EUROPEAN UNION AGENCY
FOR CYBERSECURITY


# DIGITAL IDENTITY

## Leveraging the Self-Sovereignty Identity (SSI) Concept to Build Trust

JANUARY 2022

# ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu

## CONTACT

For contacting the authors, please use eID@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

## CONTRIBUTORS

Nick Pope, Michał Tabor, Iñigo Barreira, Nicholas Dunham, Franziska Granc, Dr. Christoph Thiel, Arno Fiedler

## EDITORS

Evgenia Nikolouzou (ENISA), Viktor Paggio (ENISA), Marnix Dekker (ENISA)

## ACKNOWLEDGEMENTS

ENISA would like to thank the members of the eIDAS Cooperation Network who participated in the survey for their valuable contributions and feedback to the report.

## LEGAL NOTICE



## COPYRIGHT NOTICE



ISBN: 978-92-9204-555-5 - DOI: 10.2824/8646 - Catalogue Nr.: TP-09-22-024-EN-N

# EXECUTIVE SUMMARY

The eIDAS Regulation enables the use of electronic identification and trust services by citizens, businesses, and public administrations to access online services or manage electronic transactions. A key objective of this Regulation is to remove existing barriers to the cross-border use of the electronic identification means used in the Member States in public services for, among others, the purpose of authentication. This Regulation does not aim to interfere with electronic identity management systems and related infrastructures established in the Member States. Rather, its goal is to ensure that secure electronic identification and authentication can be used to access cross-border online services offered by Member States.

The past nearly two years have proven to be a globally challenging period, in which eIDAS has been under revision and the COVID-19 pandemic has urged the development of new models for social life, business, and administration of government. To address these challenges, this report explores the potential of self-sovereign identity (SSI) technologies to ensure secure electronic identification and authentication to access cross-border online services offered by Member States under the eIDAS Regulation. The maintenance of continuity in social life, businesses and administration has accelerated the reflection on the possibility of a need for such decentralised electronic identity.

Over the last few years, a new technology has emerged for identification called "self-sovereign identities" (SSI). This technology gives identity holders greater control over its identity by adding features which provides a degree of distribution of identity related information. This includes the ability of identity holder to have multiple "decentralized identifiers" issued for different activities and to separate out the attributes associated with an identifier in "verifiable credentials". This gives the holder greater control over how its identity is represented to parties relying on the identity information and, in particular greater control over the personal information that it reveals to other parties.

**The present study critically assesses the current literature and reports on the current technological landscape of SSI and existing eID solutions, as well as the standards, communities, and pilot projects that are presently developing in support of these solutions. This study takes a wide view of decentralised electronic identity, considers possible architectural elements and mechanisms of governance, and identifies security risks and opportunities presented by SSI in view of cross-border interoperability, mutual recognition, and technology neutrality as required by eIDAS.**

The following are the main points arising from an analysis of the application of self-sovereign identity standards and implementation as described in this report:

- SSI technology, as applied in the standards and solutions identified in Section 1 and rationalised into a single architecture in Section 2, provides an effective basis for digital identities which protects the privacy of personal data. In particular:
    - Decentralised digital identities can be used to support pseudonyms for privacy of identity,
    - Verifiable credentials enable the separation of potentially private attributes from the digital identity all the user selection of attributes to be revealed to relying parties to ensure privacy of attributes which it is unnecessary to reveal, and
    - The ability to hold multiple authentication keys in a wallet with separate identity documents from different controllers enables the user to cryptographically separate transactions maintaining privacy by avoiding links between the separate transactions.

- For the governance of the elements of the architectural elements of an SSI solution (Section 3), there is a need to consider:
  - Certification of wallets,
  - Audit and oversight of DID controllers,
  - Audit and oversight of VC issuers,
  - Audit and oversight of DID and VC registries, and
  - All the above are interdependent and the governance of the DID controller and VC issuer also need to ensure that the other elements of an SSI architecture are also properly governed.
- When risk of the architecture of SSI is considered, the following key security measures need to be implemented:
  - Data minimalization – for use only necessary data,
  - Consent and choice – in which the user controls the process and data used for identification, and
  - Accuracy and quality – in which all parties can trust identification data stored and provided by the wallet.
- Lastly, it is recognised that there may be a role for ongoing support for technologies such as X.509 PKI, OpenID Connect, and existing national identity schemes. Thus, if SSI is to be adopted, further consideration should be given to co-existence between existing technologies and SSI.

# TABLE OF CONTENTS

# ABBREVIATIONS

| | |
|---|---|
| ABT | Advanced blockchain technology |
| AICPA | American Institute of Certified Public Accountants |
| API | Application program interface |
| CD | Committee draft of an international standard |
| CEN/CLC JTC | Joint technical committee of CEN and CENELEC |
| DID | Decentralised identifier (as specified by W3C) |
| DIF | Decentralised Identity Foundation |
| DLT | Distributed ledger technology (e.g. blockchain) |
| EC | European Commission |
| EBP | European Blockchain Partnership |
| EBSI | Joint initiative from the EC and the EBP |
| eID | Electronic identity |
| eIDAS | Regulation (EU) No 910/2014) |
| eIDAS 2.0 | Proposed revision to eIDAS in COM/2021/281 final |
| ESSIF | European Self-Sovereign Identity Framework of EBSI |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| FIDO | Fast Identity Online (FIDO Alliance) |
| GDPR | General Data Protection Regulation (EU) 2016/679 |
| HTTP | Hypertext transfer protocol (as specified in IETF RFC 2068 and subsequent documents) |
| IoT | Internet of things |
| ISO | International Standards Organization |
| ISO/IEC | Joint international standardization by ISO and the International Electrotechnical Commission |
| ISO TC | Technical committee of ISO |
| ISO TR | Technical report of ISO |
| JSON | JavaScript object notation |
| LoA | Level of assurance |
| mDL | Mobile Driving Licence |
| MS | European Union Member State |
| NGI | Next-generation internet |
| OIDF | OpenID Foundation |
| PGP | Pretty Good Privacy |
| PKI | Public key infrastructure |
| QR Code | Quick response code |
| SA | Secure area |
| SDK | Software development kit |
| SHA256 | Secure hash algorithm (256 bits) |
| SIOP | Self-issued OpenID Connect Provider |
| SME | Small- and medium-sized enterprises |
| SSI | Self-sovereign identity |
| TL | Trusted list |
| TSP | Trust service provider |
| URI | Uniform resource identifier |
| UUID | Universally unique identifier |
| VC | Verifiable credential (as specified by W3C) |
| W3C | World Wide Web Consortium |
| WG | Working group |
| X.509 | International Telecommunication Union standard defining the format of public key certificates |
| ZPK | Zero-proof knowledge technology |

# INTRODUCTION

Self-Sovereign Identities (SSI) are being seen as the next generation of digital identities across open networks; this is especially true of the Internet. This follows on from decades of experience with digital identities starting with centralised identities based on a hierarchy of authorities, such as X.509 Certification Authorities, moving on to federated identities, in which separate communities with several hierarchies cooperate to share trusted digital identities. The federated approach has further evolved in a more user-centred form of identity, such as developed by OpenID, OAuth and FIDO, but this still generally depends on a form of centralised control over the allocation of identities.

Self-sovereign identity technology allows the user to have further control of its identity. The basic concept of SSI, such as that developed by W3C and other communities described in this report and described in the seminal paper "The Path to Self-Sovereign Identity",[1] is that the user has control of its identity, which can be related to multiple formal identities issued by different authorities for different activities. The binding of the user-centred identity to other identifiers, as issued by recognised authorities, is called a "verifiable credential" (VC). This approach also allows user attributes, such as age or qualification, to be used instead of a formal identifier to control access to service based not on the full identity but rather on a user's specific and relevant attributes.

In Europe, under the first eIDAS Regulation (Regulation (EU) No 910/2014),[2] a federated approach was taken to identification of European citizens and organisations, with each Member State issuing a formal identifier to their nationals and a system of cross-recognition between nations. This has been found to have had a limited uptake. In recognition of the advantages of a more flexible approach to its citizens, the recent proposed revision to eIDAS (COM/2021/281 final),[3] hereafter referred to as eIDAS 2.0, is based upon an EU Digital Identity Wallet, which can be used to hold not only an EU Digital Identity but also known attributes and other independently issued credentials of the identified entity. This report does not directly consider the architectural implications of applying SSI technologies to eIDAS 2.0.

This report covers an extensive range of topics related to the emergence of SSI, specifically as the technology has been deployed as a means of electronic identity. The growth of the technology has been as fast as it has been organic, budding several expert- and user-led communities in addition to European Commission-driven initiatives aimed at integrating SSI within the extant fabric of eID solutions and regulatory framework developed in the current and proposed future eIDAS Regulation.

This paper describes the present landscape of the SSI ecosystem through an exploration of the standards groundwork which already make contact with the technology; with existing, robust SSI communities; and an examination of current eID strategies in Europe and the projects that are incorporating SSI into these national eID strategies. In particular:

- Section 1 is a presentation of this background research on the current SSI global landscape of SSI standards, communities, eID initiatives and current EU national SSI and eID initiatives. Within the scope of this study, ENISA has also issued a survey that asked Member States about the status of any activities relating to the use of SSI for

[1] http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

electronic identities; a summary of the findings can be found in Section 1.4.5, the questions for which are located at the end, in the 6.A Annex.

- Section 2 describes the necessary architectural underpinnings of the SSI tools.[4]
- Section 3 then explores the mechanisms of governance in place to manage the architectural elements of SSI.
- Section 4 is a natural follow-up to these prior topics, identifying the major points of security threats to the actors and assets identified in Section 2that may pose a risk to the successful use of SSI technology.
- Section 5 is a presentation of the conclusions based on the previous sections.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

# 1. CURRENT GLOBAL AND EUROPEAN SSI LANDSCAPE

## 1.1 STANDARDS

### 1.1.1 W3C Specifications

#### 1.1.1.1 Description and current status

The World Wide Web Consortium (W3C) is an international community in which member organisations, a full-time staff, and the public work together to develop web standards. W3C's primary activity is to develop protocols and guidelines that ensure long-term growth for the web. W3C is one of the main actors in the area of SSI because it has drafted and developed a number of foundational standards and technical implementations.

The following represents a non-exhaustive list of these activities, standards and implementations:

- Decentralized Identifiers (DID) v1.0: This is a specification for SSI. Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID.[5]
- Verifiable Credentials Data Model 1.0: This is a specification of verifiable identity and attribute assertions.[6]
- Decentralized Identifier (DID) Resolution v0.2: DID resolution is the process of obtaining a DID document containing information (e.g., public authentication key) associated with a given DID. This is one of four required operations that can be performed on any DID ("Read"; the other ones being "Create", "Update", and "Deactivate").[7]
- Issuer APIs and Verifier APIs: The VC HTTP API repository contains a standard API specification for constructing and verifying objects that conform to the Verifiable Credential Data Model specification, along with documentation, integration and compatibility tests, as well as related assets for the test and integration process.[8]
- Linked Data Vocabulary: This specification describes a linked data vocabulary for asserting VCs related to residency and citizenship information, such as given name, family name, country of citizenship, birthday, and other attributes used to determine the citizenship status of a citizen.[9]
- Credential Handler API 1.0: Credential Management Level 1 describes an imperative API enabling a website to request a user's credentials from a user agent, and to help the user agent to correctly store user credentials for future use. User agents implementing that API prompt the user to select a way to handle a credential request, after which the user agent returns a credential to the originating site. This specification defines capabilities that enable third-party web applications to handle credential requests and storage.[10]

[5] https://www.w3.org/TR/did-core/
[6] https://www.w3.org/TR/vc-data-model/
[7] https://w3c-ccg.github.io/did-resolution/
[8] https://github.com/w3c-ccg/vc-http-api
[9] https://w3c-ccg.github.io/citizenship-vocab/
[10] https://w3c-ccg.github.io/credential-handler-api/

We now turn our focus on the first two standards: DIDs and the verifiable credential data model.

#### 1.1.1.2 Decentralised Identifier

DIDs are a component of larger systems, such as the VC ecosystem, and identifies any subject that the controller of the DID decides that it identifies. Essentially, a DID is a uniform resource identifier (URI) that associates a DID subject with a DID document. DID documents can express cryptographic material, verification methods or services, which provide a set of mechanisms that enable a DID controller to prove control of the DID. The DID itself is a simple text string consisting of three parts: the DID URI scheme identifier, the identifier for the DID method, and the DID method-specific identifier.

#### 1.1.1.3 Verifiable Credentials

This specification provides a mechanism to express different sorts of credentials (e.g., driver's licenses, university degrees, government-issued passports) on the web in a way that is cryptographically secure, privacy-respecting, and machine-verifiable. The verifiable credentials data model enables the expression of different education qualifications, healthcare data, financial account details, and other sorts of third-party verified machine-readable personal information on the web.

#### 1.1.1.4 Applicability to eIDAS, SSI and European eID

These W3C standards are the core on which SSI implementation is based and could also serve as a basis for alignment with European legislation including future changes to eIDAS as well as GDPR. DIDs are part of the VC ecosystem and can be used to identify any subject (natural or legal persons), a characteristic which could be used under eIDAS as an identification use case and be used to link an eIDAS electronic identifier to a DID.

#### 1.1.1.5 Security risks and mitigation

DIDs and VCs, as specified by the W3C specifications, illuminate some specific security considerations, including the binding of identity, non-repudiation, key and signature expiration, key rotation, revocation, recovery, encrypted data, integrity, and level of assurance, most notable among others.

These specifications also have certain privacy considerations. For instance, personal identifying data, such as a government-issued identifier, shipping address, and a user's full name, can be easily used to determine, track, and correlate an entity. Combinations of information – even information that does not seem personally identifiable – such as a birthdate and a postal code, can have very powerful correlation and de-anonymising capabilities.

### 1.1.2 Decentralised Identity Foundation (DIF)

#### 1.1.2.1 Description and current status

The Decentralized Identity Foundation is an organisation focused on developing the foundational elements necessary to establish an open ecosystem for decentralised identity and ensure interop between all participants.[11] While DIF is itself responsible for developing standards and specifications building on those specifications produced by W3C for SSI, it is their members who produce reference implementations.

The following are the working groups in DIF:[12]

- **Identifiers and Discovery:** Covers the range of DID types, including but not limited to W3C DIDs.
- **Authentication:** Focuses on formats and protocols for authentication and authorisation using DIDs, DID documents and VCs, taking into account existing authentication

[11] https://identity.foundation
[12] https://identity.foundation/#wgs

protocols such as OAuth2 OpenID, User Managed Access (UAM2.0), WebAuthn, FIDO, and TLS. It does not, however, consider PKI. This work is taken forward in DID_SIOP[13] which is adopted as part of the OpenID OATH 2.0 specifications (see Section 1.3.2).

- **Claims and Credentials:** Focuses on formats for credentials based on W3C VCs.
- **DID Communications:** Focuses on protocol and data exchange formats for authentication message exchange based on DIDs.
- **Sidetree Development and Operating:** Focuses on protocols for "sidetrees", creating scalable DID networks that can run atop any existing decentralised anchoring system (e.g., Bitcoin, Ethereum, other distributed ledgers, or witness-based approaches) and can be as open, public, and permissionless as the underlying anchoring systems they utilise.
- **Secure Data Storage:** This group focuses on data models, APIs, security, and other related topics for secure data storage including that of personal data. This includes a HTTP-based interface comparable with W3C DIDs and VCs in "Identity Hubs" and "Encrypted Data Vaults", a specification which has been adopted by ESSIF.

An analysis of identity management concepts including DID is carried out in ISO TR 2329 "Overview of existing DLT systems for identity management", which is referenced in the following Section 1.1.3.

The DIF is a growing body; its members are willing to deliver a complete stack of open-source software for DIDs and VCs, including storage, exchange, communication and registries. A number of these draft specifications are stable and have been implemented by other groups such as Hyperledger (see Section 1.2.2) and ESSIF (see Section 1.2.3).

#### 1.1.2.2 Applicability to eIDAS, SSI and European eID

DIF specifications are very relevant to the case of SSI interoperability. Its framework document around the use of DIDs should be taken into account in the development of a European electronic identification. The Identity Hub specification provides for a useful shared data store for protecting personal data. The work with OpenID Connect on authentication should also be considered. Additionally, the sidetree protocol could be useful in linking a European electronic identification to a more global framework for SSI.

The work of the group is very relevant to the further development of standards building on the use of W3C DIDs and VCs such as may be carried out by the European Telecommunication Standards Institute (ETSI). To this end, a cooperation agreement between DIF and ETSI ESI would also be useful.

#### 1.1.2.3 Security risks and mitigation

The DID Secure Data Storage specifications consider requirements for secure storage of personal data.

### 1.1.3 ISO TC 307 and CEN/CLC JTC 19

#### 1.1.3.1 Description and current status

ISO TC 307 is concerned with standards for blockchain and distributed ledger technologies. The list of working groups established under the TC 307 purview includes the following:

- **WG 1 – Foundations**
  This group has published the standard ISO 22739, which provides a common set of vocabulary for blockchain and DLT.[14]

[13] https://didsiop.org/
[14] https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en

- **WG 3 – Smart contracts and their applications**
  This group has produced a working draft of TR 23642, an overview of best practices and issues regarding smart contracts, which is of indirect relevance, but not directly applicable, to SSI.

- **JWG 4 – Security, privacy and identity for blockchain and DLT**
  This group is joint with ISO JTC1 SC27 (which itself covers information security, cybersecurity and privacy protection). Current activities include:
  - Final draft TR 23249: Overview of existing DLT systems for identity management. This document is close to being finalised for publication. It includes useful information on a number of DLT systems for identity management. This list includes several systems investigated further in this report.
  - Working draft TR 23644: Overview of Trust Anchors for DLT-based Identity Management (TADIM). This document considers various existing schemes for trust management such as the PKI trust anchors, federated (bridged) PKI, and EU Trusted Lists, as well as other SSI-based schemes. This work may, in the future, lead to useful input to a governance framework.

- **WG 5 – Governance**
  This group is preparing a draft of TS 23635: Blockchain and Distributed Ledger Technologies – Guidelines for Governance. This document identifies nine principles for the governance of DLT systems, compares DLT governance with other governance frameworks and identifies some DLT-specific considerations. It also considers the governance of different type of DLT architectures, including both permissioned and permissionless.

- **WG6 – Use cases**
  This group has documented use cases for DLT in draft TR 3242 and is starting work on the analysis of data flows.

- **CEN-CLC JTC 19**
  The scope of CEN-CLC JTC 19 is stated to be: “To prepare, develop and/or adopt standards for Blockchain and Distributed Ledger technologies covering the following aspects:
  - Organisational frameworks and methodologies, including IT management systems;
  - Processes and products evaluation schemes; and
  - Blockchain and distributed ledger guidelines.

“This joint technical committee focuses on European requirements, especially in the legislative and policy context, and will proceed with the identification and possible adoption of standards or other relevant documentation already available or under development in other SDOs or regulatory bodies, which could support the EU Digital Single Market and/or EC Directives/Regulations. Special attention will be paid to ISO/TC 307 standards. If required, these standards will be augmented by CEN TRs and TSs.”

So far, the group has agreed to one activity, which is to work with ISO/TC 307/JWG4 on use of distributed ledgers for identity management.

Whilst a few general documents have been published, much of the work in TC 307 is still immature. However, it is expected that, in the next year or so, some important standards will be produced as a result of this work.

#### 1.1.3.2 Applicability to eIDAS, SSI and European eID

The work on identity management is still in early stages but could have significance for the future work on European electronic identities. The work on governance, particularly in relation to DLT-based identity management, may, in the longer term, have relevance to a European electronic identity scheme.

#### 1.1.3.3 Applicability to governance

The general work of TC 307 on governance in Draft TS 23635 are of note. The work on identity management and trust anchors in working draft TR 23644 may eventually lead to a more globally acceptable basis for governance.

#### 1.1.3.4 Security risks and mitigation

In working draft TR 23644, there is some early consideration of risk and trust management, which may be of relevance as the document progresses.

### 1.1.4 ISO/IEC 23220 and 18013-5

#### 1.1.4.1 Description and current status

ISO/IEC JTC1: SC17, which is concerned with cards and security devices for personal identification, is actively working on a multipart standard for mobile identities, to be ISO 23220. Currently only part 1, about generic architectures, has been published and this is available as a Draft International Standard. Work on technical specifications for the other parts has started, although no working drafts are yet generally available.

ISO/IEC 23220, entitled "Cards and security devices for personal identification – Building blocks for identity management via mobile devices" is to consist of the following parts:

- Part 1: Generic system architectures of mobile eID systems
- Part 2: Data objects and encoding rules for generic eID systems
- Part 3: Protocols and services for issuing phase
- Part 4: Protocols and services for operational phase
- Part 5: Trust models and confidence level assessment
- Part 6: Mechanism for use of certification on trustworthiness of secure area

The same committee has already published a standard for a mobile driving licence (mDL) application: ISO/IEC 18013-5. This has just been approved following a final ballot and is expected to be published in a few months following minor editorial updates.

#### 1.1.4.2 Applicability to eIDAS, SSI and European eID

The upcoming standard ISO/IEC 23220 is a strong contender for the basis of wallets on mobile devices, although, as the standard is still immature, its applicability to a European electronic identity is yet to be confirmed. The standard for a mobile driving licence (mDL) ISO/IEC 18013-5, which is expected to be published shortly, could provide a useful indication of the likely direction of ISO/IEC 23220.

#### 1.1.4.3 Applicability to governance

ISO/IEC 23220 Part 6 may provide the basis for certification of wallets. However, as yet, how this fits in with existing common criteria certification and upcoming EU certification schemes is yet to become clear.

#### 1.1.4.4 Security risks and mitigation

The architecture specifically addresses concerns over privacy through applying the principles as identified CD 23220-1 clause 5.2, in particular, for minimalization of data released in order to maintain privacy:

- Partial release of user attributes, thereby enabling the user only to release attributes as required by the relying party,
- Ensuring that identifiers at the protocol level are used that only cryptographically link to other transactions as considered necessary,

- Use of pseudonyms: The use of domain specific identifiers, which avoids the use of the same unique identifier for all transactions, for example, using different identifiers for public and private sectors.

## 1.2 SSI COMMUNITIES

This section describes the main commercial groups implementing SSI-based infrastructures.

### 1.2.1 Sovrin

#### 1.2.1.1 Description and current status

The Sovrin Foundation is a non-profit organisation established to administer the Governance Framework governing the Sovrin Network (of blockchain nodes), which is a public service utility that enables SSI on the internet. The Sovrin Foundation is an independent organisation that is responsible for ensuring that the Sovrin identity system is public and globally accessible. The Sovrin Network is a permissive network with nodes (called Stewards) required to meet audited requirements for trust services based on general AICPA (American Institute of Certified Public Accountants) requirements.

The Sovrin system includes the use of Cloud Agents, which hold wallet information under the control of users. This shares similarities with the CEN EN 419 241-1 based server signing systems and could provide a path forward for providing assured security of wallets without depending on security elements within user devices.

The Sovrin network is, at the time of drafting, one of the most mature networks for SSI and is still evolving building on the work of W3C (Section 1.1.1), DIF (Section 1.1.2) and Hyperledger (Section 1.2.2).

Further information on Sovrin can be found on their website.[15]

#### 1.2.1.2 Applicability to eIDAS, SSI and European eID

Sovrin's global service is open to the public providing SSIs with credentials (called claims). It is self-regulated but has useful experience that should be taken into account for a European electronic identity. The use of Cloud Agents, as adopted by Sovrin, could provide a way forward for assurance of wallets through an adaption of CEN 419 241-1/2 to support European electronic identity wallets.

Also, while the general approach to providing SSIs does not specifically address requirements for trusted credentials relating to identity, Sovrin's experience has direct relevance.

#### 1.2.1.3 Applicability to governance

Sovrin has a strong, self-regulated governance scheme in which only nodes (Stewards) are audited against general requirements for security controls based on the AICPA Trust Services Criteria. These criteria have similarities to the ETSI audit scheme and has already been seen as equivalent by the CA/Browser Forum. A comprehensive set of documents about Sovrin governance can be found on their website.[16]

#### 1.2.1.4 Security risks and mitigation

The Sovrin Network has a governance scheme that addresses general security requirements of trust services relating to SSI not specifically aimed at EU (i.e., non-qualified) regulations. Requirements for privacy and/or GDPR are specifically addressed by Sovrin.

[15] https://sovrin.org/library/
[16] https://sovrin.org/library/sovrin-governance-framework/

### 1.2.2 Hyperledger

#### 1.2.2.1 Description and current status

Hyperledger is an open-source community hosted by The Linux Foundation developing blockchain frameworks, tools and libraries. Areas of specific relevance to this study include the framework, Hyperledger Indy, library Ursa and the toolkit Hyperledger Aries.

Based on code contributed by the Sovrin Foundation (see Section 1.2.1), Indy was Hyperledger's first "identity-focused" blockchain framework, joining Hyperledger in 2017. Indy is a purpose-built distributed ledger for decentralised identity, and includes verifiable credentials based on zero-knowledge proof (ZKP) technology, DIDs, a software development kit (SDK) for building agents and an implementation of a public, permissioned distributed ledger.

Ursa is an independent crypto library migrated out of the Hyperledger Indy framework. Its purpose was, for security reasons, to keep crypto code separated and maintained only by a narrow group of experts.

Aries is a toolkit focused on the creation, transmission, storage and use of verifiable digital credentials. It allows secure messaging to exchange information using protocols that enable connectivity between peer-to-peer agents controlled by different entities: people, organisations and things.

There is no centralised repository in Indy; users use their own endpoints and wallet with individual data to store data. Users access the wallet through the User Agent and private key. A user can also have multiple DIDs on Indy; for each of them, the issuer generates a separate pair of public and private keys. The users can log in using their own private keys on the network to access their wallet.

Validator nodes are trusted parties who validate identities and transactions within the distributed network. The validator nodes run on the Plenum protocol, which allows a group of servers run by the validators to come to common agreement about the validity and order of events. Validator nodes store the data in a Merkle tree for each ledger, and ledgers are backed by a Merkle tree where each new transaction is hashed with SHA256 and added as a new leaf to the tree. Indy has a revocation functionality, in which the verifier refers to check the validity of a credential.

Observer nodes, which do not participate in consensus building, are optional and could help provide scalability for large numbers of clients. Observers can be standbys from whom clients can read data on a ledger.

Further information on Hyperledger can be found on their website.[17]

#### 1.2.2.2 Applicability to eIDAS, SSI and European eID

Indy is the most advanced SSI solution based on blockchain and should be considered as one of technologies for the implementation of a European electronic identity wallet. According to the proposed revision of eIDAS, VCs will be issued by TSPs and named "electronic attestation of attributes". Those trust services within the Hyperledger framework are the Stewards and trust anchors. The Indy network also provides the revocation functionality, which is required by eIDAS.

#### 1.2.2.3 Applicability to governance

The first actor in the Indy network is called a Steward. The Steward adds other nodes and actors to the distributed ledger. All the organisations or individuals are initialised by Steward on

[17] https://www.hyperledger.org/

the ledger with the role trust anchor before they can perform all activities. For practical use, Stewards (and Trustees) are important members of a governing body that holds the ultimate responsibility in maintaining the level of trust and credibility of the whole network. Each trust anchor can issue their own independent and unique schemas and credential definitions. For example, an issuer can share some information (e.g., a certificate) with a user and a user can share the certificate with a verifier. The verifier would then verify that the information in the certificate is indeed issued by an issuer who is a trust anchor in the Indy network.

#### 1.2.2.4 Security risks and mitigation

For security reasons, changing the value of passwords has long been a standard practice in the industry. A similar best practice for blockchain networks would be to replace an existing encryption key with a newly created one, a process called the “rotation of a key”. In Indy, whenever a new user joins the network, he or she is assigned a new public DID (also known as a Verinym or a Verkey). Later, using this key information on this user can be derived from the ledger.

### 1.2.3 ESSIF

#### 1.2.3.1 Description and current status

The European Self-Sovereign Identity Framework (ESSIF) is part of the European blockchain service infrastructure.[18] The EBSI is a joint initiative from the European Commission and the European Blockchain Partnership (EBP)[19] to deliver EU-wide, cross-border public services using blockchain technology. ESSIF aims to implement a generic SSI capability, allowing users to create and control their own identity across borders without the need to rely on centralised authorities.

ESSIF is based on W3C specifications for DIDs and the verifiable credentials data model as well as the DIF specification for an identity hub. A set of specifications issued by ESSIF were revised in Q2 2021,[20] building on the earlier first version specifications issued in 2020.

One notable use case for ESSIF is a generic and interoperable SSI framework. This framework would define the necessary specifications and build the supporting services and capabilities that would allow citizens to create, control, and use their own digital identity (including identification, authentication, and many other types of identity-related information) without having to rely on a single, centralised authority. Because ESSIF is a part of a broader ecosystem of decentralised identity, it will interact with other systems and platforms of public and private organisations.

The ESSIF v2 documentation[21] currently references architecture specifications that have already been issued for ESSIF v1, including data models and architectures:

- Nodes and ledgers for DIDs including endorsement and revocation,
- Verifiable credentials (including verifiable IDs),
- Verifiable presentations, and
- User and enterprise wallets.

More information about ESSIF[22] and EBSI[23] can be found online.

#### 1.2.3.2 Applicability to eIDAS, SSI and European eID

ESSIF is specifically aimed at alignment with European legislation, including eIDAS and GDPR. It includes features such as an eIDAS signature gateway to facilitate interoperability with

[18] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi
[19] https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership
[20] https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/ESSIF+Reference+Architecture
[21] https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/1.3.2.2.+Verifiable+Credentials+ESSIF+v2
[22] https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/Learn
[23] https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/EBSI+Documentation+Home

existing eIDAS X.509 certificate-based infrastructures. Additionally, elements of the ESSIF framework can make use of elements of the current eIDAS framework, in particular:

- ESSIF Verifiable IDs can be obtained using current eIDAS notified eIDs,
- ESSIF Verifiable IDs can be issued using an advanced electronic signature of the issuer created through an eIDAS Bridge with a qualified certificate. This might be extended to provide a qualified electronic signature, for example using an EN 419 241-1 remote signing system operated by a qualified trust service provider.

#### 1.2.3.3 Applicability to governance

In EBSI v1, technical governance is implemented with a classical IT centralised model. This means that the major operations of governance, including the creation of the code base, onboarding of nodes, onboarding of use case applications and decisions on management of the node are all managed centrally, either by the European Commission's Directorate-General for Informatic (DIGIT) or the Member State node host, depending on the operation.

#### 1.2.3.4 Security risks and mitigation

The high-level security measures of EBSI v2 are identified in the security track summary online.[24] This includes EBSI_V2_SMID_001 End user identification/authentication based on EU Login and EBSI wallet.

### 1.2.4 Latin America and Caribbean Chain (LACChain)

#### 1.2.4.1 Description and current status

LACChain is a global alliance integrated by different actors in the blockchain environment and led by the Innovation Laboratory of the Inter-American Development Bank Group (IDB LAB) for the development of the blockchain ecosystem in Latin America and the Caribbean.

Their objective is to accelerate the enabling and adoption of blockchain technology, including SSI, in the region to foster innovation as well as for a number of socially and economically oriented goals. Offering an open platform with minimal restrictions, LACChain is organized as a consortium for the management and administration of an infrastructure that is categorized as public-permissioned, following the classification of ISO (ISO/TC 307).

This work on infrastructure is classified into the DLT layer, the ID layer, and the "digital money" layer. LACChain ID, the working group behind all the identity developments, details all the concepts related to SSI (DIDs, VCs, digital wallets, and blockchain, among others) addressing technological, regulatory, and framework matters. LACChain has also enabled a full set of open-source tools to enable compatibility between identity services on top of the LACChain Networks.

#### 1.2.4.2 Applicability to eIDAS, SSI and European ID

LACChain is a global service open to the public, focusing on Latin America and the Caribbean, providing self-sovereign identities with credentials. It has experience, implementation and applicability that may be taken into account as an implementation example for a possible European SSI-based eID. It is also applicable to wallets across several devices (mobile and cloud).

The LACChain framework is fully aligned with and mentions eIDAS and GDPR consistently throughout. It also compares the different data protection and electronic signatures regulations from the different Latin American and Caribbean countries.

[24] https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/Security+track+summary

#### 1.2.4.3 Applicability to governance

LACChain has developed its own governance scheme and the structure focuses on:

- Governance of the decentralised registries and blockchain networks,
- Governance of the block generation (consensus protocol),
- Governance of the DID registries,
- Governance of the trusted lists (TLs), and
- Governance of the keys and credentials.

More information can be found at the Inter-American Development Bank site[25] and the LACChain ID framework.[26]

#### 1.2.4.4 Security Risks and mitigation

LACChain is committed to meet and follow GDPR and how to converge with SSI considering the different risks. There are six main areas cited to achieve this:

- **Consent:** Solutions that comply with user consent are efficient because (i) it is no longer necessary for third parties to exchange identity subject information and (ii) it is much easier to reach out to and ask the identity subject for consent.
- **Data portability:** Data portability is provided by digital wallets, where an individual can store their keys, credentials, and data. Cloud and mobile wallets are presently the most portable options.
- **Data protection by design and by default:** All aspects of the SSI model developed by LACChain, including DIDs, VCs, verifiable presentations, identification, authentication and authorisation, digital repositories and wallets, and a decentralised registry, are designed to protect data by default.
- **Pseudonymisation:** Pseudonymisation is a direct benefit of SSI. In order to guarantee pseudonymisation, suitable DID registries and DID methods must be used. These will allow an identity holder to manage as many pseudonymous identifiers as desired so that they can interact with various services securely. They can authenticate without revealing more data. Pseudonymity is also one of the main advantages of DID documents and verifiable presentations over the traditional X.509 for electronic identification.
- **Records of processing activities:** As data is connected to identifiers, and individuals are responsible for sharing their own credentials, digital wallets should be able to keep a private record of processing activities. Additionally, public and decentralised blockchain registries allows for more pseudonymous traceable data; nobody will be able to correlate identifiers if suitable solutions are developed.
- **Right to erasure (right to be forgotten):** The right to erasure is always challenging as it implies that one must (i) know exactly where the data is, (ii) be able to authenticate themselves to those who own their data so they can ask them to erase it, and (iii) not have personal data in immutable and decentralised registries. SSI enables the achievement of the first two goals with much more ease than other digital identity models, but the third goal must be carefully taken care of. Bad implementations of SSI and blockchain could very easily violate data privacy.

[25] https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignity-digital-wallets-and-blockchain
[26] https://lacchain-2.hubspotpagebuilder.com/lacchain-id-framework (LACCChain)

## 1.3 EXISTING EID INITIATIVES

### 1.3.1 eIDAS 2.0

Details of eIDAS 2.0 requirements and how SSI can be applied to the requirements are not included in this paper. However, of relevance are the key points of the new proposal in the context of self-sovereign identity, as follow:

Title: *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (Brussels, 3.6.2021, COM(2021) 281 final, 2021/0136 (COD))*

- Harmonised conditions for the establishment of a framework for European Digital Identity Wallets to be issued by Member States.
- Union citizens and other residents as defined by national law will able share securely data related to their identity in a user friendly and convenient way under the sole control of the user.
- Technologies used to achieve those objectives should be developed aiming towards the highest level of security, user convenience and wide usability.
- Member States should ensure equal access to digital identification to all their nationals and residents.
- Service providers should communicate their intent to rely on the European Digital Identity Wallets to Member States. That will allow Member States to protect users from fraud and prevent the unlawful use of identity data and electronic attestations of attributes as well as to ensure that the processing of sensitive data, like health data, can be verified by relying parties in accordance with Union law or national law.
- European Digital Identity Wallets should allow users to electronically identify and authenticate online and offline across borders for accessing public and private services.
- Wallets can also serve the institutional needs of public administrations, international organisations and the Union's institutions, bodies, offices and agencies.
- Offline use would be important in many sectors, including in the health sector where services are often provided through face-to-face interaction and ePrescriptions should be able to rely on QR-codes or similar technologies to verify authenticity.
- European Digital Identity Wallets should benefit from the potential offered by tamper-proof solutions such as secure elements, to comply with the security requirements under this Regulation.
- The European Digital Identity Wallets should also allow users to create and use qualified electronic signatures and seals.
- Member States should issue European Digital Identity Wallets relying on common standards to ensure seamless interoperability and a high level of security.
- The conformity of European Digital Identity Wallets with those requirements should be certified by accredited public or private sector bodies designated by Member States.
- European Digital Identity Wallets should ensure the highest level of security for the personal data used for authentication irrespective of whether such data is stored locally or on cloud-based solutions, taking into account the different levels of risk.
- Use of biometrics to authenticate is one of the identifications methods providing a high level of confidence, in particular when used in combination with other elements of authentication.
- Any entity that collects, creates and issues attested attributes such as diplomas, licences, certificates of birth should be able to become a provider of electronic attestation of attributes.
- Relying parties should use the electronic attestations of attributes as equivalent to attestations in paper format.
- Private relying parties providing services in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the use of European

Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by national or Union law or by contractual obligation. Where very large online platforms require users to authenticate to access online services, those platforms should be mandated to accept the use of European Digital Identity Wallets upon voluntary request of the user.

- Users should be under no obligation to use the wallet to access private services, but if they wish to do so, large online platforms should accept the European Digital Identity Wallet for this purpose while respecting the principle of data minimisation.
- Attributes provided by the qualified trust service providers as part of the qualified attestation of attributes should be verified against the authentic sources either directly by the qualified trust service provider or via designated intermediaries recognised at national level in accordance with national or Union law for the purpose of secure exchange of attested attributes between identity or attestation of attributes' service providers and relying parties.

### 1.3.2 OpenID/OAuth2

The OpenID Foundation (OIDF) is a non-profit international standardisation organisation of individuals and companies committed to enabling, promoting, and protecting OpenID technologies. Formed in June 2007, the Foundation serves as a public trust organisation representing the open community of developers, vendors, and users. OIDF assists the community by providing needed infrastructure and help in promoting and supporting expanded adoption of OpenID.

OIDF has worked with DIF (see Section 1.1.2) to a define an extension to the current specifications for authentication based on decentralised identifiers DID_SIOP.[27] Specifications for Self-Issued OpenID Connect Provider (SIOP)[28] is a part of OAuth 2.0 and complies OpenID Connect Core 1.0, which are the underlying protocols for all popular social login schemes. This guarantees the dataflows and user journeys remain the same compared to what users are using today.

OpenID is an open standard and decentralised authentication protocol. It allows users to be authenticated by cooperating sites (also known as relying parties) using a third-party service, eliminating the need for webmasters to provide their own ad hoc login systems, and allowing users to log into multiple unrelated websites without having to have a separate identity and password for each. Users create accounts by selecting an OpenID identity provider and then use those accounts to sign onto any website that accepts OpenID authentication. According to OIDF, there are more than 50,000 websites that either issue or accept OpenIDs on their websites, with over one billion OpenID enabled user accounts.

Published in February 2014 by OIDF, OpenID Connect is the third generation of OpenID technology. It implements an authentication layer on top of the OAuth 2.0 protocol (see below). It allows clients of all types, including web-based, mobile, and JavaScript clients, to verify the identity of the end-user based on the authentication performed by an authorisation server, as well as to request and receive information about authenticated sessions and end-users in an interoperable and REST-like manner. OpenID Connect includes a new authentication request message, a new ID token, which contains claims about the authentication and is represented as a JSON Web Token (JWT), and new request/response messages to get additional user data. OAuth 2.0 Authentication Servers implementing OpenID Connect are also referred to as OpenID Providers (OPs). OAuth 2.0 Clients using OpenID Connect are also referred to as relying parties.

[27] https://didsiop.org/
[28] https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

The other work and contribution of the OpenID Foundation is organised by different working groups (WG) focused on a specific problem, technology, or opportunity for which the members will deliver a document or series of documents, after which they may disband or create a revised charter for further work:

- **AB/Connect WG29**
  The AB/Connect working group is a combined working group of the Artifact Binding Working Group and the Connect Working Group aimed at producing the OAuth 2.0 based "OpenID Connect" specifications.
- **Enhanced Authentication Profile (EAP) WG30**
  The purpose of this working group is to develop a security and privacy profile of the OpenID Connect specifications that enable users to authenticate to OpenID Providers using strong authentication specifications. The resulting profile will enable use of IETF Token Binding specifications with OpenID Connect and integration with FIDO relying parties and/or other strong authentication technologies.
- **eKYC & IDA WG31**
  The eKYC and Identity Assurance working group is developing extensions to OpenID Connect that will standardise the communication of assured identity information, (i.e., verified claims and information about how the verification was done and how the respective claims are maintained.
- **Financial-grade API (FAPI) WG32**
  The goal of FAPI is to provide JSON data schemas, security and privacy recommendations and protocols to:
  - Enable applications to utilise the data stored in the financial account,
  - Enable applications to interact with the financial account, and
  - Enable users to control the security and privacy settings.
- **FastFed WG33**
  The purpose of this working group is to develop a meta-data document specification, APIs, and workflow to enable an administrator to federate an identity provider and a hosted application that supports one or more of OpenID Connect, SAML, and SCIM and enable configuration changes to be communicated between the identity provider and hosted application.
- **HEART WG34**
  The HEART working group intends to harmonise and develop a set of privacy and security specifications that enable an individual to control the authorisation of access to RESTful health-related data sharing APIs, and to facilitate the development of interoperable implementations of these specifications by others
- **International Government Assurance Profile (iGov) WG35**
  The purpose of this working group is to develop a security and privacy profile of the OpenID Connect specifications that allow users to authenticate and share consented attribute information with public sector services across the globe. The resulting profile will enable standardised integration with public sector relying parties in multiple jurisdictions. The profile will be applicable to, but not exclusively targeted at, identity broker-based implementations.

[29] https://openid.net/wg/connect/
[30] http://openid.net/wg/eap/
[31] http://openid.net/wg/ekyc-ida/
[32] https://openid.net/wg/fapi/
[33] https://openid.net/wg/fastfed/
[34] https://openid.net/wg/heart/
[35] https://openid.net/wg/igov/
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- **MODRNA WG36**
  The MODRNA (Mobile Operator Discovery, Registration & autheNticAtion) working group will develop a profile of OpenID Connect intended to be appropriate for use by mobile network operators (MNOs) providing identity services to RPs and for RPs in consuming those services as well as any other party wishing to be interoperable with this profile. Additionally, it will identify and make recommendations for additional standards items.

- **Research & Education (R&E) WG37**
  The purpose of this working group is to develop a set of profiles for the OpenID Connect specifications to ease the adoption of OpenID Connect in the Research and Education (R&E) sector. The profiles will consider existing practices of federated identity management in the R&E sector, current international standards to represent users that belong to R&E institutions, as well as the existing international trust fabric based on R&E identity federations and multi-lateral trust exchange. The working group will also actively look for the engagement of the R&E international community.

- **Shared Signal & Events WG38**
  The goal of this working group is to provide data sharing schemas, privacy recommendations and protocols to:

  - Share information about important security events to thwart attackers from leveraging compromised accounts from one Service Provider to gain access to accounts on other Service Providers (mobile or web application developers and owners).
  - Enable users and providers to coordinate to securely restore accounts following a compromise.
  - Internet accounts that use email addresses or phone numbers as the primary identifier for the account will be the initial focus.

### 1.3.3 Horizon 2020 Initiatives

Horizon 2020 is a funding program for research and innovation in the EU, initiated by the European Commission in 2014. It aims to strengthen and secure Europe's global competitiveness. With a total funding of over 80 million Euros, the program was until then the biggest EU research and innovation program. The program aims at addressing three major challenges, including advancing scientific excellence, fostering competitiveness and market leadership, and resolving large societal challenges.

Within the nine different program sections, several projects show a relevance for the development and implementation of self-sovereign identities. The average budget of these projects is 5.5 million Euros. Most of these projects intend to achieve interoperability, usability, and European standardisation, and have underlined the need to create a European solution by creating eIDAS-compliant solutions. In these cases, SSI is seen as a means to enable transnational identification while complying with existing standards and regulations, such as eIDAS or GDPR.

The SSI-relevant projects receive funding from at least four different programmes. Most are covered under H2020-EU.2.1. – Industrial Leadership,[39] which aims at enabling new,

[36] https://openid.net/wg/mobile/
[37] https://openid.net/wg/rande/
[38] https://openid.net/wg/sse/
[39] Other relevant funding programs include: Shift2Rail JU (H2020-EU.3.4.8.); exploring new forms of innovation, with special emphasis on social innovation and creativity, understanding how all forms of innovation are developed, succeed or fail (H2020-EU.3.6.2.2.); strengthening security through border management (H2020-EU.3.7.3.); improving cyber security (H2020-EU.3.7.4.); ensuring privacy and freedom, including on the internet, and enhancing the societal, legal and ethical understanding of all areas of security, risk and management (H2020-EU.3.7.6.); supporting the EU's external security policies including through conflict prevention and peace-building (H2020-EU.3.7.8.).
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

sustainable products, processes and services and their competitive deployment, as well as advanced manufacturing and processing to address major societal challenges.[40]

The identified projects base their technical solutions on distributed ledger technology (ISO 22739:2020) and cover different topics and domain fields in which they implement the technology. Examples of covered domain fields include the digital economy, Next-Generation-Internet (NGI), secure society, eHealth, eGovernment, mobility, and big data.

KRAKEN follows a decentralised, user-centred approach for the exchange of personal data. Built on existing Blockchain data infrastructures, KRAKEN is developing a trusted and secure personal data platform with state-of-the-art privacy aware analytics methods to preserve the privacy and self-sovereignty of personal data. The Data platform will consider trust and security levels from national identity schemes and thereby ensuring eIDAS-compliancy.[41]

The project IMPULSE carries out user-centred and multidisciplinary impact analysis for the integration of blockchain and AI in eID in public services, consideration of existing eID systems and standards, such as GDPR and eIDAS.[42]

The project MGOV4EU provides a bridge between eIDAS and the Single Digital Gateway to create an open ecosystem and to enable secure and user-friendly mobile government services to be used across Europe. mGov4EU mobilises the existing eIDAS interoperability infrastructure ("eIDAS Layer") for cross-border eGovernment processes. GDPR-conformity is reached through the usage of hardware-backed secure elements together with integrated convenience elements like biometric sensors.[43]

The project 5GZorro aims to use Distributed Ledger Technologies (DLT) to implement flexible and efficiently distributed security and trust between the different parties of a 5G end-to-end service chain.[44]

The project AI4HEALTHSEC promotes the exchange of reliable and trustworthy incident-related information between the ICT systems and units that make up the HCIIs without revealing sensitive company data.[45]

The project D4FLY offers a simple identity verification for border crossings using a border control kiosk equipped with advanced registration, verification and recognition functions and smartphone applications. Their solution includes a non-stop-on-the-move system for biometric verification. D4Fly investigates "potential advantages of a blockchain technology for identity verification".[46]

The EU-funded eSSIF-Lab project is an innovation project aiming to reinforce internet reliability with electronic identities through the development and adoption of SSI technologies. The goal is to advance the broad uptake of SSI as a next-generation open and trusted digital identity solution.[47]

GLASS creates a blockchain-based distributed Framework "European Common Services Web". At its core stands a citizen-oriented e-governance model that simplifies big data-exchange and

[40] https://cordis.europa.eu/programme/id/H2020-EU.2.1.1
[41] https://cordis.europa.eu/project/id/871473
[42] https://cordis.europa.eu/project/id/101004459
[43] https://cordis.europa.eu/project/id/959072/de
[44] https://cordis.europa.eu/project/id/871533
[45] https://cordis.europa.eu/project/id/883273/de
[46] https://cordis.europa.eu/project/id/833704
[47] https://cordis.europa.eu/project/id/871932/de
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

common services of public administration across the EU. The Solution includes a distributed file storage system that records every transaction among users; a distributed application ecosystem (dapp) for the provision of mobile services; a WaaS platform (Single Sign-On Wallet as a Service) and a middleware gateway framework for the establishment of secure communication channels between operational stakeholders and the integration of existing e-governance systems.[48]

NGI Assure aims at creating scalability, interoperability and sustainability through “Advanced Blockchain Technologies” (ABTs), converting cutting-edge research into standards that are accepted in all types of application areas and thereby achieving the objectives of the “Next Generation Internet” initiative.[49]

## 1.4 EU NATIONAL SSI AND ELECTRONIC IDENTITY WALLET INITIATIVES

### 1.4.1 Germany

#### 1.4.1.1 Description and current status

The German Federal Ministry of Economic Affairs initiated the Showcase Programme “Secure Digital Identities" in 2019, aimed at the development of German eIDAS solutions that are user-friendly, trustworthy, and economical, accessible for the administration, businesses – especially SMEs – and the population. In total, four projects have been selected to implement and test their solutions throughout Germany in different cities and communities over the next three to four years. The selected projects can be regarded as a wide-ranging test lab for SSI applications, as all act in the field of SSI.

The aim is to create new ID ecosystems in which users can digitally identify themselves to service providers or authorities with a mobile device, without media discontinuity and regardless of location. The solutions refer to the identification of people, the identification of things or a combination of both.

The use cases of the projects cover 10 fields: Education, health, hospitality, tourism, trade, logistics, mobility, energy, Industry 4.0, IoT, access management, public administration, and the financial sector.

The main objectives are:

- Strengthening the digital sovereignty of the citizens,
- Demonstrating the everyday benefits of secure digital identities to citizens,
- Showing wide application possibilities,
- Simplifying access to digital business and administrative services, and
- Improving the usability of secure digital identities (e.g., replacing the username-password paradigm).

#### 1.4.1.2 Applicability to eIDAS, SSI and European eID

The aim is to build an infrastructure that allows the secure exchange of proofs that is suitable for Europe-wide use and works equally for the identities of people, institutions and things on the basis of SSI. The implemented solutions are smartphone-based, and the verifiable credentials are filed in digital wallets. So far, three of the projects have begun the implementation phase.

The first project, IDunion, implements a decentralised public key infrastructure, using the European cooperative *Societas Cooperative Europaea S.C.E* as a governance authority, which,

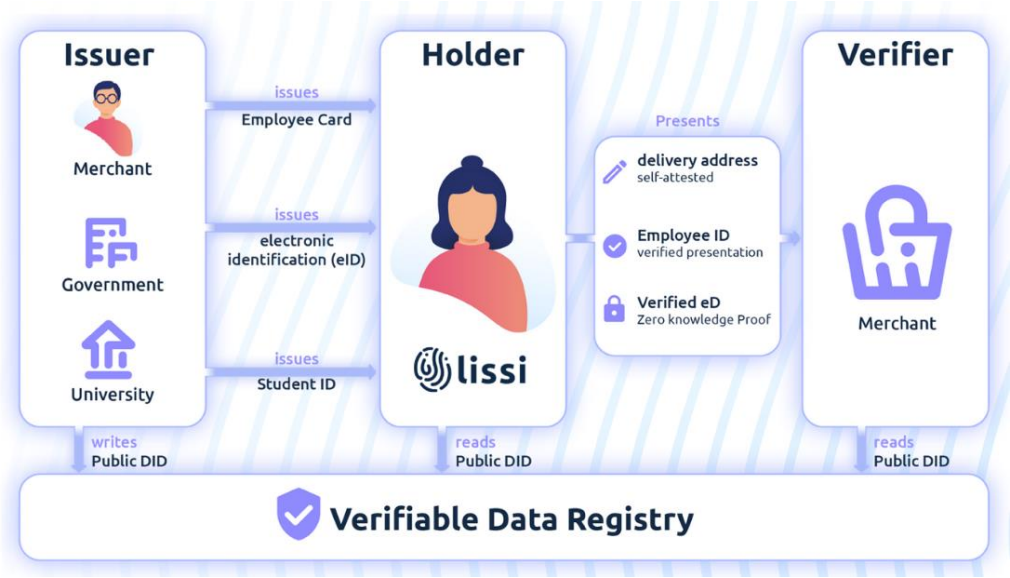
[48] https://cordis.europa.eu/project/id/959879/de
[49] https://cordis.europa.eu/project/id/957073

as a legal entity, determines the rules of the network and its implementation. They have developed their own wallets (Lissi and Estatus) and agents.

The second project, ONCE, develops and implements secure digital identities for administration, transport and the hotel industry. The ID systems used in ONCE are eIDAS-compliant and correspond to the security and trust requirements that the different areas of application demand.

The final project presently undergoing implementation, ID-ideal, focuses on the development of a trust framework considering existing SSI standards based on W3C and DIF.

**Figure 1:** ID Union SSI project framework (source: Lissi)




These solutions must all be GDPR and eIDAS-compliant and based on available standards. The specific use cases in the field of personal identification should be usable on a mobile device and address the security levels "low" and "substantial" described in eIDAS. Application scenarios in business and administration, which require the security level "high" in eIDAS, should use the eID function of the identity card / electronic residence permit / eID card for EU citizens or another available solution according to eIDAS "high".

#### 1.4.1.3 Applicability to governance

The proposed open ID ecosystem and interoperable ID solutions relies on the development of a trust network, for example, that concerns semantic interoperability, procedures for dealing with different levels of assurance (LOA). One focus of the implementation should be the interaction between different ID solutions or different providers.

The solutions should thus build on existing European electronic identity infrastructure and ensure the state remains the origin of the citizen's core identity. They should be based on international norms and standards so that the results can easily be transferred to other municipalities, cities or metropolitan regions, including outside of Germany.

#### 1.4.1.4 Security risks and mitigation

A potential challenge is to achieve interoperability among the different projects and their approaches. Especially with regards to other ongoing projects of the German chancellery or EU initiatives such as GAIA-X.

### 1.4.2 Spain

Spain released its first standard defining a reference framework for the management of identification in 2020. This standard allows individuals and organisations to create and self-manage their own digital identity without the need to resort to a centralised authority. It was produced by Aenor, the Spanish Association for Standards, and has become an UNE (One Spanish Norm) standard, entitled UNE 71307-1.

This standard was published on 9/12/2020, and on 11/1/2021 it was published in the BOE (Spain Official Bulletin), a process which officially approved and made it legally binding. The next step is to promote this standard to the CEN/CENELEC to become a European standard. On 11/2/2021, an autonomous community in Spain legislated the Blockchain Digital Identity, though it is waiting for approval at the national level.

More information can be found on the UNE website.[50]

#### 1.4.2.1 Description and current status

This standard, entitled “Digital Enabling Technologies. Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. Part 1: Reference Framework”, is about DIDs, blockchain and other identity management solutions for a decentralised identity.

Standardised decentralised identity information management models ensure that organisations maintain the security of their processes and that individuals protect their privacy and avoid identity theft, in contrast to traditional centralised models.

This Spanish norm meets the following conditions. It:

- Is technologically neutral,
- Is compatible with other international standards related to digital identity,
- Meets the requirements of GDPR,
- Meets eIDAS and the ENS (Spanish National Security schema),
- Allows the implementation of DID management systems,
- Takes into consideration the SMB needs, and
- Is adequate for the use between natural and legal persons.

The standard, which has begun the process of becoming a European standard, has been developed as part of UNE’s committee covering blockchain and distributed ledger technologies, CTN 71/SC 307, with the participation and consensus of all parties involved.

The CTN 71 on digital enabling technologies was established at the behest of the Secretary of State for Digitization and Artificial Intelligence. Technical standards establish a common language, providing security and confidence in new technologies, and are thus a pillar for the success of digital transformation.

#### 1.4.2.2 Applicability to eIDAS, SSI and European ID

This standard sets a reference framework to manage decentralised identities and takes into consideration the different standards for SSI, for example from the W3C, and those related to the EU electronic identity. This standard is also compliant with the requirements set forth by eIDAS and GDPR.

[50] https://www.en.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0064986

#### 1.4.2.3 Applicability to governance

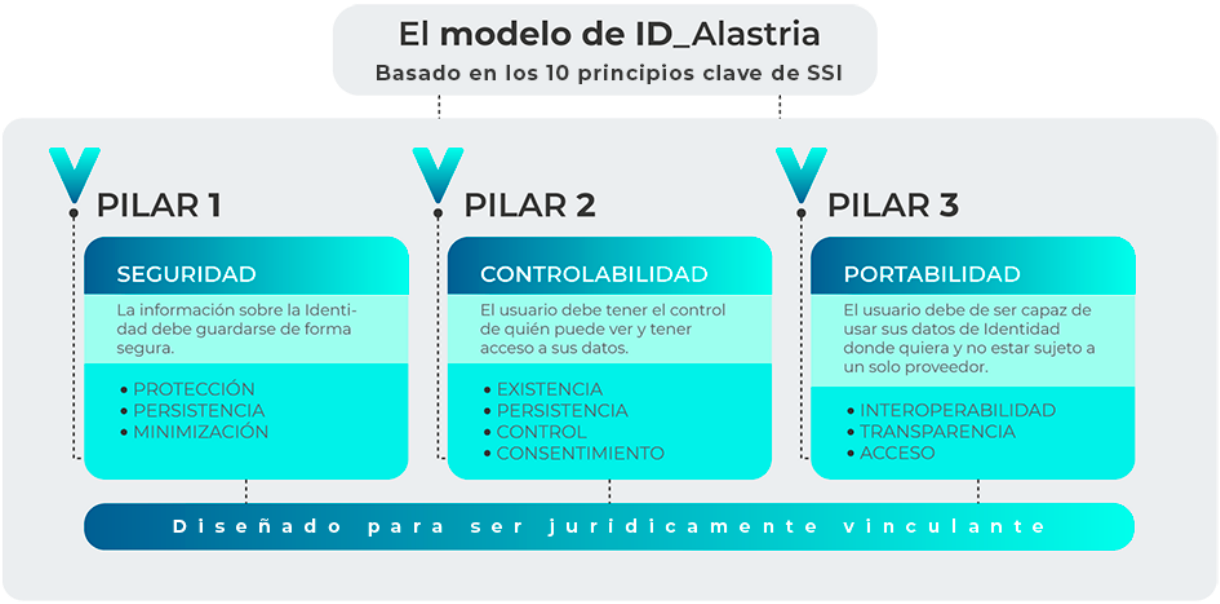
This standard indicates some governance protocols related to:

- DID and credentials lifecycle,
- DID and credentials requisites, and
- Requirements for protocol messages.

#### 1.4.2.4 Security risks and mitigation

Alastria, which is a not-for-profit association of multi-sector entities and is one of the main contributors to the development of this standard, has released a model based on 10 key principles for SSI.[51] These 10 principles are grouped by different pillars, which are Security, Controllability and Portability, with specific governance processes for all of them, illustrated in the figure below.

**Figure 2:** Alastria's ID model




There is presently an ongoing project named PNE 71307-2: Digital Enabling Technologies – Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies, Part 2: Guidelines.[52]

### 1.4.3 Netherlands

#### 1.4.3.1 Description and current status

Delft University is a government partner for digital identity. The University is receiving a five-year funding for a research project to develop an open-source, production-ready SSI. Their operational open-source prototype for a digital identity is integrated with the European Commission EBSI infrastructure. Furthermore, they are currently in discussions with the Netherlands, Sweden and Singapore about a live cross-border trail of SSI+Euro. Delft University released some specific documents regarding the Netherlands and SSI during the last few years. This section focuses on two of such documents, which were published in 2018 and 2020.

[51] https://alastria.io/en/
[52] https://www.une.org/encuentra-tu-norma/busca-tu-norma/proyecto/?c=P0054798

The 2018 study reflects how digital identity largely remains unresolved because, after many years of research, there are still remain concerns over trusted communication over the Internet (e.g., phishing). One solution for the provision of identity within the context of mutual distrust, this paper presents a blockchain-based digital identity. Without depending upon a single trusted third party, the proposed solution achieves a passport-level legally valid identity. This solution for making identities self-sovereign, builds on a generic provable claim model for which attestations of truth from third parties need to be collected. The claim model is then shown to be both blockchain structure and proof method agnostic. Four different implementations in support of these two claim model properties are shown to offer sub-second performance for claim creation and claim verification. Through the properties of SSI, legally valid status and acceptable performance, this proposed solution is considered to be fit for adoption by the general public.

The 2020 study reflects how digital identity is essential to access most online services, and that digital identity is often outsourced to central digital identity providers, introducing a critical dependency. While SSI offers citizens ownership of their own identity, proposed solutions concentrate on data disclosure protocols and are unable to produce identity with legal status. It has been identified how related work attempts to legalize identity by reintroducing centralization and disregards common attacks on peer-to-peer interactions, missing out on the strong privacy guarantees offered by the data disclosure protocols. IPv8 is presented to address this problem, a complete system for passport-grade SSI. This design consists of a hierarchy of middleware layers which are minimally required to establish legal viability. IPv8 comprises a peer-to-peer middleware stack with Sybil attack resilience and strong privacy through onion routing.

#### 1.4.3.2 Applicability to eIDAS, SSI and European ID

IPv8 was initiated in 2016 and created in tight collaboration with both government and industry. This design complies as much as possible with existing standards for authentication. The IPv8 design choice for security and privacy is that the verifiable claims are stored in encrypted form. Unlocking these encrypted claims requires passport-grade facial recognition. This component in IPv8 is supplied by IDEMIA, the Netherlands' paper-based passport supplier. All code of IPv8 is available on GitHub and is provided under the GNU LGPL 3.0 license.[53] This approach is also GDPR compliant.

#### 1.4.3.3 Applicability to governance

The cited documents were created in cooperation with the Dutch National Office for Identity Data (Ministry of the Interior and Kingdom Relations). As such, it was the second digital identity model in the world to be sanctioned by a government after Estonia.

#### 1.4.3.4 Security risks and mitigation

For a central trusted third-party: the solution is from D-H to PGP and PKI, but this requires identity to be tied to a public key. The variety of solutions and these become honeypots for attacks. For a non-central trusted third-party: the solution is based on SSI. The paradigm trust changes from trusting each other to trusting the user. This can be achieved by the use of blockchain, though risks still remain.

One solution would be SSI over blockchain, with no power to the owner, no third-party control of attributes, and therefore it would be a permissionless, open enrolment. An IPv8 application may also be defined and implemented.

[53] https://github.com/Tribler/py-ipv8

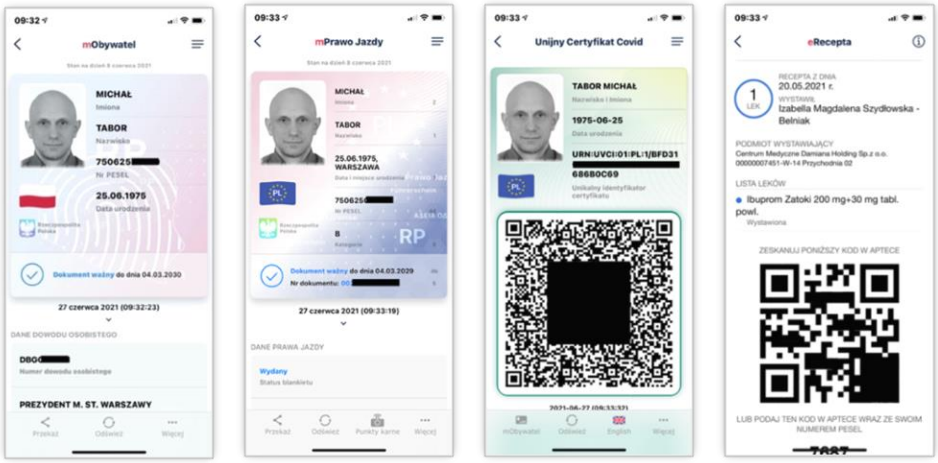
## 1.4.4 Poland

### 1.4.4.1 Description and current status

In 2018, Poland introduced a public mobile application, which is provided by the Ministry of Digital Affairs. The legal basis for the application was established at the same time by law. An application called mObywatel (English: “mCitizen”) allows downloading, storing, and presenting electronic documents, such as an ID card or a driver’s license, and transferring these documents between mobile devices or ICT systems. Additionally, the application allows verification of the integrity and authenticity of the electronic document.

The mObywatel app is supported by the IT system provided by the Ministry of Digital Affairs. The system allows downloading an electronic document containing the user’s information from public registers; other information corresponding to the legal situation of the user; containing data used for identification of the user. A downloaded electronic document is an official copy of an official document issued in the form of other than electronic form.

**Figure 3:** Credentials presented by mObywatel – (from left to right) ID card, driving license, COVID certificate, ePrescription




Functionally, mObywatel is a digital wallet for documents and services. The application presently offers the following functionalities:

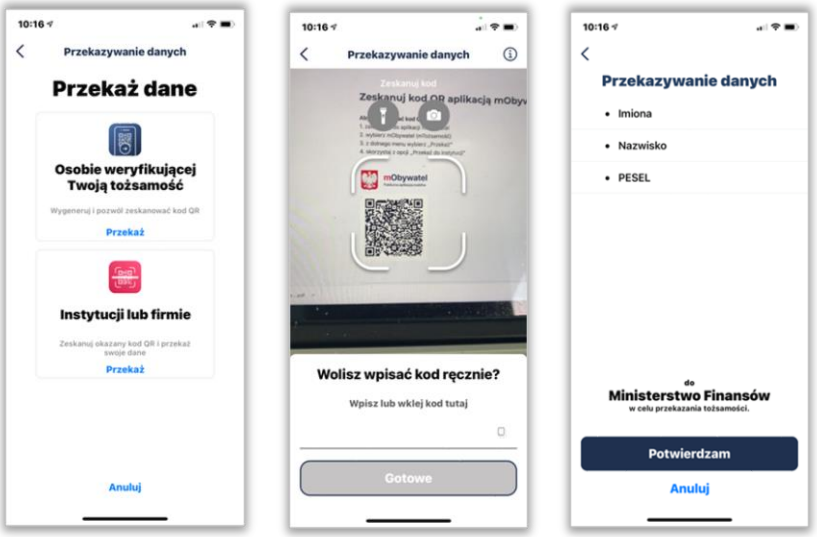
- Download and presentation of identification data from identity card
- ePrescription data presentation
- Large family discount card presentation
- EU vaccination passport
- Presentation of driver's qualifications
- Check a driver’s penalty points
- Show and review the details of vehicle document
- School or student card document presentation
- Electronic identification to online services
- Electronic tickets e.g., train, local transport

Application to the enrolment process authenticates to state registers with Trusted Profile a national identification scheme (substantial level of assurance) or electronic national identity card (high level of assurance). Access to the application is secured with a password. It is also possible to turn on the fingerprint or face recognition authentication with an additional PIN confirmation at the user's request. The application creates a secure internal environment, encryption based on random data (salt) and data provided for user authentication (password).

User keys and X.509 certificates are generated by the supporting IT system and stored in a secure environment. User certificates are valid for one year, and after that period user is asked to repeat the enrolment process using nationally recognised identification means. After enrolment, a new set of keys and certificates are generated and secured by a password-protected environment; thus, it is impossible to change the password. In cases when a new password is needed, a new enrolment is required.

All credentials stored in the app are signed with the digital signature of the Ministry of Digital Affairs – which is only one authoritative source for the application. The application allows the presentation of stored credentials by signing them with user keys. mObywatel application and other verification application (mVerifier) use signed credential presentation to validate the presented document on another smartphone. The application keeps track of all validations. The validity of user and validator certificates can be additionally verified online.

**Figure 4:** Electronic identification with mObywatel




mObywatel allows electronic identification to external online services. The online service initiates the electronic identification by presenting a QR code and online use of the IT system from the Ministry of Digital Affairs. A mObywatel user then uses their smartphone to confirm private data to be transferred to the online service.

To date, mObywatel is neither an official, nor a notified electronic identity scheme. However, mObywatel is presently one of most developed case studies for a solution for the development of a European Digital Identity Wallet.

Further information on mCitizen can be found on the Polish government website (Polish only).[54]

#### 1.4.4.2 Applicability to eIDAS, SSI and European eID

mObywatel is the only one official eID application with functionalities of the European Digital Identification Wallet. While mObywatel uses its own PKI X.509 certificates for credential issuance and presentation, it does not follow common structures for verifiable credentials. For example, it is not known if a non-traceability rule is obeyed. mObywatel does not allow the use and storage credentials issued outside of the Ministry of Digital Affairs IT system. The application uses a software protected environment for the storage of keys and data; no internal

[54] https://www.gov.pl/web/mobywatel

nor external secure component is used to store user keys, keys are generated on external HSMs.

Based on digital signatures and X.509 certificates for data exchange, credential issuance and credential presentation, mObywatel can be used as an electronic identification scheme for online services. Validity and trust are based on PKI and root certificates. The revocation is checked in every transaction. Additionally, the application allows offline electronic identification based on device-to-device data presentation. The enrolment process also makes use of electronic identification schemes.

#### 1.4.4.3 Applicability to governance

mObywatel is under internal governance of Ministry of Digital Affairs (Prime Minister Office), and there is no publicly available information about applicable standards. However, all public administration systems in Poland are legally mandated to have an information security management system following standards like ISO 27001.

#### 1.4.4.4 Security risks and mitigation

The mObywatel secure environment is based on software encryption in tandem with the user's random data (salt) and password. Keys and certificates have one-year period of validity, requiring a re-key and recertification every year to complete a full (re-)enrolment process. Data stored in the wallet is from an official state registry and digitally signed by Ministry of Digital Affairs.

### 1.4.5 Survey Results: Current SSI Activities in Selected EU MS

To prepare an introductory review of the current situation regarding SSI in each Member State, ENISA issued a preliminary survey to the relevant national bodies about any SSI-related work that is either foreseen or that which is presently being undertaken. This survey was aimed to collect information on:

- SSI-related work within the respondents' organisation/nation,
- The goals of these activities,
- The possible timeframe of the SSI-related work,
- The technology used,
- The scope of the work,
- Interoperability requirements for cross-border transactions, and/or
- Possible security risks and opportunities that SSI presents.

Whilst most respondents have stated, at the time of this draft, that it is too early to respond, the results from seven MS offer some insight into experience with the application of SSI in their countries.

The following is a summary of key points from answers submitted by Austria, the Czech Republic, Denmark, Luxembourg, Poland, Portugal, and Sweden.

#### 1.4.5.1 Description of SSI-related work

- Most respondents cited involvement with ESSIF and EBSI – for example, the Technical or Policy Working Groups – focusing on aligning existing eGovernment infrastructures with SSI technology, specifically in the identification of gaps and incompatibilities
- Other normative activities included working with the new EU Toolbox,
- Research activities and pilot projects,
- Training for state employees, implementation of government-issued credentials,

- National digital wallet schemes, such as Portugal's id.gov.pt application, and the Polish *Publiczna Aplikacja Mobilna* (Public Mobile Application)[55] (see also section 1.4.4 of this report).
- Luxembourg is working on several pilot projects, including a diploma use case for the University of Luxembourg[56] as well as a Europass credential for professional certificates and secondary school diplomas, GovTechLab[57] research towards "a digital transformation of the public sector", and the recent Infrachain Hackathon,[58] which focused on demonstrable applications of the "Public Sector Blockchain".

#### 1.4.5.2 Goals

- Contribute to the understanding of SSI and its benefits,
- Come to an understanding of zero zero-knowledge proof (ZKP) capable SSI implementations,
- Identify potential benefits of SSI within the public sector and map the barriers for the realization of these benefits,
- Practical experience in SSI through pilots, research and involvement in EBSI/ESSIF, and
- Provision of national digital identities based on wallets.

#### 1.4.5.3 Possible timeframes

The responses varied to the question about milestones of present SSI-related work, between a general statement of continual cooperation with the EBSI/ESSIF working groups, ongoing work on national digital identity projects, and a citation of specific planned projects between six months and two years.

#### 1.4.5.4 Implemented technology

The list of employed technologies in pilot projects include, for Sweden, Hyperledger Indy, Aries, Ursa, and Besu. For Luxembourg, a private Ethereum blockchain used, for example, for the previously mentioned Public Sector Blockchain, and an open-source enterprise and end-use wallet called walt.id,[59] which is based on EBSI/ESSIF. Portugal cited use of the Xamarin (.NET) platform and Java for development.

#### 1.4.5.5 Scope

- All pilot projects thus far are aimed at serving the public sector, including, natural and legal persons.
- Sweden also included IoT devices and processes, as they are defined by the ISO/TC 307 Identity Working Group.

#### 1.4.5.6 Cross-border interoperability

- The verifiable credential data model can be implemented in several ways. Further work is required, however, to make this interoperable.
- Relying parties need to support multiple verifiable data registries.
- The SSI architecture needs to be platform- and technology-neutral and should not rely on a specific technology for how data are stored and retrieved. Rather, interfaces for the exchange of identity data should be standardized.
- Identifying citizens to national registries must be able to leverage the existing national eID/e-Service infrastructures, ensuring that existing investments in a well-functioning infrastructure are protected.

[55] More information at https://id.gov.pt (Portuguese only)
[56] More information at https://ebsilux.lu/
[57] More information at https://govtechlab.public.lu/en.html#challenges
[58] More information at https://challenge.infrachain.com/
[59] More information at walt.id

#### 1.4.5.7 Security

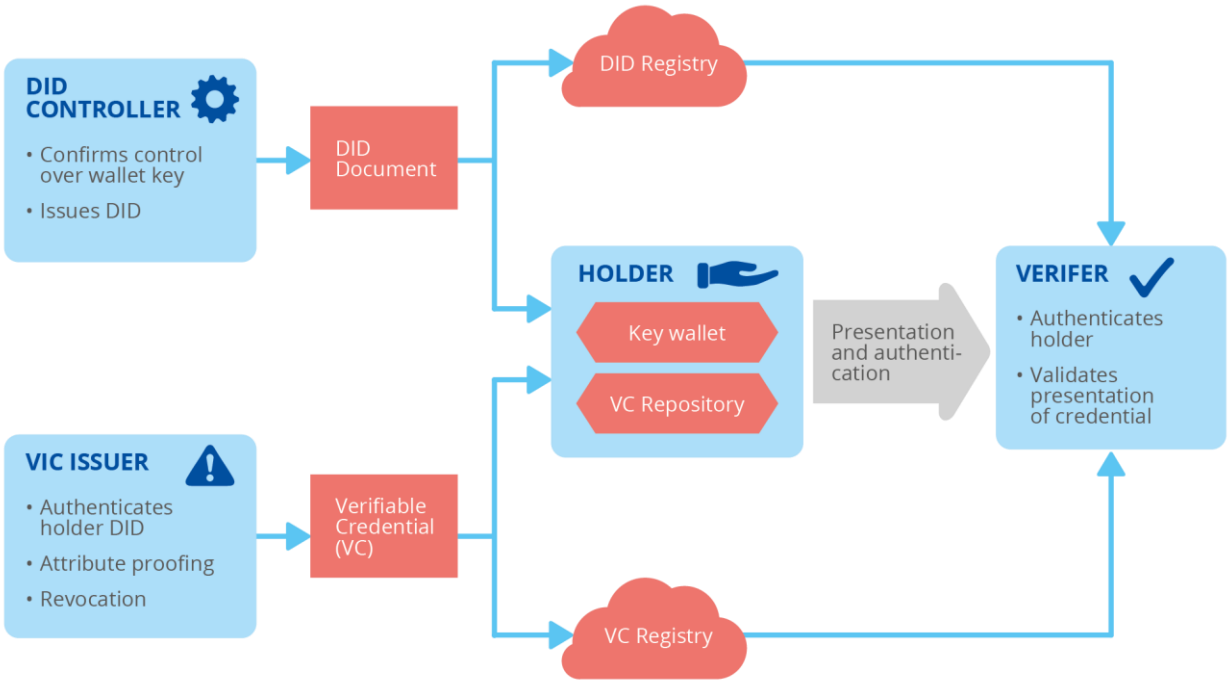
- SSI has the benefit of having no single point of failure.
- Increasing demand on user associated with user control is worrying.
- 'Privacy by demand', with features such as sector-specific identifiers, is crucial. This is hard to achieve in typical SSI (DLT/DID-based) systems, especially when these unique and persistent identifiers are created sector- or service- or MS-specific in the very moment they are requested.
- It is important that freshness of attributes (e.g., representation, mandates, professional capacity, custody of minors, etc.) is maintained. This can only be achieved with online/cloud-based wallets.

# 2. ARCHITECTURAL ELEMENTS FOR SELF-SOVEREIGN IDENTITY

The following basic model is a synthesis of the architectural elements of self-sovereign identity schemes derived from the systems described in the documentation referenced in Section 1. This is not intended to be an implementable architecture that represents any real system but is provided to make it possible to analyse the governance and risks of an SSI scheme.

It may be possible to combine the functions of the Controller and the use of DID with the functions of VC issuance.

**Figure 5:** Basic architectural elements for SSI




The basic architectural elements can be described as follows. The basis of the description is taken from the document identified in the right-hand column. Additional information may be added to further clarify this within the context of this report.

**Table 1:** Basic architectural elements for SSI

| Element | Description | Based on |
|---|---|---|
| **Decentralised Identifier (DID)** | A type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID.<br>Within the context of this report, only natural and legal person are considered as subjects. A DID may be considered as a form of pseudonym as used in eIDAS as it is not directly linked to a formal identifier of the natural or legal person. | W3C Decentralized Identifiers (DIDs) v1.0 |
| **DID Document** | DID documents contain information associated with a DID. They typically express verification methods, such as cryptographic public keys, and services relevant to interactions with the holder.<br>A DID document may be signed by a DID Controller. | W3C Decentralized Identifiers (DIDs) v1.0 |
| **DID Controller** | The controller of a DID is the entity (person, organization, or autonomous software) that has the capability – as defined by a DID method – to make changes to a DID document.<br>The following secure processes for the DID controller are identified by this report:<br>• Proof of possession or control of the holder of its private key<br>• Issuance of a unique DID to the holder | W3C Decentralized Identifiers (DIDs) v1.0 |
| **Verifiable Credential (VC)** | A set of one or more claims made by an issuer. A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. | W3C Verifiable Credentials Implementation Guidelines 1.0 |
| **VC Issuer** | A role an entity can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder. The following secure processes are for the DID controller are identified by this report:<br>• Authentication of the holder as identified by its DID<br>• Proofing that the claimed attributes belong to the holder<br>• Revocation of a holder's attributes | W3C Verifiable Credentials Implementation Guidelines 1.0 (Issuer) |
| **Presentation** | Data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier. A verifiable presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. | W3C Verifiable Credentials Implementation Guidelines 1.0 |
| **Repository** | A program, such as a storage vault or personal verifiable credential wallet, that stores and protects access to holders' verifiable credentials. The use of the repository is restricted to the holder or other authorised parties. | W3C Verifiable Credentials Implementation Guidelines 1.0 |

| Element | Description | Based on |
|---|---|---|
| **Key Wallet** | Application used to generate, manage, store or use private and public keys. This may need to be protected by specially protected "secure element" within the Wallet. The use of the keys is restricted the holder. | |
| **Wallet** | In this report, Wallet is used to cover the repository of verifiable data (DID documents, verifiable credentials) and a Key Wallet.<br>A wallet may be considered as a form of Secure Area (SA-Application) as defined DIS 23220-1 (see Section 1.1.4) clause 3.33 and 3.35.<br>As described for Sovrin (see section 1.2.1), this may be supported through use of an agent service that is remotely accessed from the user's device and controlled through use of multiple authentication factors. This concept is also supported by DIS 23220-1. | ISO DIS 23220-1 Generic system architectures of mobile eID systems |
| **DID Registry** | In order to be resolvable to DID documents, DIDs are typically recorded on an underlying system or network of some kind. Regardless of the specific technology used, any such system that supports recording DIDs and returning data necessary to produce DID documents. In this report this is referred to as the DID document registry. The DID registry can be based on a distributed ledger such as blockchain. | W3C Decentralized Identifiers (DIDs) v1.0 (Verifiable data registries) |
| **VC Registry** | A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials. Some configurations might require correlate identifiers for subjects. Some registries, such as ones for UUIDs and public keys, might just act as namespaces for identifiers. | W3C Decentralized Identifiers (DIDs) v1.0 (Verifiable data registries) |
| **Holder Authentication** | The protocol exchange to obtain authorized access to a resource. | RFC 6749<br>The OAuth 2.0 Authorization Framework |

# 3. GOVERNANCE OF A DIGITAL IDENTITY FRAMEWORK

## 3.1 SSI AND GENERAL GOVERNANCE

The governance of SSI-based schemes is still undergoing development. Most experience in governing an SSI scheme comes from Sovrin, as described in Section 1.2.1. Sovrin has taken an approach similar to that applied by many PKI services, including eIDAS Trust Services, which is as follows:

- There is a governing body which oversees the operation of the SSI service providers and sets the rules for assuring the operation of the SSI service providers,
- Conformity assessment of the provider by an independent assessor against the assurance rules set by the governing body, and
- A means for relying parties to assess whether are considered trustworthy by the governing body.

ISO and CEN (see Section 1.1.3) are in the early stages of developing standards for managing trust based around SSI with working drafts looking at trust anchors.

## 3.2 GOVERNANCE OF WALLETS

The user has control over the use of their wallet. The user can decide whether to use any particular wallet, as well as select a particular DID or verifiable credential within a wallet, to authenticate their identity to a relying party.

The security of SSI depends on the security of the wallet software and environment, in particular, that the keys and, for privacy, the verifiable data, are under the sole control of the holder and cannot be leaked to other parties.

Thus, the security of the wallet will need to be certified against specific criteria to give assurance for the security of wallets.

## 3.3 GOVERNANCE OF DID CONTROLLERS

The issuance of DID of documents puts responsibilities on the DID controller issuing the DID document to ensure that:

- The identifier is unique and cannot be used by an entity other than the holder,
- The verification means held in the DID document is directly associated with keys a wallet under sole control of the holder, and
- The DID document is secured such that it the data cannot be modified and if authenticated as coming from a trusted DID controller.

This may be assured, for example, through audit by an accredited auditor against criteria for DID controllers.

## 3.4 GOVERNANCE OF VC ISSUERS

The issuance of verifiable credential puts responsibilities on issuer to ensure that:

- The DID used to identify the subject of the VC belongs to an identifiable entity,
- The credentials placed within a VC are proven to belong to identified entity,
- The VC is secured such that it the data cannot be modified and if authenticated as coming from a trusted DID controller, and
- Any credential that is no longer valid is revoked.

This may be assured, for example, through audit by an accredited auditor against criteria for issuers of verifiable credentials.

## 3.5 GOVERNANCE OF DID AND VC REGISTRIES

A reliable source of information regarding the issuance and revocation is considered to be necessary which is available, across borders, independent of the wallet. This is thought to be necessary so that relying parties may validate the status of verifiable data (e.g., certificates or credentials) independent of the wallet holder. Technologies such as distributed ledgers may be employed, governance of registries may need to be considered separately (e.g., as a qualified trust service).

## 3.6 INTERDEPENDENCE

The governance of the different elements of an SSI architecture cannot be considered in isolation. The VC issuer depends on the DID, as issued by the DID controller, being uniquely assigned to entity identified by the DID controller and on the sole control of the authentication means being under the sole control of the document. The DID controller needs to be assured that the authentication means is held securely in a certified wallet. Both the DID controller and the VC issuer depend on the registry to provide relying parties with the latest state of the DID document and verifiable credential.

# 4. DIGITAL IDENTITY CONSIDERATION OF RISKS

The following considers the risks associated with the possible architectures given in Section 2. Article 8 of eIDAS establishes assurance levels for notified electronic identification schemes, which needs to specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.

Commission Implementing Regulation 2015/1502 presents general risk considerations to the main processes of the electronic identification scheme: enrolment, ID means management, authentication, and management. For each of those processes, the Regulation states controls corresponding to the required level of assurance. The approach presented in 2015/1502 refers to the scheme and responsibility of the issuer of electronic identification means. Regarding the proposed in Section 2 architecture, new assets are identified and so new security considerations about requirements maybe necessary. Optionally, after further consideration, a new version of Regulation 2015/1502 may be necessary.

## 4.1 SECURITY MEASURES

Self-sovereign electronic identity solutions operated according to what is proposed in Section 2 concerning architecture point to a wallet as central component. This component takes part in most processes and data exchanges. The following standards present security measures for such wallets: ISO/IEC DIS 23220-1, ISO/IEC 29100 and ISO/IEC 19286.

**Data minimization:**

1. Partial release of user attributes for the purpose of data minimization.
2. Unlinkability of transactions at the cryptographic or protocol level. Use only identifiers that are required to establish necessary linkability.
3. Domain-specific identifiers or pseudonyms – a form of identifiers that avoid using the same unique identifier for a user in all its interactions.

**Consent and choice:**

4. In a user-centric system, users have control over their data and attributes. They can exert informed consent, whether the holder attributes are managed and used by a wallet or another entity.

**Accuracy and quality:**

5. The user's attributes shall be bound to the legitimate holder.
6. Protocols executed between the wallet and other components protect against eavesdropping at the communication and logical layer.
7. Protection of attribute authenticity and integrity of the attributes: Attributes released to the relying entities are consistent with the issuer's attributes.
8. Revocation of attributes prevents the revoked attributes from being used in future transactions or ensuring that such use would be recognized as illegitimate by verifiers.
9. The update of attributes changes attribute values.
10. Cloning protection that protects against the illegitimate reproduction of the credentials and user's attributes. Cloning may illegitimately give parties using cloned credentials privileges they would not otherwise hold.

The wallet shall enable the user to securely request and obtain, store, select, combine and share, in a manner that is transparent to and traceable by the user, the necessary legal person identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services.

The scheme for an SSI also features many actors playing different roles. To properly measure the risk, it is important to describe different perspectives of each actor. The following figure represents the main actors of an SSI architecture as described in Section 2 above and the responsibilities of each actor.

**Figure 6:** SSI Actors and their responsibilities

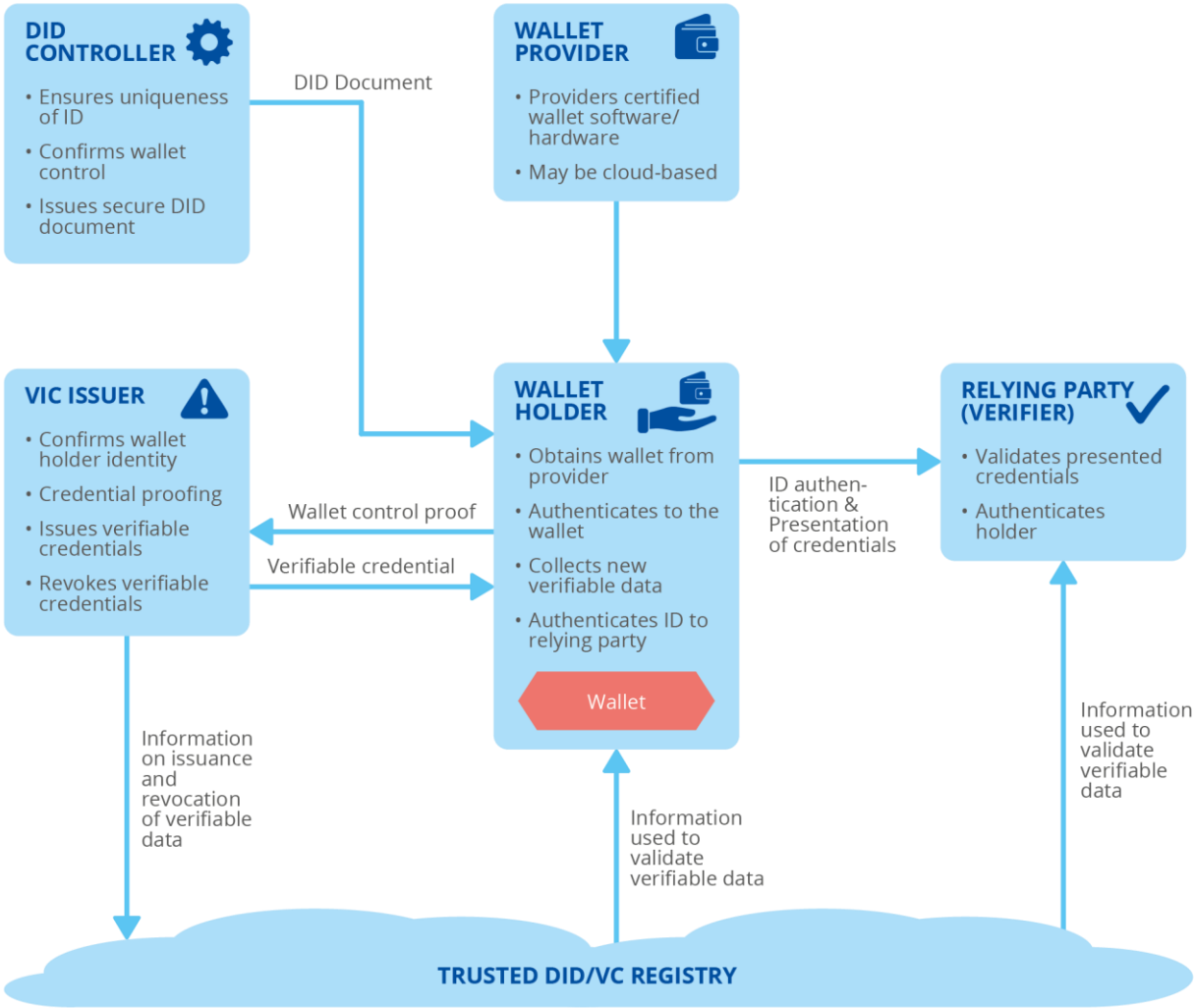


**Table 2:** Key security measures from the perspective of those actors.

| Actors | Security Measures |
|---|---|
| **Identified entity** | Capability of collecting accurate and relevant verifiable data from the trusted issuer |
| | Protects confidentiality of private data, including private keys (data under control) |
| | Identification means can be used only by identified entity |
| **Relying party** | Presented verifiable data is trusted and belong to identified entity |
| **Trusted issuer** | Issues verifiable data, which is considered as trusted |
| | Operates in secure and trustworthy manner |
| | Compliance with law (e.g., GDPR, eIDAS) and applicable standards |
| **Wallet provider** | Operates in secure and trustworthy manner |
| | Compliance with law (e.g., GDPR, eIDAS, NIS) and applicable standards |

## 4.2 ASSET IDENTIFICATION

The information security risk management standard (ISO/IEC 27005) provides guidelines for the identification of risk based on the identification of primary assets, which are processes and information. In the context of a European electronic identity, the identification of assets is based on the architecture presented in Section 2.

### 4.2.1 Primary assets (processes)

- Obtaining of the wallet
- Wallet management (may be supported only by some trusted issuers)
- Wallet control proof
- Verifiable data issuance
- Relying party authentication
- Identified entity presentation and authentication
- Issuance and revocation of verifiable data to registry
- Validation of verifiable date

### 4.2.2 Primary assets (data)

- Identified entity authentication means (e.g., private keys)
- Verifiable data (may include private data)
- Repository data (assumed not to include any private data)

## 4.3 RISK IDENTIFICATION

Once the assets have been identified, a threat analysis may be carried out. Threat identification is an essential step in the risk assessment cycle. A threat is a potential for a particular threat source to successfully exploit a specific vulnerability on an asset.

Threats can be accidental or deliberate, man-made or natural, internal or external, technical or physical. The list below lists threats that correspond to the architecture presented in Section 2.

The following section contains an example list of potential threats to the identified above assets.

### 4.3.1 Process: Obtaining of the wallet

#### 4.3.1.1 Security context

A wallet is the main component of the solution and is required to be certified as meeting the requirements of the regulation. A wallet is held and operated by the user. The user should be aware of downloads and use legitimate wallet applications that secure keys, identity and identification processes. An unauthorised wallet can cause an actual security loss for the user, leading to risks that include a lack of confidentiality of their data and a possible key compromise.

#### 4.3.1.2 Threats

- Delivery of a malicious wallet software – not from the certified source
- Attacks on the wallet during delivery, installation or once installed

### 4.3.2 Process: Wallet management

#### 4.3.2.1 Security context

Wallet management covers two primary subprocesses: key management and revocation management. Keys are stored in the wallet (device itself, connected secure component or cloud). A compromised key can cause false or corrupted identification and use of stored attributes and can significantly and negatively impact the wallet user. In cases where the device containing a wallet is lost, users can revoke their wallet; thus, the online and fast revocation process impacts the wallet user's security.

#### 4.3.2.2 Threats

- Unauthorised wallet management – including keys and verifiable data
- Unavailability of revocation of the wallet itself

### 4.3.3 Process: Wallet control proof

#### 4.3.3.1 Security context

Whenever a verifiable data is issued, it is crucial to prove the subject of that data has control over authentication means (e.g., private key). All processes regarding electronic identification schemes on levels substantial and high cover authentication, with high probability, confirm that only identified entity has control over authentication means.

#### 4.3.3.2 Threats

- Replay attack on control proof
- Modification of control poof
- Unauthorised use of wallet

### 4.3.4 Process: Identity attribute proofing

#### 4.3.4.1 Security context

Before issuing verifiable data, the trusted issuer must confirm the identity attributes of the wallet holder to be included in the verifiable data.

#### 4.3.4.2 Threats

- Identity proofing threats (e.g., ENISA ID proofing report)

### 4.3.5 Verifiable data issuance

#### 4.3.5.1 Security context

The wallet is a solution capable of storing verifiable data issued by trust parties. These verifiable data can originate from services with different levels of assurance, but the wallet holder should be able to trust them. Whenever the issuer gives verifiable data, the wallet holder confirms actual possession and demonstrates other necessary attributes. It is essential to ensure that the verifiable data is issued in the trustworthy manner.

#### 4.3.5.2 Threats

- A verifiable data issued by fraudulent issuer
- Trusted issuer security is compromised
- Verifiable data issuance to holder is compromised (e.g., man in the middle, wrong person handover)
- Private data not protected against confidentiality

### 4.3.6 Process: Relying party authentication

#### 4.3.6.1 Security context

The wallet reveals private data to known and authenticated relying parties. The relying party requests the holder's data in the process, which should be under the control of the aware user. For this purpose, relying parties shall be able to authenticate themselves before requesting a user's identity. The wallet shall then validate and confirm this authentication.

Wallet holders should be able to authenticate relaying party before revealing sensitive identity data and attributes to avoid disclosure of private information. This security measure may also counter phishing and identity theft.

#### 4.3.6.2 Threats

- Relying party authentication means compromise
- Authentication exchange compromise (e.g., man in the middle)

### 4.3.7 Process: Identified entity presentation and authentication

#### 4.3.7.1 Security context

In this process, the wallet holder presents to the relying party its own identity attributes based on verifiable data stored in the wallet. The presentation can include a selective disclosure of attributes (e.g., being over 18). The wallet holder is authenticated by its authentication means. Verifiable data may contain private data and other data which is assumed to be confidential for non-authorised parties. For security reasons in this process, private data should not be revealed to external parties; data also should be protected against authenticity and integrity to prove its accuracy to the relying parties.

#### 4.3.7.2 Threats

- Wallet holder authentication means compromise
- Authentication exchange compromise (e.g., man in the middle, replay attack)
- Presentation data compromise (e.g., fraudulent data presented)
- Private data not protected against confidentiality

### 4.3.8 Process: Issuance and revocation of verifiable data to registry

#### 4.3.8.1 Security context

Some part of verifiable data can be shared to the registry which will be available for other parties. This data shouldn't contain private data but can collect different data relevant for other parties, including online status data. The revocation process is part of verifiable data management. Some data which is not relevant anymore or user lost control over this data can be revoked. Revocation data is checked during the validation process. For some use cases, revocation can be an essential part of ensuring that verifiable data is correct.

#### 4.3.8.2 Threats

- Private data published to the registry (loss of confidentiality)
- Revocation process unavailable
- Revocation postponed
- Registry compromise

### 4.3.9 Process: Validation of verifiable data

#### 4.3.9.1 Security context

In this process, the relying party receives verifiable data and verifies it against security measures. This process confirms origin from a trusted source, the authenticity of presentation by wallet holder and integrity of the data. Additionally, the relying party confirms the validity of verifiable data in the registry.

#### 4.3.9.2 Threats

- Lack of trust anchors
- Compromise of validation data (e.g., corruption, masquerade)
- Registry unavailable

### 4.3.10 DATA: Wallet holder authentication means (e.g., private keys)

#### 4.3.10.1 Security context

The wallet authentication means are the main security component of the model. These data are used in many security processes: proof of possession when the wallet is initiated. Every time wallet is authenticated to the trusted issuer or presents verifiable data to the relying party.

#### 4.3.10.2 Threats

- Wallet security compromise (e.g., tampering)
- Theft or loss of devices (wallets, etc.)
- Unauthorised use of wallet

### 4.3.11 DATA: Verifiable data (may include private data)

#### 4.3.11.1 Security context

Verifiable data is stored in the wallet by identified party and presented to a relying party. The relying party trusts that this data is accurate, authentic and integral. Verifiable data shall be presented only to authorised parties to protect data privacy.

#### 4.3.11.2 Threats

- Loss of confidentiality
- Loss of integrity
- Loss of authenticity

### 4.3.12 DATA: Registry data (assumed does not include any private data)

#### 4.3.12.1 Security context

Registry data is essential for revocation and validation processes.

#### 4.3.12.2 Threats

- Loss of availability
- Loss of integrity
- Loss of authenticity

# 5. CONCLUSIONS

This report covers a range of topics related to the emergence of SSI, specifically as the technology has been deployed as a means of electronic identity. Section 1 presents an overview of the current landscape of the SSI ecosystem through an exploration of the standards groundwork which already make contact with the technology; with existing, robust SSI communities; and with an examination of current eID strategies in Europe and the projects that are incorporating SSI into these national eID strategies. Section 2 offers a basic model of the architectural elements of a possible SSI scheme. While not intended to represent an implementable architecture of any real system, it lays the groundwork for the discussion about governance mechanisms and the risks inherent to such an SSI scheme in Section 3.

Presented below are the main points arising from an analysis of these assessments of the development, application, governance and risks of self-sovereign identity, standards and their implementation, as described in this report, in consideration of concepts critical to eIDAS, such as cross-border interoperability, mutual recognition, technology neutrality and security:

- SSI technology, as applied in the standards and solutions identified in Section 1 and rationalised into a single architecture in Section 2, provides an effective basis for digital identities which protects the privacy of personal data. In particular:
  - Decentralised digital identities can be used to support pseudonyms for privacy of identity,
  - Verifiable credentials enable the separation of potentially private attributes from the digital identity all the user selection of attributes to be revealed to relying parties to ensure privacy of attributes which it is unnecessary to reveal, and
  - The ability to hold multiple authentication keys in a wallet with separate identity documents from different controllers enables the user to cryptographically separate transactions maintaining privacy by avoiding links between the separate transactions.
- For the governance of the elements of the architectural elements of an SSI solution (see Section 3), there is a need to consider:
  - Certification of wallets,
  - Audit and oversight of DID controllers,
  - Audit and oversight of VC issuers,
  - Audit and oversight of DID and VC registries, and
  - All the above are interdependent and the governance of the DID controller and VC issuer also need to ensure that the other elements of an SSI architecture are also properly governed.
- When risk of the architecture of SSI is considered, the following key security measures need to be implemented:
  - Data minimalization – for use only necessary data,
  - Consent and choice – in which the user controls the process and data used for identification, and
  - Accuracy and quality – in which all parties can trust identification data stored and provided by the wallet.
- Lastly, it is recognised that there may be a role for ongoing support for technologies such as X.509 PKI, OpenID Connect, and existing national identity schemes. Thus, if SSI is to be adopted, further consideration should be given to co-existence between existing technologies and SSI.

# 6. REFERENCES

| Source/Classification | Title/Link |
|---|---|
| **Communities** | Sovrin<br>Hyperledger<br>LACChain |
| **General** | Rolling plan on ICT standardisation on Blockchain and Distributed Ledger Technologies |
| **DIF** | Decentralised Identity Foundation |
| **EC** | Guidance for the application of the levels of assurance which support the eIDAS Regulation<br>Overview of Member States' eID strategies<br>SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market |
| **EBSI** | Experience the future with the European Blockchain Services Infrastructure (EBSI) EBSI Documentation<br>European Self-Sovereign Identity Framework (ESSIF)<br>eIDAS Supported Self-Sovereign Identity |
| **ESSIF** | ESSIF Reference Architecture<br>European countries join blockchain partnership<br>Joining Forces for Blockchain Standardisation<br>Security track summary<br>SSI eIDAS Bridge<br>Verifiable Credentials ESSIF v2 |
| **ENISA** | eIDAS Compliant eID Solutions<br>Remote ID Proofing |
| **EU Blockchain Observatory and Forum** | EU Blockchain Observatory and Forum |
| **INATBA** | Decentralised Identity: What's at Stake? |
| **Initiatives** | OpenID<br>Self-Issued OpenID Provider (SIOP)<br>DID SIOP<br>Horizon 2020 projects framework |
| **ISO** | ISO/TC 307 – Blockchain and distributed ledger technologies<br>ISO WD TR 23644 Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM)<br>ISO DTS 23635 – Blockchain and Distributed Ledger Technologies – Guidelines for Governance<br>ISO 29115:2013 – Entity authentication assurance framework<br>ISO 22739:2020 – Blockchain and distributed ledger technologies – Vocabulary<br>ISO DTR 23249 – Overview of existing DLT systems for identity management |

| | |
|---|---|
| | ISO DIS 23220-1 Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: Generic system architectures of mobile eID systems<br>ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application |
| **NIST** | Digital Identity Guidelines<br>NISTIR 8202: Blockchain Technology Overview |
| **Regulations** | Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015<br>Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015<br>Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC<br>Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity |
| **UNCITRAL** | Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services |
| **W3C** | Citizenship Vocabulary v0.3 - A Linked Data vocabulary for expressing attributes related to citizenship<br>Credential Handler API 1.0<br>Decentralized Identifier Resolution (DID Resolution) v0.2, Resolution of Decentralized identifiers (DIDs)<br>Decentralized Identifiers (DIDs) v1.0<br>DID Specification Registries<br>Issuer APIs<br>Use Cases and Requirements for Decentralized Identifiers<br>Verifiable Credentials Implementation Guidelines 1.0<br>Verifiable Credentials Data Model 1.0<br>Verifier APIs |
| **SSI – Additional references** | A Survey on Essential Components of a Self-Sovereign Identity<br>*Blockchain for Self Sovereign Digital Identity*<br>Design-Pattern-as-a-Service for Blockchain-based Self-Sovereign Identity<br>Federation of Attribute Providers for User Self-Sovereign Identity<br>In Search of Self-Sovereign Identity Leveraging Blockchain Technology<br>Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion<br>Self-sovereign identity: Legal compliance and the involvement of governments<br>Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution<br>Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology<br>Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain<br>Towards Self-Sovereign Identity using Blockchain Technology |

# A ANNEX: NATIONAL STATUS INFORMATION SURVEY - QUESTIONS

See section 1.4.5 for a summary of responses.

| QUESTIONS |
| --- |
| **1.** Please identify any SSI-related work you are involved in within your organisation (i.e., conceptual, normative, legal, science/research, implementation, other). |
| **2.** Please describe the goal of your SSI-related work and any current pilot projects. |
| **3.** Please identify a possible timeframe or milestones of your SSI-related work. |
| **4.** Please indicate any technology you are using and implementing and provide any further sources of technical information. |
| **5.** Please indicate if this work is private or public. What is the scope (natural and/or legal persons)? |
| **6. Future Plans:** What different use cases do you foresee for SSI to address EU digital ID? |
| **7. Cross-border:** What are the interoperability requirements you have identified regarding SSI in order to support eID schemes for cross-border transactions? |
| **8. Security:** Please identify possible security/trust risks and/or opportunities that SSI presents to your national eID strategy. |

TP-09-22-024-EN-N

## ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

**ENISA**
European Union Agency for Cybersecurity

**Athens Office**
Agamemnonos 14, Chalandri 15231, Attiki, Greece

**Heraklion Office**
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-555-5
DOI: 10.2824/8646