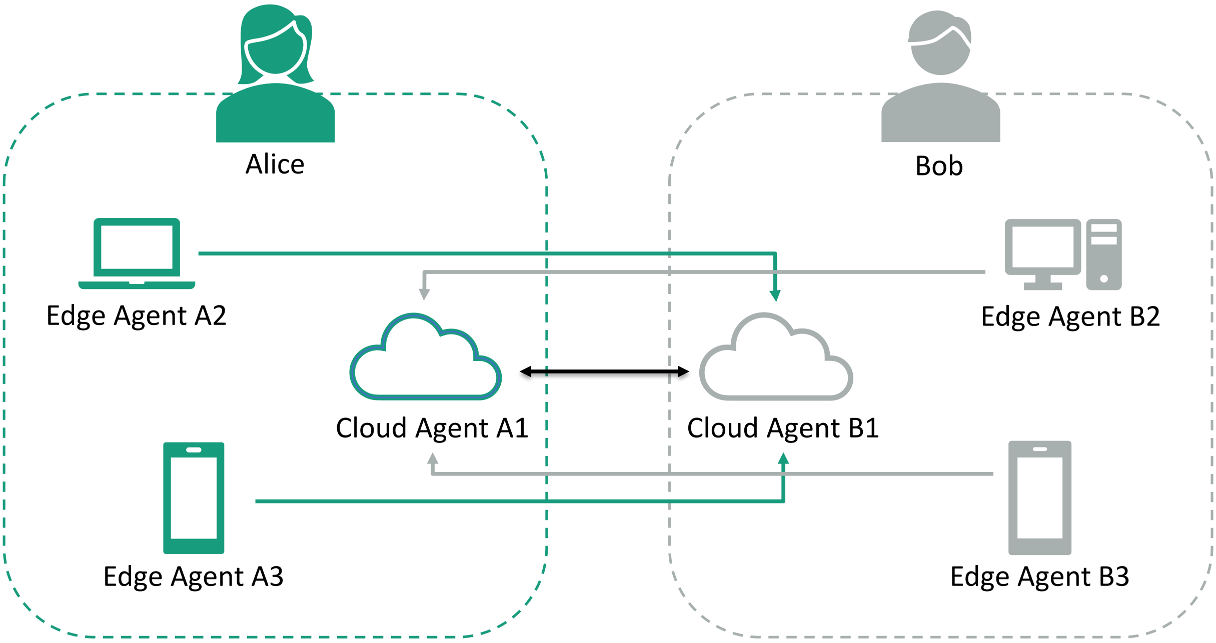


Figure 9: Agent-to-Agent communication

contrast, cloud agent runs on a server that is accessible to the identity holder, forming a permanently accessible endpoint.

It also enables the communication between different edge agents. This situation is illustrated in figure 9. Hubs are special agents that provide and manage any data and services that would otherwise need to be stored and operated by end-users (Vescent et al., 2018). Hubs focus primarily on aspects of identity data exchange (Hardman, 2019a).

Further technologies and concepts for the use of SSI

In addition to the basic building blocks, additional concepts are relevant for SSI solutions. These can provide enhanced security, increased privacy, the improved authentication of identities, and protection in case of device and key loss.

Key rotation

Keys should be changed at regular intervals to prevent security risks. Key rotation involves revoking previous keys and adding new keys. In addition to the rotation, there is also the option to revoke keys permanently. It is not necessarily enough to forget a key, as this does not protect against compromise. In the event of smartphone theft and the associated loss of an edge agent, it must be possible to revoke the device’s authorization. Thus, the value to attackers is low, even if they manage to compromise the agent (Reed et al., 2019).

Key rotations at regular intervals have the following advantages (Reed et al., 2019):

(1) Technological change: Encryption technologies are constantly being developed. With the rotation of the keys, the encryption technology can also be changed. This makes the SSI solution more secure.
(2) Unprofitable attacks: Even if an attacker can steal keys, key rotation quickly renders them unusable. Thus, attacks are less profitable than under traditional circumstances.
(3) Changing needs: After certain activities are completed, the associated keys are also no longer needed. As keys expire, they automatically become invalid after a specific time.

Key rotations of DID keys require the approval of one or more agents, depending on the provision of the DID document. After the agents’ consent has been obtained, the updated keys must be communicated to the users' contacts. This is done via an existing microledger connection of the other participants or by updating the DID document in the distributed ledger.

Technical foundations

Distributed-Ledger-Technology (DLT)

One of SSI's principles is to make as little personal data as possible available to the public to protect users' privacy. This principle gives rise to the following two problems:

First, in some cases, it is necessary to disclose data to the public. For example, for issuers, it makes sense to reveal the public identifier and the associated service endpoint for the general public in the DID document.

Second, not every credential is valid indefinitely. Therefore, there must be a way for the issuer to revoke credentials and their associated attributes. This is referred to as revocation. For example, it should be possible to revoke the driver's license credential for someone who drove drunk. The holder cannot technically be forced to delete the VC. Therefore, there must be a way for the verifier to track the timeliness of the VC.

Theoretically, a verifier could directly send a request to the issuer of the VC, asking for its revocation state. One approach to implement this would be a service endpoint operated by the issuer specifically for this purpose. In this case, the provisioning and requesting of data must be standardized in terms of data format and protocol. However, such a solution would undermine SSI's efforts to avoid direct interaction between issuer and verifier. Platforms can be a useful alternative, as they bring a certain degree of standardization and offer fail-safety.

These platforms must fulfill the following functions (Hardman, 2019a):

(1) Publish DIDs to make them known to the largest possible number of identities, especially for issuers.
(2) Providing a revocation registry, which is a way to verify that VCs are still valid.
(3) The publication of credential schema definitions, as the associated schemas must be publicly available to ensure semantic interoperability of VCs.
(4) The publication of agent authorization so that agent authorization can be revoked in addition to VCs.

The use of a centralized platform would likely create dependencies and lock-in on this platform. DLTs, i.e., decentralized, distributed systems, can circumvent precisely these problems of a central platform. Blockchains, representing a sub-area of DLTs, are used in well-known SSI solutions such as Hyperledger Indy. Blockchains are distributed data structures that allow transactions grouped in blocks to be stored transparently, chronologically and tamper-proof (Lockl, Schlatt, Schweizer, Urbach, & Harth, 2020). DLTs and blockchains exhibit several advantages for an SSI architecture:

(1) Reliability: The decentralized, redundant blockchain architecture makes it more robust than a central server structure against failures and compromise.

(2) Immutability: Once written to a blockchain, the transactions and the data stored with them on the blockchain cannot be changed or manipulated without great effort.

(3) Transparency: All participants in the network can see all transactions equally. Status changes, such as new identifiers, are made available to all participants in the network simultaneously.

(4) Cryptographic signatures: Transactions must be signed by the transaction originator. This means that the origin of the data in the transaction can be directly assigned to a participant.

(5) Sequential ordering and time-stamping: The block architecture of a blockchain, which cryptographically relates the individual blocks to one another, creates a chained list. This means that the blocks and, thus, the individual transactions are automatically arranged chronologically. The timeliness of the data, such as the content of a revocation registry, can therefore be easily verified.

However, there are also caveats to consider when a blockchain solution is implemented as part of an SSI solution. For example, as little data as possible should be stored on a distributed ledger to avoid any potential bottlenecks. In addition, no personal data should be stored on such a (distributed) ledger in plain text. Even the encrypted storage of personal data on a shared ledger is risky. Future technical advances (e.g., quantum computing) could break asymmetric encryption, even if is still considered safe for the next years (Vescent et al., 2018). In Europe, the GDPR also requires personal data to be corrected or deleted if the individual requests it (Article 16 GDPR - Right to rectification, 2018). As blockchains have the inherent property of cryptographic tamper resistance, personal data must not be stored on the blockchain from a legal point of view.

Credential revocation

As described in the previous chapter, a publicly accessible validity registry is needed through which issuers can revoke VCs. Only in this way can issuers respond to evident fraud or misconduct. It must also be possible to revoke unchangeable, permanent VCs if issued in error. For example, even a birth certificate may need to be revoked and corrected in rare cases, for instance, if it contains a typo. The possibility of revocation must therefore be available for a large number of VCs.

The revocation registry should be implemented in SSI solutions in such a way that the following requirements are met (Hardman, 2018):

(1) Performance: The revocation check should be as straightforward and quick as possible.
(2) Privacy: The review and publication in the revocation registry should preserve the privacy of all parties involved.
(3) Contactless: It should be possible to check the status of the VC without contacting the issuer directly.

Due to the revocation registry requirements, SSI architectures often rely on DLTs for publishing them. In the following, we illustrate how revocation registries can be implemented using the Hyperledger Indy blockchain as an example.

Indy uses cryptographic accumulators. A cryptographic accumulator is a one-way membership function that can show that an entry is part of the accumulator, but the other parts need not be revealed to do so. An accumulator can be thought of as a number that is the product of many large prime numbers. It requires a lot of computational effort to calculate single prime factors from this product. However, the proof that a prime number is part of the accumulator results from a simple division, revealing the own prime factor and the product of the remaining ones. High-performance cryptographic accumulators used in practice can add new values to the accumulator without increasing their length. Together with the accumulator, the issuer of a VC publishes a tails file containing the factors for the product (the accumulator). Each entry in this document is assigned to a VC of a certain definition. The owner of a VC is aware of the respective entry. From the so-called witness delta, a remainder is published and updated together with the accumulator by the issuer of the VC. The issuer of the VC must also publish the tails file. It can be used to prove that one owns a valid factor contributing to the product and, thus, a non-revoked VC.

In a "positive" accumulator, only the VCs that have not yet been revoked are referenced. Thus, the validity can be easily verified without having to contact the issuer directly. This process is also called proof of non-revocation. In Hyperledger Indy, the proof of non-revocation is provided by the holder, proving to the verifier that it can derive the accumulator’s value using the factor referenced in the VC and the public witness delta as displayed in the accumulator. The verifier can thus verify that the holder arrived at the correct result because the answer is on the ledger but does not know the calculation details (Hardman, 2018). In this way, the privacy of all parties involved in the verification process can be preserved.

Zero-knowledge proofs

ZKPs are a critical component in the SSI paradigm. They play an important role for the communication between the prover and the verifier, solving a dilemma between these two parties. The privacy of individual users requires personal information to be hidden from others. ZKPs allow privacy to be maintained because only the necessary information is presented to a verifier. There is usually a trade-off between minimizing the information provided (privacy), and the verifier's legitimate interest to check the validity of the holder's credentials and properties. ZKPs are a cryptographic solution to the tension between the prover's personal privacy and the verifier's integrity. The latter is enforced in such a way that the former is compromised as little as possible (Ben-Sasson, Bentov, Horesh, & Riabzev, 2018).

Explanation of a simple zero-knowledge proof

Imagine that your friend Bob is color blind. You have two billiard balls; one is red, one is green. Otherwise, the two balls are identical. Since you have fooled Bob several times, he doubts that the two balls are distinguishable. So how do you prove to him, without a third party, that his guess is wrong?

A solution to this dilemma may be given as follows: You give Bob both balls, one in his left hand, the other in his right hand. Bob now takes both hands behind his back. He may secretly exchange the balls or keep them in his hand. After this is done, Bob brings out both balls again, and you must now "guess" whether the balls were switched. By seeing the difference between the two colors, you can immediately tell whether Bob switched the balls behind his back or not. However, if the balls were indistinguishable, you could only guess correctly with a probability of 50 percent. To rule out a possible chance hit, repeat the experiment n times until the probability that the correct assignment was just luck is small enough for Bob. So, Bob now knows that the balls have different colors, but not which ones, and not even how the balls can be distinguished. ZKPs take a similar approach.

SSI and zero-knowledge proofs

The ZKP in the example requires a high degree of interaction since information must be repeatedly passed back and forth between the two parties with the addition of an arbitrary component. Therefore, this ZKP is called an interactive ZKP. However, the ZKP becomes practical only as a non-interactive ZKP, where multiple messages are broken down into a single message. Therefore, regular communication over a long period is unnecessary.

ZKPs used in SSI solutions have the task of proving that the holder has special knowledge. He must show that he knows the issuer's signature, which confirms a particular attribute. This is proved with a ZKP using VCs without the prover showing the whole VC and in particular not its signature to the verifier. This means that ZKP-oriented VCs can be used to selectively disclose information without revealing the contents of the entire VC.

In addition, different types of evidence can be made possible (Nelson, 2018):

(1) Range Proof: Is a person between 18 and 40 years old?
(2) Membership: Is a person a citizen of Germany?
(3) Comparison: Do the identities of the subjects of two VCs match?
(4) Computational Integrity: Are the results of calculations correct?

ZKPs in the SSI context are usually not computationally expensive. The most frequently used and implemented ZKP in Hyperledger Aries, for example, is a proof based on so-called Camenisch-Lysyanskaya signatures (CL) (Camenisch & Lysyanskaya, 2002). Many fundamental design decisions of existing SSI concepts have been decisively shaped precisely by this ZKP approach.

Instead of combining the individual credential attributes into a single message in a collision-resistant hash function, CL signs them so that each subset of these attributes can be presented together individually with a valid, but non-correlatable signature. The advantage is that information can be selected, and not all information needs to be revealed to the verifier (Abramson, 2019). This process is defined as selective disclosure.

Furthermore, ZKPs make it possible to combine different VCs as desired without revealing strongly correlating attributes that are the same in both VCs. Any subset of the attributes of the VCs assembled in the VP can be presented together with a valid signature and a proof that they were issued to the same underlying secret. There is no need to disclose any further linking reference, such as the subject’s first and last name or public binding key on both certificates. This makes the information included in a VP more controllable (Hardman, 2019a).

Concepts of authentication

In the following, two concepts are presented that enable the authentication of users.

(1) Link-Secret authentication

A link secret is a random number that nobody knows except the holder himself. The holder created the link secret and transmits it in obfuscated form to the issuer, who embeds it in the VC alongside various claims and signs it. The signature of the VC includes the identity-specific part (blinded link secret) and several visible attributes. The link secret cannot be extracted from a blinded link secret by the issuer. It can only be cryptographically proven that multiple blinded link secrets have the same link secret as their origin. Therefore, VCs issued over one link (issuer - holder) can be verified in another link without loss of privacy using changeable pseudonyms. Thus, it can be shown to the verifier that multiple VCs were issued to the same link secret and thus presumably to the same user (Abramson, 2019). In later steps, it can then be proven that two VCs were issued to the same identity.

However, preventing the deliberate disclosure (e.g., sale or sharing) of the link secret must be made as difficult as possible, as it can be used to assume the full identity of another person. This can be achieved, for example, by using secure hardware in cell phones.

(2) Biometric authentication

Another approach involves coupling a variation of the link secret to the physical user identity using biometrics to create biometrically. Biometrics establish identity-based behavioral and physical characteristics such as fingerprints, face, iris, voice, and gait (Hardman, Harchandani, Othman, & Callahan, 2019). Biometrics take an essential role in many identity use cases because of its ability to identify individuals and their uniqueness. However, its use depends on various factors, such as matching accuracy (Callahan, Hardman, & Othman, 2019).

There is a tension in specifying biometric attributes: complete biometrics (e.g., a full scan of the iris) is a perfect correlator but strongly intrudes on the privacy of the reference person. Incomplete biometrics, however, lead to a lower level of assurance.

Biometrics can significantly reduce fraud with VCs by making it very difficult for the illegitimate holder to use the VCs under a false identity. However, the benefits of biometrics do not come without negative aspects (Hardman et al., 2019). Care must be taken to design processes so that define rights and responsibilities depending on the use case. Privacy must be protected as well as a sufficiently secure identity verification must be ensured (Hardman et al., 2019):

(1) The direct biometric matching and proof of a biometric data set (pocket pattern) between holder and verifier may lead to correlation and thus privacy issues.

(2) In many cases, it makes sense to use a provider that checks that biometrics match (Biometric Service Provider Pattern). In this model, the verifier does not receive information about the holder's biometric data but must trust the Biometric Service Provide. To increase trust, multiple Biometric Service Providers can also be involved in the process.

(3) A third option is identity verification based on many non-uniquely related, weak biometric properties (low-fi layers pattern). For example, eye color is not a strong identifier. However, the combination of eye color, height, age, and a genetic fingerprint matching for one percent of the population, may be sufficient for the verifier to prove their identity. In this way, the verifier can also determine which requirements for unique identifiability are necessary for a particular application.

Biometric methods still offer great potential for research and implementation as they are essential in making SSI solutions even more secure in practice while preventing fraud and identity theft.

4 SSI offers a wide range of practical application possibilities

Application possibilities

Overview of different possible applications of SSI

In addition to the already described application of SSI for end users on the Internet, the SSI paradigm offers many new possibilities for organizations and individual actors. Three examples of applications are described in more detail below.

SSI for healthcare

The most common and prominent use case of SSI to date is personal identities, as discussed earlier. SSI can be used to create forgery- and tamper-proof digital versions of important personal documents such as ID cards, passports, birth certificates or medical prescriptions. These digital proofs of identity can also be used to provide secure, password-free access to web services. The use of SSI is also conceivable for general applications, as shown below using the example of e-prescriptions issued by doctors for patients:

1. The connection invitation

First, the patient's agent (holder) must be connected to the doctor’s agent (issuer) who is to issue the e-prescription as VC. In this process, first a secure communication channel is established. For this purpose, the physician determines an existing communication channel to transmit the patient's request - for example, via the patient’s e-mail address. Via this point of contact - or, for example, via a display or poster in the doctor’s office - the doctor sends the patient a QR code that contains an invitation link to connect both parties: an "out-of-band mechanism“.[2]

2. The connection request

The patient can now scan the QR code to send a secure message back to the doctor using the public key and service endpoint linked in it. Suppose the patient wishes to accept the connection invitation. In that case, the patient creates a new DID with an associated DID document for the emerging connection relationship between the patient and the doctor. The patient's wallet application puts this information in a connection request and sends it back to the physician.

3. The connection response

The inviting doctor's agent or digital wallet receives the patient's connection request at the other end and decodes it to find the corresponding message containing the connection request. The identifier in the message informs the doctor which invitation to associate this message with. The doctor then stores this received information in the patient's connection record. In the process, the physician also creates a DID and a DID document, packages them into a response message, and then sends this message back to the patient.

4. The final connection

The patient also follows this process and saves the received doctor’s DID and DID document in the corresponding connection record. The patient and the doctor are now connected via a secure, private, and end-to-end encrypted messaging channel.[3]

5. Issuing the prescription

After the medical examination and the successful connection of the patient's agent and the doctor's agent, the doctor - with all the necessary information based on the medical examination and the patient's file - issues the patient a corresponding prescription for medical treatment via this connection. The patient receives the VC and stores it in their digital wallet. If necessary, the revocation registry associated with the VC is updated by the physician immediately. This can be done either in the issuance or, for example, cumulatively in the evening.

6. Initialization of drug dispensing by the pharmacy (verifier)

In the next step, the actual dispensing of the drug begins. Using the digital wallet, the patient asks the pharmacy for a specific medication - according to the prescription issued. The pharmacy then wants to receive specific data from the patient that can be verified that the origin of the requested attributes can be traced back to a trusted advisor, in this case, the doctor. The query is made in a standardized scheme, a so-called proof request. This includes the attributes to be presented (name of the patient, name of the physician, medication, expiration date), the

[2] The invitation is a JSON file that contains a unique identifier and the same kind of information as the DID document - in particular, it also contains a public key and a service endpoint.

[3] The process of establishing a connection (items 1-4) in real-world applications ranges from a few confirmation prompts to being fully automated.

accepted issuers (public keys of trusted physicians) and, if applicable, a proof that the VC is not expired.

7. The digital proof

The patient's digital wallet can fulfill this request by transmitting the attributes to be presented based on a VC stored in it that fulfills the requirements formulated in the proof request - including a proof that the physician issued these exactly like this.[4] This VP can be checked by the pharmacy using the doctor's public key and - if a check for revocation is required - the public state of the revocation registry (locally, from a blockchain, or a trusted database).

8. Approval of medicines

After the pharmacy has verified the validity of the provided prescription information, the approval to dispense or ship the corresponding medication ultimately occurs after verification and processing. In the real-life application of the e-prescription example, multiple uses of e-prescriptions must also be prevented as a rule. Although a unique ID of e-prescriptions could be used to detect the multiple redemption of e-prescriptions, this would prevent multiple uses only in the same pharmacy (or the pharmacies participating in the verifier's system). Additional double-spending mechanisms are necessary for ensuring the prevention of multi-usage across pharmacies. For example, blockchain technology can help prevent multiple dispensing with a decentralized system, such as pairing the VC with a token that does not contain sensitive data and only prevents double usage. Alternatively, the pharmacy could connect with doctors and ask them to revoke the prescription after usage; however, in this case the benefit from not needing a communication channel between doctors and pharmacies would be gone.

SSI for e-commerce

This pattern holds enormous potential as the digital transformation advances, as it can be extended to other examples of e-commerce and other supply chain use cases. Worldwide, the turnover in e-commerce increases by almost 15 percent each year and will be around two trillion euros by 2020 (Statista, 2020). This highlights the enormous future importance of e-commerce and the associated potential for using people-related SSI, as we describe below.

The rapid spread of social media and e-commerce providers has increased many users' awareness for privacy and data protection. Since processing payment or shipping goods always requires the use of partial identities, verification and use of user identities are also a challenge (Schneier, 2018). For example, in alcoholic beverages, the age of the person ordering can currently only be verified by the parcel service.

Personal SSI can simplify and accelerate many processes in e-commerce. Whereas specialized providers have often absorbed the financial

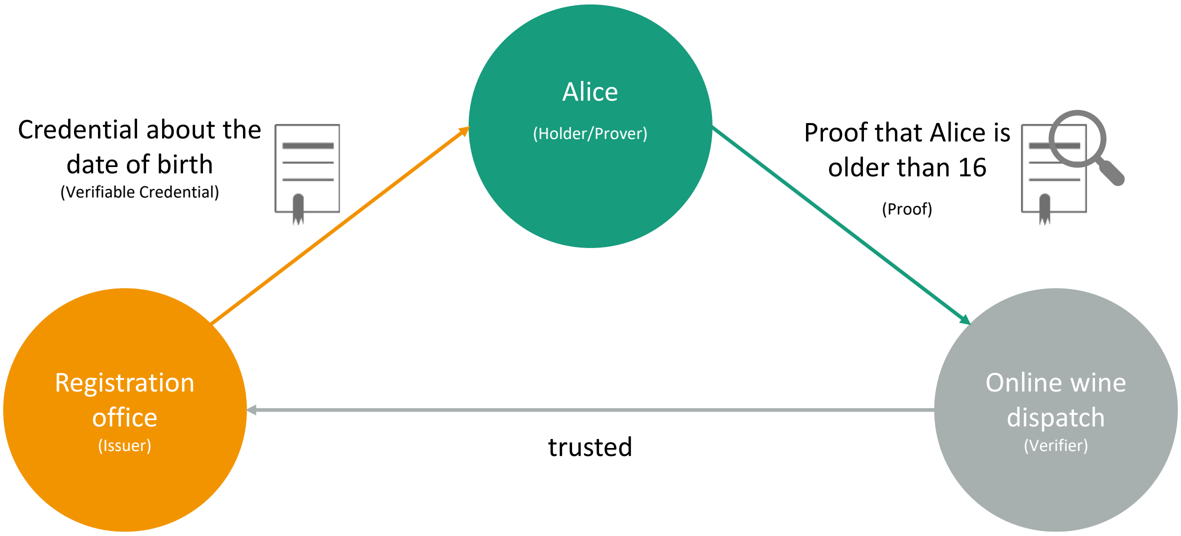


Figure 10: Example application of an SSI in e-commerce

[4] This proof can be provided in several ways - for example, by traditionally presenting the issuer's digital signature or ZKPs.

transaction risk, banks as VC issuers can provide immediate proof of financial transactions that customers present at the time of purchase. This reduces the operational risk for e-commerce providers and makes them more independent of centralized payment processors. It also makes it possible to provide proofs to government authorities, e.g., to pay income tax. In addition, elements of SSI can be combined with decentralized digital currencies, such as cryptocurrencies, in e-commerce. In addition to secure proof of identity, payment for goods can also be processed decentralized. Users can also use SSI to prove their age, for example, when purchasing alcoholic beverages (see Figure 10).

SSI for the Internet of Things

In addition to person-based SSI, the potential field of application is much wider. For example, digital identities can be created not only for people but also for machines, devices, and other smart things. The emerging Internet of Things (IoT) envisions the integration of technology-enabled physical objects into a networked society (Rosemann, 2013), enabling a variety of different interactions between people and machines (Oberländer, Röglinger, Rosemann, & Kees, 2018). Accordingly, provable digital identities are an essential prerequisite for the interaction of many potentially heterogeneous parties.

In recent years, an increasing variety of digital technologies have been integrated into cars. One use case at the intersection of IoT and SSI uses an SSI for motor vehicles. As a result, vehicles could interact with various entities, such as government agencies, toll booths, gas stations, or repair shops. So far, information about the vehicle is typically transmitted non-digitally via the vehicle registration document and the service booklet. This means that important information about the vehicle's identity can easily be manipulated and faked. The rapidly advancing development of autonomous driving underscores the need for digital vehicle identities. For example, in the foreseeable future, one can imagine an application scenario in which cabs act as autonomously driving and economically independent unit in road traffic.

A vehicle can prove its "birth" through VCs, i.e., the beginning of the vehicle lifecycle, analogously to a birth certificate for humans. The link between the digital identity of the vehicle, the Vehicle Identity (VID), and the physical object can be ensured by the Vehicle Identification Number (VIN) assigned to each car by the manufacturer (Mobility Open Blockchain Initiative, 2019). This represents a critical aspect in linking digital identity with the physical object since the object - unlike a human being with usually persistent biometric characteristics - cannot be identified by unique characteristics that are difficult to replace. The connection with the VIN is also a risk. It can be physically manipulated, especially on older vehicles. Nevertheless, the coupling of the VID with the VIN is a relatively strong connection for a physical object. Secure hardware elements in central control components of the vehicle could achieve an even higher binding strength and, thus, level of assurance by cryptographic means.

The VID can then be assigned other certificates, such as the current speedometer reading or the

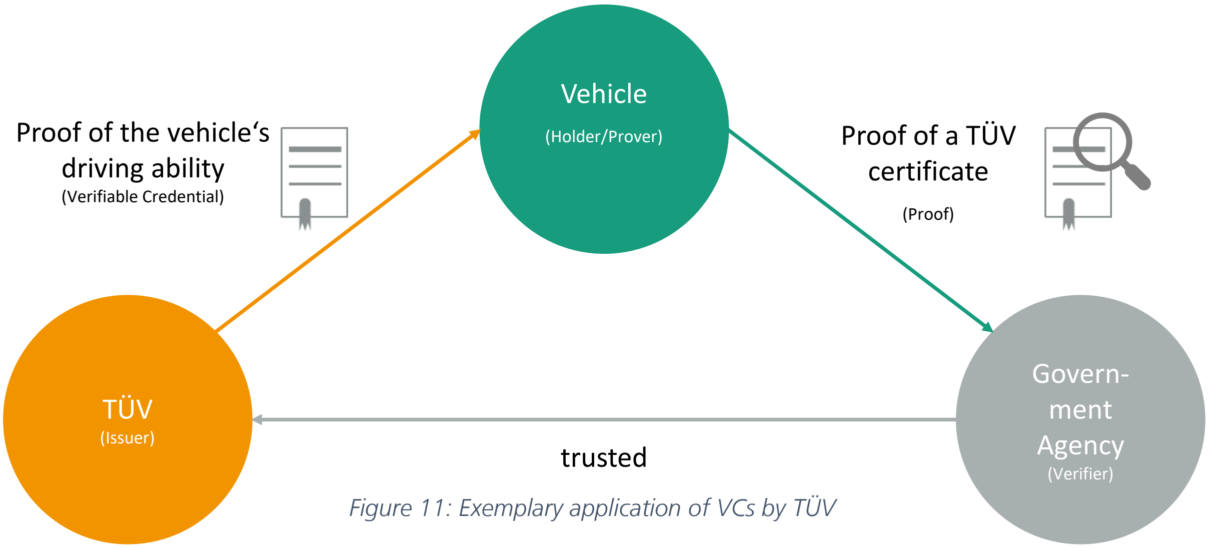


Figure 11: Exemplary application of VCs by TÜV

title deed, stored in the vehicle's wallet. Relevant entities, such as regulatory authorities, manufacturers, banks, and vehicle owners, can act as issuers and assign certain attributes to the vehicle as VCs. An example of this is the successful general inspection, which can be assigned as a VC by the TÜV (the German Technical Inspection Agency) and is required, for example, in a traffic control (see Figure 11).

According to the German Automobile Association (ADAC), the "popular" speedometer manipulations on used cars cause an annual damage of six billion euros in Germany alone (ADAC, 2019). A vehicle would also interact in an economically autonomous way via its VID with service providers such as gas stations, toll booths, or even workshops. This reduces transaction costs for vehicle owners and users but also for the service providers involved.

SSI for public institutions

In public institutions, various application examples can be found in which SSI has an advantage over existing solutions. One example is certificates, diplomas, and deeds issued by public institutions such as universities. Today, these are printed in paper form and made physically available to those who have acquired them. These documents are then used in various ways to prove certain qualifications acquired, for example, during studies. Up to now, there has been no way standardized digital way of proving that the document corresponds to an original. By contrast, there is often a need to produce certified copies by a notary's office.

In particular, the ongoing digital transformation in companies implies that applications often rely on scanned - and therefore easily manipulated - documents. For this reason, companies are increasingly turning to professional providers to check the authenticity of the documents submitted by applicants. According to estimates, approximately 500 billion U.S. dollars are generated annually with forged credentials (Goldfarb, 2019). This costly solution could be replaced using VCs by public institutions.

For example, a university could issue a certificate of current performance to all students. Upon completion, students would then receive a VC proving their final grade. Graduates can use this VC in a variety of ways. On the one hand, existing achievements can be verified when changing universities. On the other hand, non-governmental organizations can also verify these achievements as part of an application process (see Figure 12).

Since companies may be enabled to replace a large part of their compliance and background checks through VCs, this use case has a high economic potential (World Economic Forum, 2020). A pilot project in this area could also be an impetus for further digitizing administrative processes in public institutions. Table 3 summarizes the most relevant aspects of the SSI use cases presented.

SSI's economic potential

With the increasing use of the Internet by both individuals and physical objects in the context of

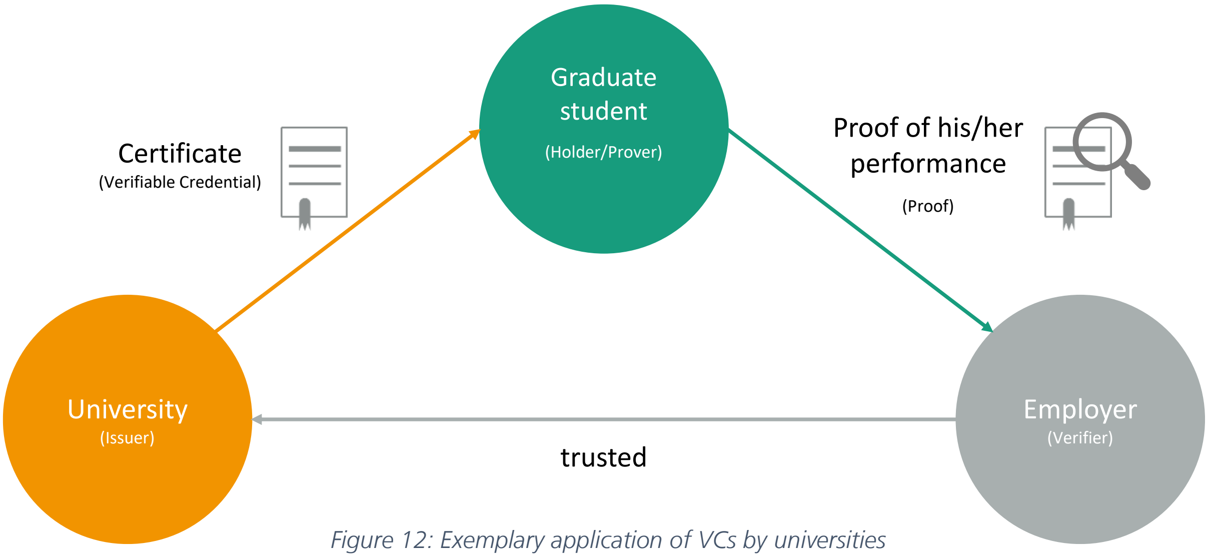


Figure 12: Exemplary application of VCs by universities

the IoT (Rosemann, 2013), the need for a secure and interoperable technical solution for digital identities is more significant than ever. Furthermore, with an estimated 4.2 billion Internet users already today, personal SSI can be applied across the globe (McKinsey & Company, 2019; World Economic Forum, 2020).

According to a study by the World Economic Forum, the introduction of SSI solutions in international air traffic could make identity management more efficient and thus lead to massive cost savings. At the same time, additional costs can be saved through improved KYC processes (World Economic Forum, 2020). In this context, using an SSI solution can simplify a significant part of banks' know-your-customer (KYC) processes (World Economic Forum, 2020). As a result, the overall SSI solutions market is expected to be worth up to $2 billion by 2023 (MarketsandMarkets, 2018). In addition, the SSI paradigm ensures counterfeit-proof certificates in the area of public institutions. The issuance of fictitious certificates of, for example, fake academic degrees deceives the public, employers, and customers and causes considerable reputational damage. Accordingly, significant cost savings are possible in public institutions with SSI.

As described in the technical building blocks, different roles are assumed by participants within an SSI network. This, in turn, also results in various interests and potential opportunities in potential monetization, e.g., the provision of cloud agents or digital wallets. This also requires operators for the technical infrastructure such as blockchain nodes and potentially agents and SSI software in general as a service for enterprises. Issuers may also have an intrinsic interest in issuing credentials: By outsourcing data sovereignty to users, issuers could implement regulatory requirements to transfer data between different countries by design.
Furthermore, by regularly requesting VPs from users in the financial sector, requirements in anti-money laundering (AML) and KYC processes can be addressed. Also, contrary to popular belief, companies, for example in the financial sector, are not always necessarily interested in storing sensitive customer data on their

Characteristics	Application scenario	Advantages of the SSI Paradigm
Individuals and organizations	Healthcare and e-commerce	• Forgery- and tamper-proof digital verification of important personal documents such as ID cards, passports, birth certificates or medical documents • Secure access to web services • Improved trust relationships with more sensitive customers (increased IT security awareness among customers) • Process improvement (e.g., easier proof of payment and address information)
Physical objects	IoT-Devices	• Self-sovereign identity management of various IoT devices (e.g., managing digital identities of automobiles over the vehicle lifecycle). • Essential role of digital identities in the field of autonomous driving (managing digital identities of autonomous vehicles).
Public institutions	University	• Self-sovereign and tamper-proof management of certificates, attestations, or deeds • Optimization of administrative processes (background compliance checks) • Recruiting (simplification of recruiting measures and operational implementation)

Table 3: Advantages of SSI in different application scenarios

infrastructures, as managing this sensitive customer data while complying with regulatory requirements ties up extensive resources. The introduction of SSI could relieve companies of this burden and thus also save costs.

Benefits for companies through SSI

In addition to the economic potential of SSI, there are other advantages for companies. For example, SSI can improve the control of access to a company's IT systems. The digital transformation in companies has led to a sharp increase in the number of existing IT systems such as enterprise resource planning, customer relationship management, e-mail, and project management tools. These IT systems are often implemented separately, creating multiple data silos that must be managed, synchronized, and protected. For example, access authorizations must be created or deleted individually for all employees. This requires time-consuming monitoring and administration of the individual systems and thus leads to many redundant processes for granting and managing access rights, some of which are still carried out in an analog (paper-based) form.

Using SSI solutions across different systems, user-friendly, fast and secure identification and authentication could save costs through redundant administration, data storage, and processes. Redundancies of outdated file versions within the data storage are reduced in the sense of the "single source of truth" and an improvement in data quality. In addition, protection against, for example, phishing attacks, identity theft, or other forms of fraud is ensured by using a consistently used asymmetric encryption process (end-to-end encryption). This also applies to authorization, e.g., the granting of write and access rights within systems. The individual granting these rights as part of user-definable access control could be eliminated if access is granted via corresponding credentials. In addition, the elimination of individual log-in passwords and usernames and the combination with multi-factor authentication methods will reduce the vulnerability to individual attack vectors within companies. In many organizations, employees still use easy-to-guess passwords to secure individual access for convenience. The use of SSI for employees in companies could better secure these accesses with a similar user experience. At the same time, new employees would no longer have to go through the tedious process of creating individual access combinations for different software tools.

SSI can also be used across organizational boundaries. Through this use, IT systems can be controlled in an uncomplicated manner across domains, thus enabling corresponding interoperability. For example, in this case, new access authorizations for external employees can be created for individual projects, which can be easily revoked using a revocation registry after the project has ended. This reduces the complexity of identity management for companies and can thus contribute to cost savings. At the same time, the risk of unauthorized disclosure of access data can be circumvented to a certain extent.

Centralized platforms as identity providers, such as Google, always bring the danger of a monopoly or at least excessive market power. Within the last few years, the focus has been on establishing decentralized platforms based on blockchain technologies. However, these often conflict with existing regulations in data protection, such as the GDPR (European Parliamentary Research Service, 2019). SSI could circumvent the disadvantages of both approaches and enable a decentralized ecosystem in identity management. Open standards and specifications can be used to create an innovative environment that is neither influenced by vendor lock-in nor patent restrictions (Wagner, Pueyo, Vandy, Bachenheimer, & Beron, 2020).

In addition, the integration of public SSI networks can improve customer experience during various business services. For example, instead of manually creating a user account with a username/password combination and credentials, new customers can use an existing digital identity to create their account. SSI creates a portable identity that individuals can use for any online process - from simple authentication requests with a single credential (e.g., service login) to complex processes such as sharing curated identity data for automated digital form filling. In this context, SSI contributes to digitizing corresponding processes by providing reusable identity attributes and thus realizing the progressive automation of processes (Wagner et al., 2020). Ultimately, this improves a website's user experience, service and product availability, data quality, and data processing and potentially results in increased user numbers and improved process efficiency.

SSI also enables improved compliance with existing privacy and data protection regulations such as the GDPR. With the release of credentials by customers, companies can prove this release at any time and thus implement "privacy and compliance by design" without additional effort in identity management. At the same time, users are also increasingly attaching importance to their (personal) data protection. SSI solutions increase users' sensitivity and attention (IT security awareness) to the topic of data protection and data use.

5 Critical view on SSI

Critical view

Governance challenges

Standardization and interoperability are arguably the most relevant governance challenges of SSI. While an increasing number of initiatives are trying to implement SSI or SSI-like solutions, a certain degree of standardization and interoperability, similar to transmission and network protocols on the internet (e.g., TCP/IP protocols), will be necessary to achieve widespread adoption. At this point, for example, the international W3C consortium has already launched initial efforts for standards such as DIDs and VCs, which aim to standardize SSI protocols. These efforts are supported by the Trust over IP Foundation[5] , which has committed itself to building a holistic architecture for digital trust on the Internet. In particular, the ability to port VCs between different networks will be crucial for the widespread adoption of person-based SSI. Likewise, the number of providers will initially be decisive to reach a broad mass of users.

Socio-economic challenges

The acceptance of SSI solutions by consumers and companies require thorough research. Even if existing initiatives enable a high degree of user-friendliness, the safe use of SSI requires integrating a second device - i.e., a second factor for authentication - which reduces user experience. Especially given the lack of use of similarly complex procedures, such as multi-factor authentication, in many centralized systems, the holistic adoption is challenging. Furthermore, the cost aspect should not be neglected at this point. The use of SSI will inevitably be associated with costs for consumers. For example, potential operators of an SSI solution will have to maintain cloud agents and DLTs. Unless there are savings in processes directly for these operators due to the security and interoperability benefits already described, the costs associated with SSI and a profit margin could be passed on to consumers, who may then have to choose between a free SSO and a paid SSI sign-on. On the other hand, however, the technical feasibility of payment in the context of a VP is unclear since the issuer is not involved in verification processes.

SSI should also not be a panacea for user privacy on the Internet. While ZKPs can ensure that only the minimum of required information is shared and transferred, this cannot guarantee privacy on its own. For example, verifiers can still request more data than they would require for the provision of their service. Due to the low effort involved, personal data can be requested in processes where this was previously not the case, such as when entering a building. If the holder willingly shares data with the verifier, the gain in privacy through SSI is partially nullified.

Legal challenges

In addition, a variety of aspects concerning regulation are still unresolved. Many of the positive outcomes of SSI can only be achieved if credential reuse is realized across sectors (credential roaming). Credential reuse is technically feasible, but credential roaming has not been widely adopted due to a lack of regulatory clarity (Wagner et al., 2020). While there are clear benefits to be gained from SSI and its technological solutions, e.g., in the area of privacy, the regulatory basis for this needs to be established. Such a regulatory approach should ideally take place in a supranational framework.

Another important aspect is the acceptance of electronic signatures. The EU launched an important initiative in this regard with the eIDAS Regulation (Regulation (EU) on electronic identification and trust services for electronic transactions in the internal market, 2014). eIDAS has created the legal framework for the use of electronic signatures since its adoption in 2016. Thereby, it gives an electronic transaction the same legal status as a paper-based transaction. In addition, other regulatory initiatives such as the European Self-Sovereign Identity Framework (ESSIF) could also give the EU a pioneering role in using SSI through standardization and cooperation with international organizations such as Trust over IP or the W3C.

In addition to the framework conditions of eIDAS, the use of the SSI paradigm faces the challenge of meeting the requirements of the GDPR. Specifically, the GDPR applies when personal data is transmitted and processed. This means that as soon as personal information can be assigned to a natural person, this person must be protected. The GDPR provides this protection. However, according to recital 14 of the GDPR, this does not apply to legal entities (Regulation

[5] For further details see: https://trustoverip.org/

(EU) 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), 2016), so not all use cases of SSI are covered by the GDPR. For example, use cases such as creating and transferring templates, standardizations, public notifications, or the public display of information about legal entities are not covered by the GDPR. Affected and relevant barriers to compliance with the GDPR that need to be considered in the architecture and functioning of SSI are the following topics:

(1) Anonymization and pseudonymization
(2) Standardization and processing of transactions
(3) Uniform understanding of roles through the definition of terms and definitions
(4) Processing of personal data

In this context, the role of blockchain technology is not to store sensitive data directly on the blockchain but only to offer the possibility to check the validity of sensitive data using, for example, revocation registries. To overcome the aforementioned compliance obstacles, SSI networks seek to enter into data processing agreements with government agencies and EU stakeholders to educate them on the subject of SSI simultaneously. As part of this, these regulators are in a state of flux due to the application of the GDPR to DLTs, so segregated data processing agreements can help support the evolution of regulators' legislation to regulate SSI ecosystems in as GDPR-compliant a manner as possible.

In this context, the use of DLTs poses another legal challenge. Since data is stored immutably, it can only be overwritten by another transaction in the append-only database, without entirely removing the old record. This contradicts the EU's GDPR, which explicitly provides for the possibility of deleting personal data. For example, such storage of personal data may become relevant in the context of the revocation registry and the associated cryptographic accumulator, as the revocation registry could be used as a link to personal data of an identified or identifiable person. ZKP-based revocation likely mitigates this as it does not reveal a correlating identifier for the VC, but nonetheless, closer investigation is required. More generally, Rieger, Guggenmos, Lockl, Fridgen, and Urbach (2019) present design principles to make blockchain solutions GDPR-compliant and therefore need to be considered in particular for SSI.

Technical challenges

Even if blockchain technology is used in SSI, this technology should always be extensively tested and questioned. For example, personal data for SSI should never be stored on such a decentralized registry. Otherwise, it may be possible to related individual identities with the identifiers used within this public network. Likewise, not all challenges regarding the scalability of public DLTs have been solved at this point. For example, the tails files, which contain entries for each issued VC of a type and are needed to use accumulators, have a file size that cannot be neglected for many entries. Thus, they are currently unsuitable for storing on DLT infrastructures and can cause bottlenecks, e.g., when they have to be downloaded and processed via mobile devices or in the IoT environment. On the other hand, work is already underway on revocation mechanisms using accumulators that are not based on tails files.

In addition, the link secrets specified for authentication are not secure identity-determining features. Unlike biometric properties, the verifier has no way of checking whether the link secret belongs to the person in question. It is possible that the link secret is passed on to other users or that several users initially deliberately select the same link secret. There are various approaches to preventing the link secret from passing on, such as using the security chip in modern smartphones, but they are not yet supported by most cell phones.

Another approach is to raise the inhibition threshold for passing on the link secret. To do this, the verifier may require much more information than is necessary. For example, an additional proof could be required about ownership of a credit card or a driver's license with the same name. In addition, a proof could be required that the same link secret has already been used in previous interactions. Another possibility would be to link the link secret to the owner's financial assets. Sharing the link secret would then be tantamount to evicting the account (Hardman & Harchandani, 2019).

Furthermore, it is possible to tie the link secret more closely to the identity and thus to a DID.

Critical view

The corresponding keys of the DID can then be derived from the link secret, for example. This derivation can, in turn, be proved without revealing the link secret. However, this procedure does not protect against an occurrence under a false DID. VCs can be tied even more strongly to a person with biometric methods but still require further implementation and are mostly dependent on specific hardware (Hardman & Harchandani, 2019).

Linking physical and digital object identities also poses a challenge for the application of SSI. Uniquely defined characteristics, such as a vehicle's VIN for VID, can be used for physical objects. However, individual care must be taken that existing identifiers can be meaningfully incorporated into an SSI architecture for objects.

With current SSI solutions, the revocation of VCs can only be performed by the issuer itself. In many cases, however, this poses a problem if the VC is revoked by a party other than the one who issued it. An example of this is an e-prescription from a doctor's office. The prescription may only be filled once, and the patient can choose the pharmacy at will. The pharmacy now has three options: It must inform the doctor that the VC has been redeemed, and the doctor then declares the VC invalid. Or it notifies all other pharmacies that the VC has already been redeemed without discrediting the privacy of the VC subject. Or all pharmacies were given the authority to revoke the VC themselves, eliminating the need to contact the doctor or the other pharmacies. This authorization for non-issuers to initiate revocations is not yet or only inadequately implemented in today's SSI solutions. How exactly this problem will be solved technically remains to be seen. Even in scenarios where the repeated use of a VC is not problematic, such as revoking a driver's license by the police in the context of a breathalyzer check, such questions arise.

6 Conclusion

Conclusion

The SSI paradigm promises a new stage in the development of digital identity management, from which a wide range of possible applications may be derived. Accordingly, the concept is already being discussed, tested, and implemented in various regional, national, and international initiatives.

This paper analyses the SSI paradigm's conceptual characteristics and technical aspects and presents three use cases as examples. It becomes clear that SSI offers advantages in individual control, data security, and full portability of identities between different services. For example, forgery- and tamper-proof digital versions of important personal documents such as ID cards, passports, birth certificates or medical confirmations can be created. However, the use cases are not limited to personal SSI but can also be, for example, digital identities of organizations and physical objects in the context of IoT solutions. This is particularly important in connection with the comprehensive digitization of companies.

Given this, SSI becomes relevant for practical application by combining several advanced technologies and concepts. For example, the use of DLT solutions could become relevant for logging multiple uses of VCs, as illustrated by the example of e-prescriptions, which cannot be addressed by the mere use of bilateral communication channels and digital certificates in the context of SSI. Furthermore, by using SSI, sensitive data can be exchanged bilaterally in a verifiable way and kept away from the blockchain, so that SSI can help bring the advantages of blockchain technology in line with legal and regulatory requirements. These functionalities enable various application scenarios in the economy, for example, for data transactions of private individuals, the management of digital identities of physical objects or the management of documents, certificates, or authentications by public institutions. Initial practical implementations suggest that SSI can significantly improve end users' individual data transactions.

Nevertheless, some challenges need to be overcome before the SSI paradigm can be deployed widely. In addition to socioeconomic challenges, legal and technical hurdles must also be overcome. We believe that the issues of governance and interoperability of SSI applications require deeper consideration. Critical questions about the extent to which an infrastructure of digital identities can be established and how it should develop must be defined in this context. In addition, cultural characteristics must be taken into account. For example, China uses a system based on a single identity that must be used for authentication for all online activities. Accordingly, state institutions can, in principle, gather far-reaching information about the activities of citizens from the digital interactions of this single identity. Consequently, it is necessary to define to what extent the infrastructure of digital identities should be designed so that cybersecurity can be in line with the privacy of the online society. In terms of interoperability, this leads to competition between proprietary and non-proprietary solutions and to the question of how these can be unified and adjusted to enable interoperability.

The uniform and individual management of digital identities are gaining increasing attention. For example, the German federal government focuses on a "European Digital Identities Initiative" to ensure uniform digital identities for the general public (Bundeskanzleramt, 2021). At the same time, the widespread integration of networked systems into our everyday lives is steadily increasing; so far, no widely adopted system for the self-determined use of digital identities has established itself. Therefore, the SSI paradigm represents a promising approach to interoperable digital identities and is thus an interesting subject for future research and practical application.

References

References

Abramson, W. (2019). CL Signatures for Anonymous Credentials. Retrieved from https://misterwip.uk/cl-signatures

ADAC (2019). Tacho-Manipulation. Retrieved from https://www.adac.de/rund-ums-fahrzeug/auto-kaufen-verkaufen/gebrauchtwagenkauf/tacho-manipulation/

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

Ben-Sasson, B., Bentov, I., Horesh, Y., & Riabzev, M. (2018). *Scalable, transparent, and post-quantum secure computational integrity*. Retrieved from https://eprint.iacr.org/2018/046.pdf

Bundeskanzleramt (2021). Digitale Identität: Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann. Retrieved from https://www.bundesregierung.de/resource/blob/992814/1881838/296c9afc2ec79f8c939360f61135aadd/digitale-identitaet-download-bk-amt-data.pdf

Callahan, J., Hardman, D., & Othman, A. (2019). Aries RFC 0231: Biometric Service Provider. Retrieved from https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0231-biometric-service-provider/README.md

Camenisch, J., & Lysyanskaya, A. (2002). A Signature Scheme withv Efficient Protocols. Retrieved from https://groups.csail.mit.edu/cis/pubs/lysyanskaya/cl02b.pdf

Cameron, K. (2005). The laws of identity. Retrieved from https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks*, *37*(2), 205–219. https://doi.org/10.1016/S1389-1286(01)00217-1

DID Communication Working Group (2019). Working Group Charter. Retrieved from https://github.com/decentralized-identity/org/blob/master/Org%20documents/WG%20documents/DIF_DID-comm_WG_Charter_v1.pdf

Regulation (EU) on electronic identification and trust services for electronic transactions in the internal market (2014).

Regulation (EU) 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) (2016).

European Parliamentary Research Service (2019). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Article 16 GDPR - Right to rectification (2018).

Goldfarb, S. (2019). Using digital identity to stamp out credential fraud and fake diplomas. Retrieved from https://www.evernym.com/blog/credential-fraud-fake-diplomas/

Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. *Frontiers in Blockchain*, *2*, 69. https://doi.org/10.3389/fbloc.2019.00017

Hardman, D. (2018). Credential Revocation. Retrieved from https://github.com/hyperledger/indy-hipe/blob/master/text/0011-cred-revocation/README.md

Hardman, D. (2019a). Aries RFC 0004: Agents. Retrieved from https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0004-agents/README.md

Hardman, D. (2019b). A Gentle Introduction to Verifiable Credentials. Retrieved from https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/

Hardman, D., & Harchandani, L. (2019). Preventing Transferrability with ZKP-based Credentials. Retrieved from https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/zkp-safety.md#technique-2-prevent-link-secret-reuse

Hardman, D., Harchandani, L., Othman, A., & Callahan, J. (2019). Using Biometrics to Fight Credential Fraud. *IEEE Communications Standards Magazine*, *3*(4), 39–45. https://doi.org/10.1109/MCOMSTD.001.1900033

References

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. *IEEE Transactions on Engineering Management*, 1–15. https://doi.org/10.1109/TEM.2020.2978014

MarketsandMarkets (2018). Blockchain Identity Management Market Size, Share and Global Market Forecast to 2023. Retrieved from https://www.marketsandmarkets.com/Market-Reports/blockchain-identity-management-market-241573621.html

McKenna, K., Reed, D., Schneider, C., & Tobin, A. (2020). Digital Identity for Commerce - An exploration of verifiable credentials and LEIs with GLEIF - YouTube. Retrieved from https://youtu.be/ag5vW4OurKs

McKinsey & Company (2019). *Digital Identification: A key to inclusive growth*. Retrieved from https://www.mckinsey.com/~/media/mckinsey/featured%20insights/innovation/the%20value%20of%20digital%20id%20for%20the%20global%20economy%20and%20society/mgi-digital-identification-a-key-to-inclusive-growth.ashx

Mobility Open Blockchain Initiative (2019). Vehicle Identity Standard. Retrieved from https://dlt.mobi/wp-content/uploads/2019/09/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Nauta, J., & Joosten, R. (2019). Self-Sovereign-Identity:-A-Comparison-of-IRMA-and-Sovrin. Retrieved from https://www.researchgate.net/profile/Rieks_Joosten/publication/334458009_Self-Sovereign_Identity_A_Comparison_of_IRMA_and_Sovrin/links/5d359f1992851cd0467b96f3/Self-Sovereign-Identity-A-Comparison-of-IRMA-and-Sovrin.pdf

Nelson, C. (2018). Zero Knowledge Proofs (ZKP): Privacy Preserving Digital Identity with. Retrieved from https://www.youtube.com/watch?v=D4iUeVbib_k

Oberländer, A. M., Röglinger, M., Rosemann, M., & Kees, A. (2018). Conceptualizing Business-to-Thing Interactions: A Sociomaterial Perspective on the Internet of Things. *European Journal of Information Systems*, *27*(4), 486–502. Retrieved from https://eref.uni-bayreuth.de/40060/

Preukschat, A. (2019). Peer DIDs: a secure and scalable method for DIDs that's entirely off. Retrieved from https://www.youtube.com/watch?v=d-5MmLLd3xY

Reed, D., Law, J., Hardman, D., & Lodder, M. (2019). DKMS (Decentralized Key Management System) Design and Architecture V4. Retrieved from https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0051-dkms/dkms-v4.md

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., & Sabadello, M. (2020). Decentralized Identifiers (DIDs) v1.0. Retrieved from https://www.w3.org/TR/did-core/

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., & Urbach, N. (2019). Building a Blockchain Application that Complies with the EU General Data Protection Regulation. *MIS Quarterly Executive*, *18*(4), 263–279. https://doi.org/10.17705/2msqe.00020

Rosemann, M. (2013). The Internet of Things: new digital capital in the hands of customers. *Business Transformation Journal*, *2013*(9), 6–15.

Schneier, B. (2018). Can Consumers' Online Data Be Protected? Retrieved from https://www.schneier.com/blog/archives/2018/02/can_consumers_o.html

Sporny, M., Longley, D., & Chadwick, D. (2019). Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web. Retrieved from https://github.com/decentralized-identity/org/blob/master/Org%20documents/WG%20documents/DIF_DID-comm_WG_Charter_v1.pdf

Statista (2020). eCommerce - weltweit, Marktprognose. Retrieved from https://de.statista.com/outlook/243/100/ecommerce/weltweit

Tobin, A. (2019). An Introduction to Self-Sovereign Identity - YouTube. Retrieved from https://www.youtube.com/watch?v=HMrBP55xROc

Tobin, A., & Reed, D. (2017). *The Inevitable Rise of Self-Sovereign Identity*. Retrieved from

References

https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Tönsing, F. (2015). Digitale Identitäten – Was braucht man zukünftig für eine vertrauenswürdige digitale Identität? In U. Bub, V. Deleski, & K.-D. Wolfenstetter (Eds.), *Sicherheit im Wandel von Technologien und Märkten* (pp. 55–61). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-11274-5_9

Vescent, H., Young, K., Hamilton Duffy, K., Sabadello, M., Zagidulin, D., & Caballero, J. (2018). *A Comprehensive Guide to Self Sovereign Identity.*

Wagner, K., Pueyo, X. V., Vandy, N., Bachenheimer, D., & Beron, D. (2020). *Decentralized Identity: What's at Stake: A Position Paper by the INATBA Identity Working Grupd*. Retrieved from https://inatba.org/wp-content/uploads/2020/11/2020-11-INATBA-Decentralised-Identity-001.pdf

World Economic Forum (2020). *Reimaging Digital Identity: A Strategic Imperative*. Retrieved from http://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf

Project Group Business & Information Systems Engineering

The Project Group Business & Information Systems Engineering of the Fraunhofer FIT unites the research areas of Finance & Information Management in Augsburg and Bayreuth. Expertise at the interface of financial management, information management and business informatics, and the ability to combine methodical know-how at the highest scientific level with a customer-, target- and solution-oriented approach, are among its special characteristics. Currently, our team consists of about 80 researchers and more than 140 student assistants.

Our research activities are thematically bundled in different research areas, which gives us extensive expertise in different areas of business informatics. This enables us to transfer current research results into practical solutions in applied research projects with numerous companies from different industries, thus creating long-term "win-win situations". In addition, we can incorporate the knowledge gained into our numerous courses to provide our students with theoretically sound and practically relevant, and up-to-date content. Our goal is to synergistically complement our range of topics with suitable research areas in the future.

Fraunhofer Blockchain Lab

The Fraunhofer Blockchain Lab was founded based on these principles, characterized by the interdisciplinary combination of economic, legal, and technical competencies. Blockchain solutions are designed, developed, and evaluated in the Blockchain Lab, which is now known far beyond national borders. Together with numerous partners from business and science, intensive work is being done to comprehensively investigate the potential of blockchain technology and to make it accessible.

At our location in Bayreuth, we have been supporting companies and public institutions in the context of applied research projects, as well as in the development of individual and demand-oriented solutions in the field of blockchain technology since our foundation in 2016. Even though blockchain technology became known through its initial application as the basis of the cryptocurrency Bitcoin, it quickly became apparent that the actual potential of the blockchain extends much further. For example, in addition to business logic mapped by so-called smart contracts, digital and self-managed identities can also be implemented with blockchain support.

In 2016, we were one of the first organizations in Germany to publish a white paper in which we examined the fundamentals, applications, and potential of blockchain technology and the role of intermediaries in various contexts. We have also received several awards for our work - including the Reallabore Innovation Prize from the German Federal Ministry for Economic Affairs and Energy and the eGovernment Prize for our project with the Federal Office for Migration and Refugees.