Me, myself and (SS)I

Why everybody must have a Self-Sovereign Identity in 5 years

BCG and walt.id

White Paper, August 2021

BCG Authors: B. Kronfellner and T. Merey

Walt.id Authors: D. Beron and O. Terbu

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we help clients with total transformation—inspiring complex change, enabling organizations to grow, building competitive advantage, and driving bottom-line impact.

To succeed, organizations must blend digital and human capabilities. Our diverse, global teams bring deep industry and functional expertise and a range of perspectives to spark change. BCG delivers solutions through leading-edge management consulting along with technology and design, corporate and digital ventures—and business purpose. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, generating results that allow our clients to thrive.

Walt.id is a European company that develops Self-Sovereign Identity (SSI) solutions for governments and businesses across industries.

We offer an easy and fast way to adopt SSI - particularly Europe's new decentralized digital identity ecosystem - based on robust open source products. To ensure client's success our industry-leading experts provide holistic services ranging from conception and project planning over the implementation of proof-of-concepts and production system to enterprise support and managed cloud services.

Agenda

1 “Hello Digital World” – Why we need Self-Sovereign Identity (SSI)

Over the last decades, we witnessed the world becoming increasingly digital. The internet, smartphones and continuous technological advancement created an environment in which small companies can disrupt industry giants across verticals by offering digitally native products and services. Software is eating the world.

Since 2019, COVID accelerated this process of digitization significantly and even forced industries most resistant to change to adapt. Today, more than 50% of all customer interactions are digital and the majority of products and services are partly or fully digitized.

While digitization has many upsides, it comes at a price:

- **Lack of control over data:** With the rise of platforms (e.g., Google, Facebook), data and power is aggregated in the hands of a few companies, which effectively control data and lock in users due to a lack of data portability.
- **Privacy issues:** As a result of users not being in control of their data, we witnessed numerous privacy scandals which further diminished trust in data aggregators.
- **Compliance issues:** The lack of user-centric systems means that online service providers must store user data centrally, opening them up to regulatory scrutiny.
- **Security issues:** Conventional ways of securing access to services and data, particularly password-based authentication, proved to be unreliable and caused numerous large-scale data breaches.
- **Fraud and identity theft:** Due to the lack of reliable authentication and identification tools, identity theft and other types of fraud are thriving. Online service providers and marketplaces are struggling to ensure trustworthy interactions.
- **Cumbersome user experiences:** Users are forced to juggle various methods for authentication (incl. a great number of passwords) and are increasingly forced to go through lengthy identification processes.

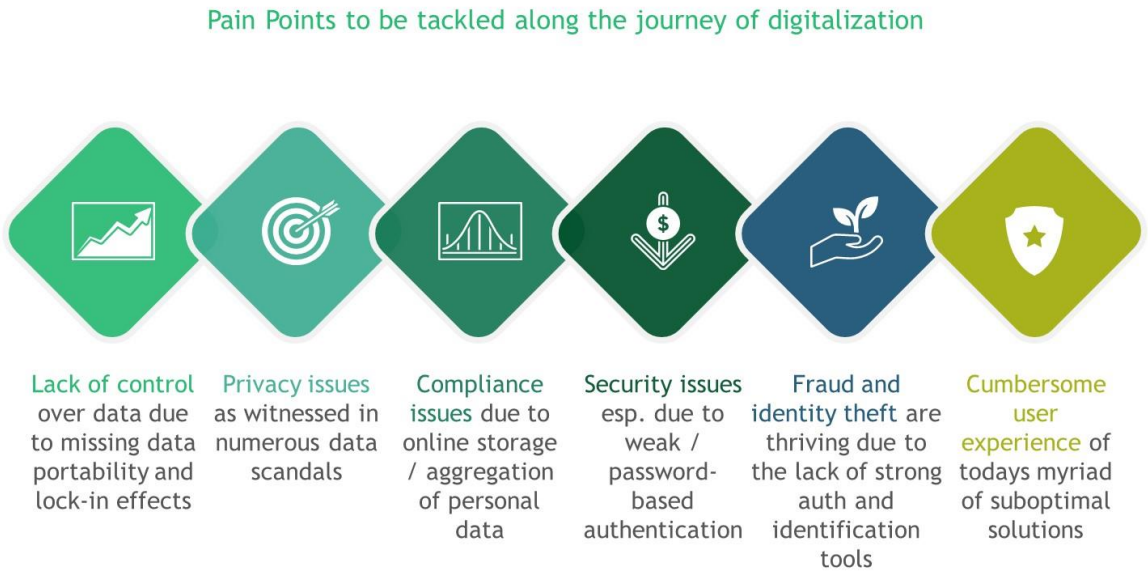

Exhibit 1: Digitalization and its main pain points that opened up the necessity for SSI

Exhibit 1 illustrate that we cannot continue to go down this path without some adaptations that address these pain points of digitalization.

2 How Self-Sovereign Identity (SSI) works

With Self-Sovereign Identity (SSI) a large shift is unfolding in the way the digital world works and this shift is leading to the extinction of data silos which lock in users and cause the fragmentation of their digital identities. Compare Exhibit 2.

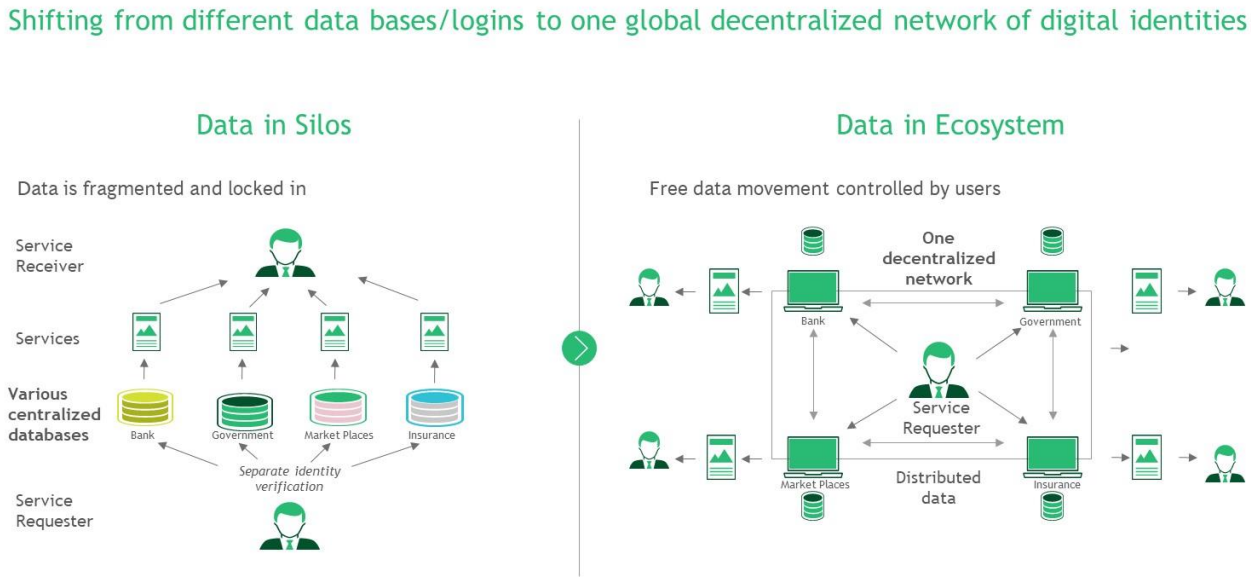

Exhibit 2: Shift with SSI from various central databases to one decentralized network

A new era of decentralized and user-centric ecosystems is on the rise that will enable individuals and organizations to control their data (e.g., from ID cards and drivers licenses over diplomas and financial records to vaccination proofs and transportation tickets) and share it more seamlessly, securely and privately than currently possible and without dependencies on centralized platforms.

To better understand how SSI ecosystems work, you may think of them as three-sided marketplaces in which individuals and organizations can take on three roles:

- **Issuers** - Organizations who store identity-related data about citizens, customers, employees or other stakeholders and "issue" such data to its associated individuals, things or organizations ("Holders") in the form of digital credentials. Issuers are the original data sources of an SSI ecosystem. For example, a government issues digital passport to its citizens or a university issues digital diplomas to its graduates.
- **Holders** – Individuals, organizations who receive digital credentials, that contain data about themselves, from various sources ("Issuers"). By aggregating and storing such credentials in so-called "wallets", Holders can build holistic digital identities that are fully under their control and can easily be shared with third parties ("Verifiers").
- **Verifiers** - Parties who rely on data to provide products and services can reliably verify and process data that has been provided by their stakeholders ("Holders"). Verifiers are

also called “relying parties” and they are usually organizations or individuals in their professional capacity.

In a way, SSI enables digital identity that works much like the “offline identities” we are already used to, but instead of having to handle paper-based identity documents, individuals and organizations get digital credentials that can simply be presented during interactions. In Exhibit 3, we illustration the functionalities of SSI ecosystems and how it works in detail.

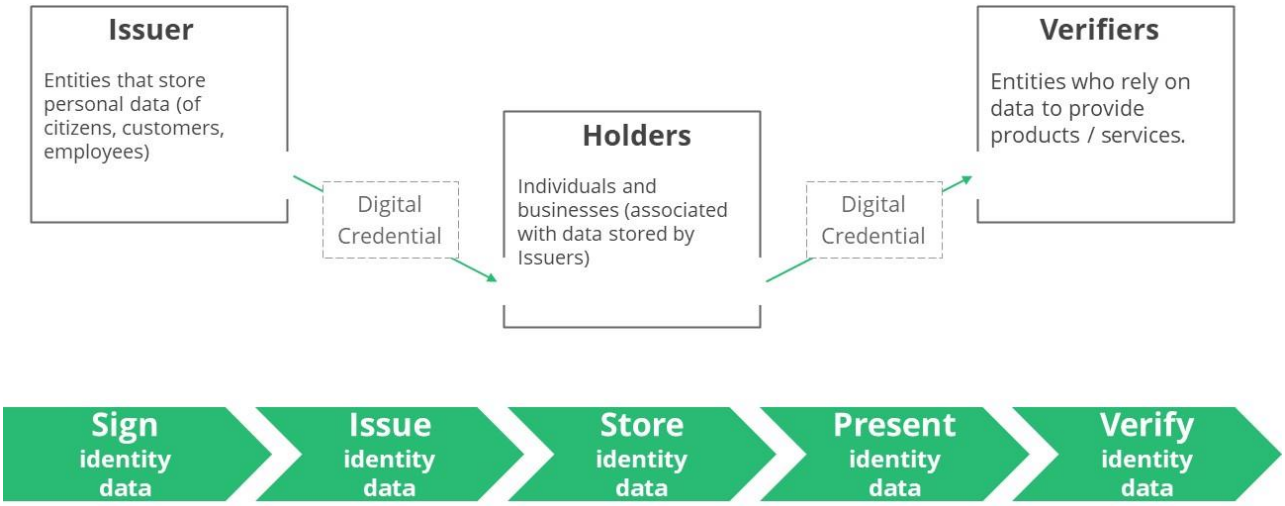

Exhibit 3: Illustration of how SSI ecosystems work

Note that a single party can act as Issuer, Holder and Verifier depending on the use case. For example, a university may issue diplomas to graduates (Issuer), manage their own accreditations (Holder) and request education records from incoming students (Verifier).

3 Why you should care about Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) is a new approach towards digital identity that promises to solve major challenges caused by digitization. The main idea is to switch from many centralized approaches to one decentralized approach. We are looking at a paradigm shift in digital identity management by which centralized solutions that create fragmented personal data silos are replaced with universal and user-centric decentralized identity ecosystems. SSI is not only establishing itself as the new global standard for digital identity, but witnesses growing adoption by major players across sectors supported by proposed regulatory frameworks.

The new standard for digital identity

SSI is a combination of novel technologies and protocols which are finally mature enough to support production systems and are standardized globally (e.g., World Wide Web Consortium, Decentralized Identity Foundation) to facilitate interoperability across systems.

Global adoption across sectors

Governments already subsidize SSI-based solutions, are adapting regulatory frameworks and are building pilot projects. Similarly, businesses are launching projects across verticals. For example:

- The **EU Commission** and member states created the "European Self-Sovereign Identity Framework (ESSIF)" and "European Blockchain Service Infrastructure (EBSI)" to enable a new European identity ecosystem in which citizens and companies can control and freely exchange data. This infrastructure is anticipated to extend the current regulatory framework for eID and Trust Services ("eIDAS").
- Individual **European member states** like Germany, France, Spain, Netherlands, Slovakia, Slovenia, Sweden, Luxemburg are already developing pilot projects and plan the launch of production systems for various use cases starting 2022.
- The **United States of America** are subsidizing the development of SSI solutions for specific public sector use cases (e.g., visas, customs) and regional governments in Canada (e.g., British Columbia, Ontario) already launched projects such as a public directory of verifiable company data.
- **Industry-leading companies** like MSFT, Workday, Salesforce, Bosch, SAP, BMW, Novartis and others are exploring SSI to gain a strategic advantage over their competition. Adoption happens globally and in almost every industry (including banking and financial services, insurance, education, employment and HR, commerce, health care, mobility, hospitality, supply chain among others).

Regulatory enforcement

The EU Commission recently announced a proposal for a regulation that will force the broad adoption of user-controlled digital identity in Europe. Among other things:

- Member states will be obliged to provide people and businesses with a digital identity solution ("wallet") and digital credentials will be considered equal to official documents.
- It will be mandatory for governments, large online platforms and service providers (including transport, energy, banking, financial services, social security, health, postal services, digital infrastructure, education, telecommunications) to accept digital credentials for user identification purposes.
- The aim is that member states agree on the framework in 2022 and the regulation must be implemented within 1 year after the proposal is approved.

> *"It is time for a European digital identity ecosystem that gives citizens full control over data and companies the opportunity to improve their product and service offerings. Self-Sovereign Identity will enable this ecosystem with the full support of the European Union and the member states."*
>
> **Daniel Du Sueil**
> Convenor of the EU member states (EU Self-Sovereign Identity Framework, ESSIF)

Unique Benefits

SSI can create significant value for your organization:

- **Frictionless Interactions:** SSI can eliminate passwords, forms and cumbersome identification processes to increase conversion rates by up to 40% (Heap, Bolt, Truelist) and decrease help desk requests by up to 50% (Gartner).
- **Reliable Data:** Today, 41% of customers provide false data due to security and privacy concerns (RSA). SSI can bring this number down to zero by taking away consumers' worries and enabling them to seamlessly share reliable digital credentials signed by trusted third parties like governments.
- **Prevention of Fraud:** SSI enables service providers to reliably and almost instantly verify consumer data in terms of data validity, integrity, authenticity, provenance. By this identity theft and document forgery can be prevented.
- **Prevention of Data Breaches:** SSI can significantly reduce the risk of data breaches by eliminating common risk factors like password-based authentication or aggregated data storage.
- **Regulatory Compliance:** SSI comes with built-in user-centric data management and ways to enhance user privacy (e.g., selective disclosure) as to ensure compliance with data protection regulations (e.g., GDPR).

4 What organizations need to do now

Governments and businesses are already adopting Self-Sovereign Identity (SSI) on a global scale. Particularly the European Union is investing heavily with its blockchain infrastructure (EBSI), digital identity framework (ESSIF) and a proposed regulation that will force the adoption of digital identity by the public and private sector in Europe.

If you are not already exploring SSI, the following steps will help you navigate the shift in your infrastructure strategy:

Identify opportunities

Analyze your business processes with a focus on multi-party interactions and identify opportunities to significantly improve various areas of your business:

- **User Experience:** Does your customer onboarding processes require the use of passwords, online forms, multi-step identity verification processes or other sources of friction? If yes, you can use SSI to streamline user journeys by replacing existing multi-step processes with a simple 1-click process.
- **Data Quality:** Do you face data quality or data consistency issues, for example, because customers provide wrong information or due to typos in forms? SSI can ensure high data quality based on identity information verified by trusted third parties.
- **Security:** Do you use passwords, store sensitive / personal data in a centralized fashion or wrestle with the elimination of other attack vectors? SSI can help you implement more secure authentication and identification while ensuring data minimization and decentralized storage.
- **Privacy & Compliance:** Is regulatory compliance (GDPR, CCPA) an ongoing challenge or do you procure third-party solutions to ensure compliance? SSI can help you to become compliant-by-design via built-in consent management and automatable fulfillment of data provisions request.
- **Process automation:** Do you struggle with process automation that would benefit from machine-readable stakeholder data? SSI can unlock reliable and machine-readable stakeholder data to power enhanced process automation.

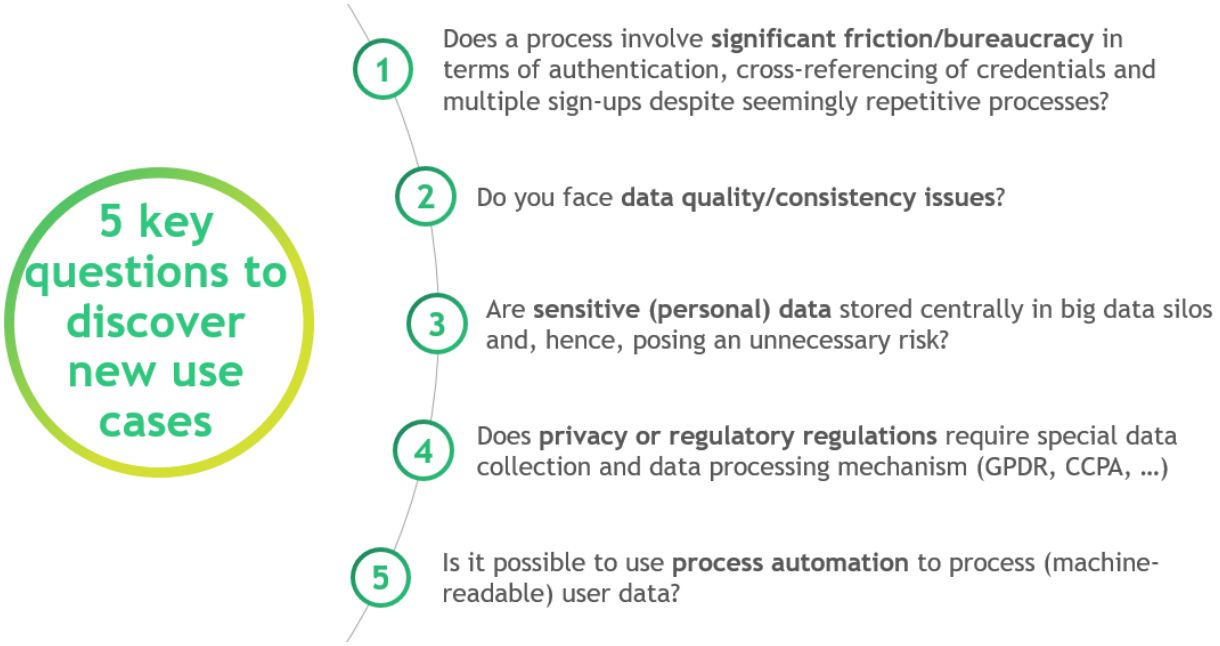

Exhibit 4: key questions to find and define use cases

Attached to this document you can find a list of exemplary use cases for inspiration.

Analyze and select use cases

Prioritize use cases based on your organization's goals, challenges and product or service portfolio. Exhibit 5 below illustrates a frame to prioritize use cases. Make sure to include risk assessments that evaluate the costs of doing nothing such as risks related to security breaches, compliance penalties and related brand damage or losing customers to competitors who adopt SSI.

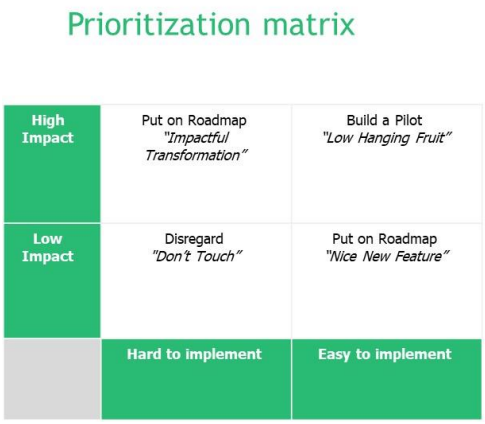

Exhibit 5: key questions to find and define use cases

Implement proof-of-concepts

Plan and implement proof-of-concepts to build up knowledge, evaluate feasibility and prove the ROI (Return on Investment) of Self-Sovereign Identity for your organisation. If you decide to pursue further initiatives, make sure to screen solutions for

- the use of open source licenses (e.g., Apache 2)
- the use of open interfaces and standard compliance (W3C, ESSIF)
- support for relevant identity ecosystems (e.g., Europe's EBSI/ESSIF),
- ease of integration with your infrastructure (e.g., support for multi-cloud, custom key stores/HSMs or legacy protocols like OpenID Connect)

5 APPENDIX: Attachment / Use Cases

The following Exhibit 6 and table lists exemplary use cases to illustrate how SSI can be applied in different industries:

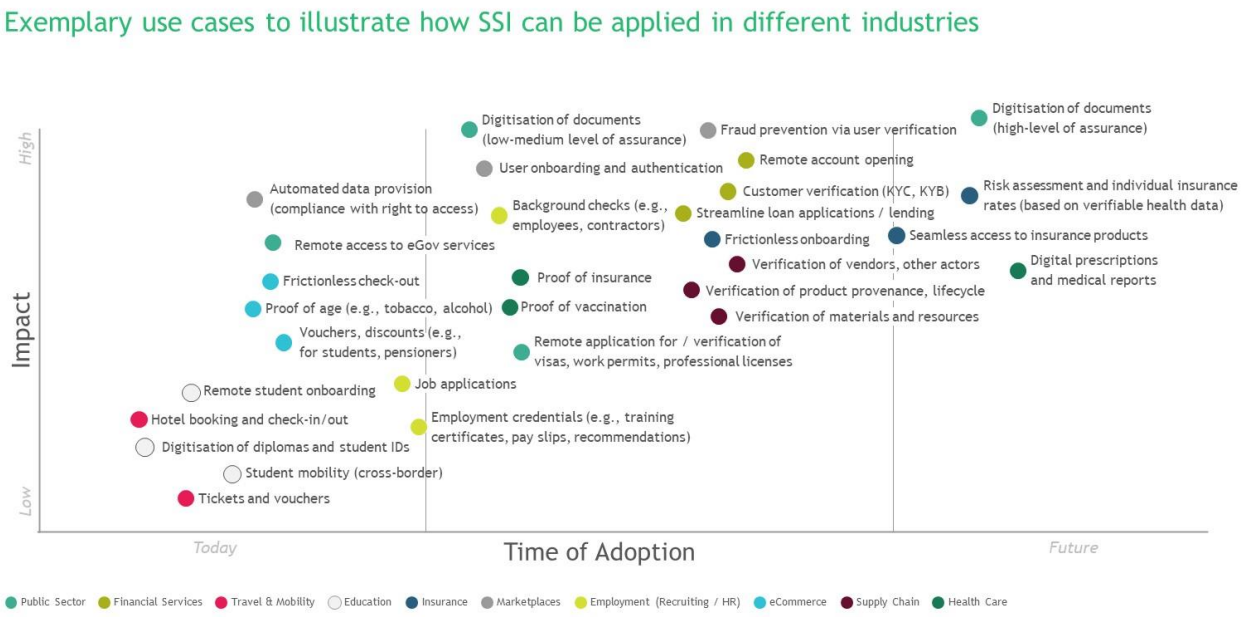

Exhibit 6: Exemplary use cases according to monetary impact and security improvement

6 Bibliography

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

P. C. Bartolomeu, E. Vieira, S. Hosseini, J. Ferreira, Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot, 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, 2019

A. Doerk, P. Hansen, G. Jürgens, M. Kaminski, M. Kubach, O. Terbu, Self Sovereign Identity Use Cases – von der Vision in die Praxis, https://www.bitkom.org/Bitkom/Publikationen/Self-Sovereign-Identity-Use-Cases, Bitkom e.V., 2020

A. Preukschat, D. Reed et al., Self-Sovereign Identity, Decentralized digital identity and verifiable credentials, Manning, 2021

O. Terbu et al., The Self-sovereign Identity Stack, https://medium.com/decentralized-identity/the-self-sovereign-identity-stack-8a2cc95f2d45, 2019

A. Tobin, D. Reed, The Inevitable Rise of Self-Sovereign Identity, https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf, 2017

Lux, Zoltán & Thatmann, Dirk & Zickau, Sebastian & Beierle, Felix, Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials, 2020

7 About the authors

BCG Authors:

Bernhard Kronfellner is an Associate Director in the Vienna office of the Boston Consulting Group. You may contact him by email at kronfellner.bernhard@bcg.com.

Tibor Mérey is a Managing Director and Partner in the Vienna office of the Boston Consulting Group. You may contact him by email at merey.tibor@bcg.com.

Walt.id Authors:

Dominik Beron is the CEO of walt.id and serves as identity expert to the European Commission and member states. You may contact him by email at dominik@walt.id

Oliver Terbu is a leading expert on Self-Sovereign Identity and a co-author of various global identity standards at the World Wide Web Consortium and the Decentralized Identity Foundation.

.