Self-Sovereign Identity in Telecommunications Services

TABLE OF CONTENTS

Abstract	5
Introduction	6
Evolution of the Identity Stack	8
Benefits of SSI for Data Privacy	9
SSI Model, Actors, Governance, and Economics	10
Value for the Carrier in this New Identity Model	12
Examples of How Telecom Can Use SSI	13
Current Adoption of SSI-Based Digital Identity	14
References	15
Copyright and Disclaimer	16

ABSTRACT

The concept of digital identity is increasingly important in today's technology-driven economy and society. The proliferation of IoT devices and decentralized infrastructures, coupled with increasing concerns about data privacy, have led to a growing need for secure and trustworthy digital identities to protect the use of personal data.

The constant evolution of technology, including the emergence of the metaverse, presents new challenges for portable identity and authentication across physical and virtual domains. This trend means organizations need to focus on trust, security, and privacy.

There is also increasing regulatory focus on privacy laws, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), as well as consumer demand for more control over their personal data. All of this further underpins the importance of digital identity.

Recent innovations now make it possible to establish a self-sovereign, or self-managed, identity (SSI), along with verifiable credential proofs of information. With this SSI and related information, users can control with whom they share their information. SSI can unlock personal data in a way that fosters greater trust between consumers and businesses while also helping companies comply with privacy regulations.

This paper examines how the traditional identity stack needs to adapt to the regulatory environment and how a new SSI standard can be applied across use cases. It also explores how SSI can help communications service providers comply with new data privacy mandates and create value for their customers.

INTRODUCTION

There have been a number of developments in technology, such as the Internet of Things (IoT), decentralized infrastructures, and growing regulatory and consumer concerns about data privacy. The need for paperless authentication during the COVID-19 pandemic has contributed to a perfect storm around the topic of digital identity. These factors have been compounding for some time and are causing digital identity to become increasingly important in the rapidly evolving, technology-driven economy and society.

A digital identity is the information that computer systems use to verify and establish trust in an organization, person, application, or device. The use of digital identities is becoming the foundation for organizations of all types, including private companies, government agencies, and civil society associations, as well as the individuals and groups they serve. Digital identity is now essential for identifying and establishing trust in the entities that an organization interacts with and should be a core part of any organization's operations. It should be a central focus for any data-driven organization that aims to be a leader in its field.

Technology Evolution

Connected cars, smart homes, smart cities, remote health, and digital industries are just a few examples of how technology is increasingly being integrated into every aspect of our lives. This constant evolution, improvement, and advancement of technology is essential for enhancing our experiences in the digital world and our extended reality. The metaverse, a virtual world where people can interact in real-time, represents the most extreme technological progression to date. A decade ago, our ability to communicate digitally was limited to voice calls and text messages. Now, with the proliferation of connected personal devices and the emergence of the metaverse, we are exploring possibilities that were once unimaginable.

However, these decentralized devices, infrastructures, and virtual worlds also create potential challenges for portable identity and authentication across physical and virtual domains. Ensuring the trust, security, and privacy of your data when connecting, sharing, or transacting with others will be of paramount importance.

Privacy Regulation

When tracking technologies became available years ago, data collection was yet not regulated for most jurisdictions. Website owners could freely collect visitors' data and use it for any purpose they wished. That has changed. The existing privacy laws were not sufficient for regulating data collection and use, so governments began passing new laws or updating the existing ones. As technology changes, governments try to keep up with the changes and requirements needed in the privacy laws.

In May 2016, the EU enacted the GDPR [1] to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business. In 2018, California passed the CCPA [2] to enhance privacy rights and consumer protection for the state's residents. Other states have enacted similar privacy laws. At the time of this report, a federal privacy bill is being considered in the US, along with amendments to Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA) [3].

Consumer Trends for Privacy

This growth in device ownership and connectivity in general has consumers thinking more about their data's privacy and security. As Figure 1 shows, consumers want to exert more control over their data and trust that digital organizations will respect their preferences when consenting to its use.

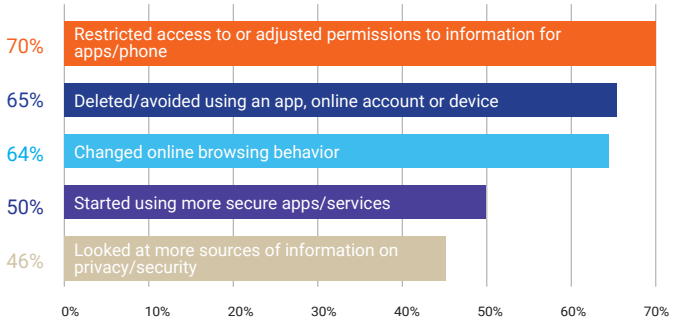


Figure 1: How Consumer Behavior has Changed Due to Perceived Privacy Issues [4]

Data Breaches

News stories about data breaches are sometimes difficult to avoid and even more difficult to digest. Data is increasingly valuable to businesses, especially data related to customers and payments. Criminals find that data is valuable too, and use it fraudulently.

USD 4.35 million
Average total cost of a data breach

83%
Percentage of organizations that have had more than one breach

Data breaches now cost companies an average of $4.35 million per incident, according to a recent security report [5]. This is the highest amount in the report's 17-year history.

Self-sovereign identity (SSI) could be used to prevent data breaches by giving individuals more control over their own personal data and reducing the number of centralized authorities that have access to their data. By using SSI, individuals would be able to create and manage their personal data and control whom they share this data with rather than relying on third parties to do so.

As the cost of breaches continues to rise, and with consumer personal information remaining the primary target, companies need to securely store customer data when onboarding them or verifying a transaction. Companies must explore whether alternative technologies such as SSI can be used to prevent them from sitting on vulnerable data silos.

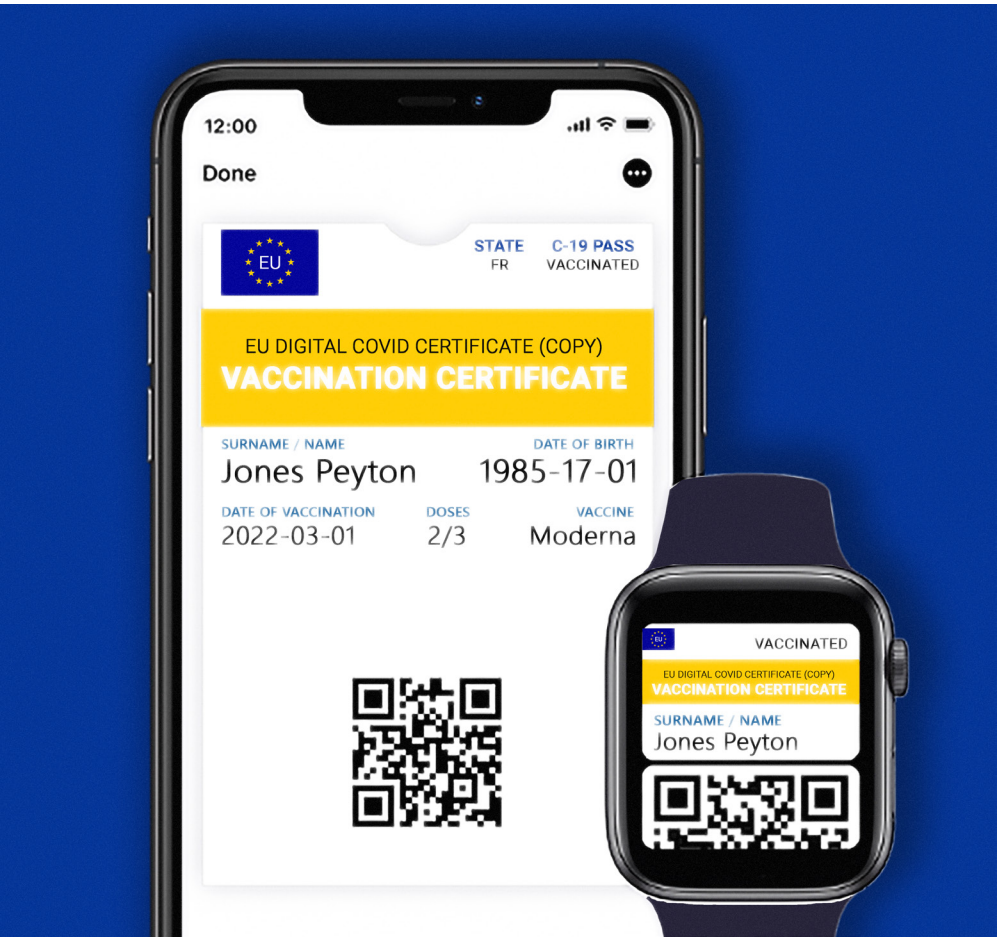
Pandemic

The pandemic saw a rise in digital identity health certificates issued by governments and health services to provide proof of vaccination, infection recovery, and certified negative test results. These could be easily verified by shops, restaurants, airlines, and hospitals, including across national borders. These certificates were based on the decentalized identity technology.

The post-COVID-19 move toward online workstyles and lifestyles has made it increasingly difficult to reject the ease consumers have experienced in their day-to-day online interactions, from working from home to buying online. To meet this demand, companies are focusing more on their digital platforms, simplifying processes for consumers, and enhancing their data management.

The Need for a New Approach to Digital Identity and Privacy

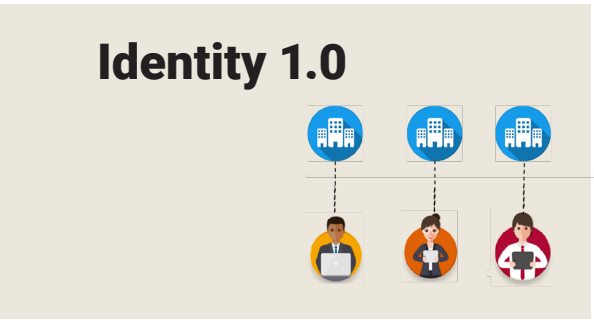
Digital identity is a rapidly evolving field with many current developments and technological advancements. However, it is a complex area that presents challenges for both individuals and businesses. There is a lack of universal standards and no one-size-fits-all solution for all needs. It is important to understand the specific needs and challenges of each party involved in the value chain and their unique user journey. Despite these challenges, digital identity has become a top priority for many organizations and is essential for effective communication with customers and suppliers.



EVOLUTION OF THE IDENTITY STACK

Over the past few years, identity and access control to internet-based applications have not evolved much beyond the initial identity stacks, which were based on controlling access to enterprise computers.

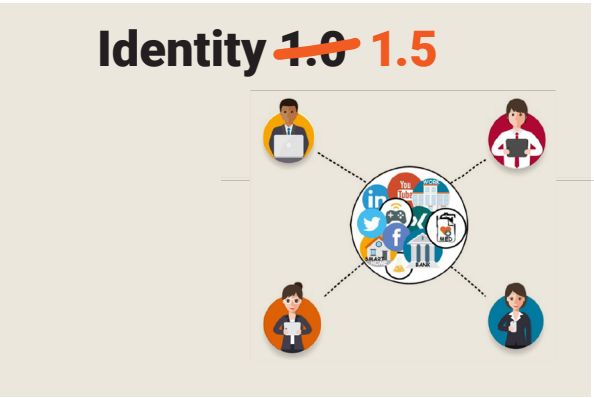
Siloed Identity



Under a siloed model that we can call "Identity 1.0," individual organizations manage databases of credentials for users. During authentication, users provide credentials and are granted access to a system's resources based on that identity.

The challenge of this model is that individual identities are applied only to specific systems, so users must juggle several different identities across platforms. This placed ownership of identity information into a loose collection of businesses. It also undermined security because people use simple and identical passwords across multiple platforms so they won't forget them.

Federated Identity



To address the problem of siloed identity, major platforms began connecting authentication systems through federated identity management. This is still fundamentally the Identity 1.0 stack, but we can call it Identity 1.5. In this model, the credentials from one platform can authenticate a user on another platform. For example, when users log in to a platform, they are given the option to use identity credentials supplied by another organization so they can be authenticated using federated identity.

The organizations managing consumers' federated identity do so because they are popular and enable them to still control and observe how those identities are used. They essentially use personal identity to mediate how people interact with the rest of the web. While this might work for general-purpose computing, it is unacceptable for enterprise use or for anyone concerned with identity and sovereignty.

Self-Sovereign Identity

SSI refers to a model where individuals and organizations have ownership and control over their own identity.

This new approach to identity, known as "Identity 2.0," is not mediated or provided by third parties. It cannot be traded, sold, or modified without the user's knowledge. It is similar to a passport, which is issued by the government but ultimately belongs to the individual who holds the physical document and has the power to present it as they see fit.

SSI recognizes that personal information is a valuable commodity for businesses, but it is also a critical aspect of a person's or organization's identity that should be under their control.

Although the concept of SSI has been difficult to achieve in the past, new models and technologies are making it more feasible.

Blockchain

The blockchain is a decentralized and unchangeable record of digital transactions on a particular network. The fundamental principle of a blockchain is that individuals on the network own the information or assets being exchanged.

Although blockchains are often associated with cryptocurrency, private blockchain ledgers can also be used to provide permanent identification credentials to individual users. In this model, the credentials are owned by the individual who holds them, rather than the network as a whole, promoting a form of self-sovereignty.

Decentralized Identifiers

Decentralized identifiers (DIDs) are a global technical standard for secure, cryptographic identifiers designed by the World Wide Web Consortium (W3C). These identifiers use peer-to-peer technology to eliminate the need for intermediaries to authenticate and own identification information. DIDs are gaining popularity as an open and flexible standard. The EU has even developed a schema for DIDs as the foundation of the European Self-Sovereign Identity Framework.

BENEFITS OF SSI FOR DATA PRIVACY

SSI is a unique type of digital identification that differs from both traditional physical IDs and other digital IDs. One key feature of SSI is its use of a secure, peer-to-peer network, illustrated in Figure 2, that connects the issuer, verifier, and owner of the ID. This network allows for greater control and autonomy for the individual owning the ID, making SSI a potentially more effective and efficient option for identifying oneself and accessing services.

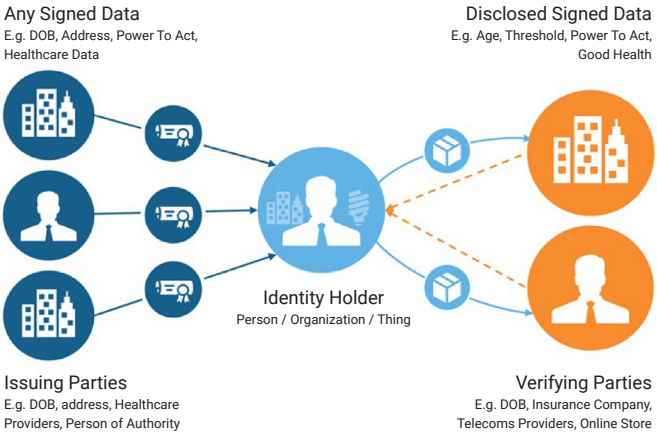


Figure 2: Identity-Owner-Centric Approach to Data Sharing

In SSI systems, data about the identity holder is stored in a "verifiable credential" that is cryptographically signed by the issuer. This credential is held only by the identity holder, who can choose to present it to a verifier when they need to be verified. The use of cryptographic hashing in SSI systems ensures that these credentials are tamper-proof and secure. Additionally, the SSI provider does not have visibility into the exchange of credentials, making the process of issuing credentials faster and simpler. These characteristics of SSI make it a powerful tool for secure, efficient identity verification.

SSI solutions prioritize the security and privacy of users. With SSI, users can register or apply for services across multiple platforms using a single unique identification, making it more portable and convenient. In addition, SSI can provide a cost-effective way to improve identification systems and access to resources because it can reduce administrative processes and server load for service providers. By allowing individuals to choose what personal information they share, SSI can also improve information privacy and protect sensitive data. Figure 3 summarizes these benefits.

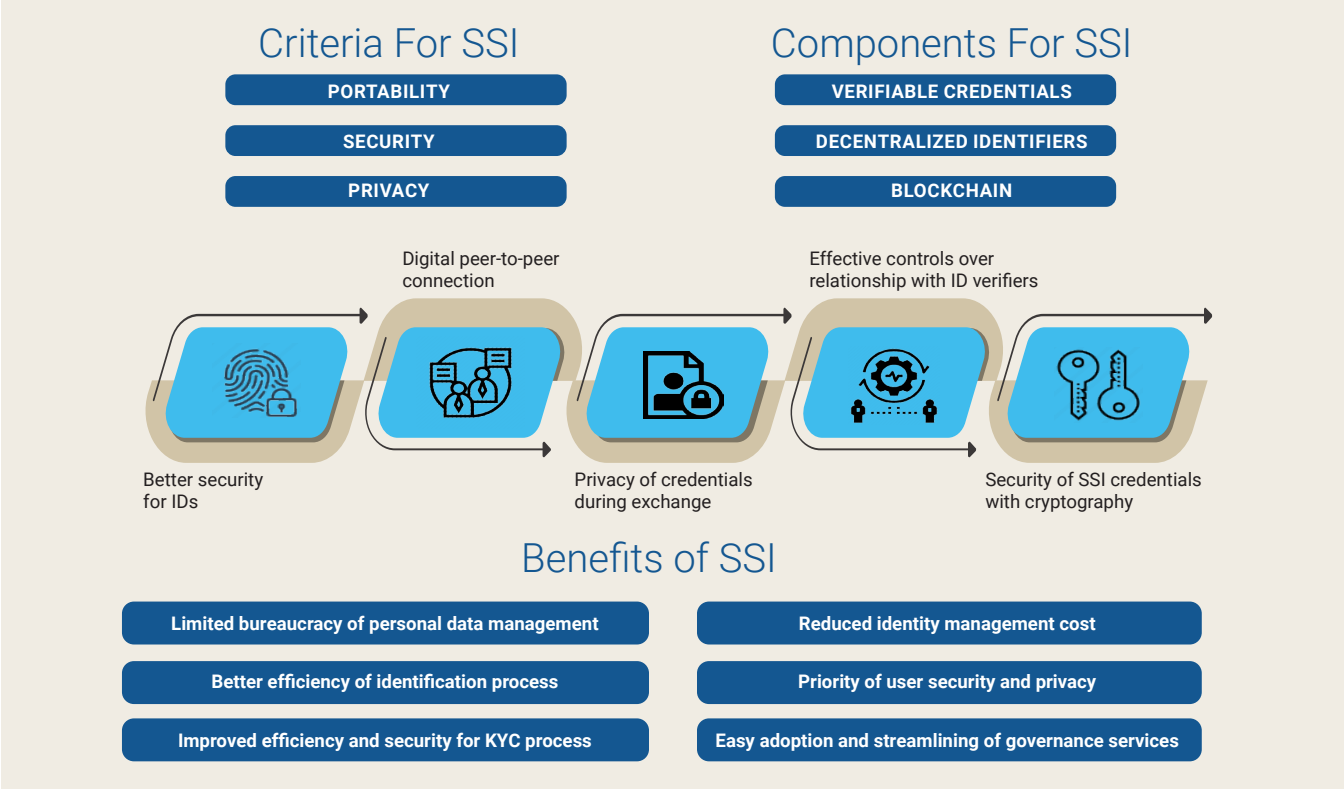


Figure 3: SSI Components and Benefits [6]

SSI MODEL. ACTORS, GOVERNANCE, AND ECONOMICS

Digital decentralized trust models such as SSI are often compared to traditional physical credential issuance and use because they "disintermediate" trusted third parties. In decentralized models, the focus is on establishing trust between key players in the system:

- Issuers and Holders
- Holders and Verifiers
- And Governance Frameworks, covering all three

The Issuer decides if, when, and whom they should issue a credential to (Holder). They want to make sure that the right people get the right credentials for the right reasons and that the credentials they issue are current and valid for their use.

The Holder earns and receives cryptographically signed credential(s) from the Issuer. By proving that they have right credential(s), the holder can gain access to products and services.

The Verifier (aka Relying Parties in this context) offers products and services to Holders on condition that they can prove that they have the right credentials. They want to make sure that the credentials offered by the Holder are trustworthy and "good enough" to confirm access to their products and services.

The Verifier will cryptographic check the content of the verifiable claims presented by the holder, to check things such as:

- Who issued the data?
- Has it been tampered with?
- Was it issued to the Holder?
- Has it been revoked?
- Whom does the data refer to (if not the Holder)?

Governance

But why would the Verifier trust the Issuing organization(s)? Figure 4 illustrates a governance framework, which is a set of rules and processes that helps to ensure trust in SSI systems. By establishing clear guidelines for Issuers, a governance framework enables Verifiers and Holders to trust the verifiable claims that have been cryptographically signed by the Issuer and presented by the Holder. This helps to ensure the integrity and reliability of the SSI system because it provides a clear understanding of the roles and responsibilities of each party involved.

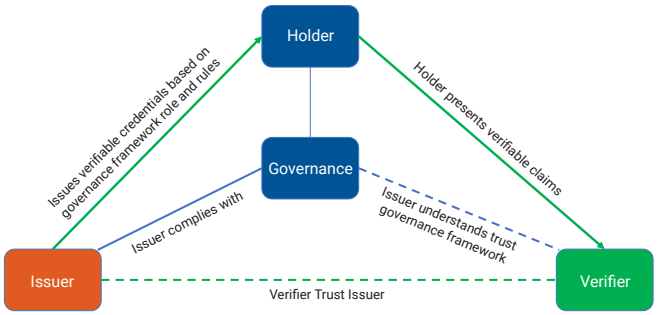


Figure 4: Governance Framework for Issuers Enables Trust by Verifiers and Holders [7]

In an SSI model, it is possible for multiple governance frameworks to coexist and be used by Holders to present verifiable claims to different Verifiers. For example:

- A government agency might provide a framework for issuing government IDs.
- While a financial regulator might provide a framework for verifying bank account details.
- Similarly, a local authority might provide a framework for verifying proof of residency.
- A health authority might provide a framework for issuing health data.

This allows Holders to present the appropriate verifiable claims to different Verifiers, depending on the specific needs of each situation.

Economics

Identity has been commercialized in numerous ways, from straightforward transactions like paying for a passport to more complex and opaque models like targeted advertising. SSI will likely have an impact on these existing models, potentially replicating some, destroying others, and creating entirely new ones. It is difficult to predict exactly how SSI will shape the commercialization of identity, but it is clear that it has the potential to significantly change the way that identity is used and valued in various contexts.

SSI introduces new opportunities and business models (Figure 5) that can be explored through the following bilateral transactions:

1. Holders may pay to gain and retain credentials from Issuers.
2. Holders and Verifiers may exchange value in their transactions.
3. Issuers may retain their license to issue credentials by meeting quality and operational requirements and paying license fees to the governance framework.
4. Verifiers may pay a fee to be checked and registered on a trusted list, which may be available to Holders. The Verifier may also pay a fee to access the public keys, verifiable credential registry, and revocation data on the blockchain.
5. The cost of the credential, paid to the Issuer by the Holder, may include a portion of the fee that is paid to fund the governance framework.
6. Verifiers may use a blockchain token to pay for access to Issuer and Holder public keys, with the Issuer receiving a revenue share for the checks made.

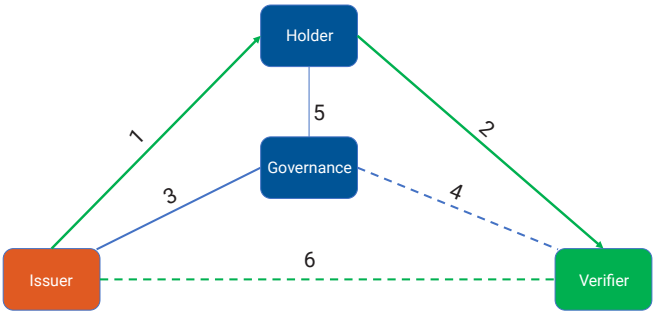


Figure 5: New SSI-Enabled Business Models to Consider [7]

SSI has the potential to create a virtuous cycle of growth (Figure 6), where the benefits of lower costs and improved user experience drive greater adoption by Holders, Issuers, and Verifiers. As more people use SSI, the cost of implementing and maintaining the system may decrease, further improving the user experience and encouraging even more adoption. This cycle of growth could lead to widespread adoption of SSI, bringing significant benefits to all parties involved.

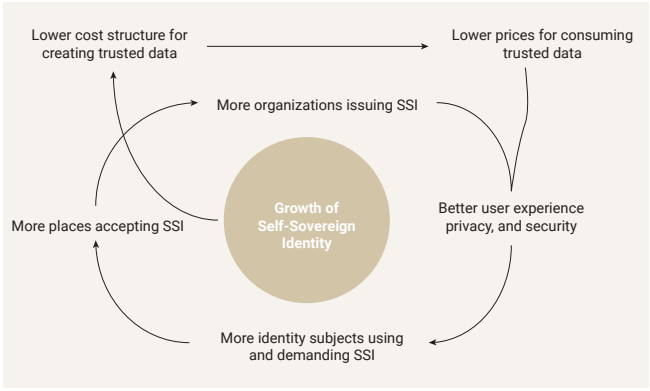


Figure 6: Vision on the Virtuous Flywheel of SSI Growth [8]

SSI has the potential to drive growth and innovation in several ways:

- As more issuing organizations use SSI to provide trusted data to identity subjects, there will be increased incentives for organizations to participate in the system.
- The greater the adoption of SSI credentials, the more organizations that are willing to accept them as a secure and efficient way of verifying identity.
- The growth in SSI usage will attract more companies to develop software and integrate SSI into their products and services, leading to enhanced features and functionality.
- As SSI credentials become more common, the cost of verifying identity through SSI will decrease, leading to lower prices for consuming trusted data.
- These lower prices will make it more affordable for individuals and companies to access a wider range of organizations and services that accept SSI, improving the overall user experience and increasing privacy and security.

VALUE FOR THE CARRIER IN THIS NEW IDENTITY MODEL

SSI has the potential to create value for telecom carriers in several ways:

- **Improved customer experience:** SSI can enable telecom carriers to offer their customers a more personalized and convenient experience. For example, customers could use their SSI to easily access their account information, purchase new services, or make changes to their account without having to go through multiple authentication steps or provide personal information each time.
- **Enhanced security:** SSI can improve security by enabling telecom carriers to verify the identity of their customers more accurately and efficiently. This can reduce the risk of fraud and identity theft, which can have significant financial consequences for both the carrier and the customer.
- **Increased efficiency:** SSI can streamline internal processes and reduce the need for manual verification, which can save time and resources for telecom carriers.
- **New business opportunities:** SSI can create business opportunities for telecom carriers, such as offering identity verification services to other organizations or enabling secure online transactions.
- **Competitive advantage:** By adopting SSI, telecom carriers can differentiate themselves from their competitors and potentially gain a competitive advantage in the market.

EXAMPLES OF HOW TELECOM CAN USE SSI

This use case is really quite simple. Provide basic details about yourself, typically including:

- Your full name
- Your address
- That you are alive and your image matches a valid piece of ID

To do this, many organizations are allowing self-onboarding, where a user uploads one or more government IDs that are matched to a selfie, along with a liveness test (are you real?). This set of tests prove that the user physically matches a valid ID, with AI recognizing if the government ID is valid against a known set of tests. This provides the base layer of KYC and a degree of AML compliance.

Further "ID proofing" can include:

- Matching the location of the user to the location of their phone
- Background checks
- Social media matches and scans
- Education credentials
- Asset identification
- Employment/contract verification

Each of these may be augmented with other data that is key in for your organization or industry, such as health data, family members, or asset history.

Again, don't forget about IoT devices because they can be "credentialed." When those credentials expire (due to either time or usage), maintenance can be automated very easily (and you can ensure the technician is capable/certified for that device, too).

Customer Service

When a customer need help, service staff typically first verify the identity of the person they are speaking with through methods like knowledge-based authentication (KBA) or multifactor authentication (MFA) — especially when the interaction involves sensitive information. These processes can be frustrating for customers and may not always provide a clear picture of the user's identity.

With SSI, customers are issued a customer credentials upon onboarding and then use those to initiate a service call while also ensuring that the person on the other end is verified to be representing the organization the customer is calling. This eliminates the need for the service staff to ask for personal details, product details, and other information to confirm the user's identity. By using a valid DID, with verifiable credentials, service calls can be made more efficient and provide a better user experience.

Upselling

Upselling is a key focus for organizations as it can lead to significant revenue growth, with around 80% of typical revenues coming from existing clients. It can be more successful when there is full trust between the agent and customer, which can be facilitated by password-less access. Knowing which products the customer already has or has previously purchased allows the sales agent to make more confident and relevant upsell suggestions.

With SSI for organizations, customers don't have to be told about and sold products they already have. The sales agent also doesn't waste time trying to sell them something they already have.

Trusted Enterprise Caller

Americans received more than 50 billion unsolicited phone calls and text messages. Many of these are geared toward scamming people out of their money. [9]

SSI can be used to help a consumer trust that a phone call coming from a business (e.g., a bank, government department, hospital) is not spoofed or fraudulent. With SSI, a consumer would have a high level of confidence in the identity of the company making the call that they are whom they claim to be.

In this context, a phone call from a business to a consumer, the business would present its SSI credentials within the call to establish its identity. This is possible using VoIP by including an identity header. The consumer's phone could then verify the credentials using cryptographic checks to confirm the issuer, determine if the data has been tampered with, and verify that the credentials were issued to the business calling them. This process can provide a secure and efficient way for the consumer to verify the identity of the caller and establish trust that the call is coming from the company.

NFTs and SSI

A non-fungible token (NFT) is a unique digital identifier that cannot be copied, that is recorded in a blockchain, and that is used to certify authenticity and ownership. The ownership of an NFT is recorded in the blockchain and can be transferred by the owner, allowing NFTs to be sold and traded. SSI can help to verify the ownership and provenance of non-fungible tokens (NFTs) throughout their lifecycle, including fractions of ownership, regardless of the ledger they are hosted on. This can enable decentralized content consumption and payment, allowing creators to receive fair payment for their work and directly interact with their audiences.

SSI can also address the issue of identity tied to payments in cryptocurrency and decentralized finance (DeFi). Currently, it is not possible to verify the identity of payment receivers beyond their wallet address, which can be a problem for high-value transfers in particular. Although anonymous payments can be useful in some cases, there are also instances where it is useful to verify the recipient's identity.

A number of governments have committed to promoting the development and use of SSI as a means of improving digital identity management. SSI offers a number of potential benefits, including increased security, privacy, and convenience for individuals, as well as cost savings and efficiency for organizations.

U.S. Government and Department of Homeland Security

The U.S. Department of Homeland Security (DHS) has shown interest in exploring the potential use of SSI as a means of improving digital identity management.

The DHS has conducted research on SSI and its potential applications, including the use of SSI for identity verification in the context of emergency management and disaster response. The DHS has also funded research projects related to SSI and has participated in efforts to develop standards and guidelines for its use.

Overall, the DHS's interest in SSI reflects a recognition of its potential to transform the way that digital identity is managed and used. It is possible that the DHS may consider implementing SSI in certain applications in the future, depending on the results of its ongoing research and analysis.

Canadian Government

The Canadian government has launched consultations on a variety of digital activities, including identity, as part of its Digital Ambition project [10]. This included consultations on a federally managed digital identity framework, developing a common and secure framework, and establishing a digital identity program for the use of select digital identities for transactions with the government of Canada.

In October 2022, federal and provincial privacy regulators issued a resolution affirming the benefits of a digital ID ecosystem. Part of that statement included a comment from Canada's federal regulator, who noted that digital identity represents an opportunity to demonstrate that innovation and privacy protection can coexist [11].

European Union

The EU has taken a number of steps to support the development and adoption of SSI. This includes funding research and development projects, developing standards and guidelines for SSI, and working with various stakeholders to promote the use of SSI in different sectors.

In addition, the EU has established the European Blockchain Partnership, which aims to support the development and deployment of blockchain-based technologies, including SSI. The partnership brings together member states and EU institutions to collaborate on projects related to blockchain and digital identity, with the goal of creating a European Blockchain Services Infrastructure that can support the use of SSI and other blockchain-based technologies.

Overall, the EU's commitment to SSI reflects a recognition of its potential to transform the way that digital identity is managed and used.

The Future of Self-Sovereign-Based Digital Identity

It is difficult to predict the exact future of SSI, but it has the potential to revolutionize the way that identity is verified and managed. SSI allows individuals to have greater control over their own identity data, enabling them to choose which information they share and with whom. This can improve privacy and security, as well as provide more efficient and convenient access to services.

As more government departments, organizations, and individuals adopt SSI, it is likely that it will become increasingly integrated into various systems and processes. This could include applications in government, health care, finance, and other sectors. SSI could also play a role in enabling new business models and innovations because it provides a secure and efficient way for organizations to verify identity and access trusted data.

Overall, the future of SSI looks promising, with the potential to bring significant benefits to individuals, organizations, and society as a whole.

How to Get Involved

If you would like to participate in the work at ATIS to advance the use of SSI in telecommunications, please visit www.atis.org.

REFERENCES

[1] General Data Protection Regulation (GDPR)

[2] California Consumer Privacy Act (CCPA)

[3] Personal Information Protection and Electronic Documents Act (PIPEDA)

[4] Deloitte, Trust and Privacy Digital Consumer Trends 2020 Report

[5] IBM, Cost of Data Breach 2022 Report

[6] 101 Blockchains - Self-Sovereign Identity: The Ultimate Beginners Guide!

[7] Sezoo, How organization's can make and save money with decentralized trust models. Presented at European Identity and Cloud Conference, May 2022

[8] Cheqd, The business models of identity

[9] Youmail, robocall index

[10] Canadian Digital Ambition 2022

[11] Benefits of digital ID ecosystem will be realized only with adequate privacy pro-tections, say data protection authorities

COPYRIGHT AND DISCLAIMER

ATIS-I-0000093

Published February 2023

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

www.atis.org
For information, contact ATIS at (202) 628-6380.