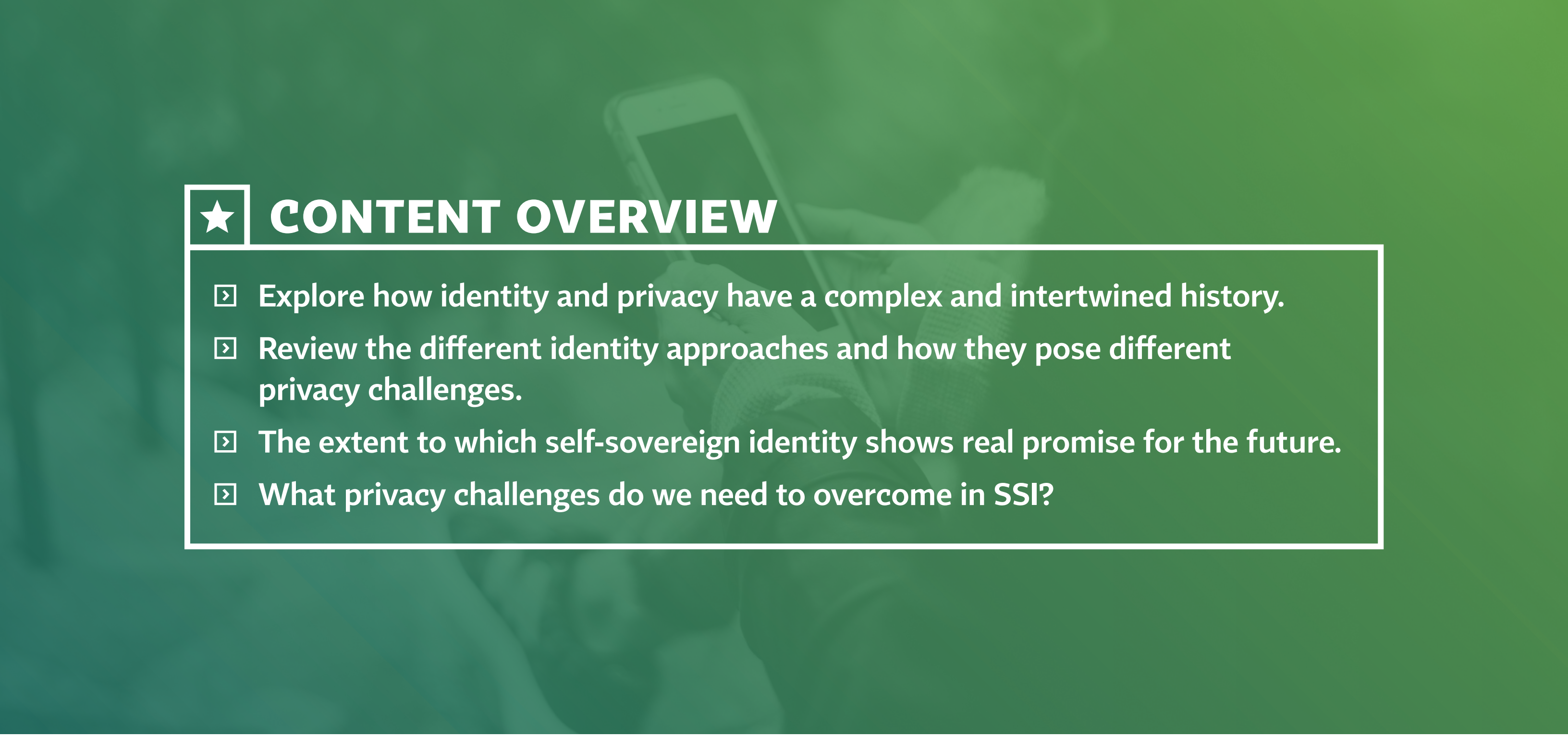
iapp WHITE PAPER

Self-sovereign identity as future privacy by design solution in digital identity?

By IAPP Principal Researcher, Technology Katharina Koerner, CIPP/US

Contents



CONTENT OVERVIEW

- Explore how identity and privacy have a complex and intertwined history.
- Review the different identity approaches and how they pose different privacy challenges.
- The extent to which self-sovereign identity shows real promise for the future.
- What privacy challenges do we need to overcome in SSI?

Executive Summary

"The internet was built without a way to know who and what you are connecting to." More than 15 years have passed since digital identity thought leader Kim Cameron shed light on the missing identity layer of the internet in his influential guidelines, "The Laws of Identity."

Since then, ongoing research and maturing technologies have led to a wide variety of segments of the digital identity landscape aiming for better online identity management. Nearly every web-based application utilized in day-to-day life leverages digital identity services. With the increasing challenge of validating the identity of individuals to prevent fraud and provide greater security, more personal information is being processed than ever before across identity processes.

Workforce identity and access management lead the way with frameworks and services for governing data and system access rights for employees, contractors, partners, or suppliers. This facilitated the development of a growing field of customer identity and access management systems based on single sign-on solutions, multifactor authentication, and user privacy and consent management.

Nevertheless, these solutions still bring with them the potential risks of identity misuse and theft. Trustworthiness of centralized platforms — that might use the collected data for user-behavior analysis and prediction systems — remain an ongoing challenge. Against this backdrop, good digital identity has been called one of the "new frontiers" in value creation for individuals and institutions around the world.

In seeking to address these challenges, new identity models, processes and regulations that provide more control and choice to the data subjects and increase transparency on how identity service providers handle personal data have emerged. Those novel approaches, often referred to as "self-sovereign identity" based on distributed ledger technology, are pushing for the next evolution of identity management models.

SSI claims that users' identities should be controlled by themselves via mobile wallets. Instead of organizations issuing or storing credentials, individuals themselves keep their identity stored in their devices and disclose personal information only as needed.

These decentralized identity solutions are closely related to the developments of Web3, the decentralized web. Aiming to cease storing personal information in central databases, Web3 expands upon peer-to-peer interactions based on distributed ledger such as blockchain as its core technology.

In our research, we encompassed desk-based work in addition to conversations with multiple thought leaders in the digital identity space to explore how identity has evolved and if SSI solutions provide increased hope for greater privacy protections now and in the future.

What we found is that digital identity is complex, with a big variety of different players and elements coming together in an effort to provide a seamless user experience. While privacy may not always be the central driver of these developments, SSI technology has the potential for better privacy protection of digital identities as it supports the users' control of their own identifiers and allows for their selective disclosure. This aligns with the principles of data minimization and purpose limitation.

At the same time, ensuring privacy by design and accountability throughout the digital identity system in compliance with different legal and regulatory privacy requirements still presents a challenge that needs to be tackled in more detail. Private-public collaboration on building infrastructure for SSI architectures and educating both organizations and end-users about their potential and real-world use cases will be indispensable for maturing the field further.

What are the components of digital identity?

Attributes and identifiers

While digital identity is increasingly taking center stage of the data-driven economy, it is an umbrella term for plenty of different approaches. Several terms are associated with digital identity.

In general, digital identity can describe a unique representation of an entity in the context of a digital service, be it a person, organization, device, SIM card, passport, software application or website. More often, it refers to the unique online or offline digital identity of a person, represented by attributes. Some attributes may be self-owned, like a name, birthdate, email address, username, or biometrics; others may be issued by institutions, such as a passport, driver's license or professional certification.

A specific set of attributes — also called identifier — is then used to identify an individual in a specific role or context. Anyone can have more than one digital identity. In a voter's register, the combination of the attributes name, address and birthdate can make up an identifier that unambiguously distinguishes a voter, but another set of attributes may identify someone as a citizen, driver, member or student.

Authentication via proofing and credentials

The initial authentication as part of the enrollment in a service is often called "identity proofing." The importance of remote identification processes became evident during the global COVID-19 pandemic, when in-person identification was often not possible. Depending on legal requirements and internal policies, it can vary how strict the identity of an entity must be shown.

Regularly, identity proofs (e.g., a passport) need to be attested and validated by a relevant identity authority (in this example, the national authority as issuer of the passport) to be accepted by an identity verifier (e.g., a police officer).

The European Union Agency for Cybersecurity and European Telecommunications Standards Institute are collaborating on an ongoing basis to support EU requirements for identity proofing, publishing reports and organizing workshops.

After an identity is proven successful, "credentials" as representations of an identity are used for ongoing authentication. Credentials are a set of attributes digitally signed by an issuer. It can be something a person knows (e.g., a password), something a person has (e.g., an access card), or something a person is (e.g., biometrics). The more factors incorporated in the authentication system, the stronger it is.

Privacy and security challenges lead to evolution of digital identity

Traditional centralized identity

To a large extent, identity management on the internet is still organized in a centralized manner. Attributes and identifiers have some privacy implementation as they are considered personal information. This personal data is stored in the databases of many different service providers, multiplying individual privacy and security risks.

Federated identity management

These problems led to the rise of federated identity management and single sign-on for authentication, offering multiple advantages. SSO enables users to sign on with just one set of credentials to access multiple applications and websites. This third-party service that stores the user's access credential is known as the identity provider. When logging in on a web application with Facebook, LinkedIn or Google, those companies act as middlemen to the web application. Federated identity management systems increase the user-friendliness of authentication procedures. At the same time, they offer strong authentication to service providers.

But while federated identity can simplify the user experience in many ways, it still requires trust in the identity provider. Much of the control over this identity data is effectively handed over to the identity provider, which can track the online services used and is able to collect information about the user's activity. This brings a risk of potential data leakage through single points of failure and data reuse, leaving surveillance concerns and privacy issues.

User-centric identity paving the way

Against this backdrop, the concept of a user-centric identity and user-centric designs drew increasing attention, claiming "every individual ought to have the right to control his or her own online identity."

New methods with a focus on decentralization for digital identity were developed, working on the interoperability of existing identity management systems and increasing opportunities for users to consent about how and with whom identity is shared. Examples include protocols such as OpenID 2.0 (2006), OAuth (2010), Fast IDentity Online Alliance (2013) and OpenID Connect (2014). However, with these approaches, the user's identifiers such as usernames and email addresses are still controlled by a centralized provider.

Evolution to verifiable credentials

At the same time, new privacy-enhancing technologies such as zero-knowledge proofs, matured. ZKPs are cryptographic protocols that allow the user to send proofs for some properties of data to the service provider, but not the actual data itself.

Initially, the use of ZKPs was realized in privacy-preserving attribute-based credentials, which introduced a paradigm change in identity solutions. Well-known examples of privacy-preserving ABC-related identity models are IBM's Idemix, Microsoft's U-Prove and the EU-financed research project ABC4Trust.

With these approaches, the user could for the first time collect credentials from various identity providers that vouch for their correctness. This information is stored in a digital wallet. Subsequently, users decide themselves on the amount of information they want to disclose to a given verifier.

The selective disclosure of personal information is achieved by hiding some of the attributes of the received credentials. At the same time, the digital signature of the issuer remains verifiable, confirming the partial information that was sent to the verifier.

With verifiable credentials, a completely new concept and opportunity was introduced into digital identity, enabling data minimization on a completely different scale. With verifiable credentials a person can prove they are above a certain age, allowed to drive a particular motor vehicle, require a particular medication, trained and certified in a specific profession, or cleared to travel internationally.

Nevertheless, the risk associated with a central identity authority — responsible for the validation of credentials — remained. Those developments and open-ended questions led to the next evolution in digital identity: verifiable credentials and user-controlled selective disclosure based on decentralized infrastructures.

Self-sovereign identity — privacy by design in digital identity?

As the developments of new technologies addressing privacy concerns in the context of digital identity intensified, the growing recognition of decentralized identity models in research and practice pushed conversation around secure online identities to a new level.

In 2016, digital identity thought leader Christopher Allen raised broad awareness about the new concept of decentralized identity in his thought-provoking article "The Path to Self-Sovereign Identity." At the same time, early public funding and joined public-private consortia in Canada, the EU, South Korea and the U.S. contributed to an increasing maturity of the field.

> ***"At all of these events I want to share a vision for how we can enhance the ability of digital identity to enable trust while preserving individual privacy. This vision is what I call "Self-Sovereign Identity.""***

While a uniform definition of self-sovereign identity is still missing, there is the common understanding that SSI is fundamentally based on the concept of using verifiable credentials that can be selectively disclosed by the user. End-users directly receive verifiable credentials from the issuers of credentials, with a cryptographic hash of the transaction reliably proving ownership.

When authenticating themselves, users can do so independently from the issuer while controlling which attributes they want to disclose or keep private. Using separate partial digital identities for different digital relationships prevents data correlation and reidentification.

Decentralization as key ingredient of novel approaches

In decentralized identity, no centralized registry, identity provider or certificate authority validating the credentials get involved. Instead, a public ledger such as blockchain or any other valid attribute attestation that offers similar functions is used to verify transactions and information.

Simplified, this means distributing the storage of identity information across a system of distributed computers, also called nodes. The nodes constitute a shared, replicated and synchronized decentralized network, which serves as register of the identity data and a platform for exchanging the identity information. Confidence in the correctness of the identity data is achieved by reaching an agreement (consensus) between the nodes.

Decentralized identifiers as the key new building block of decentralized digital identity

As a new type of globally unique identifier, decentralized identifiers constitute the basic building block of a new layer of decentralized digital identity and public key infrastructure. DIDs can refer to any subject, for example a person, organization, IoT device, data model, or any other given abstract entity.

When an issuing authority issues verifiable credentials to a user or holder, it attaches its public DID as the cryptographic counterpart to the verifiable credentials. The same public DID is also stored in the blockchain.

When an entity wants to verify the credential provided by the user, this is done by checking the DID on the blockchain. This makes the identity information instantly verifiable without necessarily relying on the issuer. In that sense, DID can be compared to URLs in a browser, which are used to locate a representation of a resource on the web.

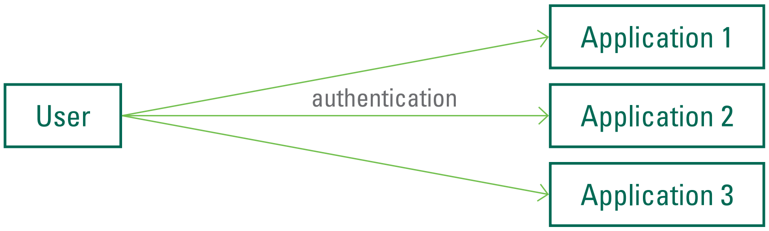
The significance of DID as the core component of an entirely new layer of a decentralized public key infrastructure for the internet has very high potential impact. One of the central collaboration spaces for decentralized web — the Rebooting the Web of Trust initiative — compares it to the development of the current largest PKI in the world, the SSL/TLS protocol for encrypted web traffic.

Privacy principles and SSI

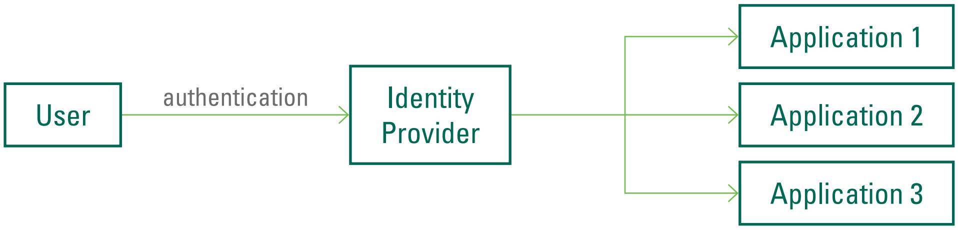
Looking at the principles of self-sovereign identity that Allen defined in his timeless article, similarities to basic privacy principles become obvious.

Focusing on the protection of user rights, Allen stresses that users must always maintain control over their identities. This includes consistent access to their own data and consent to its use. Systems and algorithms must be transparent and allow for interoperability of information and services as well as portability of identity information. Following the principle of data minimalization, only necessary personal data for a service should be collected.

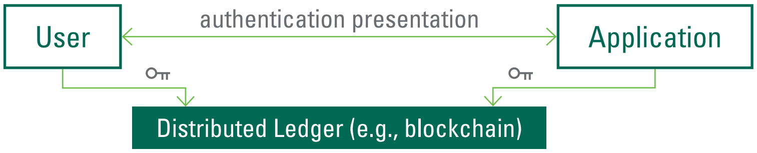
CENTRALIZED IDENTITY



FEDERATED IDENTITY



SELF-SOVEREIGN IDENTITY


User
authentication presentation
Application
Distributed Ledger (e.g., blockchain)

Increasing standardization of decentralized identity and open questions

Since the first definition of principles for SSI by Allen, the commercial implementation of primarily blockchain-based decentralized identity solutions has been grown at a fast pace. The list of functional and nonfunctional requirements of such solutions has particularized. Verifiable credentials as well as decentralized identifiers have been described in detail in recently published W3C standards.

Associated with those standards is the definition of methods for DID to realize the features described by those specifications. DID methods describe how a specific DID scheme can be implemented on a particular network, including creating, reading, updating, and deleting DID records. Currently more than 100 DID methods are registered, with prominent examples being Bitcoin, Ethereum, Sovrin, or the InterPlanetary File System. While they all support the same basic functionalities, they use different implementations schemes, e.g., how a DID is created or where and how DID documents are stored.

The interoperability between different networks remains an ongoing challenge. The transportation of verifiable credentials, respectively the main protocols for a SSI infrastructure, is not yet agreed upon.

One opportunity could be to extend OpenID Connect to support SSI, and specifying a set of protocols enabling it to present W3C Verifiable credentials. The OpenID Foundation is working on this in liaison with the Decentralized Identity Foundation.

The world's response to the concept of SSI

European countries have been spearheading the implementation of SSI for quite a while.

In 2019, Germany and Spain announced plans to cooperate on building an ecosystem of "user-centric, decentralised identities." The German federal government stated that it "recognizes that digital identity is a fundamental building block for successful digitisation. It is therefore pursuing the development of an infrastructure that allows the secure exchange of attributes, is suitable for Europe-wide use, and functions equally for identities of people, institutions, and things. The basis is the self-sovereign Identity (SSI) technology." In September 2021, Germany signed a similar declaration with Finland to drive the development of solutions based on self-sovereign identity. Also, the Netherlands has an comprehensive approach aiming at creative implementations of SSI.

In April, France announced an update of Alicem, the nation's digital identity system app, based upon self-sovereign identity. It shall enable holders of the digital wallet to generate only identity attributes they consider necessary to share.

In the U.K., a digital identity and attributes trust framework is in development, setting out the government's vision for the rules the future use of digital identities. This goes hand in hand with SSI becoming a priority for the European Union.

In 2016, the Regulation on electronic identification and trust services, known as the eIDAS, was established as a European digital identity framework to mutually recognize digital identification, but its uptake remained limited. Therefore, the European Commission introduced the new proposal in June 2021, which is currently under review.

A crucial element of eIDAS 2 is the concept of a European Digital Identity wallet. This wallet shall provide all EU citizens, residents and organizations with the ability to prove their identity across the EU. Users would be able to store credentials and features related to their identity and display them online and offline upon request, accepted in public and private services across the EU.

According to the proposal of the European Commission, the electronic identification shall use digital identity solutions that consider different technical solutions, "including the use or combination of various cryptographic techniques, such as cryptographically verifiable identifiers, unique user-generated digital pseudonyms, self-sovereign identities and domain specific identifiers using state of the art encryption technology." As the Council of the European Union pointed out in a progress report, the eIDAS 2 proposal "provides for user control and data protection and the targeted sharing of identity data limited to the needs of the specific service requested." Thus, under eIDAS 2 a self-sovereign identity structure can now be potentially employed.

In May, the European Parliament published its draft report on the proposal. Among 139 proposed amendments there are potentially impactful recommendations, such as expanding SSI to IoT devices. Another proposed amendment aims at prohibiting biometric data used for identification and authentication of a natural person in the context of eIDAS 2 being stored in the cloud.

Furthermore, the draft report suggests including a legal definition and anchoring the privacy-enhancing technology of zero knowledge proofs in the update. ZKPs shall provide the basis for the European Digital Identity, "allowing for verification of claims (…) or attestation of attributes without having to provide the source data, to preserve the privacy of the user (…) while presenting a proof with legal effect."

While the eIDAS 2 regulation remains challenging due to the high legal and technical complexity of field, the EU is already preparing for infrastructural interoperability as one key component of the EUDI wallet.

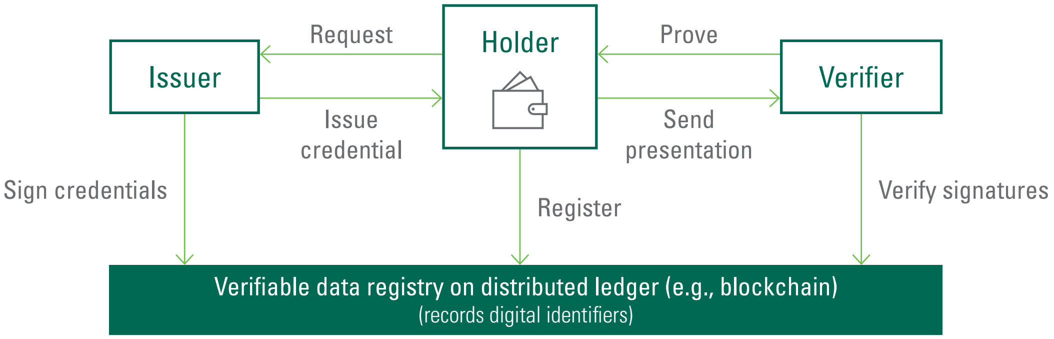
The EU Self-Sovereign identity framework is part of the European Blockchain Services Infrastructure, a joint initiative of the European Commission and the European Blockchain Partnership which consists of a network of distributed nodes across Europe with the goal to create "a generic profile for the full life-cycle of self-sovereign identity", building upon the W3C Decentralised Identifiers, W3C Verifiable Credentials, W3C Verifiable Presentations, OpenID Connect for Verifiable Credentials, GDPR, eIDAS, and other EU Regulations.

ESSIF works on a governance framework as well as specifications and guidelines for the EBSI wallet, public and private ledgers, Trusted Issuers Registries, and APIs to access diverse services. Alignment with EU regulations, particularly the EU General Data Protection Regulation and eIDAS 2, interoperability, and the preservation of democratic values in the implementation of self-sovereign identity shall be ensured.

An EU self-sovereign identity infrastructure is further supported by ongoing funding, including the European Union Digital Identity Wallet Consortium. This year, public- and private-sector companies were invited to bid for up to 37 million euros for building and running multiple use case, cross-technology pilots to implement the European Digital Identity Framework.

Another example for financing projects in the space is the European Self-Sovereign Identity Framework Lab which earlier this year selected proposals for taking part in a funded 7-month support program, aimed at completing and reinforcing the eSSIF-Lab SSI

VERIFIABLE CREDENTIALS DATA MODEL



Modified from w3.org.

Framework. The ESSIF-Lab ecosystem shall enable businesses to work with organizations and individuals on negotiation and business transactions on basis of a scalable and interoperable self-sovereign identity infrastructure.

Developments in other countries

The idea of self-sovereign identity as the future of digital identity isn't spreading just in the EU.

International organizations like the World Economic Forum and World Bank are also emphasizing the potential of this new technology, driving economic inclusion, or providing a unique and secure digital ID to individuals without valid documents, claiming identity as a human right.

Many more countries or communalities prepare for deploying digital identity models based on verifiable credentials or have decentralized identity frameworks in place, with examples including Canada, South Korea, Buenos Aires, or U.S. states like Illinois. The new U.K. draft Data Protection and Digital Information Bill, introduced July 18, 2022, includes the statutory foundations of a new Digital Verification Services Trust Framework which will apply to identity and attributes holder services including those offering SSI solutions.

Groundbreaking work was done in the U.S. state of Wyoming with its Digital Identity Act having become effective on July 1, 2021. This act offered the first definition of personal digital identity in the U.S. as "the intangible digital representation of, by and for a natural person, over which he has principal authority and through which he intentionally communicates or acts." The concept of a principal having authority over his identity is a clear restatement of self-sovereign principles.

On a federal level, the U.S. National Institute of Standards and Technology provided a white paper on blockchain identity management approaches in January 2020. In this paper, NIST recognized that traditional identity management — where organizations store the credentials or use third parties to store them by utilizing federated models — creates interoperability, security, and privacy concerns. It also provides a taxonomy for blockchain architectures and governance models, describing emerging standards and use cases and elaborates on security and privacy aspects.

A very recent development would ramp up the U.S. government involvement in the digital identity space. Building on previous work, the Improving Digital Identity Act 2022 was introduced in the U.S. Senate on July 13, 2022. The bill aims at enabling people in the U.S. to verify the identity or an identity attribute accessing a service online or through other electronic means. This includes regulation of consent-based identity attribute validation services and augment private sector digital identity and authentication solutions; aspects that had not yet been addressed by NIST.

In the private sector, major technology companies like Microsoft, IBM, Bosch or Workday are active in the development of SSI solutions.

Potential uses for SSI

Decentralized identity is thought to have a variety of potential uses, ranging from sharing publicly verifiable data or privacy-preserving solutions for individual users. Pilots and real-world applications are on the rise, while the list of potential use cases is long.

Recent applications include SSI for combating human trafficking or identity documentation for refugees. According to the World Bank's Identity for Development database, about 1 billion people lacked proof of legal identity in 2018. Several initiatives aim to create decentralized identity infrastructures and services to fill this gap, such as building credit history or delivering cash aid to refugees.

In banking, SSI could be applied for opening accounts, fraud prevention, compliance with anti-money laundering and Know Your Client laws, proof of funds, credit risk evaluation, as well as ownership, exchange and trading of financial assets. In supply chain management, it could help with asset traceability, the networks of sensors, and the internet of things.

In education, the issuance of transcripts, diplomas, and certifications as verifiable credentials can be used in job applications. In health care, potential use cases are the issuance of prescriptions, submitting claims to insurance companies, sharing health records or battling COVID. Another big arena is government services like issuance of driver's licenses and birth certificates, or the maintenance of public registries of voters.

An example use case in detail — Age verification

One concrete example of the application of the new technology to open questions in data governance is age verification. Regulators are increasingly tracking if websites and mobile applications that offer adult content, such as online betting, alcohol, cannabis, or pornography adequately protect minors from accessing their services.

In the EU, the legal requirement to protect children from harmful content is based on the EU Audiovisual Media Services Directive. A highly relevant privacy aspect, implicitly establishing the need to verify age, can further be found in GDPR Article 8(2): Online service providers have an obligation to check age and parental consent and must make "reasonable efforts" to do so, "taking into account the technologies available."

Recent regulatory guidelines emphasize the increasing importance of age verification that is built with state-of-the-art technology.

In its guidelines on consent adopted in May 2020, the European Data Protection Board emphasized that any measures for age verification should be proportionate to the nature and risks of the processing activities. The EDPB summarizes that verifying age is implicitly required by the GDPR. If a child gives consent when not being old enough to do so, it will render the processing of data unlawful. Regarding what is reasonable to collect, the EDPB argues for a proportionate approach, which "may depend upon the risks inherent in the processing as well as the available technology."

France's data protection authority, the Commission nationale de l'informatique et des libertés, echoed this in a legal opinion that emphasized the relevance of data minimization in the context of age verification. According to the CNIL, collecting information about age solely for verification purposes increases the risk of likability and identification of individual users.

Instead, the CNIL proposed several principles for a privacy-respecting age verification system: proportionality, minimization, robustness, simplicity, standardization and third-party intervention. It suggests a proof-of-age system that incorporates a double anonymity mechanism. A trusted third party could share only the strictly necessary attributes of the users' personal data with the application at stake while not identifying the website itself. In a report from July 2022, CNIL notes that current systems are circumventable and intrusive and calls for the implementation of models that are more respectful of privacy. For example, a privacy-friendly age verification system could be built on zero-knowledge proofs, CNIL's Digital Innovation Laboratory points out.

Along the same lines, the Regulatory Authority for Audiovisual and Digital Communication issued injunctions to several pornographic websites requiring them to take measures to prevent minors from accessing them. A self-declaration process to access such websites was not considered sufficient.

In the U.K., the Information Commissioner's Office published an opinion on Age Assurance for the Children's Code in October of last year. It also expands on the idea that the use of third-party suppliers may contribute to data protection compliance.

> ***For example, the ICO writes, "An organization may simply receive a 'yes or no' outcome of whether the user is under or over 18, rather than processing a copy of the user's passport or identity document."***

In the U.K., the proposal for a new Online Safety Bill from March 2022 foresees a new procedure for all web applications offering user-to-user content of sexual nature to verify that their users are over 18. The technical specifications to put this into practice are not laid out in detail, but companies will need to implement robust measures for age verification to prevent children from accessing such services, otherwise facing enforcement.

Similar developments can be observed in the EU and the U.S. In the EU, the European Commission-funded project euCONSENT is working on an EU-wide computer network for completing online age verification and securing parental consent. In the U.S. the California Age-Appropriate Design Code Act, requiring websites to verify the ages of visitors, was proposed earlier this year and moved to the Senate for consideration.

In all these cases, a growing number of solution providers offering age verification with SSI and zero knowledge proof could become a game-changer in the field.

Takeaways for privacy pros

While SSI is very promising, its features of security and privacy of these systems are not yet fully understood. Most solutions depend on using a reliable and scalable blockchain platform — a field that is very much in development on its own. The argument that transactions on the blockchain are permanent in nature and therefore might not be compatible with data subjects' rights to rectify, alter and remove data privacy, is persistent. Is any data added to a blockchain permanently available? What are technical solutions to help the data subject to utilize their rights? How does this relate to SSI?

Currently, a wide variety of different SSI approaches — including on-chain and off-chain credential storage methods — coexist. This brings with it different usability, privacy, and security implications. Against this backdrop, regulators need to ensure the enforcement and alignment of the GDPR and eIDAS to provide developers and users with sufficient legal interpretability of the new technologies and developments.

Security and privacy question posed by SSI and its complexity are still under investigation. For example, how big is the risk for correlation when more and more individual metadata is shared with various relying parties and credential issuers? Do decentralized identifiers always need to be considered personal data?

In addition, three key operational privacy challenges stand out which are likely to be central to SSI's success:

1. **Clear accountability:** In a decentralized approach it is critical to make clear who is accountable at which stage. Ensuring accountability throughout the digital identity system is a great opportunity. It enables demonstration of how organizations manage privacy and comply with applicable laws and regulations, and develop and sustain people's trust.
2. **Transparency:** Given the complexity of the solutions and to what extent, SSI needs to be explained in a user-friendly way, truly addressing the different legal and regulatory privacy requirements that exist in different countries.
3. **Key management:** Unlike traditional identity management models where identity providers are managing identity data and secret keys, in SSI this responsibility is placed on the shoulders of the users. Addressing the key management challenges in the SSI architecture is a necessary step toward the broad adoption of SSI.

Rolling out the vision of an identity standards architecture for different decentralized digital identity services and assuring their interoperability and integration with existing systems will take several years. All the while, optimal technologies for decentralized digital identity services and standardizing those technologies is still a work in progress. Ongoing research for building privacy-respecting schemes is necessary.

Nevertheless, there are several reasons why SSI technology can be seen as an effective basis for better privacy protection of digital identities. Distributed ledger technology holds the potential to balance privacy and state-of-the-art security. Supporting the users' control of their own identifiers and allowing for selective disclosure and pseudonymization aligns with the principles of data minimization and purpose limitation.

With ongoing research in the field and growing awareness of the potential for privacy protection of SSI solutions, the concepts of privacy by default and privacy by design are increasingly adopted for new architectures using distributed ledger technology. It will, however, need the private sector to follow a SSI market roadmap, and to implement and use the opportunities of SSI to complete this (r)evolution of digital identity.

Contact

Mark Thompson
Chief Strategy Officer, IAPP
mthompson@iapp.org

Katharina Koerner
Principal Researcher, Technology, IAPP
kkoerner@iapp.org

IAPP Research and Insight
research@iapp.org

Follow IAPP on Social Media

Published August, 2022.

The IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.