DoT.Mig

In Brief

Self-Sovereign Identities for People on the Move—A New Approach to Public Sector Authentication?

December 2022

DIALOGUE ON TECH AND MIGRATION

A project of the Migration Strategy Group on International Cooperation and Development

BertelsmannStiftung

G|M|F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Robert Bosch Stiftung

Author

Michael Kolain, Legal expert on digital policy, iRights.Lab Berlin

Scientific Coordinator, Research unit “Digital transformation of the state in the digital age”, German Research Institute for Public Administration
Member of the Expert Panel, European Blockchain Observatory and Forum (EUBOS)

The views expressed in this publication are the views of the author alone and do not necessarily reflect those of the partner institutions.

About DoT.Mig

The **DoT.Mig In Brief** paper series is part of the The Dialogue on Tech and Migration, DoT.Mig.

DoT.Mig provides a learning platform to connect the dots between digital technologies and their use and impact on migration policy, as well as connecting relevant stakeholders. The **DoT.Mig In Brief** paper series highlights debates and concepts relevant to navigate the emerging field of Tech and Migration.

DoT.Mig is a forum by the Migration Strategy Group on International Cooperation and Development (MSG). The MSG is an initiative by the German Marshall Fund of the United States, the Bertelsmann Foundation, and the Robert Bosch Stiftung.

Key Takeaways

1. The bedrock of any migration and mobility management is that public authorities have reliable identification documents for the person wanting or needing to move across borders. Identity documents can be provided via paper records or in a digital format.

2. Insufficient systems for digital identification and fraudulent documents are two major obstacles in the field of migration and identity management. In a digitally connected world, providing authentic digital proof related to aspects of an individual’s life is a complex endeavor. At the same time, identity data of migrants and refugees is often shared without their knowledge or consent.

3. A possible solution for this could be using “self-sovereign identities” (SSI), a new paradigm for identity management in the digital world which can potentially empower people on the move and provide them with more control and transparency regarding the processing of personal data.

4. The concept of SSI is based on a more decentralized and user-centric approach. People on the move could self-manage and share digital proof of their identity with public authorities without involving intermediaries such as the centralized IT solutions of international organizations or national governments. SSI can also overcome fears of data sharing and improve the data sovereignty of migrants as well as data quality for public authorities and companies.

5. In order to establish an SSI ecosystem for migrants that could simultaneously work for public authorities, three challenges need to be addressed:

- **A)** The core components of an SSI ecosystem must be sufficiently standardized and mass tested, and challenges of IT security must be solved.
- **B)** The SSI paradigm needs public sector buy-in to provide and run such an ecosystem for the purpose of digital identification. Otherwise, there is a risk that tech companies will provide and manage a core duty of a sovereign state: the identification and authentication of citizens.
- **C)** Migration stakeholders must jointly agree on the technical standards of an SSI-ecosystem, decide on who shall issue an identity wallet, under what circumstances—in migration or refugee settings—and find consensus on specifications for overall interoperability, for example, between the EU and UNHCR.

6. **Recommendation 1:**
Migration stakeholders should connect and engage with the EU’s current EUid initiative to boost development of a reliable and trustworthy SSI infrastructure that can be scaled worldwide, including in the field of migration. They should also consider how to contribute and benefit from the decentralized and user-centric ecosystem that the European Commission is attempting to foster.

7. **Recommendation 2:**
Migration stakeholders should swiftly come together to debate options and standards of possible core elements of SSI in the migration field. They should embrace the possibilities that trustworthy SSI components can provide and collaborate to set up a scalable, privacy-preserving, and interoperable eID ecosystem.

Introduction

Applying for a residence permit is often an intense process for both the applicant and the administrative officer. While migrants try to present proof about aspects of their life, public officers try to gain enough certainty to make an appropriate decision about the individual's future.

The **lack of valid and full documentation** about a person's identity and past life is a well-known obstacle in the fields of humanitarian and labor migration—in both a paper-based and a digitalized world. Those escaping from armed conflict are unlikely to be carrying his or her paper folder with diplomas and certificates while a person who wants to apply for a job in another continent is often unable to present certified documents that meet the standards of authenticity applied by the host country and future employer. **Fear of identity fraud and tampered documents** have raised the bureaucratic burden of proof to an immensely high level. Every decision in the migration context is thus based on a substantial amount of uncertainty. Improvements depend on the availability of sufficient documentary evidence.

But even if available, paper records can **be lost or destroyed**, and laptops or smartphones can break, resulting in **data loss**. In addition, access to cloud-storage is heavily dependent on private companies with **insufficient privacy terms**. And—as the current situation in Afghanistan has shown—sensitive data and biometric credentials are persistent after a regime change and can fall in the hands of suppressors and be **used for illegitimate surveillance purposes**.

Even where evidence can be presented, it can be difficult to prove whether a university diploma, foreign passport, language certificate, or bank statement is authentic or previously **revoked or "photoshopped"**.

SSI Light

In the SSI-movement there are proponents of a radical form that is largely based on the concept of self-attested claims. In this world-view, there exists no legitimate authority that can make any valid assumption as to the identity of a person—e.g. in regards of gender attribution, name, nationality and formal education—or issue a legitimate identity document. The background of these voices stems from the fundamental idea of cryptoanarchism which is fueled by the idea that blockchain technology can "one day replace the nation state and rid us of bureaucrats, creating a world of a million competing digital nations." (source)

However, in the existing world order of states, borders, and international migration, there is no short- or middle-term perspective for a scenario where it is not state authorities who issue ID documents to their citizens (apart from the question who would run a globe-spanning internet infrastructure in a crypto-anarchist scenario). When this paper talks about SSI, it therefore follows the assumption that there need to be institutions that issue documents and identity wallets to natural persons—and effectively ensure and control the functionality and security of the SSI-ecosystem.

The idea of an **ecosystem of "self-sovereign identities"** (SSI) promises a way out. The ability to **self-manage and share digital proof from one's private smartphone** without the involvement of strong intermediaries (who are inherently susceptible to manipulation) seems like a promising path: It could **empower the individual** and **render administrative migration processes more effective**. University diplomas, language certificates, and former residence permits could be shared using a **common technical standard** and documented with a hash-value on a blockchain—with only the identity holder being able to link and trace all the aspects of one's digital identity through a digital wallet.

As a clarification on terminology in this paper: in the context of digital identity management, "identification" refers to the self-claim to a digital system to be a certain entity or person, while "authentication" means providing proof of being this person or entity.

1. What Are the Challenges of Current Models of Digital Identification and Authentication?

As outlined above, analog modes of identification and authentication encounter risks of fraud. With digital transformation taking hold in a globalized world, it has become possible to communicate over long distance and exchange information purely through electronic means. Therefore, models of digital identification and authentication are employed, most prominently electronic identification (eID) through national eID /digital ID systems and Single-Sign On (SSO) solutions of commercial enterprises.

However, they both have limitations which SSI can help overcome.

A) **National eID solutions:** In eID solutions established by states, all of the information found on an ID card is also stored digitally—either on the chipcard itself and/or on a centralized server. eID-ready **means of identification** are therefore equipped with a chip that stores **cryptographic keys and certificates** that hold the personal information of the ID holder. The combination of a public key (stored in a public database) and a private key (accessible only by the data subject) ensures that the eID can be used as unique identifier. However, if a state fails or a government starts to manipulate or suppress this means of digital identification, its citizens are deprived of the ability to

authenticate themselves based on an official ID. In the context of migration, this goes along with the inability to prove one's identity based on a state ID and a potentially complete loss of access to public services and registries. It is also in the hand of the government to potentially exclude parts of society (such as religious minorities) from access to an eID.

The process of submitting information via a state-issued eID, especially one deploying a chipcard, to authenticate specific information or a transaction can be **time-consuming** and **complicated**. One needs to carry along the eID chipcard, remember passwords, wait for official approval of identifying information via public eID servers, and struggle with an oftentimes non-interoperable system of the transit or hosting country. Relying on a public service also comes with the risk of unwanted, illegitimate or non-transparent data sharing activities "in the background," such as collecting meta data of eID-based transactions without the knowledge of a citizen.

B) **Single-Sign-On Solutions (SSO):** Companies in the IT sector have recognized the weak points of eIDs and offer **convenient solutions for private legal transactions** through **Single-Sign On Solutions**.

Since many people worldwide have accounts with email-providers, social networks, or other digital platforms, they happily use these companies' services for the process of authentication as well. With the growing global market dominance of Big Tech companies—Alphabet, Meta, and Twitter—they have started to offer their login services to other providers of online services (SSO).

As a **pitfall from the perspective of privacy**, the providers of authentication services can use their login services to collect personal data about the users to monetize them, create individual profiles to improve personalized services, and pass them on to security agencies. As a result of the convenient availability of SSO services by private companies, it seems logical to **integrate public services** into their already established ecosystem. As an example, Apple has already started to integrate state ID and driver's licenses of some US states in the Apple Wallet. From the perspective of constitutional law and state theory this leads to the problematic situation that a **sovereign states rely on private infrastructure, data storage, and data processing facilities to perform its key duty of providing and enabling a means of identification** to its citizens. Some even see the "digital sovereignty" of states at stake if large corporations effectively run and control critical digital infrastructure. Taking this idea a step further, it could, in the future, be enough to show the QR code generated by one's Apple Wallet to enter the United States on a business visa—a national passport could be utterly redundant.

Disadvantages of Current Digital Identity Solutions

SSO-solutions of tech companies	Centralized eID-solutions of states
Decisions on technical architecture and infrastructure decided upon by commercial enterprises	Lack of transparency over data processing on state servers
Limited public oversight	Lack of interoperability and portability
No common standards for data exchange and verification. Standards can be imposed by SSO-provider.	Limited integration of data sources
Incentivizes market dominance by tech companies through network and lock-in effects	Limitation of use cases to basic authentication and public services—difficult to include private sector innovation and services
Privacy—reuse of data for monetization or personalization	Privacy—potential use of protocols and personal data for surveillance purposes
No data sovereignty—data and authentication process effectively controlled by large platform providers	eID-server as intermediary and single-point-of-failure

In contrast, the concept of SSI is an attempt to establish a **more decentralized and user-centric approach** of proving elements of one's identity online. Compared to national eIDs and commercial SSO services, SSI promotes a paradigm of digital authentication and sharing of certified documents that takes a middle road **between the risk of state surveillance of centralized or federated eID infrastructure and the commercial exploitation of personal data** necessary to identify a natural person.

2. What Is a Self-Sovereign Identity?

The term "self-sovereign identity" (SSI) describes a **new paradigm of identity management** in the digital world. Unlike prior forms of digital identity management, the concept of SSI is based on a more decentralized and user-centric approach. The notion of "self-sovereignty" implies that the control over the data that a person wants to submit to a third party—for example, a government body—is **under the sole technical control of the identity holder. In the case of migration**, the digital wallet and relevant documents would be **controlled effectively by the migrant or refugee** instead of being stored by and accessible to government bodies, banks, or social media platforms.

1 https://medium.com/hypersign/ssi-101-part-2-drawbacks-of-traditional-identifiers-and-an-introduction-to-web3-a1bf791819b0
(copyright owner Vishwas Anand, Hypermine)

However, full control over the data on a digital device intended for communication with third parties is nearly impossible because it is connected to the Internet. Where IT professionals might be able to configure their own data storage and sufficiently encrypt their devices, a typical applicant in the migration process will have neither the competency nor the technical equipment beyond mass-adapted smartphones, tablets, and app stores.

Therefore, a core technical component is a digital wallet which serves as a data container and a hub for **verifiable credentials** submitted by private or public sector entities to the identity holder. To guarantee the digital wallet is **tamper-proof, timely, and authentic**, it must be integrated into a **technical ecosystem** that contains a **decentralized data registry and network.**

Verifiable Credentials
A new way of expressing information

Blockchain / ledger
A new decentralised infrastructure

Digital Wallet
A new way to interact for/with citizens

Three key technologies for SSI according to European Blockchain Service Infrastructure (EBSI)

Promoters of SSI aim to establish a **more privacy-preserving** way of proving a person's identity online and **attributing specific proofs and documents to this identity** exchanged through a decentralized data registry. Oftentimes, SSI is discussed in the wider context of Distributed Ledger Technology (DLT), specifically blockchain. The attributes of DLT have triggered potential use cases in the field of identity management since the Ethereum Whitepaper in 2014. **However, the question of what kind of data registry is best suited for eID scenarios is still under academic and political debate**. While promoters of DLT underline the theoretical potential to reach maximum decentralization in the domain of digital identity, IT security specialists focus on unresolved issues that need to be mitigated before mass adoption. Again, others question whether blockchain technology is a suitable technological paradigm at all. Indeed, emergent technologies can have a hype cycle and fall into a "trough of disillusionment."

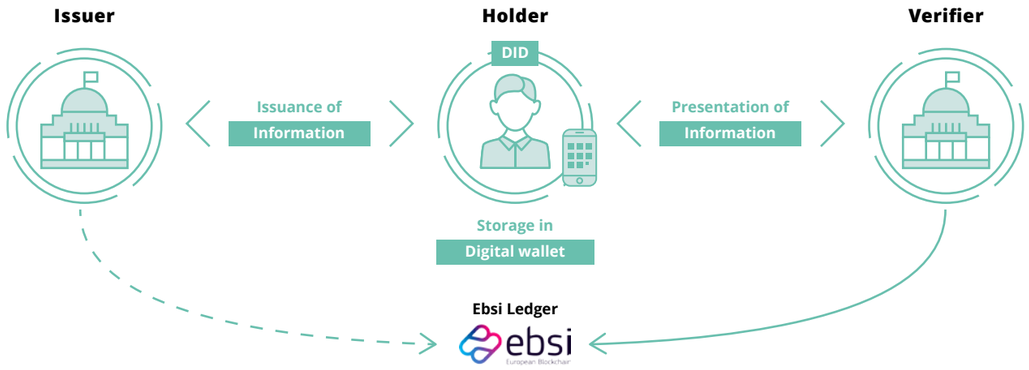
As a minimum requirement, an SSI should:

1) make **all data processing transparent to the identity holder**

2) allow the person to **disclose and share** data **according to their individual preferences**

3) avoid the **tracing and linking of credentials** by third parties, including any digital wallet provider

The basic technical architecture of SSI infrastructure has been proposed as follows:



Source: Self-sovereign scenario as proposed by European Blockchain Service Infrastructure (EBSI)

3. What Are the Promises of SSI in the Migration Field?

The concept of SSI promises a new mode of digital identity:

- An identity wallet could be the first time for many undocumented to be officially registered as an ID holder, receive certain (state or development aid) benefits, or apply for migration processes.

- With the widespread use of mobile devices (especially smartphones), SSI could provide a mode of mobile identification. A person who does not have a paper ID or smart card could identify and authenticate themselves using their mobile device. **However, the smartphones currently on the market (and in use by people on the move) often do not provide sufficient hardware components to safely store cryptographic keys and certificates**. It is thus recommended to implement modes of two-factor authentication and safe hardware components (such as a chip card) until the next generation of smartphones achieve mass adoption.

- Loss of documentation regarding one's past life or unattributable digital proof can potentially be prevented within an SSI ecosystem. After the recovery of one's identity wallet, past proof can potentially be used again. Entries on a distributed registry with a digital timestamp can be used for verification of life events in combination with SSI-compatible data storage of data issuers (for example, universities).

- A shared infrastructure for digital identity among different stakeholders in the field of migration could overcome existing data silos and reluctance to share data and empower the position of migrants who can better control their identification data and its use by government authorities.

4. Are Any Pilot Projects in the Migration Field Being Tested?

Since SSI is a relatively new technological paradigm that combines new forms of digital identification with cryptographic methods and the idea of a distributed ecosystem, there are few pilot projects covering parts of the overall SSI concept, and they are not necessarily in migration.

For example, the Swiss canton of Zug, also known as the Crypto Valley, attracts many foundations and companies working in blockchain. From early on, the city and district administration have collaborated and innovated alongside the people and businesses coming to and living in Zug. It not only allowed residents to pay their administrative fees in Bitcoin, it also implemented a pilot project in the field of SSI. In collaboration with the company uPort that develops blockchain-based identity solutions, the city of Zug set up a Zug ID. In order to use their digital ID, the users had to register and get authenticated at the city clerk's office to receive a digital attestation. They could then use it as identity credential in the uPort-wallet. The city is not able to store or access any of the data stored in the wallet. After one year, only 120 inhabitants had registered for their SSI and they currently await further public services to be made accessible with their ID.

In the Zataari refugee camp in Jordan, a pilot project based on digital identity is being implemented. As an early adopter of blockchain-based identity systems, the World Food Program's Building Blocks combined new forms of biometric authentication and the ideal of peer-to-peer-payments without a strong intermediary (such as a bank or the Mastercard network). Even though it is not adopting the main components of SSI—especially not a self-sovereign digital wallet and verifiable credentials—it is incorporating blockchain technology as a disintermediated mode of cash-for-food. This project demonstrates how digital identification and decentralized technology (here: Ethereum blockchain) can work together in the field of migration. The project can serve as a first practical experience and step towards SSI use cases in the field of migration. The technology design of the Zataari Camp could be scaled up to a SSI solution by adding digital wallets and verifiable credentials, both available in the Ethereum ecosystem. For authentication of his or her identity, a resident of Zataari camp provides a biometric iris scan which is saved in an identity database. When a resident wants to use his or her allotted aid money in the local supermarket, the sensory biometric data–the iris scan–is compared to the identity database and the payment is subtracted from a personalized account running on the Ethereum blockchain. As a result, a fully contactless payment system is combined with a running eID system using biometric data for authentication. The digital identity solution is however not self-sovereign, meaning refugees cannot choose their favorite digital wallet to interact with the Ethereum blockchain. Rather, they are faced with an IT system that stores sensitive biometrical data and an overall IT infrastructure set up and run by an international organization. In this given use case, verifiable credentials, such as diplomas or birth certificates, are not necessary since the system is only used for

registering habitants of the camp and making payments within its vicinity—both payments and identification being solved by the camp management centrally. Overall, the example serves to point out the challenges of integrating a digital identity in migration processes. By using iris scans, the program circumvents the risks of managing cryptographic keys and certificates on a smartphone or using a chipcard (which could easily be passed on to others). Although this raises privacy concerns, it recognizes that people on the move—especially in the humanitarian sector—will typically struggle with getting, keeping, and managing a digital wallet that is solely under their own control.

The project also raises an important question for the future use of digital identities in the migration sector: how should a digital identity system be accessed in order to prevent identity fraud or theft? Which security measures—such as a password, a mobile TAN, or biometric identification (Face ID) —should be implemented to access a digital wallet and submit transactions? How can a person on the move make use of his or her digital rights and self-determination over data flows in an SSI ecosystem that is inherently permeated by power imbalances?

The Zataari pilot project shows that implementing new forms of digital identification and authentication comes with major challenges and trade-offs–both on a technological-organizational and an ethical-legal level. The question remains how to balance the goal of efficiency in an overall ecosystem of digital authentication in the field of migration with the impact on human rights, especially privacy, for people on the move.

5. What Are the Three Primary Challenges of Building an SSI Ecosystem for Migration?

1. Insufficient Standardization of SSI Components

Since SSI is a relatively new technological paradigm and blockchain ecosystems are still in their early-stage, key **components are not yet standardized and have not passed mass testing**. However, in projects such as the European Self Sovereign Identity Framework laboratory (ESSIF-lab) and international standardization organizations such as ISO/AWI 7603 (Decentralized Identity standard for the identification of subjects and objects), there is ongoing work to make SSI technology market-ready.

Since the term and technical specification of the SSI paradigm are still a work in progress, no common definition has been established. Yet, since the specification of a technological paradigm such as SSI will be able and done in manifold ways, it is expected that the terminology and technical components will diversify in the process. There will not be "one SSI to rule them all" nor will every decentralized identity system hold up to the high standard of Christopher Allen's 10 principles of SSI. However, it is becoming clear that an SSI ecosystem must at least have the following components: digital wallet (DW), verifiable credentials (VC), decentralized identifiers (DID), decentralized registry, digital agents, and hubs.

All those must be commonly standardized—including their interoperability—and pass mass-testing before a trustworthy SSI ecosystem can go live. The concerns of IT security experts need to be met and efficiently mitigated through technical and organizational measures.

The discussion at a public expert hearing on the topic of "Digital Identities" on July 4, 2022 at the German Federal Parliament showed the widespread reluctance to adopt and substantial criticism of IT security aspects of the SSI paradigm:

- An identity wallet as a solely smartphone-based means of digital identification might fall short of secure key management, especially on older devices without sufficient hardware to protect private keys from third-party intrusion. IT security experts therefore call, at the least for now, for sticking with smart cards as a secure hardware element.

- The lack of sufficient standardization of key technical elements of a European Identity Wallet. Often the failed attempt of the German ID wallet is used to underline how difficult it is to come up with a market-ready, trustworthy, and reliable basic app: The federal government had released an early-stage wallet app to manage one's own driving license in a digital wallet. After white-hat hackers found glaring vulnerabilities in the overall design, the ID wallet was quickly removed and the project canned.

Those concerns must be taken seriously and effectively mitigated before a digital identity wallet can be presented as a complement to national IDs.

2. Current Lack of Buy-in by the Public Sector—Digital Sovereignty of States over their Interconnected ID Systems

The SSI paradigm still needs the buy-in of the public sector to provide and run an ecosystem for the purpose of digital identification. Otherwise, there is a risk that tech companies will provide and manage a core duty of a sovereign state: identification and authentication of citizens.

From this perspective, it seems advisable to agree on specifications for the following questions:

- How can state authorities that issue eIDs and/or digital wallets keep the necessary control and influence on the overall system and data processing activities?
- Which entities should be allowed to actively participate in running the shared and decentralized data registry of an SSI ecosystem?
- Where should the information of the digital wallet holder be stored? How "sovereign" should his or her decision be to, for example, choose commercial cloud-services over public IT providers?
- How can an interoperability framework for digital identities be legally implemented and updated at an international level? From a European perspective: What is the international equivalent of the eIDAS regulation or a comparable binding framework for minimum standards?

3. No Consensus between Migration Stakeholders on Technical Standards and Core SSI Procedures

There are also overarching challenges that will need to be solved before putting an SSI system into practice in the field of migration:

A) *How are the necessary cryptographic keys, certificates and credentials stored and managed? How should a digital wallet be accessed in order to mitigate the risk of identity fraud?*

Every form of digital identification runs into a central challenge: Whoever controls the private key can easily take control over the digital identity. This task becomes even more difficult in a largely decentralized ecosystem that is, at the same time, supposed to be user-friendly and scalable.

To establish an interoperable system of digital identification, there must be a coherent and secure mode of assigning, revoking, and using cryptographic keys and certificates. Third parties must be prevented from taking over someone's digital identity. While there are many valid experiences in the field of public key infrastructure, there is little evidence of running a fully decentralized form of key management. Either the prior knowledge needed to set-up and run a digital wallet is too high for a regular user, or technological approaches remain underdeveloped and fall short in the field of IT security.

There remains an additional challenge: How should a digital wallet be accessed on a smartphone to mitigate the risk of identity theft or fraud? To answer this question, it is crucial to determine appropriate security measures—a password, a mobile transaction authentication number (TAN), or biometric identification (Face ID)—that can be implemented for logging into a digital wallet and submitting transactions. While a simple username and password combination can easily be hacked or stolen from a person on the move, biometric identification (through FaceID, iris scans, or fingerprints) comes with a much stronger guarantee that only the rightful owner can access a wallet. Biometric authentication however not only relies on a solid database and trustworthy hardware, but also raises additional privacy concerns. Stakeholders will have to find a suitable tradeoff between security, privacy, and usability.

B) *Who can and should issue digital wallets in the migration context?*

The migration field is influenced by different stakeholders that oftentimes have differing or even conflicting interests. Big institutions such as the United Nations High Commissioner for Refugees (UNHCR) and World Bank, large companies such as Microsoft and Apple, sovereign states such as Australia and the United States, and the EU have tended to create their own IT infrastructure for authentication. This has led to non-interoperable eID-systems and widespread reluctance to share large data pools.

The paradigm of SSI shows a potential way out: A distributed system that implements advanced cryptography can enable the accurate sharing of information (such as whether someone holds a university degree validated by the respective university) via a hash-value stored on a decentralized registry without revealing the information stored in the original diploma document (birth date, individual grades, religion, etc.). The respective plain text data (the diploma) stays only in the vicinity of the data holder (the graduate) and the data issuer (the university). If different public and private entities share the same decentralized infrastructure, trust is created on a technical level, and the authentication process in migration could be drastically reduced.

Yet who issues the necessary digital wallet? The relevant stakeholders need to reach a consensus on this point if the existing data and infrastructure silos shall be overcome. Should individuals be able to select from all available digital wallet solutions that meet the common technical standards in the migration context (such as an ISO standard)? Or should the task of issuing the digital wallet be appointed to one or more entities (for example, the UNHCR)?

Follow-up questions must be considered as well, such as: Which documents need to be presented in which form in order to be issued a digital wallet in the first place? How can new stakeholders, such as national governments or international organizations, join and support the SSI ecosystem in the field of migration after it starts? How can different legislations and legal cultures reach a consensus on privacy rules and implement them in the eID-technology?

A final challenge concerning technical standardization is the lack of representation of stakeholders from the migration field. Currently, standardization organizations such as the International Standardization Organization (ISO), the European Committee for Standardization (CEN) and the Institute of Electrical and Electronics Engineers (IEEE) are dominated by stakeholders from the private sector (especially the IT industry) and academia with either a business driven or very broad perspective on SSI technology. To take the requirements in the field of migration into account when standardizing SSI components, stakeholders from the field of migration—and digital consumer protection—should strengthen their efforts to send competent representatives to standardization organizations and consortia.

Benefits of Using SSI in the Migration sector

- Shared data and decentralized transactions between different entities
- Limited visibility of information through read/write permissions
- No conflict on appointing a data intermediary between stakeholders who do not trust each other
- No single point-of-failure
- Verification processes in a transparent manner through data distribution and time-stamping
- Self-determination of users through encryption and validation
- Ex-post manipulation of data points rendered basically impossible
- Can be an important tool in developing privacy-by-design solutions
- Can provide more reliable evidence (for example, of diplomas) in the field of business migration

Challenges of SSI in the Migration Sector

- Difficulty of adopting a new technological paradigm in a running system of established institutions; for example, interoperability with running IT systems, but also paper-based processes
- Unforeseen vulnerabilities, since SSI (especially with DLT elements) is an emergent technology without an established framework of technical standardization
- Distributed systems can replace trust but do people trust cryptography?
- Surveillance methods harder to implement in a distributed network without counteracting the overall technology architecture
- Need for digital competence and literacy
- Adoption might require adjustment of overall governance structure
- Integration difficult in humanitarian scenarios: how to combine safe authentication via digital wallet with the risk of losing, changing, or common use of smartphones as well as possible privacy impacts?

6. Recommendations for Migration Stakeholders Interested in Using or Testing SSI in the Migration Field

There are two main recommendations for migration stakeholders:

1. Migration Stakeholders Should Connect and Engage with the Current EUid Initiative

The European Commission has issued a proposal to reform the eIDAS Regulation. It includes the obligation of all member states to issue every citizen an identity wallet. If the reform proposal successfully goes through the legislative process, every European citizen would be able to install a EUid app on his or her digital device to prove their identity online. A wallet that follows the SSI-paradigm would also allow to submit credentials stored and linked in their identity wallet.

This would constitute a major increase in usability compared to the status quo, where member states are only obligated to issue a national eID when accompanied by an ID card, including identity verification and submission of core data (such as name, address, birth data) to a data receiver. The reform proposal for the eIDAS regulation has been prepared and has been accompanied by different funded projects and projects, especially:

- The European Blockchain Service Infrastructure (EBSI), which is developing a core system for public services that relies on a blockchain-based system with running nodes in every member state.
- The European Self Sovereign Identity Framework (ESSIF), which aims to create a technical backbone of necessary technological components for a running SSI ecosystem.
- Plans for an EUid would create a new mode of digital identification for all European citizens (national eID) as well as non-Europeans residing in Europe (national eResidency) where an identity wallet is the core element on the personal device of the person.

In a first step, the EBSI initiative has focused on some groundwork such as ESSIF, distributed storage of immutable proofs, and trusted data sharing. However, there are already plans to transfer the findings of SSI toward, for example, asylum process management. The potential scope of the EUid could go even further: Once established, the SSI framework of the EU could provide humanitarian organizations with the technological backbone to issue documents as standardized verifiable credentials that can

be integrated in standardized identity wallets used by migrants on their smartphone. The ESSIF would provide a possibility of integrating prior digital documents alongside a DID—for example, after initiating an asylum process in a member state—in the ecosystem of public services in the EU.

Since the proposal of the EC to develop an EU-wide ecosystem of eIDs based on the paradigm of SSI is still under discussion in the European Parliament and between member states, it is unclear if the proposal to provide every EU citizen or resident with a European Identity Wallet will prevail—and if it does, with which exact usability features. However, it seems advisable for stakeholders in the field of migration to formulate their specific needs and requirements for digital identification and authentication and participate in the ongoing process of establishing a new technical backbone in the field of user-centric and decentralized digital identities.

2. Migration Stakeholders Should Swiftly Come Together to Debate Options and Standards of Possible Core Elements of SSI in the Migration Field.

With multiple states and international organizations involved in identity management in migration on the one hand, and large IT companies developing and using new modes of digital identification on the other, the task of establishing a shared understanding of how "digital wallets" function becomes increasingly complex. Without common standards and specifications, it will be difficult to create an interoperable SSI ecosystem. Initiatives like the technical committee "CEN/CLC/JTC 19/ WG 01 – Decentralised identity management" of the European standardization organization CEN can serve as a gravitational center for bundling all efforts. **Stakeholders from the field of migration should participate in this important process that will shape the technology of SSI.**

Even if EU citizens and residents could one day use a European Identity Wallet, it remains unclear who would submit a digital wallet in the field of business and humanitarian migration. There is the imminent risk of a silo mentality where the ideal of interoperable solutions in global migration falls short because different stakeholders and governments have differing values and goals concerning a decentralized and user-centric approach.

It however seems a suitable way to coordinate the efforts of states and international organizations to raise the full potential. If the UNHCR introduces SSI-based infrastructure and issues digital identities, the technical infrastructure should be interoperable with the EUid and other forms of digital identification. At least the fundamental technological standards should be initiated and implemented together.

In contrast to prior forms of digital identity management, the concept of SSI is an attempt to establish a more decentralized and user-centric approach of authenticating elements of one's identity online. Compared to national eIDs and commercial SSO services, SSI promotes a paradigm of digital authentication and sharing of certified documents that goes midway between the risk of state surveillance of centralized or federated eID infrastructure and commercial exploitation of personal data necessary to identify a natural person. Stakeholders in the field of migration should not watch the ongoing discussions and efforts in technical standardization from a distance, but actively involve themselves in designing the interoperable and widespread digital identities of the future.

Further Resources

Academic Papers

- Cheesman, M. (2022), Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity, Geopolitics.
- Grech, A., Sood, I., and Ariño, L. (2021), Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education.
- Korkmaz, E. E. (2021), Digital Identity, Virtual Borders and Social Media Digital Identity, Virtual Borders and Social Media.
- Strüker, J. et al. (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.

Videos and Talks

- Evernym – Introduction to Self-Sovereign Identity
- European Blockchain Convention – Where Do We Stand on Self-Sovereign Identity?
- NGI Forward Salon on Digital Sovereignty in eID-Solutions I: Self-sovereign,Centralised or Privatised
- Fixing Aid – Can blockchain help fix the I.D. problem for a billion people?
- Kohlhaas, P. – uPort: Self Sovereign Identity in Zug